



On Digitized Forensics – Novel Acquisition and Analysis Techniques for Latent Fingerprints based on Signal Processing and Pattern Recognition

DISSERTATION

zur Erlangung des akademischen Grades

Doktoringenieur (Dr.-Ing.)

angenommen durch die Fakultät für Informatik
der Otto-von-Guericke-Universität Magdeburg

von Dipl.-Inform. Mario Hildebrandt

geb. am 11.08.1983 in Magdeburg

Gutachterinnen/Gutachter

Prof. Dr.-Ing. Jana Dittmann

Prof. Sabah Jassim

Prof. Klimis Ntalianis

Magdeburg, den 28.09.2020

Hildebrandt, Mario:

On Digitized Forensics - Novel Acquisition and Analysis Techniques for Latent Fingerprints based on Signal Processing and Pattern Recognition
Dissertation, Otto-von-Guericke-University of Magdeburg, 2020.

Abstract

Forensic investigations are an important factor of the analysis of committed crimes to reconstruct the sequence of events and eventually to bring the offender to trial. While forensic sciences have been further developed especially within the last century, the application of novel techniques poses challenges from practical and legal perspectives. In general, novel techniques need to be assessed prior to the admission of the resulting evidence in court. In the example of the U.S. supreme court level this assessment is governed by the Federal Rules of Evidence, in particular Rule 702 addressing the expert testimony, and the Daubert challenge for scientific evidence. During the latter at least five so-called Daubert factors – “Whether a method/technique can be (and has been) tested”, “Whether a method/technique has been subject to peer review and publication”, “The known or potential rate of error of a method/technique”, “The existence and maintenance of standards controlling the technique’s operation” and “Whether a method/technique is generally accepted in the scientific community” – are assessed prior to the admission of novel techniques in court. The introduction of novel sensors and processing techniques is a growing research field as such techniques allow for analyzing new details of traces, allow for reducing the impact on other traces or increasing the repeatability of the processing steps. A part of such novel techniques could be represented by Computational Forensics, which describes the utilization of computer-based techniques in forensic investigations. As this domain is rather broad and without specific requirements, the focus of this thesis is narrowed down to the newly introduced terminology of digitized forensics – the projection of the analysis of physical traces to the entirely digital domain including the specific requirements. The intention of digitized forensics is a similar application of computer-based acquisition and processing techniques to the investigation of various types of traces. Such a similar application procedure could assist judges in their role as a gatekeeper for novel techniques in a Daubert hearing to evaluate the particular forensic soundness in a similar process. Furthermore, shared requirements and processing steps can help to derive standards, guidelines and best practices for the application of such novel computer-based forensic technologies. In conjunction with those intentions the following set of research questions is derived within the scope of this thesis:

- How could a generic digitized forensic investigation be formalized as a process and validated for the selected domain of latent fingerprints?
- Which novel challenges need to be addressed within digitized forensic investigations, in particular with respect to latent fingerprints?
- Which requirements need to be fulfilled by metrology sensory for an application in digitized forensics and what is the impact syntax and semantics of the captured sensor data related to error, loss and uncertainty?

In order to address the issue of the lack of particular standards for computational forensics, this thesis introduces a novel process model designed particularly for digitized forensics. The intention of a first-tier of phases is the general structuring of the forensic investigation process and trace handling. Afterward, a second tier of trace specific phases can be derived under the canon of the first-tier phases. Secondly, particular requirements and novel challenges regarding the digitization of physical traces are assessed and addressed within this thesis. In particular the challenges of the authenticity of the traces, the reproducibility of results and the benchmarking of processing techniques are discussed within this thesis. Towards the benchmarking and authenticity-preservation, particular supporting forensic tools are introduced within this thesis. Furthermore, a scheme for formalizing sensory for the digitization is introduced as a foundation for the selection of the application specific sensors.

The introduced process model is validated on the foundation of two application scenarios in the domain of latent fingerprint processing. In this context additional research questions are defined:

- How could and should latent fingerprints be captured and analyzed within a digitized forensics process using signal processing and pattern recognition to ensure an accurate digital representation of the physical trace?
- Which classification scheme suits a pattern recognition based fingerprint-substrate segregation best?
- How and in which way could the new technology support the detection of forged fingerprint traces?

The first application scenario addresses the challenge of separating the fingerprint pattern from the substrate data by means of statistical pattern recognition. For that, a feature space is designed and evaluated within a two-class supervised learning approach. Subsequently, the performance of the introduced approach is evaluated using automatic biometric matching with an off-the-shelf matching algorithm to approximate the resulting comparison performance of highly trained experts. The second application scenario addresses the challenge of latent fingerprint forgeries for the example of artificially printed latent fingerprint patterns. Similar to the first application scenario a feature space is designed and evaluated using a two-class supervised learning approach. In addition to that, particular influence factors are systematically evaluated using the introduced StirTrace benchmarking approach.

Overall, this thesis presents a cross-sectional topic of applied computer science to forensic sciences.

Kurzfassung

Forensische Untersuchungen sind ein wichtiger Faktor bei der Analyse von begangenen Straftaten um die Ereigniskette rekonstruieren zu können und letztendlich den Straftäter vor Gericht zu bringen. Während die Wissenschaft der Forensik im Laufe des letzten Jahrhunderts stetig weiterentwickelt wurde, stellt die Anwendung neuer Techniken Herausforderungen aus praktischer und rechtlicher Sicht dar. Im Allgemeinen müssen neue Technologien und die daraus resultierenden Beweise vor deren Zulassung vor Gericht untersucht werden. Für das Beispiel des Obersten Gerichtshofs der Vereinigten Staaten von Amerika wird dieser Vorgang durch die Federal Rules of Evidence, im Speziellen durch die Regel 702 zu Sachverständigenaussagen und durch so genannte Daubert-Tests geregelt. Für letztere werden mindestens fünf verschiedene Daubert-Faktoren vor der Zulassung des Beweismittels im Gericht untersucht – „Ob eine Methode oder Technik getestet werden kann, bzw. getestet wurde“, „Ob eine Methode oder Technik veröffentlicht und einem Peer-Review unterzogen wurde“, „Welche bekannte oder potentielle Fehlerrate die Methode oder Technik besitzt“, „Ob Standards zur Regelung des Einsatzes der Methode oder Technik existieren und gepflegt werden“ und „Ob die Technik oder Methode in der relevanten wissenschaftlichen Gemeinschaft akzeptiert ist“. Die Einführung neuer Sensoren und Verarbeitungstechniken ist ein wachsendes Forschungsgebiet, da derartige Techniken die Untersuchung neuer Details von Spuren, die Reduktion des Einflusses auf andere Spuren und die Wiederholbarkeit der Verarbeitungsschritte ermöglichen können. Ein Teil solcher neuen Technologien wird mit dem Begriff computergestützte Forensik subsumiert. Da dieses Forschungsgebiet jedoch sehr breit aufgestellt ist und keinerlei Anforderungen definiert, liegt der Fokus dieser Doktorarbeit auf dem enger eingegrenzten Gebiet der neu eingeführten Terminologie der digitalisierten Forensik – der Übertragung der Untersuchung physischer Spuren in eine vollständig digitale Umgebung inklusive der daraus entstehenden, spezifischen Anforderungen. Die Intention zur digitalisierten Forensik ist eine grundsätzlich ähnliche Anwendung der computergestützten Datensammlung und Verarbeitung zur Untersuchung verschiedener Spurenarten. Durch die ähnliche Anwendung der Verarbeitungsschritte können Richter in ihrer Rolle zur Zulassung der neuen Technologien in einer Daubert-Anhörung bei der Evaluierung der forensischen Korrektheit unterstützt werden. Darüber hinaus können gemeinsame Anforderungen von Verarbeitungsschritten bei der Ableitung von Standards, Leitfäden und Empfehlungen zur Anwendung neuer computergestützter forensischer Technologien behilflich sein. In Verbindung mit dieser Absicht wird die folgende Gruppe von Forschungsfragen innerhalb der Ausrichtung dieser Doktorarbeit abgeleitet:

- Wie kann eine generische digitalisierte forensische Untersuchung als Prozessmodell formalisiert und anhand der Domäne von latenten Fingerprints exemplarisch validiert werden?
- Welche neuen Herausforderungen müssen im Rahmen von digitalisierten forensischen Untersuchungen adressiert werden, insbesondere im Hinblick auf latente Fingerprints?
- Welche Anforderungen müssen durch Oberflächenmesstechnik für die Anwendung in der digitalisierten Forensik erfüllt werden und was ist der Einfluss der Syntax und Semantik der erfassten Sensordaten hinsichtlich Fehlern, Verlusten und Unsicherheiten?

Um die Herausforderung der fehlenden Standards für den Einsatz computergestützter Forensik zu adressieren, stellt die vorliegende Doktorarbeit ein neues Prozessmodell für die digitalisierte Forensik vor. Die Absicht der ersten Ebene von Phasen ist eine grundsätzliche Strukturierung des forensischen Untersuchungsprozesses sowie der Handhabung von Spuren. Darauf aufbauend kann eine zweite, spurenartabhängige Ebene von Phasen abgeleitet werden. Darüber hinaus werden entsprechende Anforderungen und neue Herausforderungen hinsichtlich der Digitalisierung von Spuren im Rahmen der Doktorarbeit untersucht und adressiert. Im Speziellen handelt es

sich dabei um die Herausforderung der Authentizität der Spuren, der Reproduzierbarkeit der Ergebnisse und des Benchmarkings von Verarbeitungstechniken. Hinsichtlich des Benchmarkings und der Authentizitätswahrung werden entsprechende unterstützende Werkzeuge im Rahmen der Dissertation entworfen. Darüber hinaus wird ein Schema zur Formalisierung von Sensoren als Grundlage zur anwendungsabhängigen Sensorauswahl eingeführt.

Das eingeführte Prozessmodell wird auf Basis von zwei Anwendungsszenarien im Bereich der Verarbeitung von latenten Fingerspuren validiert. In diesem Kontext werden folgende zusätzliche Forschungsfragen gestellt:

- Wie können und sollten latente Fingerspuren im Rahmen der digitalisierten Forensik mittels Signalverarbeitung und Mustererkennung erfasst und analysiert werden um eine exakte digitale Repräsentation der physischen Spur gewährleisten zu können?
- Welches Klassifikationsschema ist am besten für die Mustererkennung zur Trennung latenter Fingerspuren von Oberflächendaten geeignet?
- Wie und in welcher Form können neue Technologien bei der Erkennung gefälschter Fingerspuren behilflich sein?

Das erste Anwendungsszenario adressiert die Herausforderung der Trennung des Fingerabdruckmusters von den Oberflächendaten mittels statistischer Mustererkennung. Dafür wird ein Merkmalsraum entworfen und anhand eines Zwei-Klassen-Problems des überwachten Lernens evaluiert. Abschließend wird die Performanz des eingeführten Ansatzes anhand eines handelsüblichen biometrischen Vergleichsalgorithmusses evaluiert um die zu erwartende Vergleichsperformanz forensischer Experten abzuschätzen. Das zweite Anwendungsszenario adressiert die Herausforderung gefälschter latenter Fingerspuren am Beispiel künstlich gedruckter Fingerabdruckmuster. Vergleichbar zum ersten Anwendungsszenario wird ein Merkmalsraum entworfen und anhand eines zwei-Klassen-Problems mit überwachtem Lernen evaluiert. Darüber hinaus werden Einflussfaktoren systematisch mittels des eingeführten StirTrace Benchmarking Ansatzes evaluiert.

Insgesamt stellt diese Dissertation ein Querschnittsthema der angewandten Informatik auf das Gebiet der forensischen Wissenschaften dar.

Contents

List of Figures	xiii
List of Tables	xviii
List of Listings	xix
List of Acronyms	xxi
1 Introduction, Motivation and Scope	1
1.1 Brief Summary of Related Work and Research Gaps	5
1.2 Research Questions	8
1.3 Objectives and Addressed Research Challenges of this Thesis	9
1.4 Summary of the Contributions of this Thesis	11
1.5 Thesis Outline	12
2 Thesis Fundamentals and Related Work	15
2.1 Forensic Principles	15
2.1.1 Standards and Best Practices in Forensic Investigations	15
2.1.2 Selected Standards for Evaluating and Handling Evidence	30
2.2 Selected Legal Background for Forensic Sciences	32
2.3 Contact-Less Sensory and Substrate Properties	33
2.3.1 Selected Contact-Less Sensory for Digitized Forensics	33
2.3.2 Confocal Laser Scanning Microscopy	35
2.3.3 UV-VIS Reflection Spectrometer	37
2.3.4 Selected Substrate Properties in the Context of Latent Fingerprint Forensics	37
2.3.5 Common Preprocessing Techniques for Sensor Data	38
2.4 Selected Aspects of Pattern Recognition	40
2.4.1 Selected Error Rates and Performance Measures in Pattern Recognition	41
2.4.2 Selected Classification Performance Evaluation Approaches	42
2.4.3 Supervised Learning Approaches Utilized Within This Thesis	43
2.4.4 Benford's Law	45
2.5 A Brief History of Fingerprints in Forensics	45
2.5.1 Features of Fingerprints	45
2.5.2 Errors in the Analysis of Latent Fingerprints	46
2.5.3 Selected Biometric Preprocessing and Matching Approaches in Latent Fingerprint Forensics	47
3 The Process of Digitized Forensics	51
3.1 A Novel Model of the Digitized Forensics Process	53

3.1.1	Prerequisites and Assumptions	55
3.1.2	Strategic Preparation	55
3.1.3	Physical Acquisition	56
3.1.4	Operational Preparation	57
3.1.5	Data Gathering	57
3.1.6	Data Investigation	59
3.1.7	Data Analysis	60
3.1.8	Trace Processing	61
3.1.9	Trace Investigation	61
3.1.10	Trace Analysis	61
3.1.11	Process Accompanying and Final Documentation	61
3.1.12	Archiving of Physical and Digital Evidence Items	63
3.2	Sensory for Digitized Forensics	64
3.2.1	Syntax and Semantics of Sensor Data	64
3.2.2	Error, Loss and Uncertainty Caused by Sensory	65
3.3	New Challenges Connected to Digitized Forensics	67
3.3.1	Ensuring Authenticity of Digitized Traces	67
3.3.2	Sensor Noise and Reproducibility in Digitized Forensics	67
3.3.3	Accuracy of Pattern Recognition Methods	68
3.4	Chapter Summary and Limitations	68
4	Selected Supporting Tools for Digitized Forensic	71
4.1	Analysis of Available Sensory for the Evaluation of Digitized Forensics in the Context of Latent Fingerprints	72
4.1.1	S_1 Chromatic White Light Sensors	72
4.1.2	S_2 Confocal Laser Scanning Microscope	73
4.1.3	S_3 UV-VIS Reflection Spectrometer	74
4.2	Linking Digital Trace Representations to the Physical Trace	75
4.2.1	Processing steps during the physical acquisition at the scene of crime	75
4.2.2	Processing steps during the operational preparation	77
4.2.3	Processing steps during the data gathering	78
4.2.4	Processing steps during the trace storage	80
4.3	Benchmarking Framework for Pattern Recognition Based Approaches on the Example of Fingerprint Forgery Detection	81
4.3.1	Analysis of Potential Artifacts within the Fingerprint Forgery Processing Pipeline	82
4.3.2	Synthetic Simulation of Artifacts with the novel StirTrace Framework	84
4.4	Chapter Summary and Limitations	91
5	Application Scenario 1: Segregation of Latent Fingerprint Data from Substrate Data	93
5.1	Fundamentals of Application Scenario 1: Coarse and Detailed Scans for the Contact-Less Acquisition of Latent Fingerprints	95
5.2	Feature Space Design and Labeling for Segregating Forensic Fingerprint Trace Evidence from Substrate Data	96
5.2.1	Feature Space for Segregating Forensic Fingerprint Trace Evidence from Substrate Data	99
5.2.2	Creation of Labeling Data	107
5.3	Segregation of Fingerprint Traces from Substrate Data	107

5.3.1	Selection of the Most Suitable Available Sensor for the Digitization of Latent Fingerprints	108
5.3.2	Experimental Setup for Evaluating the Segregation of Fingerprint Traces from Substrate Date	110
5.3.3	Results for the complete feature space in a two-class supervised learning approach	113
5.4	Feature Selection	133
5.5	Chapter Summary and Limitations	136
6	Application Scenario 2: Detection of Printed Latent Fingerprint Forgeries	139
6.1	Fundamentals of Application Scenario 2: Forgery Creation and Subjective Analysis	141
6.1.1	Creation of Latent Fingerprints using Ink-Jet Printers and Artificial Sweat	141
6.1.2	Subjective Assessment and Data Gathering for Fingerprint Trace Forgery Detection	143
6.2	Feature Space Design for Fingerprint Trace Forgery Detection	144
6.2.1	Dot-Based Features	145
6.2.2	Crystalline Structure-Based Features	148
6.2.3	Benford's-Law-Based Features	149
6.3	Detection of Printed Latent Fingerprint Forgeries	150
6.3.1	Selection of the Most Suitable Available Sensor for the Detection of Printed Latent Fingerprint Forgeries	150
6.3.2	Experimental Setup for the Detection of Printed Latent Fingerprint Forgeries	151
6.3.3	Evaluation of the Three Feature Spaces	152
6.3.4	Evaluation of the Detection of Printed Latent Fingerprint Forgeries on Specific Substrate Materials	152
6.3.5	Substrate-Independent Evaluation of the Detection of Printed Latent Fingerprint Forgeries	155
6.3.6	Fusion of the Three Feature Spaces	156
6.3.7	Summary of the Evaluation of the Three Feature Spaces for the Detection of Printed Latent Fingerprint Forgeries	157
6.3.8	Benchmarking of the Detector Robustness using StirTrace	157
6.4	Feature Selection	163
6.5	Chapter Summary and Limitations	164
7	Potential Future Implications	167
7.1	Application of the Novel Process Model of Digitized Forensics to Other Types of Trace Evidence	167
7.2	Extension of the Artifact Simulation of StirTrace to other Applications	168
7.3	Potential Impact on Forensic Investigations	168
8	Conclusion	171
8.1	Summary of Contributions	171
8.2	Summary of the Results Addressing the Objectives	173
8.3	Summary of the Results Addressing the Research Questions	175
8.4	Concluding Remarks and Lessons Learned	178

9	Future Work	181
9.1	Future Research Directions Regarding the Process Model	181
9.2	Future Research Directions Regarding Sensory and Sensor Data Preprocessing	182
9.3	Future Research Directions Regarding Latent Fingerprint Investigation	182
9.4	Future Research Directions Regarding the Detection of Latent Fingerprint Forgeries	183
A	Appendix	185
A.1	Software Architecture of StirTrace	185
A.2	Formal Definition of Sensors	186
A.3	Supplemental Material for the Segregation of Fingerprint Traces from Substrate Data	187
A.3.1	Classifier Outputs for the 2-Fold Cross Validation	187
A.3.2	Successful Matches and Matching Scores from the Biometric Evaluation	197
A.3.3	Feature Selection Classifier Outputs for the 2-Fold Cross Validation	200
A.4	Evaluation of the Detection of Printed Latent Fingerprint Forgeries	207
A.4.1	Evaluation of the Detection using Dot Based Features using LMT	207
A.4.2	Evaluation of the Detection using Crystalline Structure Based Features using LMT	208
A.4.3	Evaluation of the Detection using Benford's Law Based Features using LMT	210
A.4.4	Evaluation of the Detection using Dot Based Features using MultilayerPerceptron	211
A.4.5	Evaluation of the Detection using Crystalline Structure Based Features using MultilayerPerceptron	212
A.4.6	Evaluation of the Detection using Benford's Law Based Features using MultilayerPerceptron	214
A.4.7	Evaluation of the Detection using Dot Based Features using Dagging	215
A.4.8	Evaluation of the Detection using Crystalline Structure Based Features using Dagging	216
A.4.9	Evaluation of the Detection using Benford's Law Based Features using Dagging	218
A.4.10	Evaluation of the Detection using Dot Based Features using RotationForest	219
A.4.11	Evaluation of the Detection using Crystalline Structure Based Features using RotationForest	220
A.4.12	Evaluation of the Detection using Benford's Law Based Features using RotationForest	222
A.4.13	Evaluation of the Detection using the Combined Feature Space	223
	Bibliography	225
	Index	242

List of Figures

2.1	Measurement principle of a Chromatic White Light (CWL) sensor	34
2.2	Measurement principle of a Laser Scanning Confocal Microscope based on [CFD13]	36
2.3	Measurement principle of the FTR sensor	38
3.1	Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases from [HKG+11] Highlighted by Gray Shading, Phases from [KHA+09] are Indicated by a Thicker Border	54
3.2	Generic Concept of Coarse and Detailed Scans as Exemplary Templates for Second-Tier Phases	58
4.1	Concept for ensuring a provable integrity and authenticity of digitized traces resketched from [HKD13b], implementation of the container for digitized evidence can be based e.g. on [KVL11]	75
4.2	Creation of the metadata record for an object of the crime scene based on [HKD13b]	76
4.3	Creation of machine-readable metadata records based on [HKD13b]	77
4.4	Contents of the machine-readable metadata records based on [HKD13b]	77
4.5	Trace Acquisition using DDPlusAcquire	79
4.6	Metadata for trace digitization based on [HKD13b]	79
4.7	Update of machine-readable metadata records based on [HKD13b]	80
4.8	Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases Highlighted by Gray Shading are Addressed within this Chapter	91
5.1	Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases Highlighted by Gray Shading are Addressed within this Chapter, Data Analysis is Hatched Because the Applied Evaluation is only an Approximation for a Latent Fingerprint Examiner	94
5.2	Multi-staged acquisition process with second-tier phases based on [HDP+11] and [HDV+11]	95

5.3	Latent Fingerprint Segregation Pipeline including Preprocessing Steps based on [HDV13] and [HKD+14] as Second-Tier Phases for the Data Gathering, Data Investigation and Data Analysis . . .	105
5.4	Coarse scan of blued metal M_8 with the stencil mask on top within DDPlusAcquire	112
5.5	Biometric evaluation pipeline based on the biometric pipeline from [Vie06, pp. 19–21] as second-tier phases in digitized forensics for this application scenario	113
5.6	Illustration of a 4 by 4 mm section of a sample from M_1 successfully matched using $I_{R_{optimized}}$ with J48 and I_{orig} , second fingerprint of the depletion series	123
5.7	Illustration of a 4 by 4 mm section of a sample from M_1 which is not successfully matched using any evaluated image, ninth fingerprint of the depletion series	123
5.8	Illustration of a 4 by 4 mm section of a sample from M_2 successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ with SMO, eighth fingerprint of the depletion series	124
5.9	Illustration of a 4 by 4 mm section of a sample from M_2 which is not successfully matched using any evaluated image, fourth fingerprint of the depletion series	125
5.10	Illustration of a 4 by 4 mm section of a sample from M_3 successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ with SMO, third fingerprint of the depletion series	126
5.11	Illustration of a 4 by 4 mm section of a sample from M_3 which is not successfully matched using any evaluated image, ninth fingerprint of the depletion series	126
5.12	Illustration of a 4 by 4 mm section of a sample from M_4 successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$, $I_{R_{LRb}}$ with SMO and J48, as well as I_{orig} , first fingerprint of the depletion series	127
5.13	Illustration of a 4 by 4 mm section of a sample from M_4 which is not successfully matched using any evaluated image, tenth fingerprint of the depletion series	128
5.14	Illustration of a 4 by 4 mm section of a sample from M_5 which is not successfully matched using any evaluated image, fourth fingerprint of the depletion series	129
5.15	Illustration of a 4 by 4 mm section of a sample from M_6 which is not successfully matched using any evaluated image, seventh fingerprint of the depletion series	130
5.16	Illustration of a 4 by 4 mm section of a sample from M_7 which is not successfully matched using any evaluated image, fourth fingerprint of the depletion series	131
5.17	Illustration of a 4 by 4 mm section of a sample from M_8 which is not successfully matched using any evaluated image, second fingerprint of the depletion series	131

5.18	Illustration of a 4 by 4 mm section of a sample from M_9 which is not successfully matched using any evaluated image, second fingerprint of the depletion series	132
5.19	Illustration of a 4 by 4 mm section of a sample from M_{10} which is not successfully matched using any evaluated image, second fingerprint of the depletion series	133
6.1	Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases Highlighted by Gray Shading are Addressed within this Chapter	141
6.2	Full Context Attack Chain for Latent Fingerprint Forgeries Resketched from [DiH14] as a Foundation for the Strategic Preparation for Designing Detection Approaches	142
6.3	CWL (S_1) intensity data from fingerprints on an overhead transparency, 2 x 2 mm, 12700 ppi	144
6.4	CLSM (S_2) intensity data from fingerprints on an overhead transparency, 1.3 x 1 mm, 20000 ppi	144
6.5	Signal Processing Pipeline for Circle-Based Features based on [HiD15a] as Second-Tier Phases of the novel Process Model for Digitized Forensics	145
6.6	Signal Processing Pipeline for Crystalline Structure-Based Features based on [HKS+12] as Second-Tier Phases of the novel Process Model for Digitized Forensics	148
6.7	Distribution of the most significant digits in CLSM (S_2) intensity and topography data based on [HiD15b]	149
6.8	Signal Processing Pipeline for Benford's-Law-Based Features based on [HiD15b] as Second-Tier Phases of the novel Process Model for Digitized Forensics	149
A.1	Software Architecture of StirTrace	185

List of Tables

1.1	Structure of the Thesis	13
2.1	Technical Specifications of the FRT CWL600 and CWL1mm Sensors [FRT14a]	35
2.2	Technical Specifications of the Keyence VK-x110 CLSM [KEY20]	37
3.1	Typical Information within the Process Accompanying Documentation	62
4.1	Potential Artifact Sources based on [HiD15a] and [HiD16]- ✓ denotes that a particular artifact can be caused during the specific phase of the latent fingerprint forgery creation pipeline ($AS_1 - AS_4$) or the subsequent trace digitization (AS_5)	83
5.1	Combined Feature Space for each Image I based on [HDV13] and [HKD+14]	106
5.2	Comparison of the CWL (S_1), CLSM (S_2) and UV-VIS (S_3) Sensors Regarding the Requirements: ✓ Denotes a Fulfilled Requirement, ○ Is a Partially Fulfilled Requirement, × Indicates a Non-Fulfilled Requirement	109
5.3	Substrate Materials and Number of Test Samples for the Segregation of Fingerprint Traces from Substrate Data	111
5.4	2-Fold Cross-Validation Results for White Furniture Substrate M_1 - Confusion Matrix and Classification Accuracy	114
5.5	2-Fold Cross-Validation Results for Veneered Plywood M_2 - Confusion Matrix and Classification Accuracy	115
5.6	2-Fold Cross-Validation Results for Brushed Stainless Steel M_3 - Confusion Matrix and Classification Accuracy	115
5.7	2-Fold Cross-Validation Results for Aluminum Foil (Matte Side) M_4 - Confusion Matrix and Classification Accuracy	116
5.8	2-Fold Cross-Validation Results for Golden Oak Veneer M_5 - Confusion Matrix and Classification Accuracy	116
5.9	2-Fold Cross-Validation Results for Non-Metallic Car Body Finish M_6 - Confusion Matrix and Classification Accuracy	117

5.10	2-Fold Cross-Validation Results for Metallic Car Body Finish M_7 - Confusion Matrix and Classification Accuracy	117
5.11	2-Fold Cross-Validation Results for Blued Metal M_8 - Confusion Matrix and Classification Accuracy	118
5.12	2-Fold Cross-Validation Results for Ceramic Tile M_9 - Confusion Matrix and Classification Accuracy	118
5.13	2-Fold Cross-Validation Results for Copying Paper M_{10} - Confusion Matrix and Classification Accuracy	119
5.14	Comparison of Classification Accuracy in Percent from the 2-Fold Cross-Validation Results for all Substrates	120
5.15	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_1	122
5.16	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_2	124
5.17	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_3	125
5.18	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_4	127
5.19	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_5	128
5.20	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_6	129
5.21	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_7	130
5.22	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_8	130
5.23	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_9	132
5.24	Number of Fingerprint Matches for Latent Fingerprints Digitized from M_{10}	132
5.25	Comparison of Classification Accuracy in Percent from the 2-Fold Cross-Validation Results for all Substrates with and without the Feature Selection	135
6.1	Comparison of the CWL (S_1), CLSM (S_2) and UV-VIS (S_3) Sensors Regarding the Requirements for the Detection of Latent Fingerprint Forgeries: ✓ Denotes a Fulfilled Requirement, ○ Is a Partially Fulfilled Requirement, × Indicates a Non-Fulfilled Requirement	150
6.2	Overview Test Sample from the CLSM S_2 based on [HKD13a]	151

6.3	Evaluation of Dot Based Features using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)	153
6.4	Evaluation of Crystalline Structure Based Features using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %) . .	153
6.5	Evaluation of Benford's Law Based Features using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)	154
6.6	Substrate-Independent Evaluation of Features Spaces using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %) . .	155
6.7	Substrate-Independent Evaluation of Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %) . .	157
6.8	Selected Filters and Filter Parameters for the Benchmarking using StirTrace based on [HiD15a], [Hil15] and [HiD16] - in Sum 70 Filter-Parameter-Combinations are Selected for the Benchmarking	158
6.9	Evaluation of the Detection Accuracy for Additive Gaussian Noise within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15]; best results highlighted in bold face (all accuracy values in %)	159
6.10	Evaluation of the Detection Accuracy for Median Cut Filtering within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15]; best results highlighted in bold face (all accuracy values in %)	159
6.11	Evaluation of the Detection Accuracy for the Simulation of Printer Characteristics within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15]; best results highlighted in bold face (all accuracy values in %)	161

6.12	Evaluation of the Detection Accuracy for the Simulation of Acquisition Conditions within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hi15] and [HiD16]; best results highlighted in bold face, (* feature extraction exclusively performed on I_I of S_2 , all accuracy values in %)	162
6.13	Substrate-Independent Evaluation of Combined Feature Space with an without Feature Selection using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)	164
8.1	Comparison of the Two Application Scenarios	179

List of Listings

- 5.1 Excerpt of a Classification Result File Determined on the Foundation of the Bagging Classifier; Header Describing the Data Fields - BlockID, Label from Ground Truth (if Available, Fixed to b for Substrate Block Otherwise), Probabilities for Class Assignments120

List of Acronyms

ACC	Accuracy
ACE-V	Analysis-Comparison-Evaluation-Verification
AFIS	Automated Fingerprint Identification System
Bagging	bootstrap aggregating ensemble classifier [Bre96]
CLSM	Confocal Laser Scanning Microscope
CWL	Chromatic White Light
DA	Data Analysis
DAG	Dagging [TW97]
DG	Data Gathering
DI	Data Investigation
DO	Documentation
DS	Digital Archiving
EER	Equal Error Rate
EP	Exemplar Print/Tenprint
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FNR	False Negative Rate
FPR	False Positive Rate
FRoE	Federal Rules of Evidence
FRR	False Rejection Rate
FTIR	Fourier Transform Infrared Spectroscopy
HTER	Half-Total Error Rate
IT	Information Technology
J48	Java implementation of a C4.5 decision tree [DHS00 , p. 411]
LMT	Logistic Model Tree [LHF05]
LP	Latent Print

LR	Likelihood Ratio
MLP	Multilayer Perceptron [Bau88]
OP	Operational Preparation
PA	Physical Acquisition
PCA	principal component analysis [DHS00 , p. 568]
RF	RotationForest [RKA06]
SMO	Sequential Minimal Optimization [Pla99]
SP	Strategic Preparation
SVM	Support Vector Machine [Web02 , pp. 134 – 141]
TA	Trace Analysis
TI	Trace Investigation
Tn	True Negative
TP	Trace Processing
Tp	True Positive
TS	Trace Storage

Introduction, Motivation and Scope

FICTION has been an inspiration for science and technology for a long time [Smi12]. Jules Verne's books describe submarines or helicopters decades before such machines were built and without TV shows such as Star Trek we probably would not have seen cell phones. The description or display of futuristic technologies can be an important driver towards actual technologies. Similar to science fiction often depicting a distant future, criminal investigations are subject to literature or TV shows as well.

A prominent example is Sir Arthur Ignatius Conan Doyle's Sherlock Holmes which described a new way of forensic investigations. However, recent TV shows, such as "*CSI: Crime Scene Investigation*", are probably influencing a broader audience. Such shows create a public interest in crime scene investigation. Here, new and fast techniques are used to collect and analyze different kinds of traces from crime scenes. Furthermore, such TV shows are often suspected to have triggered a phenomenon called "CSI effect" which describes a suspected impact on the juries in the U.S. legal system [FSC09, pp. 48 – 49]. In fact, it has been the subject of the cover story of the 259th issue of the NIJ Journal [She08], which summarizes the findings from an earlier paper of Shelton et al. [SKB06]. It describes the effect as a wrongful acquittal of guilty defendants if no scientific evidence has been presented within the trial.

In [SKB06] an empirical study of 1027 jurors from Washtenaw County, Michigan, is performed to investigate the effect. In total seven different types of evidence are considered: eyewitness testimonies from the alleged victim, eyewitness testimonies from at least one other witness, circumstantial evidence, scientific evidence of some kind, DNA evidence, fingerprint evidence and ballistics/firearms laboratory evidence. The study confirms that there is a significant expectation and demand of scientific evidence of 46.3% for every criminal case. Towards particular kinds of scientific evidence 21.9% of the test participants expect DNA evidence, 36.4% expect fingerprint evidence and 32.3% expect ballistic/firearms laboratory evidence. Those results are quite surprising because those types of evidence are crime-specific and not necessarily available in each case. For specific types of crimes, the expectations of the test subjects showing a higher demand for DNA evidence in murder or attempted murder and rape cases, for fingerprint evidence in cases addressing breaking and entering, theft and gun involvement. For the latter one an increased demand for ballistic evidence is shown by the study. One finding is that frequent CSI viewers have higher expectations for all kinds of

Broader "tech effect" instead of the "CSI effect"

evidence. However, there seems to be no connection to the TV watching habits of the test persons towards the demand of scientific evidence. The authors claim that the reason for this demand is a broader "tech effect" instead of the "CSI effect".

In line with the demand for the aforementioned tech effect, computational forensics [Sri10] summarizes the extension of forensic investigations with computational methods such as pattern recognition. The Technical Committee on Computational Forensics (IAPR-TC6) defines computational forensics as described in Definition 1.1 [CF18].

Definition 1.1: Computational Forensics (CF) from [CF18]

"CF is an emerging research domain. It concerns the investigation of forensic problems using computational methods. The primary goal is the discovery and the advancement of forensic knowledge. CF involves modeling, computer simulation, computer-based analysis and recognition in studying and solving forensic problems."

Definition of
Computational
Forensics

Computational
forensics in
current
investigations

In fact, in many forensic sciences computational methods are already used. For example, for fingerprint evidence implementations of the Automated Fingerprint Identification System (AFIS) [HRL11, pp. 121-153] is used to identify potential suspects based on a fingerprint trace found at the crime scene using pattern recognition techniques. Thus, the modern analysis of latent fingerprints is considered as computational forensics, even though the subsequent analysis of the fingerprint evidence is performed manually by trained experts. Fingerprint evidence and the use of AFIS is also mentioned in [Sri10] in conjunction with the case of Brandon Mayfield who was wrongfully accused of being responsible for the Madrid train bombings (see also [Off06]). Especially this case shows the need for additional standards and procedures in order to employ computational methods in forensics. An algorithm or method can only perform well in scenarios it has been designed for, if the quality of the input data is insufficient, erroneous results are likely. In digital forensics, which is by the Definition 1.1 also part of computational forensics, such limitations are summarized as the concepts of error, loss and uncertainty [Cas02]. Furthermore, due to its very nature of dealing with digital evidence, the digital forensics community has developed requirements and procedures in order to ensure the quality of the digital traces in terms of their integrity and authenticity. In traditional forensic disciplines quality assurance methods are also in place for forensic laboratories to minimize the risk of tampering with the evidence. In essence, only tested and accepted methods should be applied to a trace and the whereabouts of the evidence itself need to be documented. This so called chain-of-custody (see [IR00, pp. 206 – 207], [Sus+13, pp. 55 – 56]) contains a log covering the acquisition, transfer, analysis and disposition of evidence. This concept is likewise applied for digital and physical evidence. Computational forensics focuses on digital processing methods for the evidence, particular requirements for the chain-of-custody must be considered by forensic practitioners.

Main objective of
this thesis

The main objective of this thesis is the introduction of new processes in traditional forensics which integrate the methods from computational forensics. The focus is the integration of well-known standards and procedures from digital forensics in traditional forensic disciplines in order to create a novel, comprehensive process

model. The vision is to standardize a process which can be applied to digital data as well as to digitized traces. Overall such a process can be considered as a part of computational forensics. However, in contrast to computational forensics additional requirements must be addressed. In [HKG+11] the term digitized forensics is introduced for the first time for the investigation of physical traces in the digital domain. Within the scope of this thesis, it is defined as shown in Definition 1.2 derived from [HKG+11].

Definition 1.2: Digitized Forensics

Digitized forensics describes the processing of traditional (physical) forensic traces which involves a digital acquisition (digitization) of each physical trace at the beginning of the forensic investigation. Afterward, the forensic investigation is performed in the digital domain, whereas the physical traces are preserved and stored without any modification.

Definition of
Digitized
Forensics

Digitized forensics consists of methods for the digital acquisition of physical traces, the digital processing of traces as well as the handling and documentation of physical and digital traces. The main motivation for investigating this particular topic was a German research project called *Digi-Dak* (Digital Dactyloscopy, funded by the German Federal Ministry of Education and Research¹) focusing on the contact-less, non-destructive acquisition of latent fingerprints. Such latent fingerprints are formed by the sweat on the human skin which is left behind as an almost invisible residue after touching a surface. Since the pattern of the fingerprint is considered unique (see e.g. [PPJ02]), the presence of a latent fingerprint at a crime scene is usually strong evidence that a person has been at this location at some point in time. However, the presence of the latent fingerprint does not necessarily mean that the person has been at the crime scene at the time of the crime. Hence, determining the age of a latent fingerprint is an important goal investigated e.g. by Merkel et al. [Mer+12]. In order to be able to observe the natural aging behavior of the latent fingerprint, it is crucial to have acquisition methods that do not influence the residue which forms the fingerprint pattern. This contact-less non-destructive acquisition in combination with pattern recognition techniques to emphasize the fingerprint pattern is a part of this thesis.

Towards the main objective of this thesis of the introduction of new processes in traditional forensics, the creation of a novel process model covering the forensic processing of tangible evidence (trace evidence), as covered by the term criminalistics in [IR00, pp. 10 – 12] and its transformation into a digital representation for further processing in order to create a comprehensible, repeatable, retraceable and revokeable investigation and analysis process, is necessary. Besides this kind of trace evidence, evidence which is already in a digital form, should be processable within the overall process model as well. This is in line with the forensic science disciplines summarized in [FSC09, p. 38]. Any other kind of intangible evidence, such as psychological evaluations of suspects, are not covered by this thesis. However, due to the inclusion of digital evidence, any form of digital documentation for such intangible evidence might be handled within the scope of the process model as well. The digitization of tangible evidence and its processing within the digital domain is not intended to replace forensic

Criminalistics

¹<https://www.sifo.de/de/digidak-digitale-fingerspuren-1858.html>, last accessed 2020/01/17

experts and their decision-making process. Instead, the process is intended to reduce the workload and backlogs by e.g. automating documentation steps. A novel process model can foster the introduction of new technologies in forensic sciences as recommended in [FSC09, pp. 81 – 82]. An essential aspect of the introduction of new technologies is their particular benchmarking or validation in comparison to existing and accepted approaches [FSC09, pp. 113 – 116].

Media Forensics

The lines between digital forensics and forensics of physical, tangible traces are already blurred in some domains. One example for that is the domain of (multi-)media] forensics [KC13]. For example, in the domain of image forensics and the authentication of images, i.e. image source identification [KC13, pp. 160 – 162] either intrinsic features originating from a specific camera (also known as passive forensics [KC13, p. 160]), such as Photo-Response-Non-Uniformity (PRNU) patterns [Fri13, pp. 181 – 198] and color filter array (CFA) patterns [Fri13, p. 186], or extrinsic features (deliberately injected information, or active forensics [KC13, p. 160]), such as watermarks and steganography (see e.g. [BF04], [NT16]) can be analyzed. While the extrinsic features originate from the processing of the data in the digital domain, intrinsic features are introduced into the data based on the digitization process of the sensor and by the optical path and processing within the camera. In audio forensics particular properties of microphones as intrinsic features can be used to authenticate digitized audio signals (see e.g. [Kra13, pp. 69 – 82]). In addition to that, watermarks can be deliberately embedded into the data as additional extrinsic features for authentication purposes. However, in media forensics the media data is usually the subject of the forensic investigation. In contrast to that, in digitized forensics, in a narrow sense, the media file is just the representation of a physical trace as the subject of the investigation. However, due to the close relationship to digital forensics in terms of the formalization of the entire investigation process, the overall process of digitized forensics should be suitable to describe the process of media forensics as well. Furthermore, some forensic process models such as the Analysis-Comparison-Evaluation-Verification (ACE-V) model [HRL11, pp. 9-12 – 9-17] (see 2.1.1.1.2) require an analysis of the origin of the trace representation in the first place. Thus, even within digitized forensics some knowledge of the domain of media forensics needs to be integrated in order to recognize and explain potential artifacts from the trace digitization and processing.

The introduction of digitized forensics might help to mitigate the case backlogs [FSC09, pp. 39 – 40] by allowing for quickly transferring the analysis of digitized traces to a forensic lab with lower case load.

Thesis Design
Goal

This thesis addresses one of the issues pointed out in [IR00, pp. 64 – 65] in conjunction with the question, whether criminalistics is an autonomous scientific discipline. While the thesis does not aim on answering this question, it is supposed to provide a framework for how new technical innovations can be utilized in a common forensic process. With respect to this goal it is important to incorporate best practices from forensics in order to incorporate the domain knowledge and to make new technology more accessible to forensic experts. Thus, the process in digitized forensics should resemble manual investigation steps as close as possible in order to retain accepted investigation procedures the examiners are used to.

Novelty &
Research
Contributions

The novel domain of digitized forensics involves different research fields of computer scientists, engineers, physicists, chemists, lawyers and potentially some aspects of psychologists in terms of the presentation and interpretation of results of (semi-) automated processes. The novelty from the computer scientist point

of view is constituted by the assessment of requirements for the handling of digitized evidence as well as the pattern recognition based application scenarios in [Chapter 5](#) and [Chapter 6](#). From the research field of engineering, physics and chemistry primarily the suitable digitization techniques are relevant. The legal perspective is primarily addressed with the legal frameworks of the Daubert challenge [[DG01](#), pp. xiii-xxi] and the Federal Rules of Evidence (FRoE) [[FRE14](#)].

1.1 Brief Summary of Related Work and Research Gaps

In general the goal of forensic science is a sequence of four goals following the transfer of a pattern at the crime scene [[IR00](#), pp. 43 – 61, p. 76]:

1. Individualization,
2. Identification,
3. Association,
4. Reconstruction.

The origin of a trace is a transfer of a pattern or substance as defined within Edmund Locard's exchange principle (see e.g. [[IR00](#), p. 44]). This transfer allows for linking a crime scene to a specific object or person based on the exchanged patterns or substances. For example in the domain of fiber analysis, particular fibers from the clothing of an offender are left at the crime scene, likewise fibers from the crime scene, e.g. from curtains, carpets, etc., are transferred to the clothing of the offender. Another example are fingerprints, where the fingerprint pattern of the offender is transferred to the objects at the crime scene which were touched by the offender. However, there is a limiting factor to this exchange - the persistence of the traces. The fingerprints are a very good example for this limitation. With the contact between the finger of the offender and the object at the crime scene, substances are transferred in both directions but the particular substances from the crime scene are likely to be lost from the fingertip as soon as the offender washes the hands. In a similar manner, external influences on the crime scene, such as regular cleaning or environmental influences, might destroy or degrade the traces left behind by the offender. In addition to that, especially judges have to evaluate the hypothesis of the transfer of a trace within the course of the crime with respect to other potentially plausible hypotheses.

For the individualization of traces Inman and Rudin differentiate between biological and non-biological evidence [[IR00](#), pp. 45 – 54]. For biological evidence, usually a specific number of matching features is necessary in order to perform the individualization. In general, the required number of matching features depend on the uniqueness of the features which is usually determined with an empirical approach. A special case of biological evidence is DNA (Deoxyribonucleic acid) - the DNA of identical twins is identical, but their fingerprint patterns are different allowing for distinguishing between the two twins [[Tao+12](#)]. For non-biological evidence usually a matching between two pieces of an object or the interaction between a specific tool and an object is performed. However, oftentimes the individualization and the identification is ambiguously used as pointed out in [[Kay09](#)]. Hence, it is important to differentiate between class characteristics,

Individualization

i.e. that a pattern is a fingerprint, a toe print or a palm print, and individual characteristics that can be used to establish that the patterns or objects originate from the same source.

Identification	In [IR00, pp. 54 – 56] the identification is summarizing the determination of such class characteristics which is oftentimes sufficient for a conviction, e.g. by identifying specific illegal substances. However, from an analysis point of view the sequence of the individualization and identification chosen by [IR00, pp. 43 – 61] is misleading because even in the case of an individualization usually the identification phase is performed in the first place, e.g. by determining the origin of a pattern as a part of the analysis phase within the ACE-V process [HRL11, pp. 9-12 – 9-17] (see Section 2.1.1.1.2).
Association	According to [IR00, pp. 56 – 57] the association describes the basis for a conclusion of the contact between two objects. However, it is pointed out by Inman and Rudin that the terminology for the association is ambiguous as well and sometimes resembles parts of the individualization and identification.
Reconstruction	The reconstruction is an ordering of events in relative space and time [IR00, pp. 57 – 61] based on the physical evidence as well as any other additional information available. However, such a reconstruction is usually very challenging based on the available evidence. Thus, it can be primarily used as a plausibility check for the stories of eye-witnesses. The focus of this thesis is primarily the support of the identification and individualization of physical traces as the association and reconstruction usually requires additional information.
Process Models	Besides those final goals of a forensic investigation, more detailed process models exist to formalize the investigation process leading to this result. Such models range from a limited investigation scope such as ACE-V for the analysis of latent fingerprints [HRL11, pp. 9-12 – 9-17] to models covering the complete trace acquisition and analysis process as well as the expert testimony in court. A superficial example for such a model in the domain of digital forensics is the S-A-P (secure, analyze, present) [Ges14, pp. 68 – 69] model. This particular model consists of the secure phase where the traces are gathered, the analyze phase with the data reduction and analysis as well as a subsequent presentation phase with the creation of the report and, if necessary, an expert testimony. One of the most detailed model from the same domain is the model in [CS03] consisting of 17 phases covering the collection and analysis of digital traces as well as the explicit preparation for forensic investigations and a final review of the investigation process. Especially with respect to computational forensics and more specifically for digitized forensics no general process model exists, nor are universal requirements defined for specific stages of the trace collection, handling and analysis process. The only common ground is the need for a chain-of-custody [IR00, pp. 206 – 207] documenting the whereabouts of specific evidence items. Any interruption of the chain-of-custody reduces the evidential value of an item due to the possibility of a malicious alteration of the evidence within that undocumented gap.
Latent Fingerprint Acquisition	With respect to the two application scenarios in the context of latent fingerprint analysis within the scope of this thesis, namely the segregation of fingerprint and substrate patterns as well as the latent fingerprint forgery detection, several related work already exists as summarized e.g. in [HDV17]. In terms of the sensory various illumination techniques, such as ultra-violet-imaging [Li+13], specular reflection of light [Lin+06] or oblique illumination setups [Ble+17, pp.

108 – 110] can allow for digitizing latent fingerprints from specific substrates with or without a chemical or physical preprocessing using digital photography. The diffuse reflection of infrared radiation is utilized in [Ger20] with an oblique top measurement setup. Optical coherence tomography can be used to capture latent fingerprints covered in dust [Dub+08]. In addition to that, Fourier Transform Infrared Spectroscopy (FTIR) can be used to detect a fingerprint based on the chemical composition of the fingerprint residue [Cra+07]. Such a sensor could be also used to analyze the chemical composition of other substances or particles. However, usually a sensor is not exclusively detecting the fingerprint pattern but also particular properties of the object the fingerprint residue is located on.

In order to separate fingerprint patterns from the influence of the object or specific substrate an additional preprocessing of the digitized data is often necessary to allow for analyzing the fingerprint. In the context of digital latent fingerprint enhancement e.g. a semi-automated approach using a manual markup of the fingerprint region of interest as well as characteristic points is utilized in [YFJ11] in combination with a short-time Fourier transform, orientation field estimation using the Recursive-Random-Sample-Consensus (R-RANSAC) algorithm and final enhancement with Gabor filter banks. However, besides the required human input to the algorithm, this particular approach is designed for physically or chemically enhanced - i.e. clearly visible - fingerprint patterns which are overlaid by an additional pattern of the substrate. Other approaches such as [SI14], [Xu+17] and [CHA18] utilize dictionary-based enhancement approaches for latent fingerprints. In such approaches usually small patches of fingerprint patterns are stored within a database. The fingerprint enhancement is then performed by determining the most suitable patch for one region of the latent fingerprint. Such approaches are in general quite promising, but usually large dictionaries are required in order to create an adequate reconstruction of the fingerprint pattern. In addition to that, particular substrate patterns with similar properties to fingerprint patterns might be enhanced using such approaches as well. Moreover, such approaches are usually tuned to improve the automated extraction of feature points by closing gaps in the ridge flow which might mislead latent fingerprint examiners in their decision by misrepresenting the quality of the latent fingerprint.

Regarding the detection of latent fingerprint forgeries a study of the forgery detection performance is described in [CE14]. The results show that the overall performance of latent fingerprint examiners is low with very high error rates even when they are briefed regarding the existence of the forgeries. The challenges are comparable to the presentation attack detection in biometric systems (see e.g. [CJ18]). However, the main difference is the limitation to the analysis of the resulting pattern as no particular sensors can be used to scan the finger of the offender at the crime scene. Thus, semi-automated approaches to raise the attention of the latent fingerprint examiner if particular indicators for forgeries are present are crucial to avoid convictions of innocents.

Besides the creation of latent fingerprint forgeries with the help of ink-jet printers in [Sch09] for evaluation purposes, a more complex setup using a drop-on-demand dispenser is used in [SSG13]. However, the general principle of both approaches is quite similar, but the dispenser allows for printing a broader variety of substances and thus, potentially even more realistic artificial sweat or even real sweat, if it could be harvested. Nevertheless, due to the lower requirements in terms of necessary equipment, the forgery creation using off-the-shelf ink-jet printers currently present the larger threat for forensic investigations.

Fingerprint
Processing

Forgery
Detection

In summary, the following research gaps have been identified within the state of the art:

- \mathcal{G}_1 Lack of a general process model, covering the process of digitized forensics or computational forensics
- \mathcal{G}_2 Lack of a definition of universal requirements for specific stages of the trace collection, handling and analysis process
- \mathcal{G}_3 Lack of a sensor exclusively detecting the fingerprint residue
- \mathcal{G}_4 Lack of a fingerprint pattern reconstruction algorithm for patterns with low visibility
- \mathcal{G}_5 Lack of reliable latent fingerprint forgery detection mechanisms

1.2 Research Questions

The research questions within this thesis can be separated into three categories. The research questions in the first and most important category are related to the process of digitized forensics in general and particular challenges in conjunction with the digitization of physical traces ($\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$). The second ($\mathcal{Q}_4, \mathcal{Q}_5$) and third (\mathcal{Q}_6) category of particular research questions arise from the two application scenarios in the application field of latent fingerprint analysis for the validation of the proposed process model within this thesis.

- \mathcal{Q}_1 How could a generic digitized forensic investigation be formalized as a process and validated for the selected domain of latent fingerprints?
 - \mathcal{Q}_2 Which novel challenges need to be addressed within digitized forensic investigations, in particular with respect to latent fingerprints?
 - \mathcal{Q}_3 Which requirements need to be fulfilled by metrology sensory for an application in digitized forensics and what is the impact syntax and semantics of the captured sensor data related to error, loss and uncertainty?
-
- \mathcal{Q}_4 How could and should latent fingerprints be captured and analyzed within a digitized forensics process using signal processing and pattern recognition to ensure an accurate digital representation of the physical trace?
 - \mathcal{Q}_5 Which classification scheme suits a pattern recognition based fingerprint-substrate segregation best?
-
- \mathcal{Q}_6 How and in which way could the new technology support the detection of forged fingerprint traces?

Research
Questions With
Respect To
Digital Forensics

The first research question \mathcal{Q}_1 addresses the complete investigation process including the preparation for potential cases as well as the storage of evidence. The resulting model is the foundation for discussing all following research questions and is intended to close research gap \mathcal{G}_1 . The second research question \mathcal{Q}_2 addresses novel challenges which stem from the digitization of the traces. Having

sufficient and appropriate solutions for those challenges is essential in order to utilize novel digitized investigation techniques in a scientifically sound manner. However, even if those challenges are not sufficiently addressed, judges might still allow the usage of such new investigation techniques. The main goal of Q_2 is to enumerate residual risks of the digitized forensics investigation process and thus addressing the research gap G_2 by specifying requirements for the implementation of the digitized forensics process in general. The third research question Q_3 addresses particular requirements for sensors in digitized forensics towards closing the research gap G_2 as well as partially research gap G_3 . This is essential if the following investigation and analysis of traces is performed entirely in the digital domain.

In the application scenario of the latent fingerprint processing the research question Q_4 addresses the adaptation of the process of digitized forensics to the processing of latent fingerprints. The goal for this research question is the validation of the applicability of the overall process model resulting from Q_1 . Even though the digitization might be performed on physically or chemically preprocessed traces, a higher goal is the contact-less and non-destructive acquisition of the fingerprint patterns from arbitrary objects and substrates. The research question Q_5 addresses the essential processing steps in order to allow for analyzing the latent fingerprint patterns in line with research gap G_3 and G_4 .

The overall challenge of anti-forensics and tampering with evidence constituting research gap G_5 is addressed with research question Q_6 for the example of latent fingerprints created by artificial sweat and ink-jet printers. In this example especially the application of the sensor requirements from Q_3 is assessed for a practical application field in forensics.

Research
Questions With
Respect To
Latent
Fingerprint
Processing

Research
Questions With
Respect To
Forgery
Detection

1.3 Objectives and Addressed Research Challenges of this Thesis

The objectives of this thesis are geared towards answering the research questions from the previous subsection. Thus, the objectives can be separated into the same three categories addressing either the general process of digitized forensics (O_1 and O_2) or one of the two application scenarios O_3 and O_4 within the scope of this thesis.

O_1 Creation of a novel universal process model for digitized forensics for all types of traces on the foundation of existing process models from forensics and digital forensics and its exemplary validation for the domain of latent fingerprint processing.

O_2 Design and implementation of selected supporting tools for digitized forensics addressing current research gaps in the context of O_1 .

O_3 Design, implementation and evaluation of a novel signal processing and pattern recognition based pipeline for segregating latent fingerprint patterns from substrate data within a subset of O_1 .

O_4 Design, implementation and evaluation of a novel pattern recognition based approach for detecting latent fingerprint forgeries based on printed amino acid within a subset of O_1 .

Objectives
Addressing
Digital Forensics

The primary focus of this thesis is the process of digitized forensics. In order to allow for projecting a traditional forensic discipline into the digital space within the scope of digitized forensics or computational forensics, a suitable sensor to digitize the essential information of a trace is necessary. However, with this digitization process and the following investigation in the digital domain new challenges arise. The challenges from the computer science point of view are related to the authenticity and integrity of the digitized trace as well as assessing any kind of unintended loss, uncertainty and errors during the investigation process. This thesis addresses those challenges with a novel process model covering the process of digitized forensics in relation to traditional forensic disciplines as well as supporting considerations and tools. In line with that, the first and most important objective of this thesis is the creation of a novel universal process model for digitized forensics \mathcal{O}_1 . This model is intended to cover all the shared requirements and processing steps of the transformation of traditional forensic disciplines analyzing physical evidence to the digital domain. In addition to that, the requirements of digital forensics should be covered as well in order to create a one-size-fits-all process model for forensic investigations in criminalistics. However, by doing that, the peculiarities of a specific trace type cannot be covered within the model. The model is intended to create a common guideline for digitized forensic investigations which allow for a thorough assessment of a judge on a common ground before the admission of evidence in court which is processed by novel techniques.

The second objective \mathcal{O}_2 is intended to create the necessary tools for digitized forensics filling the existing gaps of the state of the art of available tools. For any kind of new means for the investigation and analysis of a particular trace, the effectiveness and general suitability of the new method needs to be shown. This is especially necessary to allow judges to assess the new technology prior to the admission of the investigation results in court. This legal perspective is assessed on a theoretical basis from a technical point of view on the foundation of the U.S. supreme court level requirements. However, it is worth mentioning that the author of this thesis has no legal education whatsoever. Thus, the interpretation of the legal documents and requirements is performed from a computer scientists' point of view to identify particularly necessary tools to support the digitized forensics process.

Objective
Addressing
Latent
Fingerprint
Processing

The novel process model is validated for the example of latent fingerprint processing. In particular two application scenarios in this domain are selected within the context of the process model for digitized forensics from \mathcal{O}_1 . In this domain currently destructive preprocessing methods which might interfere with other investigation goals are utilized. The addressed research challenge in this domain is the segregation of the latent fingerprint pattern from the substrate pattern in order to allow for matching the fingerprint with another pattern from known origin which represents the third objective \mathcal{O}_3 . The performance of this process is evaluated using a biometric matcher to produce reproducible results. In practice this matching process is performed manually by highly trained experts whom are able to account for differences in the patterns. Thus, the achieved matching performance can be considered as a lower bound for the performance in practice. The selected approach is the result of discussions with latent fingerprint examiners from various countries in the European Union in order to provide an approximation of the resulting quality of the captured and processed data within the scope of digitized forensics.

The last addressed research challenge and second application scenario within this thesis, is the detection latent fingerprint forgeries created with ink-jet printers. Any kind of forged trace constitutes a major challenge for forensics. Such a means of anti-forensics might mislead the forensic expert and thus, alter the result of the forensic investigation. Usually experts are trained for certain indicators for a forgery (see e.g. [CE14, pp. 28 – 29] for the example of latent fingerprints). However, the particular detection of forgeries is a challenging task with high error rates [CE14, pp. 29 – 31]. This challenge of anti-forensics for latent fingerprints is addressed for the example of artificially printed latent fingerprints by the objective \mathcal{O}_4 .

Objective
Addressing
Latent
Fingerprint
Forgery
Detection

1.4 Summary of the Contributions of this Thesis

The contributions of this thesis are closely related to the research questions and the derived objectives. As a result, the contributions can be divided into three categories – general process of digitized forensics ($\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$), application scenario 1 ($\mathcal{C}_5, \mathcal{C}_6$), application scenario 2 ($\mathcal{C}_7, \mathcal{C}_8$) – as well.

\mathcal{C}_1 A novel process model for forensics in the physical and digital domain as a foundation for modeling forensic application scenarios from a scientific point of view as well as a coarse guideline for forensic investigations in the future.

\mathcal{C}_2 Formalization of Error, Loss and Uncertainty with respect to sensor data syntax and semantics in digitized forensics.

\mathcal{C}_3 A novel approach for creating a bijective link between a physical trace and its digital representations.

\mathcal{C}_4 A benchmarking solution for simulating sensor and trace influences in image sensor data.

\mathcal{C}_5 A novel feature space for segregating latent fingerprints from substrate data as part of a signal processing pipeline in fingerprint recognition.

\mathcal{C}_6 Biometrics based evaluation of the segregation of latent fingerprints from substrate data.

\mathcal{C}_7 Three feature spaces for the pattern recognition based detection of fingerprint forgeries based on printed amino acid.

\mathcal{C}_8 Benchmarking and fusion of feature spaces for the detection of latent fingerprint forgeries based on printed amino acid.

The main contribution of this thesis is the novel process model for digitized forensics (\mathcal{C}_1) in [Chapter 3](#). In the context of this process model, error, loss and uncertainty is formalized with respect to the sensor data syntax and semantics (\mathcal{C}_2) in [Section 3.2.2](#) and [Section 3.2.1](#). The most pressing challenge of ensuring the authenticity of the digitized trace is addressed within the contribution \mathcal{C}_3 by introducing a novel approach for creating a link between a physical trace and its digital counterparts in [Section 4.2](#). Secondly, a tool for the systematic benchmarking of pattern recognition based approaches in the context of digitized

Contributions To
Digital Forensics

Contributions To Latent Fingerprint Processing	forensics is introduced in Section 4.3 which represents the contribution \mathcal{C}_4 . With respect to the first application scenario of the segregation of latent fingerprint data from substrate data in Chapter 5 this thesis contains two particular contributions. The first contribution \mathcal{C}_5 introduces a novel feature space for the pattern recognition based data segregation. The evaluation of the feature space and the biometric evaluation of the resulting fingerprint patterns is the second contribution \mathcal{C}_6 in this context.
Contributions To Latent Fingerprint Forgery Detection	With respect to the second application scenario addressing the issue of the detection of latent fingerprint forgeries in Chapter 6 the first contribution \mathcal{C}_7 consists of three feature spaces for the pattern recognition based detection. The particular evaluation of the forgery detection approach including a systematic benchmarking using the framework from \mathcal{C}_4 is representing the contribution \mathcal{C}_8 .

1.5 Thesis Outline

This thesis is structured into nine chapters and one appendix containing all supplemental materials. This first chapter contains a motivation and introduction of the topic of digitized forensics, a brief overview of the state of the art regarding forensic investigations and the two application scenarios of this thesis including current research gaps, the overall research challenges of digitized forensics, the research questions, objectives and contributions of this thesis. The [Chapter 2](#) contains the fundamentals of this thesis which cannot be considered as common knowledge within the domain of computer science. In [Chapter 3](#) the novel process model for digitized forensics, including considerations of sensor syntax and semantics, error, loss and uncertainty in the context of sensor data and decisions, as well as novel challenges which arise from the concept of digitized forensics, are introduced. The currently insufficiently solved challenges are addressed by the design and implementation of supporting tools in [Chapter 4](#). [Chapter 5](#) contains the validation of the process model for the example of the processing of latent fingerprints within the scope of digitized forensics. Albeit the focus of this application scenario is on the segregation of the fingerprint data from the substrate data, particular steps during the digitization of the fingerprint traces are summarized as well. The second application scenario for the validation of the process model is described in [Chapter 6](#) for the example of the detection of latent fingerprint forgeries created by ink-jet printers equipped with artificial sweat. Due to the very high detection performance of the proposed approach, additionally an extensive systematic benchmarking is performed using the framework which constitutes the contribution \mathcal{C}_4 .

[Chapter 7](#) contains an analysis of other application fields of the process model of digitized forensics and the proposed benchmarking framework. In addition to that, the potential future implications of digitized forensics are discussed. A summary of the thesis with respect to the research questions, objectives and contributions is contained in [Chapter 8](#). Potential future work addressing the limitations of the thesis as well as potential research paths on the foundation of this thesis are summarized in [Chapter 9](#).

The appendix of this thesis contains implementation details as well as the raw outputs of the classification and matching algorithms. The following [Table 1.1](#) summarizes the structure of the thesis in relation to the research questions, objectives and contributions.

	Question	Objective	Contribution	State of the Art	Concept	Supporting Tools	Application Scenario 1	Application Scenario 2
Research Questions								
Q_1		O_1, O_2	C_1, C_2, C_3, C_4	Section 2.2 2.1, 2.1.2.2	Section 3.1	Section 4.3 4.1, 4.2, 4.3,	Chapter 5	Chapter 6
Q_2		O_2	C_2, C_3, C_4	Section 2.1.2.1, 2.1.2.2	Section 3.1, 3.2, 3.3	Section 4.2		
Q_3		O_2, O_3, O_4	C_2	Section 2.3	Section 3.2	Section 4.1	Section 5.3.1	Section 6.3.1
Q_4		O_1, O_3	C_1, C_2, C_5, C_6	2.1.1.2, Section 2.4, 2.3.4, Section 2.5	Section 3.1	Section 4.1	Chapter 5	
Q_5		O_3	C_5, C_6	Section 2.4.3	Section 3.3.3		Chapter 5	
Q_6		O_1, O_4	C_1, C_7, C_8	Section 2.5.3 Section 2.4.3	Section 3.3.3	Section 4.3		Chapter 6
Objectives								
O_1	Q_1, Q_4, Q_6		C_1, C_2, C_3, C_4	Section 2.2 2.1, 2.1.2.1	Section 3.1	Section 4.3 Chapter 4	Chapter 5	Chapter 6
O_2	Q_1, Q_2, Q_3		C_3, C_4	Section 2.1.2.2	Section 3.3			Section 6.3.8
O_3	Q_3, Q_4, Q_5		C_5, C_6	Section 2.4.3	Section 3.2	Section 4.1	Chapter 5	
O_4	Q_6		C_7, C_4, C_8	Section 2.4.3	Section 3.2	Section 4.1	Chapter 5	Chapter 6
Contributions								
C_1	Q_1, Q_4, Q_5	O_1		Section 2.2 2.1, 2.1.1.1	Section 3.1		Chapter 5	Chapter 6
C_2	Q_2, Q_3	O_1		Paragraph 2.1.1.1.1, Section 2.3.1	Section 3.2, 3.2.2, Section 3.2	Section 4.1		
C_3	Q_1, Q_2	O_1, O_2			Section 3.3.1	Section 4.2		
C_4	Q_1, Q_2	O_1, O_2, O_4		Section 3.3.3	Section 4.3		Section 6.3.8	
C_5	Q_4, Q_5	O_1, O_3		Section 2.3.5, 2.4.4, Section 2.5	Section 3.1.2		Section 5.4 5.2.1,	
C_6	Q_4, Q_5	O_3		Section 2.4.4	Section 2.5.3 Section 3.1.2	Section 3.1	Chapter 5	
C_7	Q_6	O_4		Section 2.4.4	Section 3.1.2			Section 6.4 6.2,
C_8	Q_6	O_4		Section 2.4.3	Section 3.1	Section 4.3		Chapter 6

Table 1.1: Structure of the Thesis

Thesis Fundamentals and Related Work

This chapter contains selected fundamentals and the state of the art for the research conducted within the scope of this thesis. At first particular selected forensic principles including standards and process models are summarized in [Section 2.1](#). Afterward, an overview of the legal background for the example of the U.S. federal supreme court level is given in [Section 2.2](#). The properties of the sensory available for evaluation and substrates are summarized in [Section 2.3](#). An overview of error rates and the basics of the utilized pattern recognition techniques within the scope of this thesis is given in [Section 2.4](#). Subsequently, the application field of latent fingerprints is briefly summarized in [Section 2.5](#) as a foundation for the two application scenarios within this thesis.

2.1 Forensic Principles

This section contains the selection of forensic principles which are considered relevant for the creation of the process model of digitized forensics in [Chapter 3](#). The motivation for using existing models for an inductive modeling approach is the acceptance of those existing models. A model which is frequently applied and generally accepted in the particular domain is probably not incorrect and furthermore suitable to describe the necessary investigation steps. In the first subsection particular standards and best practices for forensic investigations in the physical and digital domain are summarized. Afterward, selected standards for the evaluation and handling of evidence are discussed.

2.1.1 Standards and Best Practices in Forensic Investigations

Forensic science relies on the scientific soundness and the proper application of the forensic methods. Thus, standards and best practices for the application of particular techniques are crucial, which is also reflected by the Daubert factors [[DG01](#), pp. xiii-xxi] (see [Section 2.2](#)). In the following subsections at first selected process models from the domain of traditional forensics disciplines are summarized. Afterward, selected models from the domain of digital forensics are summarized. The latter have usually been created on the foundation of existing process models and best practices for traditional forensic disciplines. However, those process models address the peculiarities of digital evidence. Thus, the combination of the domain knowledge from both domains is considered as a suitable approach for creating a process model for digitized forensics within the scope of this thesis.

2.1.1.1 Process Models in Traditional Forensics

The process models in traditional forensics originate from best practices and requirements to minimize the risk of error within the investigation process. The models are usually trace-dependent and incorporate a high amount of domain knowledge. However, some requirements, such as the ISO/IEC17025 [ISO17] are more generic in order to define common standards for forensic laboratories. Due to the focus of the application scenarios, the scope of this subsection is limited to the analysis of latent fingerprints, namely the ACE-V model [HRL11, pp. 9-12 – 9-17].

2.1.1.1.1 Accreditation of Laboratories based on ISO/IEC17025

The ISO/IEC standard 17025 [ISO17] defines general requirements for the testing and calibration within laboratories. The standard is not exclusively tailored to forensic laboratories, the particular requirements are applicable to all calibration and testing procedures in any laboratory. The overall goal of the standard is supporting laboratories in developing management systems for quality, administrative and technical operations [ISO17, p. 1]. Despite not being designed as a basis for certification, the standard can also be used for regulatory authorities and accreditation bodies for confirming the competence of a laboratory. The standard defines requirements from the organizational (management requirements) and from the technical point of view.

Management
Requirements

From the organizational point of view especially the requirements towards a management system are relevant for this thesis. Namely, that the policies, systems, programs, procedures and instructions need to be documented to assure the quality of the testing and calibration [ISO17, p. 3]. The policies can be considered as a process model for the application of a specific technique in order to ensure the quality of the results of an investigation. It is also required that all document changes are reviewed and approved [ISO17, p. 5], ideally with some sort of track changes mode to highlight the alterations. The requirements regarding the control of records [ISO17, p. 9] are also important to ensure the security aspect of non-repudiation as well as for the purpose of comprehensibility and retraceability of results.

Technical
Requirements

The technical requirements in [ISO17, pp. 10 – 23] address factors from the following domains:

- Personnel,
- Accommodation and environmental conditions,
- Test and calibration methods and method validation,
- Equipment,
- Measurement traceability,
- Sampling,
- Handling of test and calibration items,
- Quality assurance for the test and calibration results and
- Reporting of the results.

The requirements regarding the personnel are supposed to ensure that all employees are appropriately trained to perform the assigned tasks. This requires a training and education in order to achieve the necessary qualifications.

The accommodation and environmental conditions of the laboratory must be suitable for the performed task and utilized equipment in order to ensure the best performance of the measurements. Those conditions should be monitored, controlled and recorded. Especially if specific activities require incompatible environmental conditions, a separation is necessary in order to avoid any negative impact on the measurement results. In addition to that, any access to those areas should be controlled.

The tests and calibration methods and method validation are intended to estimate the measurement uncertainty in order to maintain reliable results. In addition to that, specific methods should be utilized in accordance to the latest valid edition of a standard. In general, appropriate methods should follow standards, the procedures described in relevant scientific publications or guidelines provided by the manufacturer. Any kind of method that has been developed by the laboratory needs to be validated and additionally must be appropriate for the intended use. However, the utilization of non-standard method is possible as well, as long as particular requirements are met. The validation of the methods is the confirmation that the specific intent of an investigation can be fulfilled appropriately. In this context it is necessary to determine the value range and accuracy of the resulting data. This does also include factors such as the reproducibility, external influences and uncertainty of the results. If computers or automated equipment are utilized for the acquisition, processing, recording, reporting, storage or retrieval of the data it is required to ensure that the software is documented and validated. Furthermore, the data needs to be protected regarding the integrity and confidentiality during all processing steps.

The equipment of the laboratory should be selected to achieve the required accuracy and in compliance with the specifications relevant to the tests and calibrations. Especially new equipment should be calibrated or checked in order to ascertain that it complies with the requirements and specifications which is also a general requirement to ensure measurement traceability. In addition to that, any equipment and its software should be uniquely identifiable. The information about the equipment should be documented including but not limited to particular tests, calibrations and certifications, the maintenance plan, repairs and location.

For the measurement traceability the calibration of the equipment should be performed on the foundation of the international system of units (SI) which rely on fundamental physical constants or using certified reference materials.

The sampling of materials should follow a sampling plan which is based on appropriate statistical methods. All relevant data and operations regarding the sampling should be documented including the utilized sampling method, the identification of the sampler, the environmental conditions and diagrams describing the sampling location.

The handling of test and calibration items govern the procedures for transport, receipt, handling, protection, storage, retention and disposal of test and calibration items. This also includes precautions to protect the integrity of such items. Any abnormalities should be documented. In addition to that, a deterioration, loss or damage of the test and calibration items should be avoided during the storage, handling and preparation.

The quality assurance for the test and calibration results is essential to ensure the

validity of the results. Any resulting data should be documented and reviewed. In addition to that, quality control data should be analyzed in order to prevent the reporting of incorrect results

Subsequently, the reporting of the results requires that the reports are accurate, clear, unambiguous and objective. In addition to that, a list of particular information to be included in the report is specified by the standard [ISO17, pp. 20 – 22]. Any opinions and interpretations should be clearly marked in the report.

Overall, the terminology of the standard [ISO17] focuses on the term 'shall' for the requirement, which leaves some margin for interpretation. Especially for the requirements regarding the quality assurance, measurement traceability and the documentation a stricter requirement, i.e. the wording must, would be probably more appropriate. However, as the standard is not intended to be the direct basis for a certification, any certification body might have stricter requirements. Nevertheless, within the scope of this thesis this standard is useful to determine the forensic readiness of a laboratory. Thus, this particular standard is highly relevant for the strategic preparation described in Section 3.1.2.

2.1.1.1.2 ACE-V Model

The ACE-V model [HRL11, pp. 9-12 – 9-17] describes the investigation process for latent fingerprints. It consists of four phases:

- Analysis,
- Comparison,
- Evaluation,
- Verification.

Analysis

During the *analysis* phase a latent fingerprint is investigated towards its quality, present features and potential anomalies. In this step a decision is made whether a fingerprint is suitable for a comparison with another fingerprint, whether it is at least suitable for an exclusion or whether it is of insufficient quality. The difference between a comparison and an exclusion is the expectation of potential results of the evaluation phase. In particular in ideal conditions the result of an evaluation can be a match, i.e. the two fingerprints originate from the same finger, or an exclusion, i.e. the fingerprints originate from different fingers. In the case of low quality or partial fingerprints the amount of visible fingerprint features might be insufficient for establishing that the two patterns originate from the same finger. However, if sufficient differences are visible in the same region of latent fingerprint, an exclusion is possible. An example for such an exclusion is a mismatching level-1 pattern (see Section 2.5.1) as the level-1 pattern is insufficient for an identification or verification but of course a matching level-1 is a requirement for a match. In particular, the following aspects of a latent fingerprint trace are assessed during the analysis phase [HRL11, p. 9-13]:

- Anatomical source of the print - e.g. finger, palm, toe
- Anatomical direction
- Presence of level-1 patterns

- Presence of level-2 patterns (minutiae points)
- Substrate the fingerprint was lifted from
- Fingerprint development medium - e.g. dusting, cyanoacrylate fuming
- Preservation method - e.g. lift, photograph, legible copy
- Additional factors - e.g. presence of level-3 patterns, scars, creases, deposition pressure, rotational movement, lateral movement

In addition to that, the case record is updated during the analysis phase of the ACE-V process.

The *comparison* phase consists of one or multiple side-by-side comparisons of the latent fingerprint with other reference fingerprint patterns. The latter are usually of a known origin and can be either latent fingerprints from other crime scenes or exemplar fingerprints that have been captured from a finger directly. Exemplar fingerprints are often collected as rolled fingerprints (rolled from fingernail to fingernail) in order to cover the complete surface of the finger. Depending on the equipment at the police precinct such exemplar fingerprints are either captured using sensors (live scans) or by applying inks to the fingers before rolling them on a sheet of paper. The comparison begins with a comparison of the level-1 pattern (macro detail) since it is rather easy to determine whether the level-1 patterns are matching. The comparison can be aborted when the patterns are different, e.g. when one fingerprint has a whorl as a level-1 pattern whereas the second print has a loop. If the level-1 patterns match or if the level-1 pattern is not visible in one of the fingerprints the comparison continues with an assessment of the level-2 patterns. During this step, the examiner attempts to match the minutiae points in each of the prints based on their type, position and orientation. However, due to potential distortions of the skin during the contact with the substrate material, this step is somewhat subjective. Hence, it is crucial that any differences can be explained plausibly. The distortions of the skin causing the deviations in the fingerprint are often not linear. Thus, this process is usually performed manually by highly trained experts. The particular tolerance for smaller differences in the fingerprint patterns depends on the overall quality of the fingerprint. Usually the tolerances are higher within low-quality fingerprint patterns.

Comparison

The conclusion of the comparison process is formulated within the *evaluation* phase. The latent print examiner decides whether the two patterns originate from the same finger based on the careful consideration of the results of the comparison and the analysis of the fingerprints. For that, the identified potentially matching level-1, level-2 and level-3 features are reviewed and assessed depending on the applicable standards. Here, in a numerical standard, a certain number of matching features must have been identified during the comparison. Alternatively, in the non-numerical standard (see e.g. [CC09, pp. 71 – 74]), the rarity of specific features is taken into account in order to formulate the conclusion. The conclusion can contain one of three different outcomes:

Evaluation

- Individualization,
- Exclusion,
- Inconclusive.

With respect to biometric systems an individualization constitutes a match between the two fingerprint patterns. In terms of forensics the individualization indicates that there is a very high likelihood that the two fingerprint patterns originate from the same finger. This requires that a sufficient number of matching features are present within the two fingerprint patterns and that all differences can be explained plausibly. If the differences cannot be explained, the comparison will probably result in an exclusion. This means, that the fingerprint patterns originate from different fingers. In other cases, i.e. an insufficient number of matching features but no different features justifying an exclusion, the result of the evaluation is inconclusive. Both outcomes, exclusion and inconclusive, are equivalent to a non-match in a biometric system.

Verification

Due to the subjective nature of the analysis, comparison and evaluation of the fingerprints, an additional step is used in the ACE-V model to minimize the risk and rate of error. In this *verification* phase at least a second latent print examiner performs the analysis, comparison and evaluation of the same pair of fingerprint patterns.

2.1.1.2 Selected Process Models for Digital Forensics

The process models for digital forensics differ in their perspective on the process of digital forensics. Some models explicitly address the system operators covering incident response and/or forensics, whereas others are geared towards crime scene investigators or expert witnesses. Secondly, some models address practitioners whereas others address the issue of forensics from a scientific point of view. In this section selected models, which form the foundation for the model in Section 3.1, are summarized. Particular advantages or drawbacks of the models are discussed within the appropriate subsections within Section 3.1. In this section the term digital assets is used to describe systems, networks and software.

2.1.1.2.1 NIST SP 800-61 r2

The NIST computer security incident handling guide [Cic+12, pp. 21 – 44] describes a four-staged process for handling an incident. This particular model is geared towards incident response rather than forensics. Nevertheless, several steps are performed in a similar manner. The following four stages of the process are used in this particular model:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

Overall the process is considered as a life cycle - i.e. any insights gained from the investigation are afterward used to increase the readiness for the next incident.

Preparation

The preparation phase [Cic+12, pp. 21 – 24] contains all actions prior to an incident. Such actions include the establishment of an incident response capability as well as preventive measures by ensuring that all digital assets are sufficiently secure. Such preparation also includes the establishment of means for communication in case of an incident, ranging from collecting contact information,

establishing reporting mechanisms to the set-up of a war room and secure storage facilities. In addition to that, hardware and software for the incident analysis need to be procured and set-up. This includes digital forensic workstation, laptops, spare digital assets for various purposes, blank media, portable printers, packet sniffer, protocol analyzers, digital forensic software, trusted versions of software to gather digital evidence and other evidence gathering accessories. For the incident analysis port lists of known malware, a documentation of the digital assets including network diagrams and specifically critical assets, baseline figures for the behavior of digital assets as well as cryptographic hashes of critical files should be collected in order to increase the forensic readiness. Additionally, from the incident response perspective clean images of operating systems and applications should be stored for the recovery of affected systems. The recommendations in [Cic+12, pp. 21 – 24] also state that each incident handler should have access to at least two computing devices to mitigate the risk of an infection of the analysis system during the investigation. Another emphasis is the prevention of incidents in the first place by performing risk assessments, strengthening the security of hosts and networks, establishing malware protection and raising the awareness of users.

The detection and analysis phase [Cic+12, pp. 25 – 34] contains a collection of attack-vector-dependent handling procedures. The signs of an incident are differentiated into the categories of precursors, i.e. signs that an incident may occur, and indicators, i.e. signs that an incident might have happened or is still ongoing. The precursors can be used to increase the monitoring of the potentially affected systems whereas the indicators should trigger a forensic investigation of the affected digital assets. With respect to the incident analysis in [Cic+12, pp. 25 – 34] also the possibility of false alarms is discussed. Thus, it is necessary to differentiate real security incidents from such erroneous precursors or indicators. Furthermore, technical defects and human error can be the root cause for an indicator as well. Each incident should be analyzed and documented using a predefined process. The initial goal is the confirmation of the incident and the determination of the extent of it with respect to the affected digital assets. Afterward, the question of who/what originated the incident and how it is occurring should be answered. Based on the gathered information all following activities can and should be prioritized based on the expected functional and information impact as well as the recoverability from the incident. Another emphasis of this phase is the documentation of the incident. In particular, all facts regarding the incident should be recorded either manually in a logbook or using various devices such as laptops, cameras or an incident tracking system. Subsequently, appropriate contact persons, such as the Chief Information Officer (CIO), the system owner or the law enforcement, should be notified about the incident.

Detection and
Analysis

The phase of the containment, eradication and recovery [Cic+12, pp. 35 – 38] is more focused on the aspects of incident response rather than digital forensics. Nevertheless, some aspects still overlap with typical decisions in forensics, e.g. whether a system should be shut down or disconnected from the network. Whereas in digital forensics those decisions are being made from the perspective of the integrity of the evidence, in incident response the risk management is the primary motivation, which also includes the availability of particular services. A special form of the containment is the redirection of the attacker to a sandbox. By doing this, the activity of the attacker could be monitored to gather additional

Containment,
Eradication and
Recovery

evidence. In general, the gathering of evidence including identifying information about the digital assets is a part of the containment within this phase. Here, also a detailed log should contain the names of the investigators, the time and the data of the evidence handling and the storage locations. The last goal of the containment is the identification and validation of the attacking hosts and the utilized communication channels. Subsequently, particular measures for the eradication of the components of the incident are utilized to restore a consistent state of the digital assets. Furthermore, the identification and mitigation of all exploited vulnerabilities is performed.

Post-Incident
Activity

The post-incident activities [Cic+12, pp. 38 – 44] contain a reflection of the incident and the course of events, a performance evaluation for the incident handling and an analysis towards potential improvements of the process. Furthermore, improvements regarding the system and potential detection mechanisms are derived. The particular policies regarding the evidence retention are important for digitized forensics as well as particular legal requirements and cost of storage need to be considered.

Due to the overall emphasis on incident response, the sequence of particular investigation steps is not necessarily suitable for forensic investigations as the detection and analysis phase might alter data within the digital assets before the actual gathering of evidence within the containment phase. However, with respect to digitized forensics, there are some similarities as the detection and analysis could be considered as the basic assessment of a crime scene including the identification of potential evidence.

2.1.1.2.2 NIJ Electronic Crime Scene Investigation Guide for First Responders

The guidelines for first responders in [MSH08, p. x, pp. 13 – 34] target on the tools and procedures for the evaluation of the crime scene. At first a very brief preparation for incidents is performed by creating an 'inventory' of personnel with special skills. As soon as the incident is detected, the following steps are performed:

- Documentation of the crime scene,
- Collection of evidence,
- Packaging, transportation and storage of digital evidence.

Documentation
of the Crime
Scene

The particular tasks can be compared to the crime scene investigation where the first responders decide which particular items might are of relevance for the committed crime. Thus, the one of the most important tasks is the documentation of the crime scene. This particular documentation contains information about the crime scene in general as well as about particular digital assets and their state, i.e. whether they are powered on and connected to a network. Just like for the crime scene investigation for more traditional evidence, such as the primary custody documentation for fingerprints as described in [HRL11, pp. 10-5 – 10-17], photographs, video recordings, notes and sketches can help to reconstruct the details of the crime scene later.

Collection of
Evidence

During the evidence collection [MSH08, pp. 21 – 30] the particular state of the digital assets should be assessed in order to minimize the risk of an alteration of

digital evidence. Particular screen contents should be preserved using photographs if possible. All connections of digital assets should be documented and labeled. In special circumstances, e.g. computers displaying potential evidence for the committed crime, additional assistance might be requested (comparable to the case of primary custody with a latent fingerprint examiner at the crime scene). The packaging, transportation and storage of digital evidence [MSH08, pp. 31 – 34] constitutes the beginning of the chain-of-custody (see also Section 2.1.2.1). In particular other traces such as latent fingerprints or biological evidence are considered as well. Here, the recommendation is to secure the digital evidence by creating forensic images (copies) before other traces are processed. In storage all the digital evidence must be inventoried, which is also a part of the chain-of-custody. Furthermore, the digital evidence should be stored in a secure, climate-controlled environment or a location which is not subject to extreme conditions including temperature, humidity, magnetic fields, moisture, dust or vibration. Within the scope of this thesis, the particular guidelines are primarily relevant for the processing of the crime scene in Section 3.1.3.

Packaging,
Transportation
and Storage of
Digital Evidence

2.1.1.2.3 Framework of Reith et al.

The framework from [RCG02] divides the forensic investigation into nine phases:

- Identification,
- Preparation,
- Approach strategy,
- Preservation,
- Collection,
- Examination,
- Analysis,
- Presentation and
- Returning evidence.

The identification phase basically involves all necessary actions to detect an incident based on the observed indicators. The particular type of the incident should be identified as well, as this likely has an impact on the following course of the investigation.

Identification

The preparation phase can be considered as an active preparation of the forensic investigation to be performed. It includes the preparation of required tools and techniques, the procurement of search warrants and monitoring authorizations as well as the support by the management.

Preparation

The approach strategy is the planning of the collection of digital evidence based on the specific technology in question and the potential impact on bystanders. An interesting aspect of this phase is the goal of minimizing the impact to the victim which could imply that less than ideal means for the data collection, such as only a selective imaging or the copying of specific files, might be used.

Approach
Strategy

The preservation phase describes the isolation, securing and preservation of the

Preservation

state of physical and digital evidence. Especially the consideration of physical evidence is important as this is a similarity to [MSH08, pp. 21 – 30] in Section 2.1.1.2.2.

Collection	The collection phase is the actual collection of the digital evidence using standardized and accepted duplication procedures. In addition to that, the crime scene itself should be documented.
Examination	Reith et al. [RCG02] describes the examination phases as an in-depth systematic search within the collected digital evidence in order to identify traces relating to the suspected crime. All potential evidence should be located and identified during this phase. The result is a detailed documentation forming the foundation for the following analysis phase. During the following analysis phase this evidence is assessed regarding the significance. Furthermore, fragments of data are reconstructed. Subsequently, conclusions are drawn based on the evidence found. In this context it is quite interesting that the authors in [RCG02] state that this particular phase does not require high technical skills which is quite the opposite of the ACE-V model [HRL11, pp. 9-12 – 9-17] in Section 2.1.1.1.2.
Analysis	In order to achieve this, the nature and considerations regarding the pieces of evidence need to be documented in detail during the preceding examination phase.
Presentation	The presentation phase contains the summary and explanation of the conclusions of the forensic investigation. An important aspect is that this summary should be written in layperson's terms using an abstracted terminology with references to the specific details. The motivation for this is the target audience for the report.
Returning Evidence	Subsequently, the phase of returning evidence contains the returning of the digital assets to the proper owner. However, any criminal evidence must be removed from the systems.

With respect to this thesis, this particular process model is relevant because it covers the physical acquisition of digital and physical evidence at the crime scene as well as the collection and investigation of the digital evidence.

2.1.1.2.4 Carrier and Spafford

The model of Carrier and Spafford [CS03] is one of the more complex models for the process of digital forensics. Furthermore, a specific distinction between physical and digital evidence as well as physical and digital crime scenes is made by the authors which is reflected in the five groups of phases of the investigation process:

1. Readiness phases,
2. Deployment phases,
3. Physical crime scene investigation phases,
4. Digital crime scene investigation phases,
5. Review phase.

Due to the explicit consideration of digital and physical evidence, this particular model is used as a foundation for the novel process model for digitized forensics in Section 3.1.

Readiness	The two readiness phases have the intention of making sure that the operations and infrastructure are suited to fully support an investigation: Operations
-----------	--

readiness phase (training and equipment for personnel), Infrastructure readiness phase (needed data exists for a full investigation, i.e. installation of CCTV).

The deployment phases are geared toward the detection of an incident. Here, the detection and notification phase describes all measures for the detection of the incident and notification of appropriate people, e.g. a 911 call or alert messages from network intrusion detection systems. In general, this phase designates the start of the investigation. The confirmation and authorization phase is intended for the justification of the forensic investigation from a technical (e.g. identification of particular attack indicators) and legal (e.g. obtaining a search warrant or authorization of company officials) point of view. Especially the confirmation of an incident bears the risk of influencing the system within a live analysis.

Deployment

The final review phase is performed to identify the potential for improvements of the investigation process.

Review

The core parts of the model describing the physical and digital crime scene investigation phases are summarized in the following subsections.

Physical Crime Scene Investigation The model in [CS03] contains six physical crime scene investigation phases:

Physical Crime
Scene
Investigation

- Preservation of the physical scene,
- Survey for physical evidence,
- Document evidence and scene,
- Search for physical evidence,
- Physical crime scene reconstruction,
- Presentation of complete theory.

The preservation of the physical crime scene in this model can be considered as universally applicable to various types of crimes serving the purpose of avoiding any alteration of the crime scene prior to the identification and collection of evidence. The particular measures for the preservation of the crime scene range from the securing of the exits, helping the wounded, detaining suspects to the identification of witnesses. During the survey for physical evidence any obvious evidence is identified. Any fragile evidence should be documented and collected in this phase. With respect to digital incidents the number and location of digital assets and documents should be determined.

During the documentation phase the condition of the physical crime scene should be documented using photographs, sketches and videos which is in line with the requirements from [MSH08, pp. 13 – 34] and [HRL11, pp. 9-12 – 9-17]. The goal of this step is the preservation of important details of the crime scene. The state and connections of digital assets should be documented as well, including the number and size of hard disk drives and the amount of installed memory. All serial numbers and asset tags should be documented as well.

The phase of the search for physical evidence consists of an in-depth search and collection of additional physical evidence. Here, particular search patterns might be applied. Furthermore, specific procedures for the collection of various types of evidence must be applied. This phase does also mark the beginning of the

digital crime scene investigation with the digital assets being collected as physical evidence. This particular phase also contains the analysis of the physical evidence by a forensic laboratory which is not further elaborated within the model. Within this thesis, this particular design decision of the model is considered as a major drawback of this model as all other steps are presented at a much higher detail. The analysis of the traces is reduced to a side note which is not even reflected in a separate phase which might be the result of a focus on digital evidence.

The reconstruction phase describes the organization of the analysis results from the collected physical and digital evidence including the documentation of the crime scene. The result of this phase are theories regarding the incident which are tested on the foundation of the evidence. Based on the physical and digital evidence a correlation is performed to link a person to digital evidence.

The presentation phase summarizes the presentation of the physical and digital evidence to a court or the management of the company.

Digital Crime Scene Investigation The investigation of the digital crime scene is performed partially in parallel to the investigation of the physical crime scene as shown in [CS03, p. 8]. The results of the digital evidence investigation are being fed back into the reconstruction phase of the physical crime scene. In particular the digital crime scene investigation consists of six phases [CS03], similar to the physical crime scene investigation:

Digital Crime
Scene
Investigation

- Preservation of the digital scene,
- Survey for digital evidence,
- Document evidence and scene,
- Search for digital evidence,
- Digital crime scene reconstruction,
- Presentation of digital scene theory.

The preservation phase for the digital crime scene contains the securing of all entry and exit points which primarily describes the network communication. Furthermore, volatile data which would be lost if the digital assets are shut down, are collected during this phase. The creation of forensic duplicates or images is also a part of this phase.

The survey phase is performed in the forensic laboratory on the foundation of the previously created forensic duplicates. The intention of this phase is the identification of obvious evidence such as malware.

The documentation phase describes the documentation of each identified piece of digital evidence including the location of the evidence and a cryptographic hash value to be able to prove the integrity of the data. Furthermore, chain-of-custody (see Section 2.1.2.1) forms should be created.

The search and collection phase describes the thorough analysis for additional digital evidence. In particular deleted files and unallocated space is scrutinized for potential evidence. In addition to that, a timeline of the file activity can be created and analyzed to trace the activities on a particular system.

The digital crime scene reconstruction phase contains the creation of a sequence of events based on the digital evidence. In addition to that, the level of trust into

the identified evidence is assessed.

Subsequently, the identified digital evidence is presented during the presentation phase.

2.1.1.2.5 Beebe and Clark

In [BC04] a two-tiered process model for digital investigations is introduced. The first tier consists of the following phases:

- Preparation
- Incident Response
- Data Collection
- Data Analysis
- Presentation of Findings
- Incident Closure

The second tier is represented by objective-based sub-phases for each first-tier phase. In [BC04] additionally other process models are compared and mapped to the proposed model of the authors. Overall the two-tiered approach seems to be very reasonable as the overall process is separated from trace or objective specific details. Thus, it is adopted for the model of digitized forensics in Section 3.1.

The preparation phase includes the risk assessment considering vulnerabilities, threats or loss/exposure; development of plans for information retention, incident response (including policies, procedures, personnel assignments, technical requirements definition), development of technical capabilities (procurement of response toolkits, etc.), training of personnel, preparation of host and network devices, development of evidence preservation and handling procedures, documentation of the results of the activities and development of legal activities coordination plan. All those tasks can be mapped to the basic goals of a prevention, detection and response to incidents followed by the investigation and prosecution. The overall goal is to achieve forensic readiness by addressing all potential issues that might arise prior, during or after an incident.

Preparation

During the incident response phase the detection and initial pre-investigation response to a suspected incident is performed. In [BC04] the detection of unauthorized activity, the reporting of this activity, the validation of the incident, an assessment of the potential impact of the incident, the development of strategies for the containment, eradication, recovery and investigation, any coordination tasks and the formulation of initial plans for the data collection and analysis are performed.

Incident
Response

The data collection phase describes the securing of digital evidence beyond the initially collected data from the incident response. Particular data sources are any measures from the live response, monitoring network data and data from network devices, volatile and non-volatile data from computer systems as well as the monitoring of such systems and data from removable media. In addition to that, methods for ensuring the integrity and authenticity of the digital evidence as well as the packaging, transport and storage of such evidence are utilized during this phase.

Data Collection

Data Analysis	The data analysis phase consists of the transformation or data reduction of the collected data, an initial survey regarding obvious pieces of digital evidence, the utilization of various data extraction techniques as well as the examination, analysis and event reconstruction based on the identified pieces of digital evidence.
Presentation of Findings	During the presentation of findings phase the relevant findings are communicated to various audiences. The particular form of the presentation depends on the target audience.
Incident Closure	With the final incident closure phase a critical review of the investigation process is performed to identify potential improvements. Particular findings from the presentation phase might result in further actions. The collected evidence should be disposed/destroyed or returned to the owner within the applicable legal framework. Subsequently, information related to the incident are collected and preserved.

2.1.1.2.6 Kiltz et al.

The model of Kiltz et al. [KHA+09] is data oriented. Thus, all necessary steps for the data acquisition from specific media are not covered. The model divides the forensic process in six phases whereas the first phase - strategic preparation - contains all measures in order to prepare an organization for the investigation of potential Information Technology (IT) security incidents. In addition to the phases, the model contains classes of methods that can be used within the scope of a forensic investigation. Moreover, the processed data is differentiated into eight different data types. However, it is worth mentioning that the data types are not mutually exclusive. In the following the model of Kiltz et al. is described in detail.

Phases of the Forensic Process The forensic process is divided into six phases in [KHA+09]:

1. Strategic Preparation,
2. Operational Preparation,
3. Data Gathering,
4. Data Investigation,
5. Data Analysis,
6. Documentation.

Those phases are integrated into the novel model for digitized forensics in Section 3.1.

Strategic Preparation The strategic preparation is performed prior to an incident in order to provide the necessary means for detecting the incident and to collect data allowing for investigating the incident in detail. In special circumstances, e.g. if no persistent data is stored within a system, the methods installed during the strategic preparation might provide the sole source of traces. Such methods include the activation of logging mechanisms, over the installation of additional software or hardware components such as intrusion detection systems. Moreover, the training of the personnel is performed during the strategic preparation. This is

equally important because the personnel need to be knowledgeable of the available tools and procedures for performing the forensic investigation. Subsequently, the creation and maintenance of a documentation of all digital assets constitutes a starting point for all further phases as soon as a symptom for an incident has been observed.

The operational preparation is another peculiarity of the model of [KHA+09]. This particular phase is performed in order to plan the course of a forensic investigation based on an observed symptom. With respect to the symptom it is important to estimate the relevance of particular forensic data sources. For example, whether data needs to be extracted from volatile memory or whether the communication behavior of a system needs to be recorded. This identification of digital assets is important to ensure that all necessary data sources are considered for the forensic investigation. Afterward, a coarse course of the data gathering, data investigation and data analysis is outlined. Such considerations are also important in digitized forensics in order to avoid the unnecessary destruction of traces.

Operational
Preparation

The data gathering is the foundation for the remainder of the forensic investigation. During this particular phase, forensic duplicates are recorded from the data sources. In the case of post-mortem IT forensics, the contents of the persistent storage media are cloned to create a forensic image. This image and the source media need to be hashed using cryptographic hash functions in order to verify that the imaging process resulted in identical data. Moreover, the hash value can be used at any point of the forensic investigation as a proof that the forensic image has not been altered. However, since the data investigation and data analysis are usually performed on the foundation of copies of the original forensic image, even a modification of the source data is not critical because it is possible to create a fresh copy. Any mistakes during the data gathering are usually hard to revert. Thus, similar to digitized forensics, it is of utmost importance to ensure that the forensic data sources are not altered unless this is absolutely necessary in order to be able to perform the forensic investigation.

Data Gathering

The data investigation describes all steps to identify potential traces which are relevant for the investigated incident. Due to the abundance of available data in modern computer systems, the minimization of data is the main goal of this step. All irrelevant data needs to be separated from the relevant data. In IT forensics this usually requires a lot of knowledge about the investigated system in order to be able to identify the anomalies which are potential indicators of compromise. In contrast to that, in digitized forensics a rather broad knowledge about forensic trace evidence is necessary in order to separate multiple traces at the same location and to forward such traces to the specific expert for a detailed analysis.

Data
Investigation

During the data analysis, the identified traces are scrutinized towards their relevance for the investigated incident and towards their plausibility. The latter is an important response to the possibility of anti-forensics in which traces might be deliberately placed, modified or deleted by an attacker. Thus, a deep knowledge about attack patterns and anti-forensics is necessary in order to perform the tasks during the data analysis. Overall, the result of this phase should be a reconstruction of the sequence of events that lead to the observed symptom.

Data Analysis

The phase of the documentation is two-fold in [KHA+09], it describes the creation of a target-audience-specific final investigation report and the detailed logging of the course of the investigation. The latter is referred to as the

Documentation

process accompanying documentation. This kind of documentation is important in order to reproduce the investigation results and to be able to identify any potential sources of error, loss and uncertainty in retrospect. Thus, both types of documentation are equally crucial for digitized forensics as well.

Classes of Methods Besides the structuring of the forensic process into distinct phases, the utilized methods are also structured in [KHA+09]. The basic idea of the classes of methods is a differentiation when a specific tool is available, how it could be applied for a forensic investigation and how it might impact the daily use of the specific IT system. In the IT domain it is quite important to be aware of specific data sources and whether those have to be explicitly activated during the strategic preparation. Thus, analyzing the classes of methods is reasonable in this domain. However, the relevance for crime scene forensics in the scope of digitized forensics is limited because specific methods are limited to the identification of potential traces and the subsequent digitization step.

Types of Forensic Data The types of forensic data are motivated by the ISO/OSI model (see e.g. [Cos98]) in [KHA+09]. The types of forensic data range from raw data, which are processed with rather generic tools, to user data, where a specific file format and encoding is usually known. The overall idea is the definition of multiple views on data sources which influence the specific tools for the investigation and particular requirements and precautions to be addressed. The eight data types in [KHA+09] are tailored for the needs of IT forensic investigations, thus, they cannot be directly used within the context of digitized forensics. Nevertheless, some differentiation of the characteristics of digitized and digital traces might be advantageous in the future.

2.1.2 Selected Standards for Evaluating and Handling Evidence

Besides the overall process of the preparation for forensic investigations, the identification and gathering of evidence, its analysis and the derivation of conclusions based on a reconstructed series of events, the actual handling of evidence is equally important in order to avoid any unintentional or intentional alterations of the traces. Furthermore, due to the often subjective nature of the interpretation of a specific piece of evidence, the comprehensible evaluation of the results and conclusions must be possible. In the following subsections the evidence handling based on the chain-of-custody [IR00, pp. 206 – 207] and the evaluation of evidence using likelihood ratios [LI17] are summarized.

2.1.2.1 Chain-of-Custody

The chain-of-custody describes the documentation of the whereabouts and handling of an item of evidence [IR00, pp. 206 – 207]. This documentation should cover the whole investigation process from the collection, testing, consumption or destruction of the evidence in chronological order. Any gaps in the chain-of-custody reduce the evidential value of the evidence and might lead to an exclusion of this evidence in court. A gap might also open the possibility for any malicious alteration of the evidence. The sample chain-of-custody provided by the U.S National Institute of Standards in Technology (NIST) [Sus+13, pp. 55 – 56] contains several information which need to be specified during the collection of the evidence:

- Property record number,
- Case number,
- Offense,
- Submitting officer (Name and ID),
- Victim,
- Suspect,
- Date/time of the seizure,
- Location of the seizure,
- Description of the evidence:
 - Item number,
 - Quantity,
 - Description of the item including model, serial number, condition, marks or scratches.

Based on this set of information the items are sufficiently described. In addition to this record about the evidence, the chain-of-custody needs to be tracked. For that, the item number, the date and time, the releasing officer (signature and ID number), the receiving officer (signature and ID number) as well as additional comments and the location are documented.

Subsequently, the final disposal of the evidence is recorded, either documenting the destruction of the evidence or the release to the lawful owner. For this process, the item numbers, date and the name and ID of the authorizing officer as well as the recipient need to be recorded as well.

As a result, a continuous log of the transfer of evidence, including the reason and locations, is created. A copy of the chain-of-custody record might be a part of the court transcript as well.

2.1.2.2 Likelihood Ratios

A Likelihood Ratio (LR) is a means to characterize uncertainty of decisions in forensics [LI17]. Unlike binary decisions in forensics (e.g. identification vs. exclusion), a quotient of the probability of two hypotheses is calculated as a result of a forensic comparison. In particular the Likelihood Ratio (LR) for a population f_1 corresponding to an observation x is defined as [LI17]:

$$LR_{f_1} = \frac{P(x|f_1)}{P(x|f_2)} \quad (2.1)$$

From a semantics point of view the LR_{f_1} describes how much more probable the observation x results from f_1 rather than from another population f_2 . Naturally, a LR of 1 describes absolute uncertainty, i.e. both populations have equal probabilities to correspond to the observation x . The same concept could be applied to a hypothesis-based notation [NPP33, p. 295].

As the decisions in forensics are often to be made on the foundation of a subjective analysis, the intrinsic uncertainty of such decisions can be expressed within the

Bayesian framework [LI17, pp. 24 – 25]. In this case the uncertainties regarding the truth of the two hypotheses H_1 and H_2 are taken into account with prior probabilities. In particular the initial posterior odds PO are determined using the same quotient as for the LR:

$$PO = \frac{P(H_1|x)}{P(H_2|x)} \quad (2.2)$$

Here, the probability of the hypothesis H_i being true based on the observation x is expressed by $P(H_i|x)$. In fact, PO is influenced by the prior odds towards the hypotheses [LI17, pp. 24 – 25]:

$$\text{Posterior Odds for } H_1 = \frac{P(H_1|x)}{P(H_2|x)} = \frac{P(x|H_1)}{P(x|H_2)} \times \frac{P(H_1)}{P(H_2)} = \frac{f_1(x)}{f_2(x)} \times \text{Prior Odds for } H_1 \quad (2.3)$$

Here, $P(x|H_i)$ describes the probability of x being observed if the hypothesis H_i is true, whereas $P(H_i)$ describes the prior odds that the hypothesis H_i is true. The weight of the evidence x within a specific distribution f_i is expressed by $f_i(x)$.

In forensic comparisons the two hypotheses usually reflect that a piece of evidence and a particular reference have the same origin or are of different origin. A major challenge in the oftentimes empirical field of forensic sciences is the determination of the prior odds, as there are no reference data for the whole population.

LRs are frequently used in the field of DNA analysis by considering the likelihood that two matching samples could originate from different people [FSC09, p. 41].

2.2 Selected Legal Background for Forensic Sciences

The legal background of this thesis is primarily based on the legal system of the United States of America on supreme court level because for this jurisdiction documented standards for the admission of evidence in court exist. Those standards, namely the Federal Rules of Evidence (FRoE) [FRE14] and the Daubert challenge [DG01, pp. xiii-xxi] differentiate between evidence based on generally accepted methods as well as rather novel scientific methods. In other jurisdictions, a judge is also required to assess the evidence before the admission in court, but usually no openly available criteria for the assessment of a particular method exist. Thus, the decision on the admission of evidence can be rather intransparent and - even worse - potentially subjective. From a scientific point of view particular criteria for the admission in combination with ideally measurable or at least quantifiable factors are preferable because a researcher without a legal background can at least determine particular tendencies towards the admissibility of evidence processed with a particular method.

Federal Rules of
Evidence

Within the scope of the federal rules of evidence in particular the seventh article on opinions and expert testimony [FRE14, pp. 15 – 16] is relevant for this thesis because particular traces are analyzed by forensic experts who are going to present the results within their testimony in court. Due to the nature of trace evidence, a special emphasis is placed on the rule 702 of the FRoE (see also [FSC09, pp. 90 – 95]) which specifically addresses the testimony of expert witnesses. This particular rule describes the qualification of the expert based on knowledge, skill, experience, training or education. In addition to that, the testimony should support the understanding of the evidence or to determine a particular fact in issue. The testimony should be based on sufficient facts or data and should be

the product of reliable principles and methods. Especially the latter requires an evaluation of particular methods in order to create standards for its application as well as potential error rates. The requirement of standards for the application of the method is additionally emphasized by the demanded reliable application of the principles and methods to the facts of the case.

Within a Daubert hearing the judge acts as a gatekeeper for the admission of scientific evidence by assessing several Daubert factors [DG01, p. 3] regarding a theory or methodology:

Daubert Factors

1. Whether it can be (and has been) tested,
2. Whether it has been subjected to peer review and publication,
3. Its known or potential rate of error,
4. The existence and maintenance of standards controlling the technique's operation,
5. Whether it is generally accepted in the scientific community.

In [DG01, p. 38] 12 additional factors have been identified which judges potentially consider during the reliability-assessment of a theory or methodology. In [Kra13, pp. 80 – 82] the Daubert standard is applied to the domain of statistical pattern recognition based forensic audio signal analysis from a scientific point of view. In particular a general-purpose forensic audio statistical pattern recognition approach is assessed based on the five Daubert factors and to some extent the rule 702 of the federal rules of evidence. The Daubert factors are primarily mapped to the testing of the methods including resulting error rates, the publication of the method in the scientific community and a compilation of standards or the cooperation without a standardization body. The assessment is performed for the audio steganalysis [Kra13, pp. 124 – 125] and [Kra13, pp. 161 – 162] for microphone forensics. In this context the potential lack of generalization is identified based on the experimental results of both use cases.

2.3 Contact-Less Sensory and Substrate Properties

A crucial component of digitized forensics is the sensory for the digitization of a physical trace. The selection of appropriate and suitable sensory depends on the properties of the suspected trace and the material the trace is present on. Such a substrate dependency is no peculiarity of digitized forensics, as in traditional trace processing oftentimes substrate-dependent processing techniques need to be utilized as well. An example for such a substrate-dependency are the processing techniques for latent fingerprints (see e.g. [HRL11, pp. 7-1 – 7-67]). In the following subsections particular contact-less sensory which is available for the evaluations within the scope of this thesis, selected substrate properties in the context of latent fingerprint processing and common preprocessing steps for the data originating from the available sensors are summarized.

2.3.1 Selected Contact-Less Sensory for Digitized Forensics

For the evaluation of exemplary methods within the scope of digitized forensics in this thesis three different sensors are available for the experiments. The selection

of the sensors merely represents the accessible sensory rather than the entirety of available sensors. A common objective for the sensors in digitized forensics is the contact-less and ideally non-destructive measurement principle. The measurement principles and properties of chromatic-confocal sensors, confocal laser scanning microscopes and reflection spectrometers are summarized in the following subsections.

2.3.1.1 Chromatic White Light Sensors

Chromatic White Light (CWL) sensors are chromatic-confocal sensors [FRT14a]. The sensor consists of a source of white light, a stack of lenses with a known chromatic aberration and a spectrometer as depicted in Figure 2.1. The light

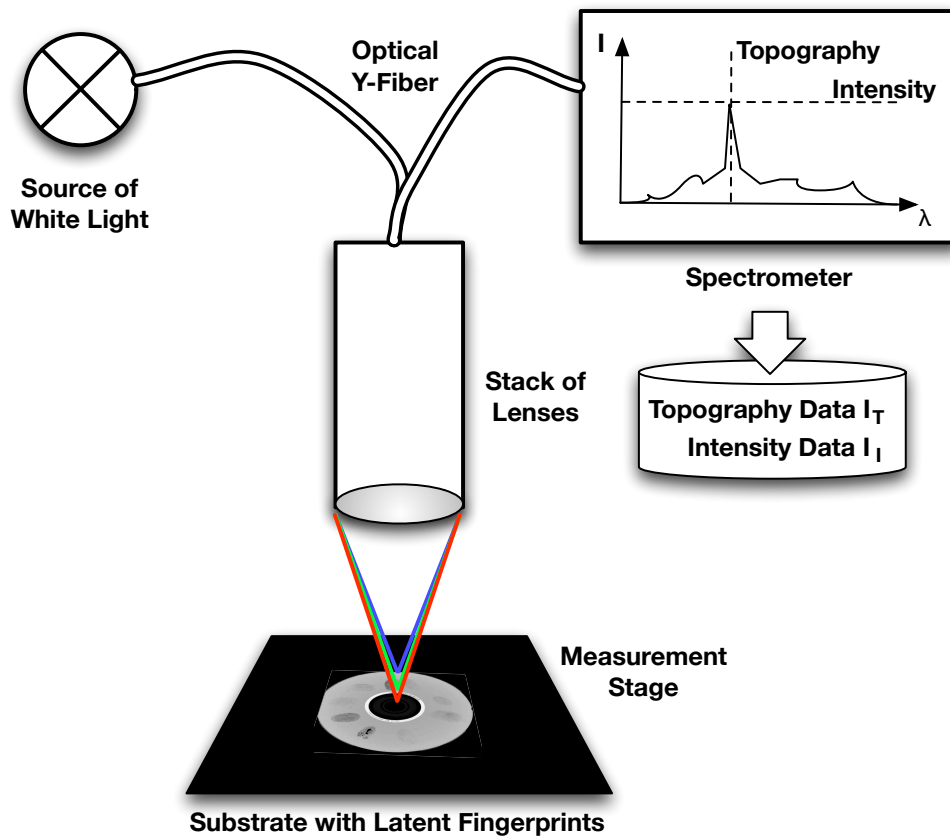


Figure 2.1: Measurement principle of a CWL sensor

from the light source is sent via the lenses to the substrate. During this emission of light, each wavelength has its own focal distance. As a result, only one specific wavelength can be in focus, depending on the distance between the lenses and the substrate material. The particular wavelength in focus is reflected with the highest intensity. The reflected spectrum of light is finally sent to the spectrometer. Based on the peak intensity, the wavelength of the focused light can be determined. This wavelength can be used to determine the distance between the lenses and the substrate based on the known chromatic aberration of the lenses. The maximum range of the sensor is determined by the degree of the chromatic aberration of the lenses, the light source and the spectrometer. However, with a source of white light, primarily the optical properties of the lenses determine the measurement range for the distance between the lenses and the substrate. The resolution of this

height measurement is determined by the resolution of the utilized spectrometer. The potential acquisition duration is influenced by the amount of reflected light. The integration time of the spectrometer needs to be configured based on the amount of captured light necessary for reliably determining the peak within the spectrum (see e.g. [Zha+17] for a dedicated analysis of the impact of integration times on measurements using near infrared grating spectrometers).

Due to the measurement principle the resulting topography (I_T) and intensity images (I_I) are perfectly aligned because the data of each pixel is extracted from the same measurement of the embedded spectrometer. The maximum dimensions of an object to be digitized with S_1 is determined by the properties of the measurement device, in this case the FRT MicroProf 200 [FRT12]. In particular an area of up to 200 by 200 mm can be digitized using this particular device. The achievable lateral and axial resolutions depend on the optical properties of the stack of lenses because the spectrometer is shared by different types of the CWL sensor as summarized in Table 2.1. The CWL600 sensor has a native

Sensor
Specifications

	CWL600	CWL1mm
Native Lateral Resolution [pixels/mm]	500	555.56
Native Lateral Resolution [ppi]	12700	14111
Axial Quantization Step (max) [nm]	6	10
Operating Distance [mm]	6.5	20
Maximum Measurement Frequency [Hz]	2000	2000

Table 2.1: Technical Specifications of the FRT CWL600 and CWL1mm Sensors [FRT14a]

lateral resolution of up to 500 pixels/mm (12700 ppi) and an axial resolution of quantization steps of up to 6 nm. The operating distance is 6.5 mm. The CWL1mm has a slightly higher lateral resolution of 555.56 pixels/mm (14111 ppi) but a lower axial resolution with quantization steps of up to 10 nm. The operating distance of the CWL1mm is 20 mm. The axial resolution for both sensors can be selected from two fixed settings whereas the lateral resolution is configurable freely. Exceeding the native resolution of a sensor is possible, however, in this case neighboring measurement spots overlap, potentially causing a blurred result.

2.3.2 Confocal Laser Scanning Microscopy

A Confocal Laser Scanning Microscope (CLSM) uses a laser as a light source (excitation source) [CFD13]. The laser beam is directed through a pinhole aperture that is situated in a confocal plane with a measurement point on the substrate and a second pinhole aperture in front of the detector. A dichromatic mirror is placed in the optical path between the laser and the detector as depicted in Figure 2.2. This mirror reflects the laser beam through the objective lens to the substrate whereas the reflected light is passing through the mirror towards the detector. The two pinhole apertures ensure that only in-focus (confocal) light rays can be detected by the detector. All reflected light rays that are not confocal are blocked by the pinhole aperture in front of the detector. Different focal planes are digitized by refocusing the objective lens within the Confocal Laser Scanning Microscope (CLSM). The laser beam is diverted within the CLSM in order to digitize multiple points of the substrate. The result of the measurement process

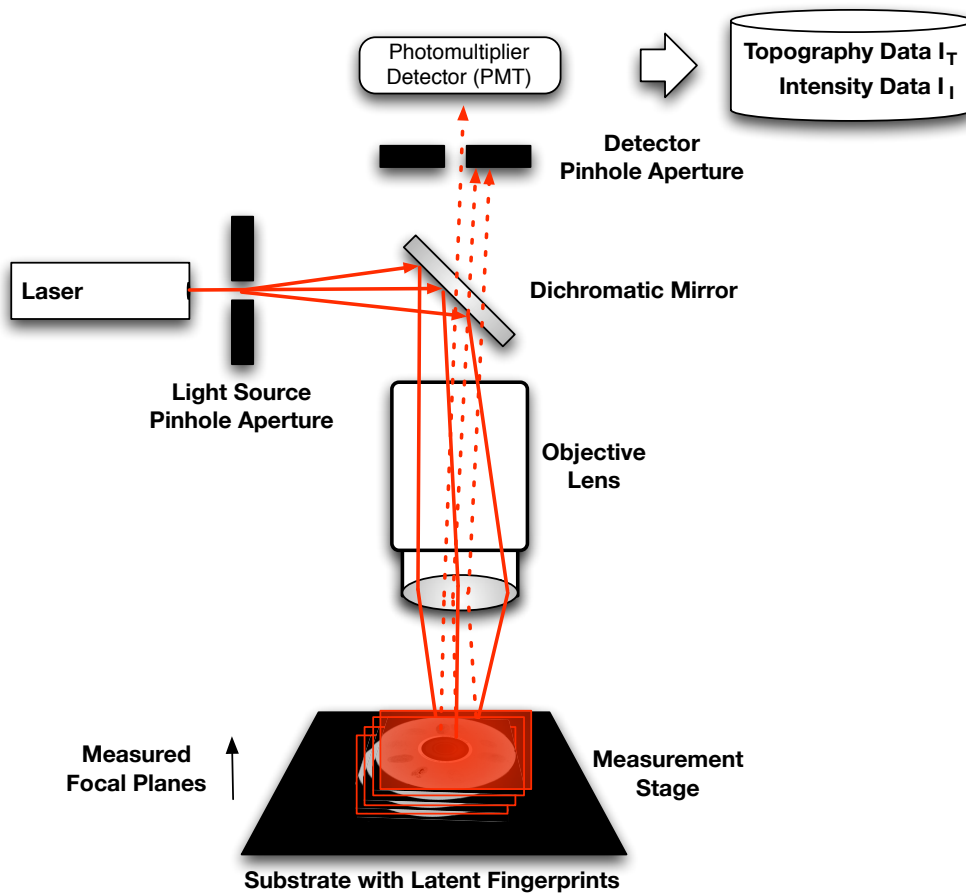


Figure 2.2: Measurement principle of a Laser Scanning Confocal Microscope based on [CFD13]

are two different images: the topography/height map I_T and the light intensity I_I captured by the detector module. In practice, a CLSM behaves like an area sensor due to the fast diversion of the laser beam and the automatic refocusing of the objective lens. However, the acquisition area is limited by the utilized objective lens. Furthermore, the lateral resolution is determined by the objective lens as well. On the other hand, the axial quantization is configurable in a CLSM by choosing different distances between two measured focal planes. This will also affect the measurement duration as an increased number of focal planes results in an increased measurement duration.

The Keyence VK-x110 CLSM [KEY20] is equipped with four different objective lenses resulting in four different settings for the digitized area as summarized in Table 2.2. Besides the topography image I_T and the intensity image I_I the Keyence VK-x110 is able to capture a conventional light microscopy image using a color camera resulting in a third image I_C . The standard image resolution can be doubled by using the microscope in a super resolution measurement mode. However, the utilized objective lens limits the ability for topography measurements with the confocal measurement principle based on the lens-specific depth of field. The larger the depth of field of a lens, the larger is the resulting height of the focal plane because all the focused light can pass the pinhole aperture in front of the detector.

A drawback of the confocal microscopy is the limited scan area for digitizing

Lens		10x	20x	50x	100x
Digitization Area [μm^2]		1350 x 1012	675 x 506	270 x 202	135 x 101
Image Resolution (Standard) [pixels^2]		1024 x 768			
Native Resolution [pixels/mm]	Lateral	758.52	1517.04	3792.59	7585.19
Native Resolution [ppi]	Lateral	19266.37	38532.74	96331.85	192663.70
Operating Distance [mm]		16.5	3.1	0.54	0.3
Depth of Field [μm]		7.31	3.11	1.03	0.73

Table 2.2: Technical Specifications of the Keyence VK-x110 CLSM [KEY20]

objects. This can be partially compensated by acquiring multiple scans and stitching them together to form a larger image. However, due to the involved image processing and the diversion of the laser beam within one scan, the stitched results likely contain artifacts.

2.3.3 UV-VIS Reflection Spectrometer

The FRT FTR sensor [FRT14b] is a UV-VIS reflection spectrometer setup. In particular two light sources - a halogen lamp and a deuterium lamp - cover the UV to the near infrared light spectrum. The broadband light spectrum is sent to the substrate via an optical fiber as depicted in Figure 2.3. The reflection of the light spectrum is then captured by the same y-fiber and sent to a spectrometer. The detection range of the spectrometer covers a spectrum from 163 nm to 844 nm capturing 2048 values for each measurement spot. Due to the lack of optics the native resolution of this setup is rather low, with a measurement spot of a diameter of 100 μm . Depending on the amount of reflected light, the integration time of the spectrometer needs to be configured similar to the CWL sensor in Section 2.3.1.1. However, in contrast to the CWL sensor the measurement stage of the FRT MicroProf 200 [FRT12] is stopped for the duration of the measurement. The resulting image data is an array of 2048 images representing the intensity value for a specific wavelength of light: $I_{0\dots2047}$. The native lateral resolution of each of those images is 10 pixels/mm or 254 ppi. However, overlapping measurement points can be selected to increase the resolution of the resulting images at the cost of potentially blurred image contents.

Sensor
Specifications

2.3.4 Selected Substrate Properties in the Context of Latent Fingerprint Forensics

In [HRL11, pp. 7-4 – 7-5] surface materials are separated into the two classes of porous and nonporous substrates.

A porous substrate has an open surface structure which can absorb substances such as fingerprint residue. From a forensic perspective this absorption process increases the durability or persistence of the trace. On the other hand, specific chemical reagents are necessary to reveal the absorbed fingerprint pattern [HRL11, pp. 7-14 – 7-23]. Examples for porous substrates are paper, cardboard or wood.

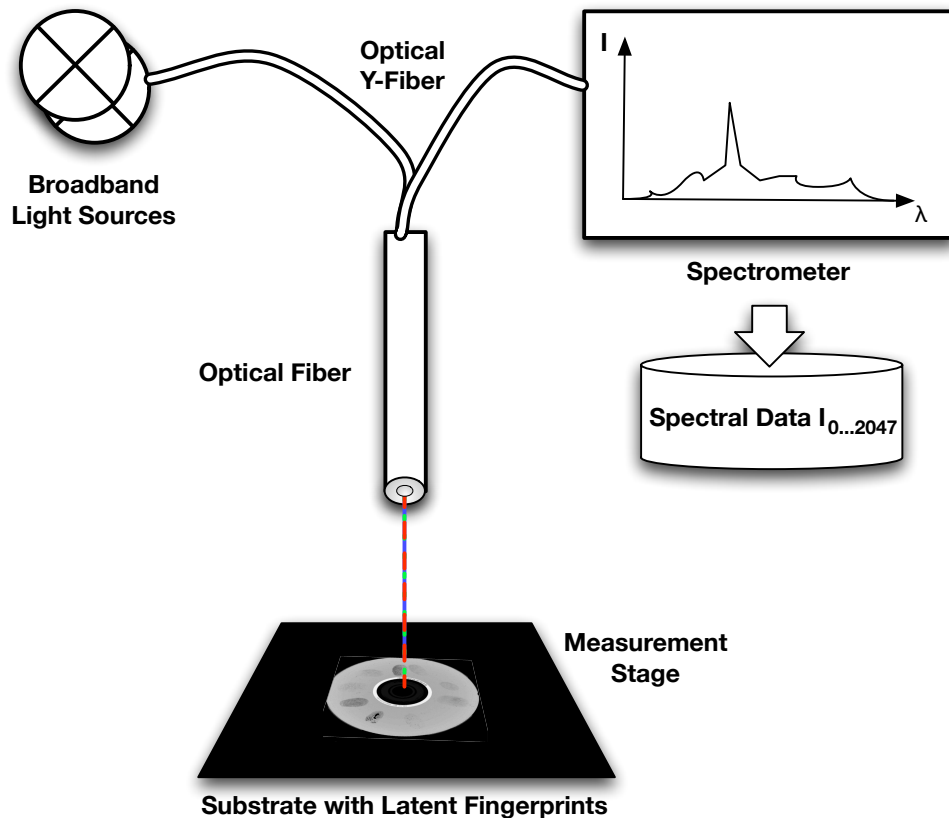


Figure 2.3: Measurement principle of the FTR sensor

Nonporous substrates do not absorb the fingerprint residue. As a result of that, the fingerprint pattern formed by the sweat residue from the skin can be damaged more easily because it is solely deposited on top of the substrate. The simple method of the dusting with powders can render the invisible pattern visible by depositing additional dyes on the areas with sweat residue. In addition to that, specific chemical processes can be used to deposit materials for rendering the fingerprint pattern visible. Examples for nonporous substrates are glass, metal, plastics, lacquered or painted wood and rubber [HRL11, p. 7-4].

Besides those two classes of substrates an intermediate class of semi-porous substrates is defined in [HRL11, p. 7-4]. This particular class of substrate materials is characterized by a partial absorption of the sweat residue. As a result either the treatment methods for porous and nonporous substrates might be used to render the fingerprint pattern visible. Examples for such substrates include but are not limited to glossy cardboard and magazine covers.

Texture vs.
Structure

Another influence factor is summarized in [HRL11, p. 7-4] as the surface texture. Such a macroscopic texture of the surface can be described using various roughness measures [Bhu01, pp. 52 – 77]. However, within the scope of this thesis this texture is referred to as surface structure as a substrate might have any kind of visual pattern which does not reflect its presence in the roughness measures. In a computer scientist's point of view this visual pattern is considered as a texture.

2.3.5 Common Preprocessing Techniques for Sensor Data

Within a pattern recognition pipeline, e.g. in the context of biometrics [Vie06, pp. 19–21], the digital data output of a sensor is usually preprocessed prior

to any extraction of features. The intention of such preprocessing is usually the removal of artifacts which would otherwise have negative impacts on the feature extraction or the emphasis of specific desired properties within the data, e.g. specific patterns. The following subsections summarize a selection of such preprocessing techniques which are utilized within the application scenarios in Chapter 5 and Chapter 6 within this thesis.

2.3.5.1 Least-Squares-Method for Tilt-Correction

With sensory operating on the nanometer-scale even a slightly tilted placement of an object could cause a gradient within the resulting scan data. While such an effect is often negligible for intensity data, any topography measurements are significantly influenced regarding the observed value ranges within the scan data. With respect to the utilized sensory within this thesis, as summarized in Section 2.3.1, the degree of the tilting is usually quite small because any large deviation from a perpendicular measurement would result in invalid, i.e. non-existent, values. Thus, the tilting would likely result in a gradient but not in any considerable degree of distortion of the scan data in comparison to the physical object. As a result, it is usually sufficient to compensate the gradient within the scan data rather than performing any affine or projective image transformation (see [Sze11, pp. 143 – 152]) compensating the distortion. This is in general desirable as the sole compensation of the gradient does not result in an interpolation regarding the pixels of the scan data and their particular semantic location on the substrate.

Within the scope of this thesis the least-squares method [Sze11, pp. 275 – 276] is used to compensate the gradient resulting from a tilted digitization of the object. The least squares method uses a linear regression to minimize the sum of squared errors between each point x of an image and the corresponding point x' of a plane. Afterward, the plane is subtracted from the image data resulting in a removal of particular gradients and shifted values within the scan data.

2.3.5.2 Unsharp Masking

High frequencies within the scan data can be emphasized using unsharp masking [Sze11, pp. 103 – 104]. The unsharp masking is performed by subtracting a blurred version of the scan data from the original scan data. The blurring of the scan data reduces high frequencies within the blurred image. By subtracting this blurred image from the original scan data, the lower frequencies are suppressed emphasizing the higher frequencies.

Such a preprocessing is advantageous if the substrate contains a low frequency pattern. Furthermore, particular sensors might intrinsically result in low-frequency patterns within the scan data. Such an example is the confocal laser scanning microscope described in Section 2.3.2. Due to the non-perpendicular measurement throughout the scan area a barrel effect is caused within the resulting scan data. This particular effect can be compensated using the unsharp masking. Thus, this particular method is used as a preprocessing for the application scenario in Chapter 6.

2.3.5.3 Sobel Operators

Sobel operators [Sze11, p. 104], [Shi10, p. 57] are 3×3 linear filters which can be used as simple edge detectors. The Sobel operator represents horizontal and vertical derivatives centered on the pixel. The edge detection or rather emphasis

of edges is the result of larger differences between neighboring pixels resulting in larger gradients. This particular filter is used as a preprocessing in the application scenario in [Chapter 5](#) to emphasize the pattern of the fingerprints within the digitized data.

2.3.5.4 Gabor Filtering

Gabor filtering can be used for an oriented and band-pass filtering [[Sze11](#), p. 121], i.e. to emphasize particular frequencies with specific orientations within the image. The Gabor function utilizes the product of a cosine of the frequency with a Gaussian with a specific standard deviation. The result is a local wave pattern which can be used as a filter for image data. With respect to fingerprint patterns in [Chapter 5](#) a set of such filters could be used to emphasize the pattern within local areas of the scan data. However, the frequency and the standard deviation need to match the properties of the fingerprint.

2.4 Selected Aspects of Pattern Recognition

Pattern recognition in general is described in [[DHS00](#), p. 1] as the act of the processing of raw data and deciding on an action based on the category of the pattern. This process is independent of computer systems and is performed in the everyday life over and over again. One example is the selection of the proper key for a lock from a key chain - based on the pattern of the door including its location, the correct key, i.e. the category, is selected based on the shape, appearance and location. In forensics similar tasks are performed by comparing patterns from fragments of objects or patterns resulting from a specific tool. Here, in contrast to the daily utilization of pattern recognition, particular feature points are assessed. Nevertheless, the task boils down to a question of perception.

Pattern
recognition
pipeline

Such a perception task can be projected to computer systems in order to automate the decision-making (see e.g. [[DHS00](#), pp. 1 – 19]). For that, a basic pattern recognition pipeline can be utilized. It consists of the steps of the

- Sensing/acquisition of a sample,
- Its preprocessing,
- Segmentation,
- Feature extraction and
- Subsequent classification.

The preprocessing is intended to simplify all following tasks without losing any relevant information. Within the segmentation step, the preprocessed image is divided into regions of interest and the background in order to prepare the feature extraction. During the feature extraction, particular properties of the regions of interest are measured, resulting in features characterizing the relevant information of the pattern. Within the classification phase, the particular feature space is used to assign a category to the data.

The nature of this classification process depends on learning and adaptation of the selected approach. In a case of supervised learning, a model has to be created based on training data. In such a case, labeled data is used to train a

model. However, there are some limitations of such an approach. First of all, the labeling data or ground truth must be available or obtainable. Secondly, a representative set of training data is necessary for the model generation. Any bias or errors in the training data and its labeling would eventually result in biased or erroneous decisions, as during the training the distance between the model and the labels of the training data is usually minimized. Another potential issue is the risk of over-fitting. In such a case, the decision boundary is closely fitted to the training data which might lead to very complex models. In addition to that, any non-representative distribution of the training data would result in an inappropriate decision boundary leading to errors during the utilization of the model for classification tasks with novel patterns that are contained in the training data. Each novel pattern might contain small variations in comparison to the training samples. Thus, an appropriate determination of the decision boundary during the training phase has a significant influence on the performance of the pattern recognition system. The issue of generalization is an important property of the trained model. In [DHS00, pp. 1 – 19] it is postulated that a complex decision boundary would likely hinder a good generalization of the model.

In unsupervised learning, the classification algorithm forms clusters or natural groupings of the input patterns [DHS00, pp. 1 – 19]. A typical input for such learning approaches is the hypothesized target number of clusters.

In a reinforcement learning approach, an input is presented to a classifier which determines a category for that particular input. Afterward, this result is assessed and the classifier is being told whether the assigned category is correct or incorrect. With such an approach, the performance of the classifier will gradually improve with the number of presented samples.

In the following subsections at first error rates and performance measures are summarized within the context of pattern recognition. Afterward, the algorithms for statistical pattern recognition, which are utilized within the two application scenarios within this thesis, are briefly summarized. Subsequently, Benford's law [Ben38] as an observable phenomenon in natural data is described.

2.4.1 Selected Error Rates and Performance Measures in Pattern Recognition

For the evaluation of classification models, particular performance measures are an important aspect. Such performance measures can be used to compare different approaches with each other. In two-class problems (considering one class as positive and one class as negative), such as the two application scenarios in this thesis, two types of errors can be specified based on the Neyman-Pearson decision rule (see [Web02, pp. 14 – 15]):

- Type I errors: False Negative (Fn),
- Type II errors: False Positive (Fp).

A type I error/false negative is a sample being erroneously classified as negative instead of positive. Similarly, a type II error/false positive describes a sample being erroneously classified as positive instead of negative. In this context True Positive (Tp) are all correctly classified positive samples whereas True Negative (Tn) are all correctly classified negative samples. Based on the two types of

errors the False Negative Rate (FNR) and False Positive Rate (FPR) could be determined as potential performance measures based on [Web02, pp. 14 – 15]:

$$\begin{aligned} FNR &= \frac{Fn}{Fn+Tp} \\ FPR &= \frac{Fp}{Fp+Tn} \end{aligned} \tag{2.4}$$

In particular, the FNR is determined by the proportion of positive samples being incorrectly classified as negative. The FPR is the proportion of negative samples being classified as positive. Depending on the naming conventions for the two classes the FPR can be seen as a false alarm rate in the context of an anomaly or attack detection, whereas the FNR would map to a false miss rate in such a context.

The accuracy is another performance measure. From a semantics point of view the Accuracy (ACC) represents the relative amount of correctly classified samples. Based on the notation in this section it can be determined as follows:

$$ACC = \frac{Tp + Tn}{Tp + Tn + Fp + Fn} \tag{2.5}$$

Similarly, the so called Half-Total Error Rate (HTER) provides the inverse information by representing the relative amount of incorrectly classified samples:

$$HTER = 1 - ACC = \frac{FNR + FPR}{2} = \frac{Fn + Fp}{Tp + Tn + Fp + Fn} \tag{2.6}$$

However, a limitation of those performance measures is the potential bias introduced by unequal numbers of samples within the classes of positives and negatives. For example in a scenario with ten samples for each of the two classes and one misclassification per class, the FNR, FPR and HTER would be 10% whereas the ACC would be 90% - in an extremely imbalanced scenario with only one sample in the class positive and 19 in the class negative the same single classification error for each class would result in the same ACC of 90%, the same HTER of 10% but a FNR of 100% and a FPR of $\frac{1}{19}\%$ (5.26%). In such an extreme scenario the error rates can be very misleading. For that reason all experiments in the two application scenarios in Chapter 5 and Chapter 6 are equally balanced for the evaluation of the classification performance.

However, the raw classifier evaluation results in Section A.3.1 and Section A.4 contain additional performance measures automatically determined by the WEKA data mining software [Hal+09].

2.4.2 Selected Classification Performance Evaluation Approaches

In order to determine the error rates from Section 2.4.1 as performance indicators, the trained models from supervised learning need to be systematically evaluated. The availability of labeled data for training and testing is a requirement for this step. The labeling data is the ground truth for the evaluation. If sufficient data is available, the labeled data could be separated into independent training and test data sets. Within the scope of the WEKA data mining software [Hal+09] this can either be done by using a so-called percentage split or by providing a separate file with the test data. In the case of the percentage split, the sequence of the samples, called instances, is randomized. Afterward, the training and test

data sets are created based on the selected percentage split. The particular class distributions are retained during this step - i.e. any bias in the data is projected to the resulting training and test data sets. If separate training and test sets are supplied in the first place, any differences in the bias of each data set might lead to a skewed evaluation result.

The second evaluation option is the cross validation or leave-one-out-method [Mur12, p. 24]. In such an approach, the available data is separated into n equally sized partitions of the original data. Similar to the percentage split, the class distributions within each partition resemble the class distribution within the whole data set. In case of the leave-one-out-method only one feature vector is removed from the training sets. Afterward, particular classifiers are trained using $n - 1$ partitions of the data and evaluated with the remaining partition. This process is repeated n times. Thus, every single instance of the original data set is evaluated using a trained classifier model.

2.4.3 Supervised Learning Approaches Utilized Within This Thesis

All evaluations of supervised learning approaches within this thesis are performed on the foundation of the WEKA data mining software [Hal+09] in the version 3.6.6. In particular, for the two application scenarios in Chapter 5 and Chapter 6 the classifiers SMO [Pla99], J48 (Java implementation of a C4.5 decision tree [DHS00, p. 411]), Bagging [Bre96], Multilayer Perceptron [Bau88], Logistic Model Tree [LHF05], Dagging [TW97] and RotationForest [RKA06] are utilized. The following subsections summarize how those classifiers create the model during training.

2.4.3.1 SMO Classifier

The Sequential Minimal Optimization [Pla99] (SMO) classifier is a special approach to train a Support Vector Machine [Web02, pp. 134 – 141] (SVM). A SVM maps pattern vectors to a high-dimensional feature space constructing a hyperplane defining the decision boundary [Web02, p. 134] by maximizing the distances between the nearest points of opposite classes and the hyperplane within the feature space. Thus, in the original sense, support vector based classifiers are intended to address binary classification problems. The intention of SMO in [Pla99] is an increased training speed for large classification problems by optimizing the quadratical programming problem in the inner loop of the SVM learning algorithm. Instead of using numerical optimization steps, the SMO approach decomposes the quadratical programming problem into sub-problems which can be solved analytically. The implementation of the SMO classifier in the WEKA data mining software [Hal+09] is also capable to deal with missing values and nominal attributes. Furthermore, a normalization of the features (attributes) is performed by default.

2.4.3.2 J48/C4.5 Decision Trees

The C4.5 algorithm (see e.g. [DHS00, p. 411]) and its Java implementation J48 in the WEKA data mining software [Hal+09] is an example of training a decision tree. The path in the decision tree from the root to a particular leaf is basically a sequence of questions or tests, whereas the leaf contains the assigned class. This property of the classifier is a major advantage as its decision-making process is

easy to explain. During the training, the training set is split into subsets whereas the splitting criterion of a node should increase the normalized information gain based on one feature within the feature space. This step is recursively repeated. In order to minimize the size of the resulting tree, the tree can be pruned by deleting redundancies within the path to a leaf using the technique called C4.5Rules [DHS00, p. 411].

2.4.3.3 Bagging Ensemble Classifier

The bootstrap aggregating ensemble classifier [Bre96] (Bagging) generates multiple versions of classifiers or predictors during the training in order to create an aggregated predictor. The training of the Bagging predictor is performed on a sequence of equally sized training sets as subsets of the supplied training data [Bre96]. Based on each subset an independent model is trained using the utilized learning algorithm. In case of the nominal classes in the two application scenarios in Chapter 5 and Chapter 6, the Bagging classifier achieves this aggregation by the simple means of a majority vote. In particular in the default setting of the WEKA data mining software [Hal+09], a set of reduced-error pruning decision trees are trained during the training of the Bagging classifier.

2.4.3.4 Multilayer Perceptrons

A Multilayer Perceptron [Bau88] (MLP) is an artificial neural network consisting of an input layer with n neurons, where n equals the dimensionality of the feature vectors in the training set, followed by one or multiple layers of intermediate neurons and subsequently a layer of e outputs, where e equals the number of class labels. The neural network is trained by adjusting the connection weights of each neuron based on the ground truth of the training sample and the observed error at the output layer (back propagation in [Bau88]).

2.4.3.5 Logistic Model Trees

A Logistic Model Tree [LHF05] (LMT) is a combination of the concepts of logistic regression models and decision trees. The difference between a model tree and an ordinary decision tree is that the leaves contain regression functions instead of the assigned class label, in the case of the logistic model tree the leaves contain logistic regression functions. The particular attribute tests within the inner nodes are retained in comparison to decision trees. The logistic regression functions in the leaves model the class membership probabilities based on the feature space.

2.4.3.6 Dagging Ensemble Classifier

For the training of a Dagging [TW97] (DAG) classifier, the training data is partitioned into subsets of the original training data as well. However, in contrast to the training of the Bagging classifiers, the subsets are disjoint subsets of the training set. In its default configuration in the WEKA data mining software [Hal+09] each subset is used to train a Decision Stump classifier [IL92] which is a decision tree with only one level. For the classification using the Dagging classifier a majority vote of the results from each Decision Stump is performed in order to assign the final class label.

2.4.3.7 RotationForest Ensemble Classifier

For the training of the RotationForest [RKA06] (RF) ensemble classifier the feature set is split into a pre-defined number of subsets. In general, the subsets can be either disjoint or intersecting, but disjoint subsets are selected in [RKA06]. Each subset of features is used in conjunction with a subset of classes to perform a principal component analysis [DHS00, p. 568] (PCA) on the defined subspace. The intention for this step in [RKA06] is the avoidance of identical coefficients from the PCA. The resulting vectors with coefficients are organized in a sparse matrix which is used to construct the training set of a classifier. In the utilized default setting of the WEKA data mining software [Hal+09] in Chapter 6 the J48/C4.5 decision tree is used as the classifier. For the classification using RF, the confidence for each class is determined by an averaging method for the trained trees. The largest confidence is then considered as the class of the processed feature vector.

2.4.4 Benford's Law

Benford's law [Ben38] describes an observation regarding the most significant digits within natural data. In particular Benford observed that the probability of occurrence p for a specific most significant digit d with $d \in [1, 2, \dots, 9]$ can be determined using the following equation:

$$p(d) = \log_{10}\left(1 + \frac{1}{d}\right), \quad d \in [1, 2, \dots, 9] \quad (2.7)$$

This phenomenon can be exploited in forensics as any deviation from those probabilities might be an indicator for tampering with the data. However, in order to establish sufficient scientific ground for such a claim, the natural distribution of most significant digits need to be determined for this particular use case.

2.5 A Brief History of Fingerprints in Forensics

The history of the usage of fingerprints in general and in forensics in particular is summarized, amongst others, in [HDV17]. The scientific foundations for the fingerprint matching date back to the 18th century. However, the uniqueness of fingerprint patterns is established empirically since no two identical fingerprint patterns have been observed on two different persons to date [Mal+09, p. 35]. Even identical twins have different fingerprint patterns which originate from ridge formation process of the fetus [Ash99]. This section provides a brief overview of the aspects of fingerprints relevant for this thesis.

2.5.1 Features of Fingerprints

A fingerprint pattern is usually broken down to three different feature levels [Cha+04, p. 30 – 32]:

- Level-1: Macro Detail - overall pattern,
- Level-2: Points - major ridge path deviations (minutiae points),
- Level-3: Shape - intrinsic ridge formations (ridge shape, pores).

The level-1 pattern is formed by the overall ridge flow of each fingerprint. In general five different types of level-1 patterns are used: simple arch (also known as plain arch), tented arch, right loop, left loop, whorl. The level-1 pattern is usually clearly visible. In some cases, additionally core/loop and delta points are determined for the level-1 pattern [Mal+09, pp. 38 – 41]. In this case, the number of core and delta points can be used to determine the type of the pattern - left loops, right loops, and tented arches have one core and one delta point, whorls have two core and two delta points, arches have no core or delta points. From the perspective of the forensic identification or verification of identities, a matching level-1 pattern is a requirement for complete fingerprints but it is not sufficient for establishing the claim that both patterns originate from the same person.

In biometrics and forensics usually level-2 features - minutiae points - are used for determining whether two fingerprint patterns originate from the finger. Usually two or three basic minutiae types are used:

Minutiae Types

1. Ridge ending (ending of a particular ridge path),
2. Bifurcation (split of the ridge path),
3. Dot (short isolated ridge path).

Other, more complex minutiae types can be formed by the combination of those three basic minutiae types. Such complex minutiae points are an important factor in the non-numerical fingerprint matching standard in forensics (see e.g. [CC09, pp. 71 – 74]). In this particular standard, the rarity of specific minutiae points is taken into account for the matching. In contrast to that, the numerical standard just defines a threshold for the minimum number of matching minutiae points.

The third level of features requires a much higher acquisition resolution [JCD07]. In particular at least an acquisition resolution of 1000 ppi is necessary for a reliable detection of such features. In addition to the pores of the sweat glands which are analyzed within a poroscopy [Ash99], the edges of ridges can also be analyzed in forensics.

Within the scope of this thesis, the evaluation in Section 5.3.3 solely relies on the level-2 minutiae points.

2.5.2 Errors in the Analysis of Latent Fingerprints

In [Ule+12] a False Positive (Fp) is an erroneous individualization of two non-matching fingerprints. A prominent example for this is the Brandon Mayfield case [Off06]. An exclusion of two matching fingerprints is considered as a False Negative (Fn).

The reproducibility (inter-examiner agreement) and repeatability (intra-examiner agreement) is analyzed in [Ule+12] for the matching of latent fingerprints within test conditions compliant to the ACE-V model. The performed experiments are carried out using 72 latent fingerprint examiners and a total of 744 image pairs. Each examiner was asked to perform the comparison for 25 of those matching pairs twice with a temporal distance of approximately seven months. Each experiment in [Ule+12] is two-fold - at first the value of the latent fingerprint is determined, afterward, the actual comparison is performed.

Repeatability

The average repeatability (intra-examiner) of the initial decision regarding the value of a fingerprint is reported at 89.7% for a two-class problem (of value/no value for identification) and 84.6% for a three-class problem (of value for

identification, of value for exclusion, no value). Even complete reversals are reported in 1% of the tests. Even with shorter intervals of a median of 7 days between two tests of the same sample, the average repeatability is as low as 92.2% for the two-class problem and 88.8% for the three-class problem. The reproducibility (inter-examiner) of the evaluation of the value of the latent fingerprints is reported to be unanimous for 42% of the cases. However, for this particular experiment the more challenging examples are selected in [Ule+12]. Besides the initial assessment of the value of the latent fingerprint, the actual matching is evaluated in the second part of the experiments in [Ule+12]. Here, in 1.8% of the cases an individualization decision is reported for latent fingerprints that are previously classified as value for exclusion only. For the repeated tests a false negative rate of 8.8% is reported. However, only 30.1% of the errors are repeated. In [Ule+12] it is estimated that another latent fingerprint examiner would reproduce the same error in 19% of the cases. For the individualization of easy to medium challenging comparisons a repeatability rate of 92% and a reproducibility of 85% is reported. For at least difficult comparisons the repeatability drops to 69% whereas the reproducibility drops to 55%. The results for the exclusion are quite similar with a repeatability rate of 88% and a reproducibility of 77% for easy to medium comparisons. For difficult comparisons the repeatability rate is reported at 70% and the reproducibility at 50%. Those results show that the ACE-V method with a separate examiner performing the same comparison for verification purposes is absolutely crucial to reduce the expected error rates.

Reproducibility

The experiments show that the decision-making is a subjective process. This is also backed by [Dro+11] reporting that there are inconsistencies regarding the number of recognized feature points between different latent fingerprint examiners (reproducibility) as well as for the same examiner at different analysis attempts (repeatability). For that reason a biometric system is selected for the evaluation in Section 5.3.3.2.

Subjectiveness

2.5.3 Selected Biometric Preprocessing and Matching Approaches in Latent Fingerprint Forensics

Biometric Systems are pattern recognition systems as well. The biometric pipeline e.g. in [Vie06, pp. 19–21] consists of the four phases acquisition, preprocessing, feature extraction and classification as a specialized form of the pattern recognition pipeline summarized in Section 2.4. Such systems also require training (enrollment in [Vie06, pp. 19–21]). After this training, the biometric system can be either used for the purpose of the verification of identities or the identification (see e.g. [Vie06, pp. 19–21]). In a verification approach, the identity and the biometric trait are presented to the biometric system which then determines whether the identity claim is justified based on the comparison of the presented data with the template from the enrollment stage. In an identification case, only the biometric data is presented which is then compared to all templates in order to determine the identity of the person. With respect to latent fingerprints in forensic investigations both operating modes are utilized. The identification is performed by an Automated Fingerprint Identification System (AFIS) [HRL11, pp. 6-1 – 6-33] which is supposed to compile a ranked list of potential candidates for a manual comparison by forensic experts. This manual comparison basically represents the verification mode.

Since the application scenario in Chapter 5 primary deals with the preprocessing

of latent fingerprints for further analysis in forensics, the focus of this section is primarily the biometric preprocessing of latent fingerprints instead of the biometric preprocessing of fingerprint patterns in general. Within AFIS such a preprocessing is manually applied to the digitized latent fingerprints [HRL11, p. 6-24] – potential processing steps from the domain of image processing are the histogram equalization, image intensity rescaling, image intensity adjustments (definition of high and low thresholds), local or global contrast enhancement, local or global background subtraction, sharpness adjustments (application of a high-pass filter suppressing lower frequencies within the image), background suppression (low-pass filter suppressing high frequencies within the image), gamma adjustments as well as brightness and contrast adjustments. In addition to that, Gabor filters (see [Sze11, p. 121]) as a form of oriented band-pass filters are used to emphasize the fingerprint ridge lines in a local context.

Feature
Extraction

After such preprocessing steps, the feature extraction can be prepared and performed. Primarily the level-2 features described in Section 2.5.1 are extracted within the scope of AFIS [HRL11, p. 6-24 – 6-27]. The automatic feature extraction is usually performed on the foundation of a binary image with black pixels representing fingerprint ridges and white pixels representing the valleys of the pattern. This binary image is then processed by a thinning algorithm which reduces the ridge width to only one pixel. Based on the resulting thinned image, each pixel is analyzed towards the number of pixels in its direct neighborhood for determining minutiae points within the image:

1. Two black pixels in the neighborhood of a black pixel: Pixel is part of a ridge line,
2. One black pixel in the neighborhood of a black pixel: Pixel is a ridge ending,
3. Three black pixels in the neighborhood of a black pixel: Pixel is a bifurcation,

Additionally, the orientation of the minutiae points can be determined based on the ridge flow.

Matching
approaches

The automated matching of latent fingerprints is a challenging task as the fingerprint pattern can be distorted based on factors such as pressure or surface properties. Thus, the performance of automated approaches is usually less accurate than the manual comparison by forensic experts [HRL11, p. 6-27]. The vast majority of current matching approaches relies on the set of minutiae points. The matching approach described in [HRL11, pp. 6-27 – 6-28] relies on the comparison of the minutiae sets within aligned fingerprint images. In particular, the matching algorithm tries to find corresponding minutiae points based on their location, type and orientation. Based on the number of matching minutiae points and particular variations between the two patterns a confidence level - the so-called matching score is determined. Such matching scores are the typical output of a biometric system to express the similarity between a sample and the corresponding template. The final classification result can be determined by applying a threshold to the matching score of the biometric system. This particular threshold describes the operating condition of the biometric system influencing the achieved error rates. More advanced approaches towards the automated matching of latent fingerprints such as [Kri+19], take rarer minutiae types into account. In particular partial latent fingerprints are aligned with the

matching tenprints based on the location of the rare minutiae points. Based on the minutiae points of the latent fingerprint and the matching subset of minutiae points from the tenprint the least square fitting error is determined in order to modify the matching score of the standard minutiae-based matcher. The evaluation results yield a significantly improved identification rate for three different evaluated minutiae-based matchers.

With respect to biometric systems, the error rates differ from those in pattern recognition summarized in Section 2.4.1. The matching of biometric samples can either result in a false match or a false non-match [Mal+09, pp. 14 – 22]. If the classification problem is a verification of an identity using biometrics, the two errors are comparable to the false positive/type I error and false negative/type II error in a two-class classification problem. The False Match Rate (FMR) and False Non-Match Rate (FNMR) in this case are also known as the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). In an identification scenario the error rates are semantically different because the comparison is performed in a one-to-many fashion. In this case the false match rate describes the rate of the acceptance of an impostor by the biometric system. An impostor is a person that is not enrolled by the biometric system. Thus, any impostor should be rejected during the matching. The false non-match rate is the rate of the rejection of persons which are enrolled to the biometric system. Oftentimes, the Equal Error Rate (EER), the particular error rate where FMR and FNMR are identical, are used as a performance indicator for biometric systems.

In order to process fingerprint patterns with AFIS at first the patterns need to be digitized (acquisition phase of the biometric pipeline). The patterns to be digitized originate either directly from a finger, the so-called Exemplar Print/Tenprint (EP) for all ten fingers of a person, or from a crime scene in case of the latent fingerprints or in short Latent Print (LP) [HRL11, pp. 6-9 – 6-10]. Within the operation of AFIS all potential matching tasks between EP and LP are possible [HRL11, p. 6-10]:

1. EP-EP: Query using a set of known tenprints against the existing tenprint database,
2. LP-EP: Query using a latent print against the tenprint database,
3. LP-LP: Query using a latent print against the latent prints from other crime scenes,
4. EP-LP: Query using a set of known tenprints against the latent prints from crime scenes.

The EP-EP comparison is primarily performed to identify previously created records within the database. The LP-EP matching is used to identify potential candidates matching a latent fingerprint found at a crime scene. With the LP-LP matching potential cases related to the investigated crime scene should be identified. The EP-LP matching is performed to identify previously committed crimes of a person which is newly enrolled to AFIS using tenprints.

The result of an AFIS query is usually a ranked list of candidates based on the highest achieved matching scores. The intention of an AFIS system is the identification of potentially matching candidates for a queried fingerprint pattern. Thus, within the resulting ranked list of candidates the false non-match rate

Error Rates

Automated
Fingerprint
Identification
System

should be as low as possible to ensure that the matching candidate pattern is not missed. In contrast to that, the goal of the manual comparison by the forensic expert during ACE-V (see 2.1.1.1.2) process is to keep the false match rate as low as possible to avoid the conviction of innocents.

The Process of Digitized Forensics

This chapter addresses the process of digitized forensics by covering both, the handling of physical traces as well as the handling of traces in the digital domain. In order to create this novel process model, several existing process models are analyzed towards particular requirements and incorporated into a new integrated model covering all essential steps of the process of forensics, independent of the particular type of trace on an abstract level. Existing models address forensic investigations and structure them based on different perspectives. However, usually only selected aspects are covered by each model. In the more traditional forensic investigations often such models attempt to summarize the crucial steps of the investigation in order to provide a guideline and the foundation for a certification of forensic laboratories. A selection of such models relevant for this thesis is summarized in [Section 2.1.1](#). Additionally, legal requirements, as summarized in [Section 2.2](#), must be addressed in order to ensure that the evidence is admissible in court. In digital forensics the process models describe the process from different perspectives as well as summarized in [Section 2.1](#).

The alternative to this novel integrated model for digitized forensics is the application of domain-specific process models. The advantage of such domain specific models usually a higher level of detail and domain knowledge integration regarding the peculiarities of a specific type of trace allowing for a more detailed step by step guideline for the collection, investigation and analysis. However, such an attempt bears the risk that different standards exist in different domains, increasing the necessary effort to assess particular forensic methods with respect to a Daubert challenge [[DG01](#), pp. xiii-xxi] - in particular regarding the Daubert factors addressing the existence and maintenance of standards for using a method as well as the known or potential rate of error. Examples for the differences as well as the higher level of detail in domain specific models are the model for digital forensics from [[KHA+09](#)] (see [Section 2.1.1.2.6](#)), which also covers specific data types and classes of methods as domain knowledge and the ACE-V model [[HRL11](#), pp. 9-12 – 9-17] (see [Section 2.1.1.1.2](#)) for the analysis and comparison of latent fingerprints, which additionally contains an explicit verification phase to minimize the risk of error. Those two exemplary models illustrate the differences in the definition of phases as well as the included processing steps, as the ACE-V model is usually instantiated with some representation of a fingerprint. All particular steps to create this representation are not a part of this model but subject to the assessment of the trace. An integrated framework for digitized forensics could

Alternatives

provide a guideline for the collection, investigation and analysis of specific types of traces allowing for integrating the domain specific models to increase the level of detail while allowing for the assessment of a complete investigation method based on a commonly used process. The main advantage of such an approach is the possibility to incorporate generic requirements into the integrated process model, basically defining a minimum standard for forensic investigations and their assessment in court. This, however, cannot and is not intended to replace domain specific requirements for the application of a method. As a result, the novel process model for digitized forensics is intended to represent a superset of forensic process models for physical evidence as well as digital evidence integrating the requirements of the covered domains from an evidence handling, processing and analysis point of view, without covering domain specific peculiarities in detail. The idea is to allow for projecting domain specific process models on the process model for digitized forensics which is analyzed for the specific domain of latent fingerprint examination within the scope of this thesis. The goal of this chapter is the introduction of a novel process model describing the required steps of digitized forensics in the physical and digital domain addressing research question Q_1 . This is achieved by combining and extending existing and accepted process models and requirements for forensic investigations. Even though the focus of this thesis is on the investigation of latent fingerprints as the second most frequent type of trace evidence in crime scene investigation, the design goal for the novel process model is achieving an applicability for various physical traces as well as digital forensics. Hence, the model does not cover any trace specific methods or requirements such as data protection regulations. Nevertheless, generic requirements, e.g. retention times for trace evidence, are taken into account. The model is created from the perspective of applied computer science focusing on signal processing and pattern recognition for the preparation, digitization and processing of traces. Furthermore, particular challenges and sensor requirements are discussed in order to address research question Q_2 and Q_3 .

Q_1 :
Formalization of
the Digitized
Forensics Process

Q_2 : Novel
Challenges, Q_3 :
Sensor
Requirements

This chapter is structured as follows:

3.1	A Novel Model of the Digitized Forensics Process . . .	53
3.1.1	Prerequisites and Assumptions	55
3.1.2	Strategic Preparation	55
3.1.3	Physical Acquisition	56
3.1.4	Operational Preparation	57
3.1.5	Data Gathering	57
3.1.6	Data Investigation	59
3.1.7	Data Analysis	60
3.1.8	Trace Processing	61
3.1.9	Trace Investigation	61
3.1.10	Trace Analysis	61
3.1.11	Process Accompanying and Final Documentation	61
3.1.12	Archiving of Physical and Digital Evidence Items	63
3.2	Sensory for Digitized Forensics	64
3.2.1	Syntax and Semantics of Sensor Data	64
3.2.2	Error, Loss and Uncertainty Caused by Sensory	65
3.3	New Challenges Connected to Digitized Forensics . . .	67
3.3.1	Ensuring Authenticity of Digitized Traces	67

3.3.2	Sensor Noise and Reproducibility in Digitized Forensics	67
3.3.3	Accuracy of Pattern Recognition Methods	68
3.4	Chapter Summary and Limitations	68

The chapter introduces the novel process model for digitized forensics in [Section 3.1](#). This model incorporates steps of traditional forensics and the challenges of long-term archiving as well. Afterward, [Section 3.2](#) addresses aspects of the sensory utilized for digitized forensics. This is especially important because the quality and accuracy of the results of the sensing process during the data gathering constitute the foundation of the entire forensic investigation in the digital domain. Subsequently, particular challenges tied to the digitization are discussed in [Section 3.3](#). The contents of this chapter have been peer reviewed and published in part within the scope of the following publications as joint work with the co-authors Jana Dittmann, Claus Vielhauer, Stefan Kiltz, Ronny Merkel, Marcus Leich, Matthias Pocs, Michael Ulrich, Ina Großmann, Thomas Fries and Carsten Schulz (in descending order of the frequency of co-authorship): [\[KHA+09\]](#), [\[HKG+11\]](#), [\[HDP+11\]](#), [\[HDV+11\]](#), [\[HKD11\]](#), [\[HML+11\]](#) and [\[HKD13b\]](#).

In parallel to the development of the process model in this chapter, an independent, data focused process model for forensics is derived from the identical starting points within the PhD thesis of Stefan Kiltz [\[Kil20\]](#). Despite the similarities of some phases, the focus of the two models is different with respect to the inclusion of the physical crime scene and physical evidence.

3.1 A Novel Model of the Digitized Forensics Process

The novelty of digitized forensics is that, in contrast to computational forensics, an entire forensic investigation is performed in the digital domain. Nevertheless, the physical traces play an important role, e.g. for verifying the results of an investigation or to allow for investigating the same trace using new technologies after several years. Thus, digitized forensics needs to cover the digital as well as the physical domain regarding the trace collection, processing and handling. Moreover, especially for new investigation techniques, the process model should allow for investigating a trace using multiple different techniques in order to show the effectiveness and reliability of new techniques before they are used in court. Within the scope of this thesis an inductive modeling approach is used for combining selected forensic process models and particular requirements to form a novel process model covering the aspects of digitized forensics.

The foundation for the process model is the model published in Hildebrandt et al. [\[HKG+11\]](#) dividing the digitized forensics in seven phases ranging from a strategic preparation to the preparation of a final report. While this model already extends the model of Kiltz et al. [\[KHA+09\]](#) (see [2.1.1.2.6](#)) by a phase dedicated to the physical acquisition of evidence at the crime scene, the model is extended further by addressing the requirements of storing physical and digital evidence and a creation of a link between the various representations of the trace based on [\[HKD13b\]](#). The entire process is illustrated in [Figure 3.1](#). The primary focus of this thesis consisting of the seven phases from [\[HKG+11\]](#) is highlighted in a light gray shading. In addition to that, in any subsequent subsection the addressed phases of the process model are highlighted in gray shading within the miniaturized figure of the process within the margin note.

Novel Model the
Digitized
Forensics Process

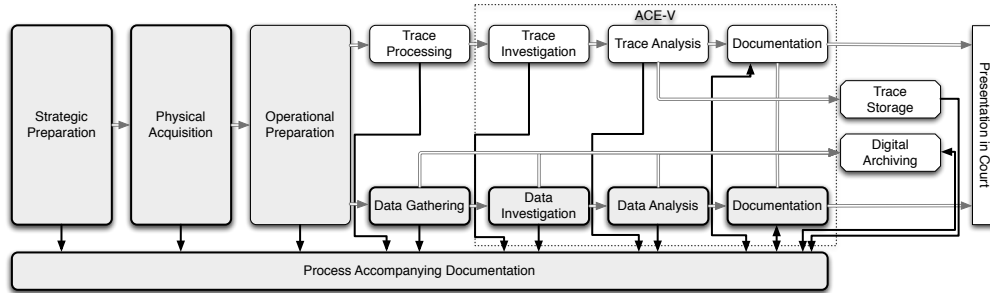
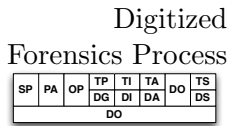


Figure 3.1: Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases from [HKG+11] Highlighted by Gray Shading, Phases from [KHA+09] are Indicated by a Thicker Border

The process model contains a *strategic preparation* which contains all tasks that are performed in order to be prepared for the case work. The objectives and tasks of the *strategic preparation* are described in detail in Section 3.1.2. A particular case starts with the *physical acquisition* of objects containing traces during the crime scene investigation. With this physical acquisition, the chain-of-custody for each trace is started as summarized in Section 3.1.3. Hence, the concept introduced in [HKD13b] should be employed in order to register a trace and all relevant metadata. The last shared phase of traditional forensics and digitized forensics is the *operational preparation* as described in Section 3.1.4. Afterward, the trace is either digitized within the phase of *data gathering* for allowing for a digital investigation or further processed during the *trace processing* in order to allow for a manual investigation of the trace. The data gathering is described in detail in Section 3.1.5, whereas the trace processing is summarized in Section 3.1.8. The following three phases are a part of the well-known ACE-V methodology in forensics as described in Section 2.1.1.1.2. They describe the initial investigation of a trace towards its suitability for further processing in the digital domain (data investigation, see Section 3.1.6) and in the physical domain (trace investigation, see summary in Section 3.1.9). This primarily resembles the analysis phase of ACE-V where e.g. the number of usable features of a trace is determined. Afterward, each suitable trace is analyzed in order to identify the source of the trace. The *data analysis* is described in Section 3.1.7, whereas typical tasks of the trace analysis are summarized in Section 3.1.10. Subsequently, all findings of the forensic investigation are summarized in a *final documentation*. Furthermore, in parallel to each investigation step, particular findings, applied methods, assumptions, etc. are documented within the *process accompanying documentation*. This log of the course of the investigation is supposed to allow for reconstructing and comprehending the results of the entire forensic investigation. Both documentations as well as considerations towards the *presentation in court* are discussed in Section 3.1.11. Additionally, the digitized and physical traces and the documentations need to be stored or archived. The particular requirements for the *trace storage* in conjunction with a non-destructive digitization and the *digital archiving* are discussed in Section 3.1.12.

Two-Tiered
Modeling of
Phases

Overall the model follows a two-tiered approach similar to [BC04] in Section 2.1.1.2.5 as trace specific details are not contained in the first tier of phases as depicted in Figure 3.1. Any trace-specific details, such as peculiarities of the processing of latent fingerprints, DNA or tool marks, could be represented by a second tier of trace-specific sub-phases. Such an approach allows for achieving the

objective \mathbb{O}_1 of an universal process model for digitized forensics, which would otherwise be neither feasible nor practical due to the necessary amount of domain specific knowledge and procedures to be integrated into the phases of the model. With the two-tiered approach, the first tier of phases can represent the common ground for forensic investigations, ensuring a general course of the investigation in line with accepted standards and methods. The second tier of trace-specific sub-phases can be used to map specific tasks and procedures to the first-tier phases. Within this thesis, this is performed in the two application scenarios within the context of latent fingerprint processing in Chapter 5 and Chapter 6.

3.1.1 Prerequisites and Assumptions

The overall objective of digitized forensics is to shift the investigation of forensic traces to a digital representation of the trace while the physical counterpart can be preserved in its original condition. Of course, this concept is tied to several prerequisites and assumptions. First and foremost, one or multiple sensors are required to digitize the necessary information representing the trace. If a trace cannot be digitized with existing sensors, digitized forensics is simply not possible. This also includes an unacceptable amount of loss of information, see Section 3.2.2, during the acquisition process. Secondly, it is important that a physical trace can be preserved in its original state. This requires that the rate of deterioration of the trace can be minimized or even stopped with appropriate storage conditions. If this is not possible but the process of deterioration can be stopped using physical or chemical treatment, such a modification of the trace might be the preferred option.

Within the scope of the thesis, the general assumption is that the digitized forensic method has been generally accepted, e.g. by passing several Daubert tests [DG01, pp. xiii-xxi]. In a transition phase, where digitized forensics is introduced for a particular trace, the traditional forensic processing method could be utilized in parallel to show the effectiveness of the new method. In discussions with latent print examiners the advantage of bringing the physical evidence to court was mentioned. This is a case where the traditional processing is necessary in order to render the latent print visible - with all the consequences in terms of the integrity of the trace.

3.1.2 Strategic Preparation

The Strategic Preparation (SP) is a very important step in forensics. In traditional forensics the effectiveness of treatment methods for traces are thoroughly tested in order to determine the conditions when and how a method should be applied. This is also very important for training forensic experts in order to minimize the risk for error.

The ISO/IEC17025 [ISO17], see Section 2.1.1.1.1, describes standards for laboratories. Those standards also contain specific tasks for a strategic preparation, such as the documentation of competence requirements [ISO17, 6.2.2, p. 5], the setup and maintenance of specific facilities and environmental conditions [ISO17, 6.3, p. 6] or access to and maintenance of specific equipment [ISO17, 6.4, pp. 6-8]. In addition to that methods need to be selected, verified and validated.

In process models for digital forensics such a preparation is described e.g. by Carrier and Spafford [CS03] (see Section 2.1.1.2.4), Beebe and Clark [BC04] (see Section 2.1.1.2.5) and Kiltz et al. [KHA+09] (see Section 2.1.1.2.6). In

Transition phase from traditional methods to digitized forensics

SP: Strategic Preparation

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

Strategic Preparation in Traditional Forensics

Strategic Preparation in Digital Forensics

incident response a similar preparation is described e.g. within the NIST Special Publication 800-61 r2 [Cic+12, pp. 21-24] (see Section 2.1.1.2.1). The overall goal of the actions within the described preparation phases is very similar and in line with the ISO/IEC17025, the preparation should increase the forensic readiness by procuring the necessary tools, training the personnel as well as installing logging and detection mechanisms to gather data for the case of an incident. It is more concerning that some official guidelines for digital forensics, e.g. in [MSH08, p. x], almost neglect the importance of the strategic preparation for potential incidents - instead of enumerating special skills, the guide suggests compiling a list of required skills and training for specific tasks in digital forensics.

Strategic
Preparation in
Digitized
Forensics

In digitized forensics this preparation phase is even more important. Especially when multiple traces are likely to be present on the very same object from a crime scene. In this case it is crucial that the crime scene investigator and the personnel in the forensic laboratory are aware of any potential trace on the object and the impact that a particular acquisition technique might have on every single trace. Additionally, it is necessary to determine the proper collection and storage conditions for the suspected cluster of traces. Moreover, the possibility of the traces influencing each other should be known. In essence during the strategic preparation an extensive experimental evaluation of potential traces and combinations thereof is necessary. In addition to that, required forensic tools for the processing of the traces need to be procured or developed and evaluated during the strategic preparation. One example for the latter is the design and evaluation of feature spaces for pattern recognition based techniques such as the two application scenarios in Chapter 5 and Chapter 6. Especially the evaluation or benchmarking of each utilized technique is important in order to determine the error rates in conjunction with its application. This is also a requirement in order to address the Daubert factor [DG01, p. 3] of the known or potential rate of error.

From an organizational point of view the personnel should be trained for the digitization of specific traces with the specialized sensory. Secondly, especially for more exotic combinations of traces, a list of the capabilities of the forensic laboratories should be prepared and maintained. This would ensure that the best suited forensic laboratory can be identified for specific objects from the crime scene.

3.1.3 Physical Acquisition

During the Physical Acquisition (PA) all potential traces are collected at the crime scene. With this phase the chain-of-custody is initiated and each item is bagged and tagged in order to make it identifiable and to ensure the authenticity with respect to the origin of the object containing the trace. In some cases experts for specific types of traces might be present at the crime scene, known as primary custody [HRL11, p. 10-4], in order to assess the evidential value of the traces before the relevant and usable traces are collected. The step of the physical acquisition is the most crucial step of the forensic investigation because any missed trace or error during handling will result in an unintended loss causing uncertainty and potentially errors further down the investigation process.

PA: Physical
Acquisition

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

Physical
acquisition:
foundation of the
forensic
investigation

In order to preserve the evidential value of the traces, it is also necessary to record the location and condition of each collected object. The necessary documentation is summarized for latent fingerprints in [HRL11, pp. 10-4 – 10-10]. Besides the collection of potential traces, it is also necessary to acquire samples from any

person that has been present at the scene of crime legitimately at a time before the crime took place.

3.1.4 Operational Preparation

The Operational Preparation (OP) is an important step towards avoiding crucial errors during the forensic investigation. During this phase all information about the scheduled investigation should be carefully considered in order to line out a course for the investigation.

In the context of digitized forensics, the decision about the appropriate sensory to digitize a trace or a combination of traces is made. This decision can be complicated, especially when multiple traces are suspected to be at the same spot because a specific sensing technique might have an impact on one of the traces. Thus, it is absolutely necessary to define a specific sequence for acquiring the traces in order to avoid losing vital information about the traces. A prime example for that is a fingerprint trace as the second most frequent type of trace evidence in criminal investigations - besides the fingerprint pattern, the residue on the surface forming the latent fingerprint likely contains DNA from the person who left the fingerprint at the crime scene. However, DNA, nowadays the most frequent type of trace evidence, can be degraded by UV radiation, which on the other hand could be a technique for detecting the latent fingerprint.

In essence, this operational preparation is the most important step in order to avoid loss, errors and resulting uncertainties as described in [Section 3.2.2](#).

3.1.5 Data Gathering

The Data Gathering (DG) is the first step of the investigation where traditional forensics and digitized forensics diverge from each other. During the data gathering one or multiple sensors (see [Section 3.2](#)) are used to digitize the trace. This digitization process follows the acquisition sequence defined during the operation preparation. For the resulting digital representations of the trace it is necessary to maintain a digital chain-of-custody which ensures that any tampering with the evidence can be detected and that the digitized trace can be traced back to the physical object it was obtained from.

In order to be able to prove the authenticity of the digitized trace multiple requirements must be met:

1. A comprehensive link between the physical trace and each digital representation must be established as described in [Section 3.3.1](#) and [Section 4.2](#),
2. The utilized sensors, configuration and acquisition conditions need to be documented within the process accompanying documentation as described in [Section 3.1.11](#),
3. All storage conditions of the trace that might have caused a deterioration of the trace need to be documented,
4. Specific locations of the trace need to be documented, especially if multiple traces are present on the same object.

Especially the first requirement is crucial in order to prove the authenticity of the trace. If the trace itself is not visible to the bare eye, it is likely that the

OP: Operational Preparation - planning the specific forensic investigation

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

DG: Data Gathering as the starting point and foundation of digitized forensics

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

Creation of a link between a physical trace and its digital representations is crucial

effectiveness and accuracy of new digitization methods needs to be shown in comparison to traditional trace processing, as described in Section 3.1.8, in order to pass a Daubert challenge [DG01, pp. xiii-xxi]. After a specific method has been generally accepted by courts as being suitable for digitizing the specific traces, a maintenance and adherence to standards for the utilization of the sensors should be sufficient. Those standards will likely require specific acquisition conditions and settings for the sensors which is also documented following the second requirement. The third requirement is primarily a result of the natural deterioration of unprocessed traces. This is also a means of quality assurance for the forensic laboratories. The fourth requirement is similar to the documentation of the object locations at a crime scene. This requirement can be met by a two staged digitization process with a coarse and multiple detailed scans as summarized in [HDP+11], [HDV+11], [HKD11] as well as Section 5.1 for the example of latent fingerprints representing trace-specific second-tier phases.

The general concept of coarse and detailed scans is illustrated in Figure 3.2.

Concept of
Coarse and
Detailed Scans

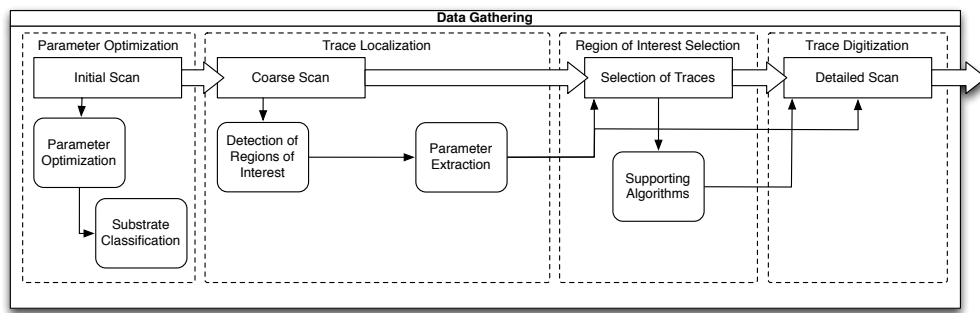


Figure 3.2: Generic Concept of Coarse and Detailed Scans as Exemplary Templates for Second-Tier Phases

The first step is a parameter optimization for the given physical object. This can involve one or multiple initial scans in order to find the appropriate parameterization of the sensor for the digitization process. Afterward, one or multiple coarse scans can be performed for the purpose of localizing potential traces. Before the identified traces are acquired using detailed scans, a selection of the relevant region of interest might be performed using additional scans. Such a step might be advantageous in order to minimize the impact of the forensic analysis, e.g. by excluding traces that are not relevant for the investigated case. Thus, an additional selection process can reduce the workload of forensic experts and might additionally avoid collecting data about persons which are not involved in the case but might have been at the scene of the crime at any time before or after the investigated events.

Coarse scans

The objective of the coarse scan is twofold – it is a means of documentation as well as a technique for locating potential traces. In order to achieve the objective of the documentation it is necessary to digitize the object in a manner that itself and its positioning could be identified within the coarse scan. In order to achieve that, a sufficient area of the surface of the object should be covered by the coarse scan. In addition to that, the acquisition resolution of the coarse scan and the utilized sensors should be suitable in order to identify potential traces. On the other hand, it is advantageous if no identifying features are present within the coarse scan. The resulting benefit is that the coarse scan would be privacy compliant and thus – in theory – could be stored indefinitely for the purpose of documentation.

The detailed scan is the digitization of a specific trace adhering to the requirements in terms of sensors and resolutions to allow for the forensic analysis of the specific trace – i.e. a forensic comparison to identify the subject associated with the trace. A detailed scan is the foundation for any following forensic processing in the digital domain. Thus, any loss during this digitization will potentially influence the outcome of the entire forensic investigation.

Detailed scans

3.1.6 Data Investigation

The main purpose of the Data Investigation (DI) is the assessment of the trace. Overall the following steps are performed within the data investigation:

DI: Data Investigation as the first step of the ACE-V process in the digital domain

1. Segregation of the trace data from the captured surface data (preprocessing),
2. Separation of multiple traces within the preprocessed data,
3. Assessment of the quality of the trace (Analysis Phase of ACE-V, see Section 2.1.1.1.2).

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DO
						DS
						DO

During the first step, the trace data needs to be segregated from any captured non-essential surface or substrate information in order to allow for a thorough forensic analysis of the trace characteristics. In traditional forensic investigations this is usually a part of the trace processing with chemical or physical agents in order to prepare the trace for further investigation. Whereas such a preprocessing is usually irreversible in the real world, multiple digital approaches can be evaluated because the unaltered digitized data as well as the physical trace can be preserved in an unaltered form. As the segregation of the trace from any other captured data is essential for the forensic analysis, it is a special emphasis of the practical evaluation within this thesis as described in Section 5.2 for the example of latent fingerprints.

Data Segregation

The second step is necessary in order to allow for analyzing multiple traces, potentially of a different kind, which are present on the same spot of the analyzed object. If both traces are visible within the same detailed scan, they usually need to be separated during the data investigation and then forwarded to the particular experts for each type of trace. If the traces are of the same type, e.g. two overlapped fingerprints or two fibers, the separation might be also deferred to the data analysis to be performed by an expert for this particular type of trace. However, even if the separation is performed during the data investigation, it is necessary that the data processing history is available to the forensic expert in order to allow for explaining any differences or anomalies within the processed data.

Trace Separation

The third step of the data investigation is the assessment of the quality of the trace. It is in line with the first step of the ACE-V methodology which contains the analysis of the trace. However, especially if the data investigation is solely performed by a forensic technician without any in-depth knowledge about the specific type of traces, this quality assessment is just an indicator for the expert who is assigned with the task of analyzing the trace. In general, a basic understanding of the quality of a trace is necessary during the data investigation in order to assess the effectiveness of the applied digital preprocessing.

Trace Assessment

DA: Data
Analysis for
Evaluating the
Forensic
Hypothesis

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DS	
DO							

3.1.7 Data Analysis

The Data Analysis (DA) is the core of the decision-making process in digitized forensics. Based on the gathered and preprocessed data forensic experts for the specific type of trace thoroughly analyze the trace using the ACE-V methodology [HRL11, pp. 9-12 – 9-17] as summarized in Section 2.1.1.1.2. Following this methodology, the data analysis consists of the following steps:

1. Analysis - Evaluation of the trace including its quality, usability for different comparisons and explanation of any anomalies,
2. Comparison - Comparison of the trace found at the crime scene with a second trace, usually with known origin,
3. Evaluation - Evaluation of the results of the analysis and comparison steps in order to back or disprove the hypothesis of the two traces originating from the same source,
4. Verification - Independent analysis, comparison and evaluation performed by another forensic expert to minimize the risk of error.

ACE-V: Analysis

Due to the large number of degrees of freedom, the ACE-V process is usually performed manually by highly trained forensic experts. During the analysis each trace must be thoroughly assessed in order to identify its peculiar features, the overall and local quality as well as the usability for the comparison, e.g. based on the number and rarity of specific characterizing features. Secondly, the plausibility checking and explanation of anomalies, e.g. based on the substrate the trace was lifted from, is an important step during this phase. Especially the latter contributes to the high number of degrees of freedom.

ACE-V:
Comparison

During the comparison the specific features identified during the analysis are compared and matched to the features of a second sample, usually with a known source of origin. This comparison can be performed based on the number of matching features considering their type and relative location or by additionally considering the rarity of the specific features. Overall, the utilized types of features depend on the specific trace that is investigated. Oftentimes, the scientific foundation of the comparison relies on the exchange principle formulated by Edmond Locard, see e.g. [IR00, p. 44] - any contact with another person or object will result in an exchange of physical traces. Thus, matching traces should be present on the questioned object, e.g. from the crime scene and on the reference object.

ACE-V:
Evaluation

The evaluation step consists of the careful consideration of all features in order to back the hypothesis that the two traces originate from the same source or have been in contact. Furthermore, all indicators for backing the alternative hypothesis that both traces are not related to each other need to be considered. Afterward, a decision is formulated by the forensic expert. Depending on the type of trace the decision could be formulated binary (match no match) or in the form of a likelihood ratio between the two hypotheses as summarized in Section 2.1.2.2.

ACE-V:
Verification

During the verification independent forensic experts perform the same investigation of the trace. Afterward, the results are compared and, if necessary, discussed in the case of significant differences. In such a case an additional investigation might be performed by another expert. The overall goal of this step is the minimization of the risk of error as the investigation is subjective to some extent.

3.1.8 Trace Processing

The Trace Processing (TP) highly depends on the nature of the forensic trace. In particular some traces such as firearm and toolmarks [Org20a] are directly investigated within special microscopes suitable for a comparison. Thus, usually no special trace processing is necessary unless the specific toolmarks are covered with other traces or contaminants. In such a case, the other traces should be recovered in the first place, before the object is cleaned for the trace investigation and trace analysis. Fingerprints [Org20b], the materials analysis [Org20c] or DNA analysis [SWG20] oftentimes require a special preprocessing to render the trace visible or to separate it from a multitude of other traces.

As a result, the availability of sensors for the digitization of the peculiarities of a special kind of trace is a prerequisite for digitized forensics.

TP: Trace
Processing

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

3.1.9 Trace Investigation

The Trace Investigation (TI) can be considered as a preassessment of the trace from a crime scene regarding the presence of other traces and its overall quality. In the case of an additional trace processing for rendering the trace visible, the trace investigation does also cover aspects of quality assurance in order to judge whether a particular processing method was effective. Thus, the trace investigation is quite similar in its scope compared to the data investigation in digitized forensics as described in Section 3.1.6.

TI: Trace
Investigation

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

3.1.10 Trace Analysis

The Trace Analysis (TA) describes the actual analysis process of a particular type of trace. The analysis might be performed on the physical trace itself or by using photographs or copies of the trace. The differences in comparison to the data analysis in Section 3.1.7 primarily originate from the differences of the trace representation. However, in both cases, the analysis is usually performed manually by highly trained experts. Here, it is important that generally accepted tools and methods are applied within the scope of forensic standards as required e.g. by the Daubert standard [DG01, pp. xiii-xxi] or the Federal Rules of Evidence [FRE14].

TA: Trace
Analysis

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

3.1.11 Process Accompanying and Final Documentation

The phase Documentation (DO) can be divided into two different documentation steps serving different purposes [KHA+09]:

1. Process Accompanying Documentation - a detailed log of the forensic process investigating a specific trace,
2. Final Documentation - a comprehensive summary of the forensic investigation prepared for a specific group of target audience.

DO:
Documentation

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

A documentation is a requirement in [ISO17, 6.5, p. 8] and mandatory in order to maintain the metrological traceability. This documentation should contain all means and parameters that have been used to investigate a trace. In digitized forensics this process accompanying documentation should cover all phases of the forensic investigation including the strategic preparation. The overall purpose of this documentation is the creation of a comprehensible course

Process
Accompanying
Documentation

of the investigation that could be reproduced by other forensic experts. Since the utilized techniques in traditional forensics and digitized forensics differ, the content of the documentation will be different as well. In traditional forensics e.g. concentrations of chemical agents or particle sizes are important influence factors on the preprocessing results and might affect the entire investigation. In digitized forensics the utilized sensors, sensor settings and applied digital tools and models for pattern recognition have a similar impact on the forensic instigation. Particular information which should be a part of the process accompanying documentation for each phase of the forensic investigation are summarized in Table 3.1. Especially in combination with the documentation of the storage

Phase	Information to Document
Strategic Preparation	Training of the personnel, training of digital models and utilized training data, available sensory and software
Physical Acquisition	Location of the objects containing traces at the crime scene, relative position of the objects at the crime scene, conditions at the crime scene (temperature, humidity, light exposure)
Operational Preparation	Expected traces on the object, tools and methods to apply, required storage conditions to minimize the trace deterioration
Data Gathering	Utilized sensors and sensor settings, hash values and signatures of the resulting data
Data Investigation	Applied digital preprocessing methods, settings and models, hash values and signatures of the resulting data
Data Analysis	Present features, trace quality, comparison and evaluation results, applied tools and settings for supporting the analysis, hash values and signatures of the resulting data
Trace Processing	Concentrations of physical or chemical agents to process the trace, settings of devices
Trace Investigation	Preassessment results regarding the trace, quality assurance methods applied
Trace Analysis	Present features, trace quality, comparison and evaluation results
Trace Storage	Storage conditions
Digital Archiving	Data protection strategies, key management, utilized algorithms

Table 3.1: Typical Information within the Process Accompanying Documentation

conditions of the trace it is possible to reevaluate the case after a long time considering the deterioration of the trace in such conditions. Such a reassessment of the traces has been performed in the past with the advent of DNA evidence and novel DNA extraction techniques [Sch+11].

Final
Documentation

The final documentation serves as a target audience specific summary of the investigation results. Usually the results are prepared for judges and lawyers allowing them to assess the testimony of the forensic expert. The final

documentation should contain the final decision of the expert as well as a summary of the trace collection and processing in order provide the basis for assessing the trace as circumstantial evidence.

3.1.12 Archiving of Physical and Digital Evidence Items

The archiving of the traces is an important task in forensics because it is necessary in-between the phases of the forensic processing and after the investigation to allow for a reassessment of the evidence. Independent of the nature of the evidence items, it is necessary to ensure that the integrity and authenticity is maintained throughout the storage period. Oftentimes this is hard to achieve because a physical evidence item might be the subject to a natural degradation causing an intrinsic loss of integrity. However, special storage conditions might reduce the rate of degradation. Similarly, in the case of digital evidence, algorithms for ensuring the integrity and authenticity of an evidence item might become obsolete and insecure and thus might allow for tampering with the evidence. Thus, similar to special storage conditions of physical items the issue of the long-term archiving needs to be properly addressed [Huh+09]. Particular requirements for a trustworthy long-term archiving in [Huh+09] address the integrity, authenticity, readability, completeness, negotiability, confidentiality, legal compliance, availability and migratability.

With respect to digital and digitized traces, the Digital Archiving (DS) requires constant monitoring of trends and developments regarding the utilized algorithms. If a specific algorithm is going to be phased out in the near future, it is necessary to add new protection measures to the archived evidence before the previous techniques are considered insecure. Of course, this requires an overview of the inventory and the utilized protection mechanisms. Hash trees are used in [Huh+09] to ensure the integrity of data using new algorithms if necessary. In addition to that, the archiving of digital evidence on read-only media (WORM: Write Once, Read Many), can be beneficial in order to avoid any alteration of the archived data. However, in terms of storage media the longevity of the selected storage medium as well as the access to suitable media reader devices needs to be assessed on a regular basis (readability in [Huh+09]). In addition to that, software for reading the data formats need to be available. Ideally, the data formats are openly documented allowing for a vendor-independent access to the archived data. Besides the general challenges of the Trace Storage (TS) of evidence items, it is also necessary to restrict the access to those items. In particular, this is already implemented with organizational measures including the mechanism of a chain-of-custody (see Section 2.1.2.1). The chain-of-custody represents a consistent log of the possession of the evidence item without any gaps. Thus, any modification of the evidence could be traced to a specific person.

In digitized forensics, the chain-of-custody is slightly different in comparison to physical evidence as soon as a trace has been digitized during the data gathering phase (see Section 3.1.5). It is possible to create identical copies of the evidence. In addition to that, any result of a processing step can be traced back to its source data providing a more concise and more comprehensible processing history.

DS: Digital Archiving

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

TS: Trace Storage

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

Sensory for
Digitized
Forensics

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DS	
DO							

3.2 Sensory for Digitized Forensics

Sensors play a crucial role in digitized forensics. Within the phase of data gathering they create the foundation for the entire forensic investigation in the digitized domain. The main purpose of a sensor is to capture and digitize the necessary information of a trace and its nature. If an inappropriate sensor is selected for digitizing a specific trace, an unwanted loss of information is inevitable. On the other hand, even with suitable sensors, the selected sensor does have an impact on the resulting digitized trace. Such an impact could be a difference in the amount of captured data without any difference in the amount of useful information. Thus, causing potentially a more demanding search for the relevant information about the trace within the gathered data. In essence, it is necessary to differentiate between desired loss of information and unwanted loss of information. The specifics of the loss are discussed in further detail in Section 3.2.2.

Formal definition
of a sensor

Definition 3.1: Definition Sensor

A sensor S is defined as the following tuple:

$$S = \{M, O, D_{Syntax}, D_{Semantics}\}$$

Whereas M describes the measurement principle, e.g. capturing of visual light, O the mode of operation, i.e. how data is acquired either value by value or by capturing multiple values at once, D_{Syntax} describes the resulting data output and $D_{Semantics}$ describes the semantics of the data.

From a formal point of view a sensor performs a projection from one information space to another.

Ideally, this projection is fully deterministic. However, in practice environmental and technical influences will cause sensor noise, resulting in slightly different results every time a trace is digitized. Moreover, a sensor cannot capture all the information of an object containing traces. At least on the quantum physics level either the position or the energy of a quark can be measured according to Werner Heisenberg's Uncertainty Principle [Hei27]. Capturing both information at the same time is not possible.

For forensics different types of sensors can be utilized depending on the type of trace. Sensor data can range from volumetric 3D data, to 2.5D data (height maps), 2D images, multi-/hyperspectral images and data about the chemical composition of the trace. Whereas the data types for storing the digitized data might be quite similar, the type of contained information can be significantly different. This difference of syntax and semantics of sensor data is discussed in section Section 3.2.1.

3.2.1 Syntax and Semantics of Sensor Data

In digitized forensics, after the data gathering, all traces are analyzed in the digital domain. This, of course, requires to store the gathered data in specific and suitable data formats. The data format encoding of the digitized information is the syntax of the digitized traces. The specific syntax depends on the type of captured data and the specifics of the sensor, but eventually the syntax has to be represented by standard data structures such as multi-dimensional arrays of data points. The semantics of the data describes the contained information, i.e.

Syntax of
digitized traces

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DS	
DO							

its interpretation and context. Some sensors store additional data (metadata) to assist the interpretation of the data. From a semantics point of view an acquired optimal image $I_{optimal}$ can be defined as follows [HML+11]:

Definition 3.2: Definition of an image $I_{optimal}$ by an optimal sensor

An image $I_{optimal}$ is the result of a digitization process using a Sensor S . Depending on the measurement principle, $I_{optimal}$ consists of the components I_{phys} (representing the physical phenomena of a trace which should be digitized) and I_{noise} (representing the non-deterministic noise which occurred during the acquisition process): $I_{optimal} = I_{phys} + I_{noise}$.

Definition of an optimal digitized image

By this definition the semantics of an image are formed by the measured physical phenomena in combination with the inevitable noise during the acquisition process. However, for many sensors in forensics this assumption of an optimal digitization of a trace is not achievable in practice. Thus, the definition of an image needs to be extended in order to account for other artifacts within the digitized data which are no random noise:

Definition 3.3: Definition of an image I

An image I is the result of a digitization process using a Sensor S . Depending on the measurement principle, I consists of the components caused by the background object I_{back} , the trace I_{trace} (which should be digitized) and I_{noise} (representing the non-deterministic noise which occurred during the acquisition process): $I = I_{back} + I_{trace} + I_{noise}$.

Definition of a digitized image

The composition of the image I usually requires the segregation of I_{trace} from I_{back} and I_{noise} in order to allow for investigating the trace. This segregation process is discussed in Section 5.2.

3.2.2 Error, Loss and Uncertainty Caused by Sensory

Casey [Cas02] states that uncertainty is not evaluated in digital forensics. In [Cas02] uncertainties in network related evidence are the result of data corruption, loss, tampering or errors in the interpretation and analysis of the digital evidence. The PhD thesis of Stefan Kiltz [Kil20], which is written in parallel to this thesis, also addresses the issue of error, loss and uncertainty within the scope of forensics with a different perspective and approach. In general in forensics it is necessary to be aware of the rate of error or a potential rate of error, which is also reflected by the factors assessed during a Daubert challenge [DG01, p. 3]. Uncertainty is also a part of the measurement process, hence, in ISO/IEC17025 [ISO17, 7.6, p. 13] it is a requirement to identify contributions to measurement uncertainty. Within the scope of this thesis the terms are being used slightly different as stated in the definitions 3.4, 3.5 and 3.6.

Error, Loss and Uncertainty

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DO
						DS
						DO

Definition 3.4: Definition of Loss

Loss D_{loss} is any reduction of available data D_{avail} in comparison to the theoretic amount of source data D_{source} - whether it is intended or unintended: $D_{loss} = D_{source} - D_{avail}$

Definition of Loss

The goal of the data investigation, see Section 3.1.6, is the creation of loss by segregating irrelevant data from data that is relevant for the case. This data reduction is intended loss. Any kind of relevant data which is excluded during the data investigation or not captured during the data gathering phase, see Section 3.1.5, is considered as unintended loss which can be the root cause for uncertainty and errors.

Definition 3.5: Definition of Uncertainty

Definition of
Uncertainty

Uncertainty describes any decision, conclusion or hypothesis which has a probability of less than 1.

In practice there is usually some level of uncertainty in forensics. Thus, many decisions are made beyond reasonable doubt, limiting the uncertainty to a specific threshold. This procedure is also reflected within the concept of likelihood ratios as described in Section 2.1.2.2. Nevertheless, any level of uncertainty can cause erroneous decisions. Thus, e.g. in [FSC09, p. 116], it is recommended to provide a range of plausible values, e.g. using confidence intervals.

Definition 3.6: Definition of Error

Definition of
Error

Error is any kind of decision or conclusion that differs from the actual series of events, involved objects and persons at the crime scene. An error is basically the acceptance of an incorrect hypothesis regarding an aspect of the series of events.

Within the scope of digitized forensics, the main difference in comparison to traditional forensics is the digitization of physical traces. If the data gathering can be performed in a non-destructive manner, any detected loss, uncertainty or error caused during the data investigation or data analysis phase could be recovered as long as a clean copy of the digitized trace exists. Thus, the main requirement is a minimization of error, unintended loss and uncertainty during and prior to the data gathering phase. Under the assumption that all traces are identified and carefully handled during the physical acquisition, the focus within this thesis is error, loss and uncertainty caused by the sensory. Nevertheless, it is crucial to determine the error rates as described in [FSC09, pp. 117 – 122] (see Section 2.4.1). The known or potential rate of error is also one of the Daubert factors which can be assessed by a judge prior to the admission of scientific evidence [DG01, p. 3]. An additional source of errors can be a bias of the forensic expert or a witness [FSC09, pp. 122 – 124] which can result in a decision that is performed in circumstances with a rather high level of uncertainty. Such an instance of overconfidence can be fueled by contextual information increasing the pressure on the examiner to confirm the identification. Similarly, the decision of a classifier can be biased if it was trained on biased data. In this case even the error rates, confidence levels and likelihood ratios can be misleading.

Loss Caused by
Sensory

As mentioned in Section 3.2 loss is inevitable because not all data of a trace could be captured at the same time. In fact, usually only a small portion of available data can be captured by a sensor. This requires the selection of sensors suitable for digitizing the relevant data of a particular type of trace in order to avoid any major uncertainties caused by the unintended loss during the digitization process.

Each sensor is prone to specific errors during the acquisition. Those errors can be caused by the properties of the object containing the trace or the trace itself as well as the configuration of the sensor. It is important that the acquisition errors are detected and marked accordingly within the digitized data in order to allow for handling them appropriately. With respect to [FSC09, pp. 116 – 117] measurement errors can be considered as a specific kind of loss resulting in or from uncertainty (e.g. a limited measurement accuracy) or actual errors by deviating from the required standards for processing a specific trace. Examples for the latter are sample mix-ups or contamination of the sample.

Uncertainty is probably the most challenging to be evaluated or quantified for specific sensors. In practice sensors are evaluated using reference or calibration samples in order to make sure that the sensor performs at design specifications.

Errors Caused by
Sensory

Uncertainty
Caused by
Sensory

3.3 New Challenges Connected to Digitized Forensics

With the digitization of physical traces several new challenges need to be addressed in order to analyze a digital representation of a trace. In this section the two main challenges, namely the authenticity of the digital representation of a trace and the reproducibility of the acquisition process are discussed to address research gap \mathcal{G}_2 . Those two aspects are the most crucial challenges since the remainder of the forensic investigation relies on the quality and authenticity of the digitized trace.

In addition to that, further challenges are connected to the forensic investigation, e.g. the accuracy of specific methods such as models in pattern recognition, requirements of data protection regulations or secure means for long term archiving. However, those challenges are usually trace specific or an independent field of research.

3.3.1 Ensuring Authenticity of Digitized Traces

Authenticity is one of the major challenges in digitized forensics. It is necessary to prove that the digitized trace originates from the claimed physical trace (entity authenticity) and that represents it in a manner that the conclusions drawn do not differ from a traditional forensic investigation using the same features (data authenticity). However, if the digitization allows for investigating additional features which would not be available due to limitations of the traditional forensic procedures, the final conclusion, e.g. of a comparison, might be different given the extended amount of information.

In traditional forensics the authenticity of a trace is ensured by bagging and tagging each collected object in combination with a thorough chain-of-custody. Although, this system is technically not tamper-proof, it is usually sufficient since the traces are only supposed to be handled by trained professionals.

Authenticity of
traces

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

Bagging and
tagging of
physical traces

3.3.2 Sensor Noise and Reproducibility in Digitized Forensics

Sensors are usually affected by external influences causing noise. Thus, the definitions for a sensor in Definition 3.2 and 3.3 contain noise components. The root cause for noise can be for example changes in temperature, vibration or humidity. In line with the ISO/IEC17025 [ISO17] such external influence factors should be monitored and limited. However, some amount of noise is usually unavoidable. This noise will cause two consecutive digitization processes to result in slightly different data. In comparison to digital forensics, this poses a challenge

Influence of
sensor noise

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

because the integrity cannot be verified easily using cryptographic hash functions. Instead, it would be necessary to employ some kind of perceptual hash to verify the integrity of the trace contained in the digitized image.

Aging effects

A second factor influencing the reproducibility of the digitization process are aging or degradation effects of a trace, see e.g. Merkel [Mer14]. Of course, this depends on the properties of the trace, the substrate and the required time for the acquisition process.

3.3.3 Accuracy of Pattern Recognition Methods

Albeit not being a new challenge at all, the accuracy and error rates of pattern recognition methods in forensics are fundamentally important. In discussions with forensic experts it was pointed out, that especially the error rates reported by the manufacturers of a method or technique or by the researchers, respectively, are usually not achieved during the practical application of the method in forensic investigations. The reasons for that can range from non-representative test data during the initial evaluation to the deliberate reporting of non-realistic test results.

Need for
Representative
Test Data

The sole option of overcoming this discrepancy between the reported performance under lab conditions and the actual performance in real-world conditions is a standardization of the testing procedure. For that representative test data needs to be supplied by the end users. If this is not possible, e.g. for reasons like data protection regulations, at least some standardized test protocols of various influence factors should be created.

In academia the comparability is often provided by the utilization of public data sets. However, those are not necessarily representative for real forensic cases and thus, would also result in the aforementioned discrepancy between the reported and observed performance.

The determination of the error rates for the application specific scenario is an important part of the strategic preparation described in Section 3.1.2. The observed error rates are the foundation for determining the level of trust regarding the results of a method.

3.4 Chapter Summary and Limitations

This chapter introduces a novel process model for digitized forensics addressing research question Q_1 . The objective O_1 , towards the creation of a novel universal process model for digitized forensics for all types of traces, is achieved by adopting the two-tiered modeling approach from [BC04] to create a trace-independent first tier of process phases. Those phases are based on the analysis of existing models from traditional forensics, incident response and digitized forensics. The trace specific processing in the second tier is intentionally not covered by the novel process model in this thesis as the multitude of different processing strategies would exceed the scope of a thesis significantly. The resulting process model represents the main contribution C_1 of this thesis.

Within the scope of the process model, the research question Q_2 is addressed by analyzing novel, unsolved challenges arising from the digitization of the traces. As such challenges are usually not considered in computational forensics, this thesis represents a systematical analysis of the arising challenges from a computer scientist's point of view with a special emphasis on the IT security aspects of integrity and authenticity.

Additionally, the generic requirements and limitations of sensory are discussed in this chapter in order to address research question Q_3 . For that, in Section 3.2, a formal definition of sensors is introduced and the resulting syntax and semantics of the digitized data is discussed. In particular error, loss and uncertainty is defined on the foundation of data as well as probabilistic decisions during forensic investigations in Section 3.2.2.

Based on the integrated process models, the introduced novel process model for digitized forensics should be suitable to describe the forensic investigation for trace evidence as well as digital evidence on a high level. However, due to the broad variety of different traces, a limitation of this chapter is the purely theoretical assessment of the forensic process in general. Thus, it is necessary to evaluate the applicability of this novel process model for specific types of traces. Such an evaluation is performed within the scope of the two application scenarios within this thesis in Chapter 5 and Chapter 6 for the example of latent fingerprints.

Limitations

Selected Supporting Tools for Digitized Forensic

This chapter presents selected supporting tools for digitized forensics. In particular at first the three sensors available for the evaluations are formalized using the scheme introduced in Section 3.2. Afterward, particular challenges that arise from the concept of digitized forensics, as summarized in Section 3.3, are addressed by an approach for ensuring the authenticity of the digitized traces as well as a benchmarking framework for supporting the strategic preparation. This chapter is structured as follows:

4.1	Analysis of Available Sensory for the Evaluation of Digitized Forensics in the Context of Latent Fingerprints	72
4.1.1	S_1 Chromatic White Light Sensors	72
4.1.2	S_2 Confocal Laser Scanning Microscope	73
4.1.3	S_3 UV-VIS Reflection Spectrometer	74
4.2	Linking Digital Trace Representations to the Physical Trace	75
4.2.1	Processing steps during the physical acquisition at the scene of crime	75
4.2.2	Processing steps during the operational preparation	77
4.2.3	Processing steps during the data gathering	78
4.2.4	Processing steps during the trace storage	80
4.3	Benchmarking Framework for Pattern Recognition Based Approaches on the Example of Fingerprint Forgery Detection	81
4.3.1	Analysis of Potential Artifacts within the Fingerprint Forgery Processing Pipeline	82
4.3.2	Synthetic Simulation of Artifacts with the novel StirTrace Framework	84
4.3.2.1	Simulation of Noise	84
4.3.2.2	Simulation of Smudging Artifacts	85
4.3.2.3	Simulation of Distortions	86
4.3.2.4	Simulation of Artifacts Originating from the Digitization Process	87
4.3.2.5	Simulation of Substrate Artifacts	90
4.4	Chapter Summary and Limitations	91

\mathcal{Q}_2 : Novel
Challenges, \mathcal{Q}_3 :
Sensor
Requirements

The analysis of the properties of the sensory in Section 4.1 is an important foundation for answering research question \mathcal{Q}_3 and for the selection of the appropriate sensory for the two application scenarios in Chapter 5 and Chapter 6. Such an analysis is an important step during the strategic preparation in order to assess the capabilities of a forensic laboratory. Afterward, the issue of ensuring the authenticity of the digitized traces as a part of research question \mathcal{Q}_2 is addressed in Section 4.2. A particular benchmarking approach within the scope of research question \mathcal{Q}_2 , focusing on the application scenario in Chapter 6, is introduced as a supporting tool for the strategic preparation in Section 4.3.

The contents of this chapter have been peer reviewed and published in part within the scope of the following publications as joint work with the co-authors Jana Dittmann and Stefan Kiltz (in descending order of the frequency of co-authorship): [HKD13b], [HiD15a], [HiD14] and [HiD16].

4.1 Analysis of Available Sensory for the Evaluation of Digitized Forensics in the Context of Latent Fingerprints

Formal
Description of
Available Sensors

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DS
DO						

Three different sensors are available within the scope of this thesis for the evaluation of digitized forensics in the context of latent fingerprints:

- S_1 Chromatic White Light Sensor (FRT CWL600/1mm [FRT14a] mounted in a FRT MicroProf 200 [FRT12]),
- S_2 Confocal Laser Scanning Microscope (Keyence VK-X110 [KEY20]),
- S_3 UV-VIS Reflection Spectrometer (FRT FTR [FRT14b] mounted in a FRT MicroProf 200)

Each of the sensors is described in detail in the following subsections in order to allow for discussing the sensor selection in Section 5.3.1 and Section 6.3.1.

4.1.1 S_1 Chromatic White Light Sensors

A Chromatic White Light Sensor (CWL) as described in Section 2.3.1.1 is a combination of two sensors based on the definition for sensors in Section 3.2:

1. A topography sensor S_{1T} measuring the distance between lens and the substrate,
2. An intensity sensor S_{1I} measuring the highest peak in the spectrum of the reflected light.

Since both sensors are point sensors, a motorized measurement stage is necessary in order to acquire image data. Such a motorized measurement stage is one of the key components of the FRT MicroProf 200 measurement device. During the digitization process the object is moved underneath the sensor by the measurement stage allowing for digitizing arbitrary areas of the substrate. The measurement stage is controlled by additional sensory in order to ensure an exact positioning. The movement speed of the measurement stage depends on

the properties of the substrate. Since the sensor needs to be able to detect the highest peak in the reflected spectrum reliably, a certain amount of light must be captured, resulting in different substrate-dependent integration times. Any unsuitable integration time might cause unintended loss, affecting the digitized trace. Thus, the measurement frequency or speed is influenced by the substrate properties, e.g. how much light is reflected and how much light is scattered. In practice S_1 can digitize between 100 and 2000 measurement points per second. Based on the tuple items for the definition of sensors in Section A.2, S_{1T} is defined as follows: $S_{1T} = \{M_{2.2}, O_1, D_{Syntax_2}, D_{Semantics_3}\}$. In particular S_{1T} captures height maps ($D_{Semantics_3}$) of a substrate in the form of a two-dimensional array (D_{Syntax_2}) of 16 bit Integer values as a point sensor (O_1) utilizing a broad spectrum of visible light ($M_{2.2}$).

The definition of S_{1I} is very similar: $S_{1I} = \{M_{2.2}, O_1, D_{Syntax_2}, D_{Semantics_1}\}$. The only difference is the different semantics of the acquired sensor data. In the case of S_{1I} the data represents light intensity data ($D_{Semantics_1}$).

During the measurement process, the measurement stage is constantly moved underneath the sensor in order to allow for digitizing areas of the substrate. In the course of this process, an integration over a specific distance along the measurement direction is performed during the sensing process at resolutions below the native resolution of the respective sensor. Furthermore, particular measurement lines along the other lateral direction are skipped if such a lower resolution is selected.

As a result, using a lower acquisition resolution leads to a loss of additional information because specific areas of the substrate are not digitized. The effect is comparable to an interlaced image considering only one of the half images.

Furthermore, an inappropriate setting of the measurement frequency might lead to an over- or underexposure of the embedded spectrometer. This, can result in a loss of information or, in less severe cases, in an increased level of noise within the digitized data.

4.1.2 S_2 Confocal Laser Scanning Microscope

The Keyence VK-X110 [KEY20] is equipped with four different objective lenses as described in Section 2.3.2. Each objective lens has a specific scan area and resulting scan resolution. Additionally, a motorized measurement stage allows for digitizing larger areas using multiple scans. However, the stitched images are not homogeneous due to the diversion of the laser beam and the resulting non-perpendicular measurement throughout one single scanned image. With respect to the sensor definition in Section 3.2, the Keyence VK-x110 confocal laser scanning microscope (CLSM) can be considered as a combination of three sensors:

1. A topography sensor S_{2T} measuring the distance between objective lens and the substrate,
2. An intensity sensor S_{2I} measuring the measured intensity of the reflected light,
3. A color image sensor S_{2C} measuring a color image similar to a digital microscope.

Based on the tuple items for the definition of sensors in Section A.2, S_{2T} is defined as follows: $S_{2T} = \{M_1, O_3, D_{Syntax_2}, D_{Semantics_3}\}$. In particular S_{2T} captures

height maps ($D_{Semantics_3}$) of a substrate in the form of a two-dimensional array (D_{Syntax_2}) of 32-bit Integer values as a de facto area-sensor (O_3) utilizing a monochromatic red (658 nm) laser (M_1).

The captured intensity image S_{2I} , recording the gathered light intensity $D_{Semantics_1}$, is defined as: $S_{2I} = \{M_1, O_3, D_{Syntax_2}, D_{Semantics_1}\}$. Similar to the topography data S_{2T} , D_{Syntax_2} is a two-dimensional array of 32 bit Integer values. The two images S_{2T} and S_{2I} are captured using the photomultiplier tube (PMT) detector of the CLSM. Thus, both images are perfectly aligned.

This is not necessarily the case for the color image I_C captured by the color image sensor S_{2C} . This particular sensor consists of a halogen lamp ($M_{2.2}$) and a color charge coupled device (CCD) camera as an area sensor (O_3) which shares a part of the optical path of the CLSM. As the digitization area is defined by the objective lens of the microscope, the image contents of I_C are more or less aligned with the other two images. However, a miscalibration of the Keyence VK-X110 might lead to a slight offset between the laser-based images and the camera image which might result in an unintended loss of information. The sensor S_{2C} is defined as follows: $S_{2C} = \{M_{2.2}, O_3, D_{Syntax_3}, D_{Semantics_2}\}$. The semantics ($D_{Semantics_2}$) of the three-dimensional image (D_{Syntax_3}) is a four-8-bit-channel two-dimensional red-green-blue (RGB) color image with an alpha channel.

During the measurement process, the measurement stage remains stationary whereas the objective lens is moved in order to digitize different focal planes. Depending on the depth of field of the objective lens and the parameterization of the CLSM (in particular the z-pitch defining the distance between two neighboring focal planes) some height information might be missed causing a loss of information.

4.1.3 S_3 UV-VIS Reflection Spectrometer

The UV-VIS reflection spectrometer S_3 in the form of the FRT FTR sensor [FRT14b] is an example of a hyper-spectral imaging device as described in Section 2.3.3. Based on the tuple items for the definition of sensors in Section A.2, S_3 is defined as follows: $S_3 = \{\{M_{2.1}, M_{2.2}, M_{2.3}\}, O_1, D_{Syntax_3}, D_{Semantics_5}\}$. The sensor uses two different light sources to emit UV radiation ($M_{2.1}$), visible light ($M_{2.2}$) and near infrared light ($M_{2.3}$). The spectrometer sensor is a point sensor (O_1) which captures a three-dimensional array of values by sequentially digitizing multiple points of the substrate (D_{Syntax_3}). The result of the measurement process is spectral data ($D_{Semantics_5}$) consisting of 2048 intensity images for different wavelengths. Thus, S_3 could be also considered as a set of 2048 intensity sensors measuring the intensity of one fixed wavelength of reflected light.

Similar to the CWL sensor in Section 4.1.1, the measurement stage needs to be moved during the digitization in order to digitize multiple points of the substrate. However, in contrast to the CWL sensor, the measurement stage is stationary for the duration of the measurement of a single measurement point. Afterward, the stage is moved to the next measurement point until all specified points have been digitized. Thus, any lateral acquisition resolution deviating from the native resolution of 10 pixels/mm result in measurement artifacts. If a lower acquisition resolution is selected, particular information of the substrate is not digitized, resulting in a loss within the digitized trace. In case of an acquisition resolution exceeding the native resolution of the sensor, the pixel values represent overlapping measurement points which can cause a blurred result. Such a, blurred result might be the cause for uncertainty in any of the following data investigation

or analysis steps.

Any inappropriate setting of integration time can cause increased levels of noise or even a complete loss of information.

4.2 Linking Digital Trace Representations to the Physical Trace

In traditional forensics the chain-of-custody (see Section 2.1.2.1) is used to ensure the authenticity and integrity of a trace. Each time a specific object is processed a log entry is created who had accessed the object at which point in time. Even though this does not prevent any tampering with evidence, this method at least creates significant challenges for evidence tampering in combination with organizational precautions. In the digital domain the integrity of data can be proven using cryptographic hash functions as implemented e.g. in [Gar09] for digital evidence or in [KVL11] for digitized evidence. However, this requires using secure hash algorithms, where it is computationally not feasible to find collisions for similar data. The same requirements are valid for digital signature algorithms for ensuring the authenticity of the data. In addition to that, a proper key management needs to be implemented allowing for verifying the signatures and preventing any misuse of the utilized cryptographic keys. Thus, both challenges could be considered as sufficiently addressed in spite of the constant requirement of evaluating the security of the utilized methods.

The research gap \mathcal{G}_2 (see Section 1.1) addressed within this thesis is the creation of a provable link between the physical object protected by a chain-of-custody and the digitized traces protected by cryptographic methods as summarized in Section 3.3.1. A solution for this gap is introduced in [HKD13b]. The basic idea is to ensure a machine-readability of the metadata of a trace and the digitization process as depicted in Figure 4.1. The following subsections describe the novel

Creation of a link between physical objects and digitized traces

SP	PA	OP	TP	TI	TA	DO	TS
							DS
DO							

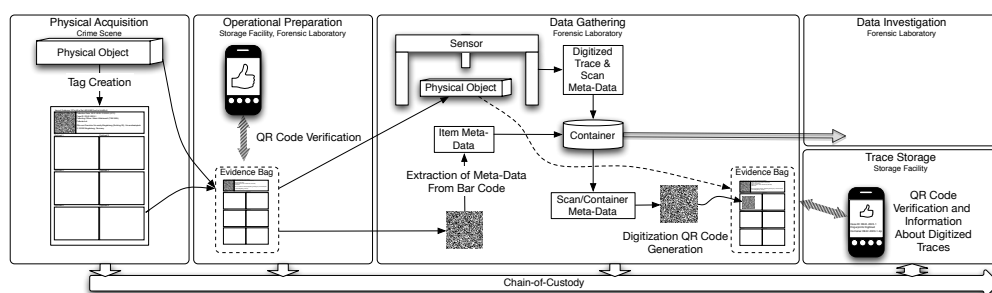


Figure 4.1: Concept for ensuring a provable integrity and authenticity of digitized traces resketched from [HKD13b], implementation of the container for digitized evidence can be based e.g. on [KVL11]

approach for the linking of digital trace representations to the physical trace based on [HKD13b] in detail.

4.2.1 Processing steps during the physical acquisition at the scene of crime

After potential traces are identified at the crime scene and their particular location is recorded, each item is collected for the transport to a trace storage facility, e.g. at the precinct. In addition to that, this step constitutes the starting point of the chain-of-custody. With the objective of creating machine-readable metadata for each trace, basically two options exist:

Additional steps during the physical acquisition

- Option a: assignment of an object ID, creation of a 2D bar code and storage of metadata in a central database,
- Option b: creation of a metadata record, embedding of the data in a quick response (QR) [Int06] or similar high-capacity bar code and placement of the bar code inside of the sealed evidence bag.

Option a has the advantage that almost no modification in the current process of evidence handling is necessary since usually object IDs are already assigned. However, all following digitization efforts need to be amended to the record stored in the central database. In addition to that, the database entry should be created from the crime scene in order have the metadata readily available when the seized object arrives at the initial storage facility.

Option b places essential metadata in a machine-readable form within the sealed evidence bag. If this evidence bag is transparent, the QR could be visible through the bag and could be verified without unsealing and opening the bag. Nevertheless, the seized objects need to be recorded separately as well in order to avoid the risk of misplacing evidence.

Selected Option

Within the scope of this thesis option b is selected as a suitable approach for ensuring the integrity and authenticity because it can be utilized even without access to the central database. In the case of transparent evidence bags the authenticity can be established on the foundation of the sealed bag and the validity of the metadata.

After all items are identified at the crime scene, a record containing the metadata needs to be created. The compilation of the metadata within the scope of the suggested approach is illustrated in Figure 4.2. The gathered set

The screenshot shows a software window titled 'Form1' with three tabs: 'Test', 'General', and 'Digitization'. The 'Digitization' tab is selected. The form contains the following fields and values:

- Case ID: DE42-2020-1
- Collecting Officer: Mario Hildebrandt
- Officer ID: T0815MH
- Crime Scene Location: Otto-von-Guericke University Magdeburg (Building 29), Universitaetsplatz 2.
- GPS Coordinates: 52.13938600;11.64533600
- Supplemental Images (e.g. Showing Item Location): IMG_3356.jpg
- Additional Notes: (empty)

At the bottom of the form is a 'Create Item' button. Below the button, the following information is displayed:


- Item ID: 9f9803f6-3c93-4774-b24d-23c417c44b1a
- Collection Date: 26.01.2020 13:55:38 (UTC)

Figure 4.2: Creation of the metadata record for an object of the crime scene based on [HKD13b]

of metadata consists of the case ID, the name of the officer responsible for the evidence collection, the ID of the officer, the location of the crime scene including GPS coordinates, an information about supplemental images and additional notes. After the information is entered, a universally unique identifier (UUID) is automatically assigned for each registered object. In addition to that, the collection date as the starting point of the chain-of-custody is recorded. Afterward, the evidence record should be printed and placed with the object itself within the sealed bag. This procedure ensures that the object and the corresponding metadata are authentic as long as the seal is intact.

An exemplary resulting evidence record for the placement within the evidence bag is depicted in Figure 4.3. The evidence record consists of a machine-readable

Item of Evidence: 2ff7a445-e7bd-4659-9663-ec5a144d96c9

	Collection Date: 26.01.2020 13:59:52 (UTC)
	Case ID: DE42-2020-1
	Collecting Officer: Mario Hildebrandt (T0815MH)
	Collected at:
	Otto-von-Guericke University Magdeburg (Building 29), Universitaetsplatz 2, 39106 Magdeburg, Germany

Digitized 1:

Digitized 2:

Figure 4.3: Creation of machine-readable metadata records based on [HKD13b]

and a human readable part. The human readable part contains the UUID of the item, the collection date, the case ID, the collecting officer and the collection location. The machine-readable part consists of a QR code containing an XML structure with the recorded metadata of the trace as depicted in Figure 4.4. In



Figure 4.4: Contents of the machine-readable metadata records based on [HKD13b]

addition to the UUID (TID), date (DATE), name of the collecting office (CO), officer ID (COID), location of the crime scene (Loc, GPS), supplemental images (IMG) and notes (NOTE), a base-64 encoded signature is stored within the QR code. In this example SHA256-RSA is used for the signature generation, however, specific algorithms should be chosen based on current recommendations e.g. from NIST SP 800-57 [Bar19].

4.2.2 Processing steps during the operational preparation

During the operational preparation as depicted in Figure 4.1, the authenticity of the object needs to be verified. This verification step is performed at least twice during the operational preparation. The first verification should be performed when the item arrives at the storage facility. The second verification should be performed when the item is transferred to the forensic laboratory. This ensures that the correct and authentic item is stored and forwarded for further processing.

Additional steps during the operational preparation

Additional verification steps might be necessary if the item is transferred, e.g. from one storage facility to a different one.

A transparent/see-through evidence bag allows for a verification without breaking the seal and should thus be the preferred option. An additional requirement for a successful verification of the trace is the management of the public keys for each potential collecting officer. This is necessary because the maximum capacity of the QR code prohibits storing the public key within it. Thus, it is necessary to prepare a list of the public keys corresponding to each officer ID during the phase of the strategic preparation. If this step is not performed, the authenticity of the item cannot be verified electronically until the key information is available.

In [HKD13b] the verification is performed using a mobile phone running a custom-made Android application. The application itself utilizes an external library for reading the contents of the QR code. Afterward, the XML structure is parsed in order to determine the collecting officer ID. Based on this ID the public key in form of an X.509 certificate is selected for the verification of the signature. In this simple example all potential public keys are stored within the app. However, in a more realistic use case probably the usage of external key servers is necessary in order to provide a certain level of flexibility. Subsequently, the contents of the XML structure as well as the result of the signature verification are displayed within the app.

4.2.3 Processing steps during the data gathering

Additional steps
during the data
gathering

Prior to unsealing the evidence bag in order to access the contained object for trace digitization, the authenticity of the object should be verified using the machine-readable QR code. Based on this information, all necessary metadata for the digitization of the trace can be automatically determined. When the authenticity has been successfully verified, the digitization process can be performed in order to acquire the detailed scans for further investigation. For that, the sample is placed on the measurement stage of the sensor. A virtual representation of the surface of the measurement stage of the FRT MicroProf 200 [FRT12] is depicted in Figure 4.5 within the purpose-built data gathering application DDPlusAcquire. DDPlusAcquire implements the steps of the fingerprint digitization including the concept of coarse scans for the localization of potential traces and the following detailed scans for the following data investigation and analysis as summarized in Section 5.1. The resulting files are stored in a storage container for digitized evidence [KVL11] which can store the digitized trace data as well as metadata about the current case and the digitization process. Ideally, the coarse scans are stored alongside the detailed scans as a means of documentation, e.g. regarding the position of a digitized trace in relation to other traces on the same object.

For such a digitization process a selection of metadata, as depicted in Figure 4.7, is recorded for a creation of an additional QR code allowing for identifying digital representations of the trace. Similar to the trace collection, the name (Tec) and the ID (TecID) of the forensic technician and optional notes (NOTE) are recorded. For quality assurance purposes the forensic laboratory (Lab) and the sensor ID (SenSer) performing the digitization should be recorded as well. The information about the sensor (Sen) serves an additional purpose because particular side-effects on concurrent traces on the same object could be determined based on this information. For example, a hypothetical sensor for the acquisition of latent fingerprints might use strong ultraviolet radiation – however, this type of radiation

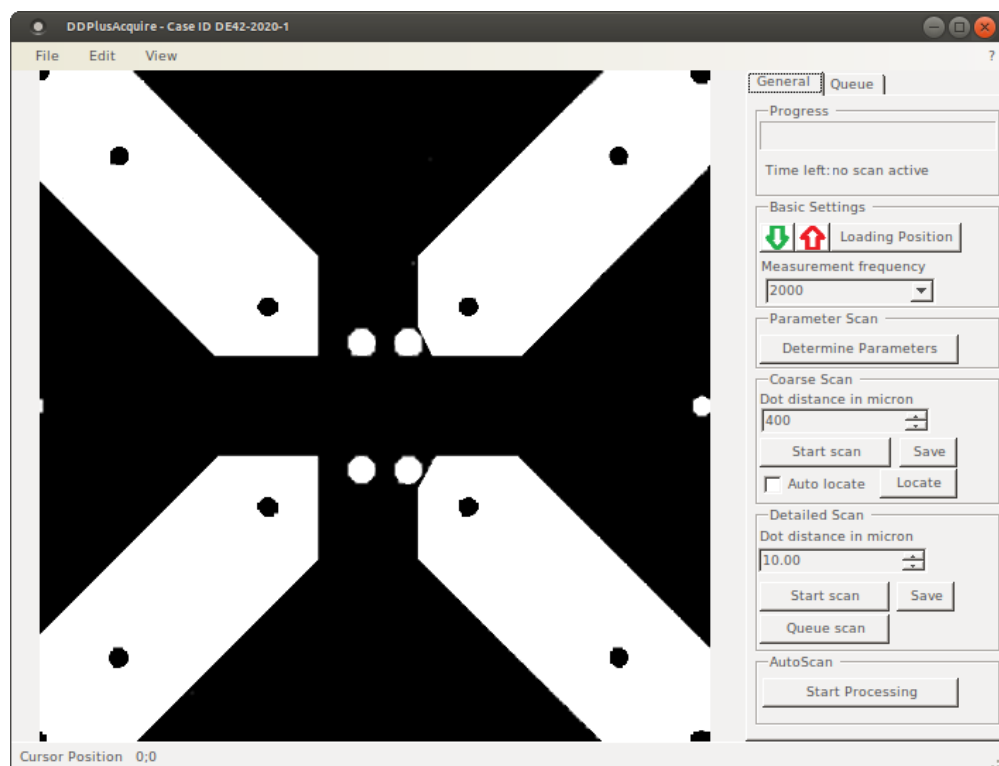


Figure 4.5: Trace Acquisition using DDPlusAcquire

Test	General	Digitization
Read Trace		
Acquisition Technician(s)		Case ID: DE42-2020-1
Mario Hildebrandt		Trace ID: 2ff7a445-e7bd-4659-9663-ec5a144d96c9
Technician ID		
T0815MH		
Forensic Laboratory		
ITI Research Group on Multimedia and Security		
Sensor		
FRT MicroProf200, CWL600		
Sensor Serial		
1279		
Container File		
DE42-2020-1.zip		
Acquired Traces		
Latent Fingerprints		
Additional Notes		
Create Item		

Figure 4.6: Metadata for trace digitization based on [HKD13b]

is known to destroy DNA. Thus, if a trace from that object has been digitized with such a sensor any subsequent acquisitions of DNA are likely impacted by this prior data gathering.

Additionally, information about the resulting data is recorded. In particular the type of acquired trace (Tr, e.g. latent fingerprints) and the storage container (Cont) - i.e. digital evidence bag - based on [KVL11] is recorded. In the case of the container format from [KVL11], the container UUID (CoID) is automatically recorded. The QR code does also contain the UUID from the physical object

(TID) and the date of the digitization (DATE). Subsequently, a digital signature for the XML record is calculated. The resulting QR code can be printed on a sticker and placed on the evidence record sheet as illustrated in Figure 4.7. The updated evidence record sheet must be placed with the physical object again


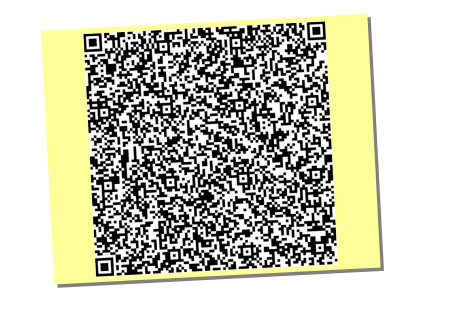


Item of Evidence: 2ff7a445-e7bd-4659-9663-ec5a144d96c9	
	Collection Date: 26.01.2020 13:59:52 (UTC) Case ID: DE42-2020-1 Collecting Officer: Mario Hildebrandt (T0815MH) Collected at: Otto-von-Guericke University Magdeburg (Building 29), Universitaetsplatz 2, 39106 Magdeburg, Germany
Digitized 1:	Digitized 2:
	
Digitized 3:	Digitized 4:
	

Figure 4.7: Update of machine-readable metadata records based on [HKD13b]

before re-sealing the evidence bag. As a result, the physical object is accompanied by a record of all digitization processes and a basic set of information about the resulting digital evidence bags as well as the nature of the acquired data. This allows for a distinct identification of all digital representations of the physical object.

In order to create a distinct link from a digitized trace to the physical object it originates from, it is necessary to record the UUID of the physical object (TID) within the digital evidence bag. Thus, the origin of the digitized trace can be determined as long as the digital evidence bag allows for verifying the integrity and authenticity of the contained data.

4.2.4 Processing steps during the trace storage

The processing steps of during the trace storage are primarily limited to the verification of the authenticity and integrity of the physical object and the evidence bag containing it. For that, the physical integrity of the evidence bag needs to be verified in the first place. If the evidence bag is intact and the seal authentic, the QR code(s) of the contained evidence record can be scanned and authenticated based on its signatures.

However, besides the authentication of the evidence, it is also necessary to

Additional steps
during the trace
storage

document the storage conditions. This is necessary in order to explain any degradation of traces on the stored object.

4.3 Benchmarking Framework for Pattern Recognition Based Approaches on the Example of Fingerprint Forgery Detection

It is highly unlikely that a pattern recognition based approach works flawlessly without any errors. Thus, it is important to be aware of the factors that might lead to increased error rates of a classifier, which is also a requirement of the Daubert factor "known or potential rate of error" [DG01, p. 3]. In order to be able to systematically evaluate and benchmark forensic techniques it is necessary to create reproducible test conditions. The potential root causes of artifacts analyzed in Section 4.3.1 originate from events prior to and during the digitization in the course of the data gathering. Although data might be modified after the digitization as well, it should be possible to restart the investigation and analysis using an original copy of the sensor scan data. This is comparable to digital forensics, where the investigation should be performed on the foundation of copies of the original data sources.

In the case of supervised learning, as described in Section 2.4.3, the classifier applies the trained model in order to assign a class label. The training process depends on the training data - any bias within the training data will likely result in a biased model. Hence, it is important to use unbiased and ideally representative training data. Judging whether a set of data is representative can be very challenging in forensics due to the large number of potential influence factors. If the training data is not sufficiently representative, it is likely that the observed error rates increase during the application of the model within the forensic practice - i.e. the model is not robust enough or over-fitted to the training data.

In order to detect such issues in the models, or to determine the limits of the application of a model, benchmarking the classification performance is an important part of the strategic preparation of a forensic investigation. Based on the benchmarking results specific standards for utilizing the method could be derived, which is in line with the Daubert criteria of requiring and maintaining standards for the use of a method and regarding the known or potential rate of error [DG01, Table 5.2, p. 39].

In biometrics a similar approach is used by Uhl et al. [HUPU13] to simulate the impact of various acquisition conditions on the performance of various matching algorithms. The process of [HUPU13] utilizes the StirMark framework [PAK98] which is originally intended for evaluating the robustness of image watermarking algorithms. In order to benchmark the classifiers trained on the foundation of intensity data from contact-less sensory the idea in [HiD15a] is, similarly to [HUPU13], the simulation of various artifacts that might occur within the creation of fingerprint forgeries as described in Section 6.1.1 and the acquisition of the potentially malicious traces as described in Section 6.1.2. However, due to the nature of the digitized images, StirMark cannot be used directly because it is limited to a maximum of 8 bits per channel and is additionally limited in terms of the image size. Thus, in [HiD14] the relevant functionality is re-implemented, resulting in the StirTrace framework¹ as described in Section 4.3.2. The focus of

Benchmarking -
Strategic
Preparation

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

¹<https://sourceforge.net/projects/stirtrace/>

StirTrace [HiD16] are artifacts caused by the creation of the latent fingerprint forgery and by the digitization step during the data acquisition phase, since the resulting data represents the foundation for all following preprocessing and investigation steps as mentioned in Section 3.1.5. The additional design goal is the retention of the properties of the original scan data, in particular the bit depth and the overall value distribution, unless specified otherwise for the performed evaluation. Overall the primary intention of the StirTrace framework is the support of the evaluation of the forgery detection approach discussed within the second application scenario of this thesis in Chapter 6.

4.3.1 Analysis of Potential Artifacts within the Fingerprint Forgery Processing Pipeline

Sources of
Potential
Artifacts

The idea of a systematic simulation artifacts within the context of latent fingerprint forgeries is presented in [HiD14]. The first set of artifacts originates from the attack chain depicted in Figure 6.2 in Section 6.1.1. In theory all four steps of the latent fingerprint forgery creation pipeline can be the root cause for artifacts:

Artifacts
originating from
the latent
fingerprint
forgery creation

AS_1 Original sample source artifacts: Artifacts already contained in the source image for the creation of the latent fingerprint forgery,

AS_2 Sample processing artifacts: Artifacts originating from the digital preparation of the printing sample,

AS_3 Sample production artifacts: Artifacts originating from the creation of the latent fingerprint forgery based on the printing sample,

AS_4 Latent forgery sample placement artifacts: Artifacts caused by the placement of the latent fingerprint forgery at the crime scene.

In addition to the artifact sources based on the fingerprint forgery creation pipeline, the digitization process during the forensic investigation can result in other artifacts subsumed as AS_5 . The artifacts that can be commonly observed during the analysis of latent fingerprint forgeries originating from an ink-jet printer are summarized in Table 4.1. Based on [HiD14] specific artifacts originating from the latent fingerprint forgery creation process can be fingerprint patterns distorted due to the force applied on the formation of the source sample (AS_1 : AS_X , AS_Y). The applied force during the contact of the finger with the substrate causes the skin to stretch. In the case of a latent fingerprint as an original source sample, the fingerprint pattern could be inverted by a very high application force as well. However, under the assumption that the quality of the printing template is assessed by the forger, in practice the root causes for distortions are more likely the result of printer characteristics (AS_3). In particular, irregularities in the paper feed or the print head movement can lead to a stretching of the printed patterns (AS_X , A_{MC} , A_{ML}). In the case of a mobile, manually operated printer as mentioned in Section 6.1.1, an irregular movement speed of the printer can result in distorted printing results as well (AS_X , AS_Y). In addition to that, printing defects can influence the quality of the latent fingerprint forgery as a part of AS_3 . In the case of ink jet printers, clogged nozzles can result in areas of the substrate not covered by amino acid [HiD14] (A_{NP}). Such artifacts are known as banding artifacts in printer forensics as described e.g. in [Mik+05].

	Exemplary Root Cause	Artifact	Abbrev.	Potential Artifact Source					Overview of Potential Artifacts Influencing the Forgery Detection Performance
				AS_1	AS_2	AS_3	AS_4	AS_5	
Noise	Sensor Noise	Additive Gaussian Noise	A_{NG}	✓		✓		✓	
	Sensor Quantization Noise	Additive Uniform Noise	A_{NU}	✓		✓		✓	
	Measurement Defects	Additive Salt & Pepper Noise	A_{NSP}	✓	(✓)	✓	✓	✓	
Smudging	Smudge Fingerprint Source Sample	Smudging	A_S	✓	✓	✓	✓		
Distortions	Printing Defects	Missing Lines	A_{ML}	✓	✓	✓			
	Printing Defects	Missing Columns	A_{MC}	✓	✓	✓			
	Printing Defects	Stretching in X Direction	A_{SX}	✓	✓	✓			
	Printing Defects	Shearing in Y Direction	A_{SY}	✓	✓	✓			
	Printing Defects	Non-Printed Area	A_{NP}	✓	✓	✓			
Digitization	Object Rotation	Rotation	A_R					✓	
	Sensor Scan Area	Cropping	A_{CR}					✓	
	Sensor Resolution	Scaling	A_{SC}					✓	
	Object Tilting	Tilting	A_T					✓	
	Sensor Parameterization	Value Range	A_{VR}					✓	
	Sensor Quantization	Bit depth	A_B					✓	
Substrate	Object Surface	Texture	A_{TX}				✓	✓	

Table 4.1: Potential Artifact Sources based on [HiD15a] and [HiD16]- ✓ denotes that a particular artifact can be caused during the specific phase of the latent fingerprint forgery creation pipeline ($AS_1 - AS_4$) or the subsequent trace digitization (AS_5)

Smudgy fingerprint patterns (A_S) could result from the original sample, the following processing or the printing process (AS_1 , AS_2 , AS_3). If the forged fingerprint sample is placed at the crime scene before the artificial sweat has properly dried, additionally the placement process could cause smudging artifacts caused by merging amino acid dots on the substrate (AS_4).

Artifacts from
the Digitization
Process within
the Data
Gathering

Artifacts caused within AS_5 are the rotation of the sample (A_R), specific limitations of the scan area A_{CR} , gradients of the sample due to non-perpendicular measurements (A_T) as described in [HiD16] and specific noise either caused by the substrate or the residue in conjunction with a specific sensor (A_{NG} , A_{NU} , A_{NSP}). Moreover, different sensor parameterizations can lead to different value ranges within the digitized data (A_{VR}) as well as different quantization steps (A_B). Subsequently, particular artifacts can originate from the substrate material from which the questioned fingerprint trace is digitized (A_{TX}). Such artifacts can be caused by either a specific texture or a structure of the substrate material.

4.3.2 Synthetic Simulation of Artifacts with the novel StirTrace Framework

The simulation of the artifacts identified in Section 4.3.1 is performed using commonly known image processing techniques. In particular the sensor data is modified using a multitude of filters which can either be applied separately or in combination. Overall, the intention is to create parameter ranges similar to StirMark [PAK98]. The following subsections describe the simulation of the identified artifacts in detail.

4.3.2.1 Simulation of Noise

The simulation of the sensor noise is performed by creating an image containing random noise matching the value range and properties of the source data originating from the sensor. In StirMark [PAK98] the degree of noise is defined by specifying noise levels. Larger values for the noise level indicate a more visible noise pattern within the resulting image. This behavior is similar in StirTrace [HiD14].

4.3.2.1.1 Simulation of Gaussian Noise

Gaussian noise A_{NG} can occur due to external influences on the sensor. Overall, it can be expected that the noise will affect single values, but will not change the overall characteristics of the resulting scan data significantly. Thus, for the simulation of Gaussian noise a mean of zero is used. The standard deviation is determined based on the value range in [HiD14]. This approach differs from [PAK98] due to the requirement to deal with bit depth exceeding 8 bits per pixel. In StirTrace the standard deviation of a single-channel image I with the target noise level L_N is determined by Equation 4.1 [HiD15a]. The functions $min(I)$ and $max(I)$ return the global minimum and maximum pixel value.

$$\sigma = 2 \cdot L_N \cdot \frac{max(I) - min(I)}{100.0} \quad (4.1)$$

Essentially, the noise level is a multiplier for the standard deviation σ of the resulting noise pattern. Based on the dimensions and data type of the input image I a noise image I_{NG} is generated with $\mu = 0$ and σ from Equation 4.1. Subsequently, the resulting additive Gaussian noise image I_{ANG} is generated by creating the pixel-wise sum of both images: $I_{ANG} = I + I_{NG}$. From a mathematical point of view, this is the addition of two matrices with the same dimensions.

4.3.2.1.2 Simulation of Uniform Noise

Uniform noise A_{NU} is a common result of the quantization during the digitization of an object within the phase of the data gathering. Within a uniform noise image I_{NU} all values are equally distributed - i.e. within the histogram of the image all values are observed with a near-identical frequency. In StirTrace the value range for I_{NU} is determined based on the value range $[P_{min}, P_{max}]$ of the input image I and the specified noise level L_N [HiD15a]:

$$P_{min} = -1 \cdot L_N \cdot \frac{\max(I) - (\min(I))}{50.0} \quad (4.2)$$

$$P_{max} = L_N \cdot \frac{\max(I) - (\min(I))}{50.0} \quad (4.3)$$

Afterward a noise image I_{NU} is created with the same dimensions as I and equally distributed values in the interval $[P_{min}, P_{max}]$. Subsequently, the resulting additive Uniform noise image $I_{A_{NU}}$ is generated by creating the pixel-wise sum of both images: $I_{A_{NU}} = I + I_{NU}$

4.3.2.1.3 Simulation of Salt&Pepper Noise

In the context of latent fingerprint digitization Salt&Pepper noise A_{NSP} can be observed within the resulting image data from optical sensors. Due to the optical effects of the fingerprint residue, the beam of light which is utilized within the measurement technique can be deflected leading to erroneous results such as scattered zero-value pixels. Besides the fingerprint residue, particular substrate properties might cause similar noise patterns of very low or very high pixel values. The Salt&Pepper noise generation is derived from a uniform distributed random number generator r with a value interval $[-0.5, 0.5]$. Within the scope of this thesis, the Salt&Pepper noise image $I_{A_{NSP}}$ is generated using the following equation [HiD15a]:

$$\begin{aligned} \forall I_{x,y} &\in I \in n \times m; n, m \in \mathbb{N} : \\ I_{A_{NSP_{x,y}}} &= \begin{cases} \min(I) & \text{if } r > -(0.5 - \frac{L_N}{200.0}) \\ \max(I) & \text{if } r < (0.5 - \frac{L_N}{200.0}) \\ I_{x,y} & \text{otherwise} \end{cases} \end{aligned} \quad (4.4)$$

A pixel $I_{x,y}$ of the input image I is replaced with the global minimum $\min(I)$ or maximum $\max(I)$ pixel value of the image within $I_{A_{NSP}}$ if the random number exceeds a threshold defined by L_N . Otherwise, the pixel value remains unaltered. Thus, the overall value range of the image is not altered by applying the additive Salt&Pepper noise. In practice Salt&Pepper noise can create global extreme values. However, such values depend on the data type of I . Furthermore, a particular sensor might not utilize the full value range of a data type. Thus, using a standard Salt&Pepper noise approach might lead to unrealistic values in the simulated data.

4.3.2.2 Simulation of Smudging Artifacts

Smudging artifacts A_S can be caused at various stages of the creation, processing, handling and analysis of latent fingerprint forgeries as mentioned in Section 4.3.1. The simulation of smudging artifacts using median cut filtering is proposed in [HUPU13]. In [HiD14] the median cut filtering is implemented using a median

blur filter where the level of filtering L_M specifies the neighborhood size for the median filter. With a neighborhood size of $L_M = 3$, each pixel $I_{x,y}$ of an image I and its 8-connected neighborhood are used for determining the median of the values replacing the pixel $I_{x,y}$ within I_{A_S} [HiD15a]:

$$\begin{aligned} \forall I_{x,y} \in I & : I_{A_{S_{x,y}}} = \tilde{M}, \text{ with} \\ M = \bigcup I_{x \pm a, y \pm b}, \forall a, b & : 0 \leq a \leq L_M, 0 \leq b \leq L_M, L_M \in (2 \cdot n + 1), n \in \mathbb{N} \end{aligned} \quad (4.5)$$

In [HiD14] L_M must be an odd number of at least 3. Additionally, for larger bit depths L_M is limited to a maximum of 5 representing the 24-connected neighborhood of $I_{x,y}$.

4.3.2.3 Simulation of Distortions

Distortion artifacts are mainly originating from the latent forgery creation process as summarized in Table 4.1. In theory, artifacts can be caused by sensor defects or a improper sensor parameterization as well. However, in such a case a sample can be digitized again. Furthermore, any defect of a properly calibrated sensor should be discovered rather quickly. Thus, the probability of such distortions originating from the digitization process can be considered nearly zero. The following paragraphs describe how the distortion artifacts A_{ML} , A_{MC} , A_{SX} , A_{SY} and A_{NP} are simulated within StirTrace.

4.3.2.3.1 Simulation of Missing Lines and Columns

Missing lines A_{ML} or columns A_{MC} can be caused by the printer when either the paper feed (usually lines) or the print head (usually columns) is not properly moved during the printing process. In addition to that particular root causes can originate from the fingerprint source sample acquisition and its preparation for the generation of the printing sample.

The simulation of missing lines or columns is rather simple with a sensor image I being considered as an $m \times n$ matrix, a missing line or column is basically the deletion of rows or columns of I . As the result the aspect ratio of an image I is altered by this function $f : I \mapsto I'$. In order to simulate missing lines, the following function is defined whereas L_F defines the frequency of omitted lines of I within $I_{A_{ML}}$. The artifact of missing lines A_{ML} is simulated based on the following definition with R_n being the n -th row of the matrix I [HiD15a]:

$$f : (\forall R_n \in I \forall n \bmod L_F \neq 0) \mapsto R_n \in I_{A_{ML}} \quad (4.6)$$

Similar to that, the artifact of missing columns A_{MC} is simulated based on the following definition with C_m being the m -th column of the matrix I [HiD15a]:

$$f : (\forall C_m \in I \forall m \bmod L_F \neq 0) \mapsto C_m \in I_{A_{MC}} \quad (4.7)$$

4.3.2.3.2 Simulation of Stretching in X Direction

The simulation of the stretching of the fingerprint forgery is performed using an affine transformation. The transformation to create the stretched image $I_{A_{SX}}$ is performed using a matrix multiplication of the input image I with a 2×3 matrix with L_X being the parameter influencing the stretching factor [HiD15a]:

$$I_{A_{SX}} = I \begin{bmatrix} L_X & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad (4.8)$$

The stretching in X direction can be used to simulate any kind of distorted aspect ratio of the original sample and the following processing steps for the creation of the latent fingerprint forgery. However, a quality assurance process of the forger should in practice avoid such distortions. Thus, primarily defects of the printer or the printer driver would cause such artifacts.

4.3.2.3.3 Simulation of Shearing in Y Direction

Similar to the stretching of a sample, a shearing of the sample could be simulated using an affine transformation. Shearing in Y direction describes a vertical shift of columns of an image I . The sheared image I_{ASY} is created with the following equation in which L_Y specifies the magnitude of the stretching effect [HiD15a]:

$$I_{ASY} = I \begin{bmatrix} 1 & 0 & 0 \\ L_Y & 1 & 0 \end{bmatrix} \quad (4.9)$$

Shearing artifacts are rarer in comparison to stretching. Besides potential errors during the acquisition and processing of the original fingerprint source sample, primarily printer driver errors or incompatibilities with the printing sample might cause such artifacts.

4.3.2.3.4 Simulation of Non Printed Areas

Non-printed areas primarily originate from printing defects such as clogged nozzles of the print head. Since the printer is used with artificial sweat with different chemical and physical properties in comparison to the original equipment manufacturer ink, such defects are rather likely. Due to the nature of the artificial sweat, there is a good chance that the forger will not identify such artifacts. The frequency and position of banding artifacts is specified using a probabilistic approach in which L_{NP} defines the probability of banding artifacts to occur. Non-printed areas or banding artifacts are simulated by replacing larger areas of the digitized sample with the median intensity value \tilde{I} of an image I [HiD15a]:

$$\forall I_y \in I \in n \times m, y \in m : \quad (4.10)$$

$$I_{ANP_y} = \begin{cases} \tilde{I} & \text{if } r \geq 1.0 - L_{NP}, r \in [0.0, 1.0] \forall r : P(r) = P(r') \\ \tilde{I} & \text{if } \exists I_{ANP_{y-n}} = \tilde{I} \wedge n < 50 \wedge I_{ANP_{y-50}} \neq \tilde{I} \\ I_y & \text{otherwise} \end{cases}$$

The random value r follows a uniform distribution within the interval $[0.0, 1.0]$. The first line of each banding artifact in I_{ANP} is determined on the foundation of the random value r . The median intensity value is chosen under the assumption that more than half of the pixels of I are not covered by artificial sweat. As a result, the median value will represent an intensity value of the substrate. Each banding artifact has an assumed height of $50\mu m$. Thus, if a line contains a banding artifact, all subsequent lines of a $50\mu m$ block also contain the median value \tilde{I} .

4.3.2.4 Simulation of Artifacts Originating from the Digitization Process

Artifacts originating from the digitization process can be expected to occur frequently because the specific influences causing the artifacts are hard to avoid. Thus, a simulation of those artifacts is very important as a part of a systematic evaluation of a novel forensic method.

4.3.2.4.1 Simulation of Object Rotation

The rotation of the physical sample usually cannot be perfectly aligned with the rotation of the sample during the printing process of the latent fingerprint forgery. The rotated image I_{A_R} is derived from the image I using an affine transformation with the parameter L_ϕ specifying the rotation angle [HiD15a]:

$$I_{A_R} = I \begin{bmatrix} \cos L_\phi & \sin L_\phi \\ -\sin L_\phi & \cos L_\phi \end{bmatrix} \quad (4.11)$$

However, the simulation of rotation artifacts A_R is only an estimation of an actually rotated sample, due to the quantization during the digitization process an image rotation with arbitrary rotation angles. Thus, I_{A_R} eventually contains interpolated intensity values instead of intensity values that originate from a different quantization of the same object during the data gathering, unless the rotation angle is a multiple of 90 degrees. Nevertheless, the sample rotation reflects a very important influence factor with respect to the feature spaces measuring horizontal and vertical dot distances motivated by the printing process.

4.3.2.4.2 Simulation of Scan Resolutions/Scaling

Analyzing the impact of the scan resolution is important in benchmarking different sensors and methods since most of the sensory to be utilized in digitized forensics can be parameterized in terms of particular digitization resolutions. In [HiD15a] the scaling of an image I is implemented using the following function with the scaling factor L_S :

$$\begin{aligned} I &\mapsto I_{A_{SC}}, \text{ with} \\ I &\in n \times m, I_{A_{SC}} \in n' \times m' : n \neq n', m \neq m', \frac{n}{n'} = \frac{m}{m'} \\ n' &= n \cdot L_S \\ m' &= m \cdot L_S \end{aligned} \quad (4.12)$$

In particular the interpolation is performed using the Lanczos interpolation over 8x8 pixel neighborhood [BB08, pp. 402 – 404].

4.3.2.4.3 Simulation of Scan Areas/Cropping

The simulation of the scan area is important for simulating the impact of fixed-area sensors such as microscopes. With such sensors, the objective lens dictates the size of the acquired area during the data gathering phase. In [HiD15a] an image I is cropped using the cropping factor L_C as follows:

$$\forall I_{x,y} \in I \in n \times m : I_{A_{CR,x,y}} = \begin{cases} \emptyset & \text{if } x < \frac{L_C \cdot n}{2} \\ \emptyset & \text{if } x > n - \frac{L_C \cdot n}{2} \\ \emptyset & \text{if } y < \frac{L_C \cdot m}{2} \\ \emptyset & \text{if } y > m - \frac{L_C \cdot m}{2} \\ I_{x,y} & \text{otherwise} \end{cases} \quad (4.13)$$

The resulting image $I_{A_{CR}}$ retains the aspect ratio of I whereas a certain number of pixels is discarded. With microscopes in mind, such an approach is reasonable because the size and resolution of the detector remains the same. The alteration of the optic path is altered by using different objective lenses, thus an increase of the spatial resolution results in a decreased scan area.

4.3.2.4.4 Simulation of Tilted Samples

With high resolution sensory in digitized forensics it is unlikely that an object can be digitized using a perfect perpendicular measurement. For a device capable of measuring axial resolutions in the nanometer range, even a slightest misplacement, e.g. caused by dust particles, can cause a gradient within the resulting scan data. Thus, in [HiD16] the tilting of an image I is simulated by a matrix addition with the tilted plane image I_{Tilt} of the same dimensions $m \times n$. The image I_{Tilt} is calculated on the foundation of the three parameters a, b and c specifying a plane in the image space. The parameters a and b describe the spacial gradients, whereas c influences an axial shift of the values [HiD16]:

$$\forall 0 < x \leq m, \forall 0 < y \leq n : I_{Tilt_{x,y}} = a \cdot x + b \cdot y + c \quad (4.14)$$

The tilted image I_{AT} is subsequently determined based on the following matrix addition:

$$I_{AT} = I + I_{Tilt} \quad (4.15)$$

For the simulation it is essential to know the peculiarities of the sensor and its specific properties in order to determine plausible parameters for a, b and c. Such a filter can also be used to benchmark preprocessing filters which are supposed to compensate such gradients within the sensor data [HiD16].

4.3.2.4.5 Simulation of Shifted Value Ranges

The simulation of shifted value ranges is necessary if a sensor produces measurement-distance-dependent results. In [HiD16] the image I_{AVR} with shifted value ranges is determined by adding a fixed value c to each pixel of the input image I :

$$\forall 0 < x \leq m, \forall 0 < y \leq n : I_{AVR_{x,y}} = I_{x,y} + c \quad (4.16)$$

Similar to the simulation of tilted sample, it is necessary to be aware of specific sensor properties that should be simulated.

4.3.2.4.6 Simulation of Acquisition Sensor Quantization

The acquisition sensor quantization is an important property of sensors utilized for the digitization of the samples during the data gathering phase. Whereas in the context of photography eight bit per pixel (and channel) are pretty common, various sensors might have different value ranges. In the case of the CWL sensor S_1 the intensity values are captured with a resolution of 12 bits which is stored within a 16-bit data type. The CLSM S_2 stores the intensity data within a 32-bit data type with a utilized value range depending on the sensor parameterization. Thus, in order to evaluate the sensor-dependency of a particular pattern recognition based model, it can be useful to project the data to another quantization bit depth. In [HiD16] the projection is performed on the foundation of the observed value range within an image I and a target bit depth of L_B :

$$\begin{aligned} I &\mapsto I_{AB}, \text{ with} \\ I_{AB} &= \frac{I - \min(I)}{\max(I) - \min(I)} \cdot 2^{L_B} \end{aligned} \quad (4.17)$$

The resulting image I_{AB} utilizes the full value range of the specified bit depth without discarding the effect of local extrema.

4.3.2.5 Simulation of Substrate Artifacts

Specialized printers might allow for printing on arbitrary surfaces. Thus, not just smooth substrates that can be printed on by ordinary ink-jet printers might contain latent fingerprint forgeries. Since the surface characteristics are inevitably captured by sensors in digitized forensics, it is reasonable to simulate the influence of different substrates within StirTrace. In general, it can be postulated that any kind of residue on a substrate, including artificial sweat, changes the surface characteristics. For example on a smooth, highly reflective substrate residue will scatter some of the incoming light of an optical sensor causing the areas covered with residue to appear darker within the resulting image I . Similar to that, on rather rough substrate materials, the residue might smooth the substrate characteristics which can also result in a higher intensity of the reflected light. Overall an image I_{ATX} with a simulated texture is considered as the addition of the input image I and a substrate image I_S in [HiD16]:

$$I_{ATX} = I + I_S \quad (4.18)$$

In order to avoid causing a significant shift of the value ranges, it is reasonable to apply filters to I_S transforming this image into a zero-mean image. By doing this, the characteristics of I_S can be transferred into I_{ATX} while retaining the global statistical properties of I .

4.4 Chapter Summary and Limitations

In this chapter the sensory which is available for the two application scenarios in Chapter 5 and Chapter 6 is formalized in Section 4.1 based on the sensor definition introduced in Section 3.2. This establishes the foundation for addressing research question Q_3 within the scenario-specific scope. With respect to the research question Q_2 on novel challenges within the context of digitized forensics, an approach for ensuring the authenticity of the digitized traces is described in Section 4.2 and a benchmarking approach designed for pattern recognition based processing steps is introduced in Section 4.3. Both supporting tools address the objective O_2 of this thesis. The approach in Section 4.2 represents the contribution C_3 of this thesis, implementing a novel approach for the creation of a bijective link between a physical trace and its digital representations. The StirTrace benchmarking approach in Section 4.3 represents the contribution C_4 of this thesis, by allowing for systematically analyzing the influence of acquisition conditions, various distortions and defects on the classification performance of pattern recognition based detectors processing image data originating from contact-less sensory.

A limitation of the approach described in Section 4.2 is the need for an extra key management. In the current form the demonstrator app needs to contain the public keys of all involved persons which is hardly feasible for a practical application.

The relations of the contents of this chapter to the process model introduced in Section 3.1 are depicted in Figure 4.8. The formalization of the sensory in

Limitations

Relation to the
Process Model
for Digitized
Forensics

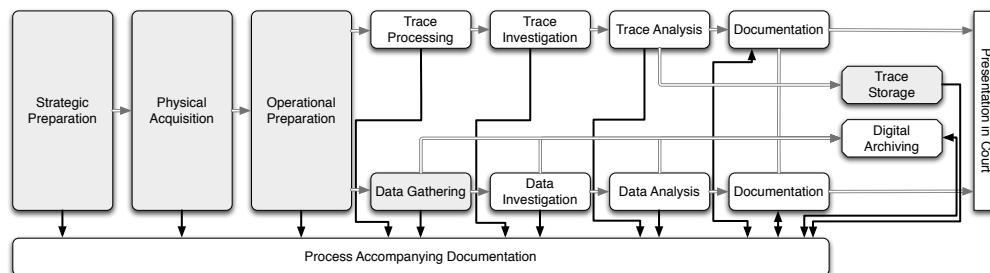


Figure 4.8: Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases Highlighted by Gray Shading are Addressed within this Chapter

Section 4.1 and the benchmarking approach in Section 4.3 address the phase of the strategic preparation by allowing for analyzing particular sensors and evaluating detection techniques. The approach for ensuring the authenticity of the digitized traces in Section 4.2 must be implemented within the strategic preparation in order to support the physical acquisition, the operational preparation, the data gathering and the trace storage.

Application Scenario 1: Segregation of Latent Fingerprint Data from Substrate Data

Forensics contains a multitude of different disciplines investigating different types of traces using different techniques requiring different expertise. Thus, within the scope of a thesis, light could only be shed on selected aspects of this broad variety of scientific fields. In particular, this thesis covers selected aspects within the scope the second most frequent type of trace evidence [McE10, p. 19, p. 60]: latent fingerprints. This chapter is structured as follows:

5.1	Fundamentals of Application Scenario 1: Coarse and Detailed Scans for the Contact-Less Acquisition of Latent Fingerprints	95
5.2	Feature Space Design and Labeling for Segregating Forensic Fingerprint Trace Evidence from Substrate Data	96
5.2.1	Feature Space for Segregating Forensic Fingerprint Trace Evidence from Substrate Data	99
5.2.1.1	Feature set 1 - Statistics Features	99
5.2.1.2	Feature set 2 - Structure Features	101
5.2.1.3	Feature Set 3 - Fingerprint Semantics Features	102
5.2.1.4	Feature Set 4 - Benford's Law-based Features	103
5.2.1.5	Feature Set 5 - Normalized Statistics Features	103
5.2.1.6	Sensor Data Preprocessing and Feature Extraction	104
5.2.2	Creation of Labeling Data	107
5.3	Segregation of Fingerprint Traces from Substrate Data	107
5.3.1	Selection of the Most Suitable Available Sensor for the Digitization of Latent Fingerprints	108
5.3.2	Experimental Setup for Evaluating the Segregation of Fingerprint Traces from Substrate Date	110
5.3.3	Results for the complete feature space in a two-class supervised learning approach	113
5.3.3.1	Cross-evaluation of the training data	113
5.3.3.2	Biometric evaluation of unlabeled data	119
5.4	Feature Selection	133

5.5 Chapter Summary and Limitations 136

Q_3 : Sensor Requirements,
 Q_4 : Latent Fingerprints in Digitized Forensics, Q_5 : Suitable Classification Scheme

The chapter introduces novel processing and handling techniques within the context of latent fingerprints in the digitized forensics process from Chapter 3 for validating the novel process model with trace-specific second-tier phases. This chapter deals with pattern recognition approaches for processing the signals of contact-less sensory in Section 5.3 addressing research question Q_3 . In particular a novel approach for segregating latent fingerprint data from substrate data in data originating from contact-less non-destructive sensory is introduced in Section 5.2, addressing research question Q_4 and Q_5 .

Particular sensors for digitizing latent fingerprints are necessary in order to achieve the goal of a non-destructive acquisition that does not interfere with the investigation of other traces. However, unless a specific sensor is available which will only detect fingerprint residue, the digitized data needs to be processed in order to localize and emphasize the fingerprint patterns. The sensors available within the scope of this thesis, namely a Chromatic White Light sensor (CWL, S_1), a Confocal Laser Scanning Microscope (CLSM, S_2) and a reflection spectrometer (FTR, S_3), inevitably sense substrate and fingerprint characteristics. Thus, novel processing pipelines for signal processing and pattern recognition are designed for those tasks in this thesis. In the following subsections the concept of coarse and detailed scans is discussed before particular classification schemes and feature spaces for the segregation of latent fingerprint patterns from the substrate data are elaborated.

As this application scenario is intended for the validation of the applicability of the process model introduced in Section 3.1, the processing steps need to be mapped to the first-tier phases of the model. The particularly involved phases are highlighted in Figure 5.1. In particular, the whole design and evaluation of the

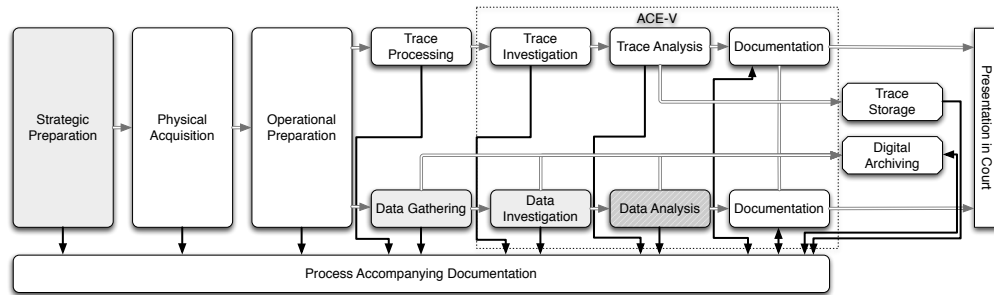


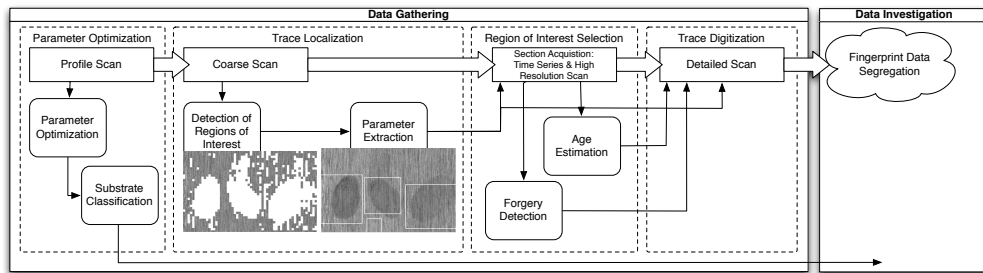
Figure 5.1: Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases Highlighted by Gray Shading are Addressed within this Chapter, Data Analysis is Hatched Because the Applied Evaluation is only an Approximation for a Latent Fingerprint Examiner

feature spaces can be considered as individual second-tier phases of the strategic preparation. The actual application of the designed approach is primarily a second-tier phase for the data investigation. In addition to that, second-tier phases of the data gathering are addressed in this chapter as well. The manual analysis and comparison of the fingerprint patterns as second-tier phases for the data analysis phase are approximated by utilizing a biometric matching algorithm. The contents of this chapter have been peer reviewed and published in part within the scope of the following publications as joint work with the co-authors Jana Dittmann, Claus Vielhauer, Stefan Kiltz, Ronny Merkel, Marcus Leich,

Andrey Makrushin, Robert Fischer, Tobias Kiertscher, Matthias Pocs, Michael Ulrich and Thomas Fries (in descending order of the frequency of co-authorship): [HDP+11], [HDV+11], [HDV13], [MHF+12], [HKD+14], [HML+11] and [HiD15a].

5.1 Fundamentals of Application Scenario 1: Coarse and Detailed Scans for the Contact-Less Acquisition of Latent Fingerprints

Within the scope of digitized forensics latent fingerprints should be located and acquired in a contact-less, non-destructive manner. This is important to allow for an acquisition using multiple sensors without risking side-effects. The main goal of the digitization is the acquisition of a detailed scan which represents the foundation for all further investigation and analysis steps. In order to determine and document the location of such detailed scans, low resolution coarse scans can be performed prior to the acquisition of the detailed scan. The overall concept consists of a multi-staged acquisition process [HDP+11] with several second-tier phases for the data gathering as depicted in Figure 5.2. At first the parameters



Acquisition Process during the Data Gathering Phase

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

Figure 5.2: Multi-staged acquisition process with second-tier phases based on [HDP+11] and [HDV+11]

for the acquisition process are optimized. This can potentially be performed on the foundation of a profile or line scan [HDV+11]. Since such scans are also performed for characterizing substrates based on roughness properties, this scan data would potentially allow for a first classification of the substrate material. During the second step potential latent fingerprints need to be detected. Ideally a large area could be analyzed in a very short time in order to detect all fingerprint traces. Within [HDP+11] a so-called coarse scan is suggested for the localization step. Within this thesis definition 5.1 is used for characterizing the properties of a coarse scan.

Definition 5.1: Coarse Scan based on [HDP+11]

A coarse scan is a low resolution scan intended for the localization of potential latent fingerprint locations on an object. The acquisition resolution of a coarse scan should be below 250 ppi to avoid any reliable extraction of features allowing for an identification or verification of the origin of the fingerprint pattern.

Definition of Coarse Scans

Besides the purpose of the coarse scan for the localization of potential latent fingerprint and the extraction of scan parameters for the detailed scan, it

serves another important function - it is a means of documentation allowing for determining the position of a trace on the object (circumstantial evidence) as well as the position in relation to other traces. Thus, additional evidential value could be derived from a coarse scan.

Prior to the acquisition of a full detailed scan additional investigations could be performed based on the acquisition of a small section of the localized latent fingerprint. One example for such an additional investigation is the age determination of the latent fingerprint [Mer14]. With such a step the amount of fingerprint evidence to be gathered could be minimized based on the time frame of the crime - i.e. very old or fresh traces could be excluded from the more time-consuming detailed acquisition. In addition to that, such an approach could minimize the privacy implications caused by the acquisition of all traces. Furthermore, the detection approach for latent fingerprint forgeries, as described in Chapter 6, might be utilized in order to exclude forged evidence before it is even captured with a more time-consuming detailed scan. However, this depends on particular requirements towards the forensic investigation which might still require the acquisition of such traces.

The detailed scan is the foundation for all following investigation and analysis steps in the digital domain. Thus, it is of utmost importance that the quality of the acquired data is as good as possible. Within the scope of this thesis the definition 5.2 for a detailed scan is used.

Definition 5.2: Detailed Scan based on [HDP+11]

A detailed scan is a high resolution scan intended for the extraction of unique features supporting an identification and verification of the origin of the fingerprint pattern. The acquisition resolution of a detailed scan should adhere to recent, widely accepted forensic standards. For the reliable extraction of level-3 fingerprint features the acquisition resolution should be at least 1000 ppi.

Definition of Detailed Scans

Such detailed scans are the foundation for all further experiments within the remainder of this chapter, as only those scans provide sufficient information for a forensic assessment of the traces based on biometric features.

5.2 Feature Space Design and Labeling for Segregating Forensic Fingerprint Trace Evidence from Substrate Data

Data Segregation

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DS
DO						

Conventional Image Processing

After potential latent fingerprints have been identified in coarse scans and acquired using detailed scans, it is important to segregate the fingerprint pattern from any other patterns that are inevitably captured by the sensor as well. Within the scope of this thesis a pattern recognition based approach is used for the segregation process. Alternatively, image processing techniques, such as the application of filters in the Fourier-domain (see e.g. [HJ04], [CCG07]) and Gabor filters (see e.g. [LYJ98], [Yan+03]), could be applied. Such methods are fairly common especially in the context of biometric systems. However, in the context of forensics any additional pattern with similar characteristics might be emphasized as well using such filters. The advantage of image processing is the lack of a need for any training phase. A filter can be applied directly on an image.

In addition to that, the parameters can be optimized in order to achieve better results. However, especially when the fingerprint pattern is hard to detect in the first place, it is challenging to verify that no additional features were created and no features were removed due to the application of the filter. While this concern is in general applicable to a pattern recognition based approach as well, it is mitigated by the need for an evaluation of the models and techniques in the first place. Thus, in line with the requirements of a Daubert challenge [DG01, pp. 1–4] "existence and maintenance of standards controlling the technique's operation" standards for the use of the method exist in terms of the models to apply or the parameterization of a classifier within a given feature space.

The design of the feature space and classification approach, including the training and/or evaluation is a part of the strategic preparation (see Section 3.1.2), whereas the final concept should be utilized within the phase of the data investigation (see Section 3.1.6). A pattern recognition based system can use the following learning strategies [DHS00, pp. 16–17], whereas the selected approach is marked in bold face:

- **Supervised Learning**,
- Unsupervised Learning,
- Reinforcement Learning.

Potential
Learning
Strategies

Overall the goal of the segregation of the fingerprint from the substrate is the subdivision of the scan data into at least two classes: fingerprint residue and substrate. However, due to the multitude of substrates and substrate properties the following classification schemes are possible, whereas the selected approach is marked in bold face:

- One Class (anomaly/outlier detection),
- **Two-Class** (per substrate: substrate/fingerprint on substrate),
- Multi-Class (all substrates: substrate/fingerprint on substrate).

Potential
Classification
Strategies

The Multi Class classification is considered not feasible within the scope of this thesis because only a selection of substrate materials is covered within the evaluation. The advantage of this approach would be a model that can be applied for latent fingerprints on all substrates. Substrate similarities can be used to classify unknown substrates as well. In addition to that, the analysis phase of the ACE-V model (see Section 2.1.1.1.2) can be supported by providing the latent print examiner a tentative list of potential substrate properties influencing the latent fingerprint. However, with any new substrate material the entire model of a supervised learning-based approach needs to be retrained which is very time-consuming. In the case of unsupervised learning a definition of multiple classes or clusters could lead to uncertainty, if the substrate material is more or less homogeneous. However, in the case of complex or composite substrates, a specification of more than two clusters might be beneficial. On the other hand, a deep knowledge about the trace and substrate properties, as well as the clustering algorithm is necessary in order to select appropriate parameters. As a result, the definition and maintenance of standards as required e.g. by the Daubert

Multi-Class
Classification

factors [DG01, pp. 1–4], would be hardly possible. With a reinforcement learning based approach, the classifier gets feedback whether the decision was correct or incorrect. In theory, such an approach can be used for the segregation of fingerprint data from the substrate as well. However, similar to the supervised learning a labeling of the data is necessary in order to provide this kind of feedback to the classifier.

Two-Class Classification

The one-class and two-class classification approaches are considered feasible within the scope of this thesis. Since the fingerprint pattern should be segregated from the background, it is self-evident that a two-class approach is reasonable. Here, in [HDV13] and [MHF+12] one class or one cluster represents the fingerprint residue whereas the second class represents the substrate and other contaminants, such as dust. Thus, a two-class classification approach is equally suitable for supervised and unsupervised learning. In particular, the two-class supervised learning based approach is evaluated in Section 5.3.3.

One Class Classification

The third option is the training of a one class classifier. Such a classifier could either be trained on fingerprint residue or on substrate data without fingerprints. The advantage of the training on the foundation of fingerprint data is that the classifier should in theory be substrate-independent because any feature vector that is not covered by the model for fingerprint residue would be considered as an outlier and thus, could be discarded. However, since the fingerprint residue usually interacts with porous and non-smooth substrates and additionally differs between multiple fingerprints even of the same person, a rather large collection of labeled fingerprint residue feature vectors is necessary. Additionally, for all substrates an accurate ground truth for the regions covered with fingerprint residue is necessary. Thus, in practice, creating a model for fingerprint residue is hardly feasible. If the classifier is trained on specific substrate materials, all deviations from the trained model can be considered as a contaminant such as fingerprint residue. The training of such a model is rather simple, because specific substrate samples can be digitized in order to extract the training data. The advantage of this approach is the independence of a ground truth labeling. However, the forensic expert must apply the correct model for a substrate to detect the correct outliers. In order to resolve this issue, reference objects without traces could be gathered at the crime scene as well. This would allow for training a model for the exact same substrate. The disadvantage of the one-class-classifier for substrates is that any contaminant is likely to be detected as an outlier. Thus, not only the fingerprint residue but also dust particles and other substances are likely to be detected.

Deep Learning

Besides the usage of hand-crafted features which are explored in this thesis, deep learning methods, such as [LFK18], [EB17], are utilized for the enhancement of latent fingerprints by other researchers. Typically, the evaluations are performed on the foundation of the, currently due to a lack of documentation withdrawn, NIST special database 27¹, which contains conventionally acquired latent fingerprint images. Deep learning is not considered within the scope of this thesis because the decision-making process of the classifier is significantly harder to explain in comparison to conventional learning strategies. With respect to a potential Daubert challenge [DG01, pp. 1–4] it is however necessary to explain the method in detail including the residual risks. However, combinations of different machine learning approaches such as learning classifier systems with deep learning components, see e.g. [Mat+16], might be suitable to solve this conflict of interest between the effort for designing the feature-space, classification performance and

¹<https://www.nist.gov/itl/iad/image-group/nist-special-database-2727a>

explainability to laymen in the future.

Overall all learning based approaches depend on the training data being representative for the expected data in real use-cases. Thus, in case of an evaluation of such a method for its admission in court, it is necessary to investigate all the residual risks originating from the acquisition, feature extraction and classification. The segregation approach can be considered as an identification step of the forensic investigation with respect to [IR00, pp. 43 – 61]. However, in order to evaluate the performance of the segregation, a biometric matching must be performed which constitutes an individualization.

5.2.1 Feature Space for Segregating Forensic Fingerprint Trace Evidence from Substrate Data

Feature Space

Hildebrandt et al. [HDV13] introduces three general feature sets for the segregation of latent fingerprint data from surface data. In addition to that, a feature set consisting of normalized statistics features is introduced within the scope of this thesis. The general concept is a non-overlapping-block-based approach using blocks $B \subset I$ with a size of $50\mu m \times 50\mu m$, corresponding to $n \times n = 5 \times 5$ pixels $B_{i,j}$ at a scan resolution of 2540 ppi. The features are extracted for every available source image I as well as preprocessed images derived from I . In addition to that, an extension of the feature set is introduced in [HKD+14]. This particular feature set employs a selected subset of the conventional image processing based fingerprint pattern enhancement (see Section 5.2) to derive features expressing the semantics of the data related to fingerprints.

5.2.1.1 Feature set 1 - Statistics Features

Statistics

The statistics features FS_1 utilize simple key figures that are also used e.g. for determining the roughness of a surface. Since fingerprint residue alters the substrate properties, areas covered with fingerprint residue will likely show different characteristics in comparison to the substrate itself.

The minimum value describes the local minimum in a block B_k of an image I :

$$B_{k_{min}} = \min(B_k); \quad B_k \in B \quad (5.1)$$

This particular feature can be useful on homogeneous, well reflecting substrates where fingerprint residue scatters some light and thus, results in a lower intensity in comparison to the substrate material.

The maximum value describes the local maximum in a block B_k of an image I :

$$B_{k_{max}} = \max(B_k); \quad B_k \in B \quad (5.2)$$

This feature can be useful for smooth substrates where fingerprint residue can be sensed on top of the substrate material within topography data.

The difference of $B_{k_{min}}$ and $B_{k_{max}}$ describes the span of values of a block B_k within an image I :

$$B_{k_{span}} = B_{k_{max}} - B_{k_{min}} \quad (5.3)$$

On smooth substrates an increased span of values could indicate any kind of contaminant. However, if the complete block B_k is covered with the contaminant, such as fingerprint residue, the value span could be quite small as well.

The average intensity of a block B_k is represented by the arithmetic mean:

$$\overline{B_k} = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n B_{i,j}; \quad B_{i,j} \in B_k \in B \quad (5.4)$$

Blocks which are almost entirely covered with fingerprint residue should show intensities deviating from the intensities of the homogeneous substrate. Thus, in theory the average intensity is a good indicator for a fingerprint as long as the sensor is able to detect any differences during the digitization phase.

Since the arithmetic mean can be significantly influenced by outliers, e.g. measurement errors, additionally the median value \widetilde{B}_k of the block B_k is determined. In a homogeneous block, \widetilde{B}_k and \overline{B}_k should be very similar. However, in the case of measurement errors \widetilde{B}_k should represent a more stable feature because half of the pixels will have a lower intensity whereas the other half will have a higher intensity than the median value.

Assuming that the sensor data is Gaussian distributed within a block B_k , the distribution of values might indicate some characteristics of the substrate or the fingerprint residue as well. Such features are also used to characterize the surface roughness [Bhu01, pp. 59–60], being summarized as features characterizing the shape of the probability density function. However, in the roughness measurement usually a profile line instead of an area is used as the foundation for the feature extraction. Within the scope of this thesis the second (variance), third (skewness) and fourth (kurtosis) moments of the values in each block B_k are suggested as features for the segregation of fingerprint residue from substrate data. The variance of the values within B_k is determined using the following equation:

$$Var(B_k) = \frac{1}{n^2 - 1} \sum_{i=1}^n \sum_{j=1}^n \left(B_{k_{i,j}} - \overline{B}_k \right)^2 \quad (5.5)$$

If the data is symmetrically distributed, the skewness $v(B_k)$, as determined with the following equation, should be zero:

$$v(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \left(\frac{B_{k_{i,j}} - \overline{B}_k}{\sigma} \right)^3 \quad (5.6)$$

When the values in a block are not symmetrically distributed, the resulting skewness value is either positive or negative with its absolute value indicating the degree of the skewness. The kurtosis $w(B_k)$ of block B_k is a measure for the pointedness or bluntness [Bhu01, p. 60] of the distribution function:

$$w(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \left(\frac{B_{k_{i,j}} - \overline{B}_k}{\sigma} \right)^4 \quad (5.7)$$

Similar to those image moments, the Mean Squared Error $MSE(\overline{B}_k)$ of block B_k is an indicator for the distribution of values in comparison to the mean intensity value \overline{B}_k :

$$MSE(\overline{B}_k) = \left(\frac{\sigma}{n} \right)^2 = \left(\frac{\left(\frac{\sum_{i=1}^n \sum_{j=1}^n (B_{k_{i,j}} - \overline{B}_k)^2}{n^2} \right)}{n} \right)^2 \quad (5.8)$$

Subsequently, the entropy of a block B_k is determined as a statistical feature in [HDV13]:

$$\begin{aligned} ENT(B_k) &= \sum_{h=1}^{n^2} -t_h \cdot \log_2 t_h, \text{ with} \\ t_h &= \frac{H(B_k|t)}{n^2} \end{aligned} \quad (5.9)$$

Here, the function $H(B_k|t)$ determines the histogram of specific values t within the block B_k , as a result t_h represents a bucket of the histogram. In a very homogeneous block only one distinct value might be observed, whereas in heterogeneous blocks each value might be represented only once.

5.2.1.2 Feature set 2 - Structure Features

Structure

The structure features FS_2 from [HDV13] are designed to express local structures within a block B_k . The features within this feature set, with the exception of the Hu moments [Hu62], are motivated by Haar-like features, see e.g. [LM02], from object detection.

The first two features determine the covariance between the upper and lower half as well as the left and right half of a block B_k :

$$Cov_{UL}(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^{\frac{1}{2}n} (B_{k_{i,j}} - \overline{B_{kU}})(B_{k_{i,(j+\frac{n}{2})}} - \overline{B_{kL}}) \quad (5.10)$$

$$Cov_{LR}(B_k) = \frac{1}{n^2} \sum_{i=1}^{\frac{1}{2}n} \sum_{j=1}^n (B_{k_{i,j}} - \overline{B_{kL}})(B_{k_{(i+\frac{n}{2}),j}} - \overline{B_{kR}}) \quad (5.11)$$

In the case of an odd number for n , the corresponding center line is not a part of the calculation. The variables $\overline{B_{kU}}$ and $\overline{B_{kL}}$ in Equation 5.10 are the mean intensity values of the upper and lower half of the block B_k , whereas $\overline{B_{kL}}$ and $\overline{B_{kR}}$ in Equation 5.11 represent the mean intensity values of the left and right half of B_k .

Specific textures, such as horizontal and vertical lines within an image I , are modeled within the line and column variance $LV(B_k)$, $CV(B_k)$ and covariance $LCV(B_k)$, $CCV(B_k)$ of a block B_k .

$$LV(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (B_{k_{i,j}} - \overline{B_{k_j}})(B_{k_{i,j+1}} - \overline{B_{k_j}}) \quad (5.12)$$

$$CV(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (B_{k_{i,j}} - \overline{B_{k_i}})(B_{k_{i+1,j}} - \overline{B_{k_i}}) \quad (5.13)$$

$$LCV(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (B_{k_{i,j}} - \overline{B_{k_j}})(B_{k_{i,j+1}} - \overline{B_{k_{(j+1) \bmod n}}}) \quad (5.14)$$

$$CCV(B_k) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (B_{k_{i,j}} - \overline{B_{k_i}})(B_{k_{i+1,j}} - \overline{B_{k_{(i+1) \bmod n}}}) \quad (5.15)$$

Such texture patterns are likely caused by a substrate property, e.g. the brush marks on brushed metal. However, fingerprint residue might cover those patterns and thus, alter the magnitude of the feature value.

All those structure features are rotation-dependent. Thus, if an object is placed differently than within the training data, the classification results might be unexpected. In order to account for this potential shortcoming, the rotation invariant Hu moments [Hu62] of a block B_k are additionally used within the feature space in [HKD+14]. The Hu moments are extracted in a multi-staged

process. At first the spatial image moments are determined for every block B_k [Ope20a] within the image I :

$$m_{ji} = \sum_{x=1}^n \sum_{y=1}^n (x^j y^i B_{k_{x,y}}) \quad (5.16)$$

Here, n determines the block size (in case of 2540 ppi scan images: $n = 5$), x and y represent the coordinates of each pixel within B_k and $i, j \in 0, 1, 2, 3$.

In the second step, the central moments are determined [Ope20a]:

$$mu_{ji} = \sum_{x=1}^n \sum_{y=1}^n ((x - \bar{x})^j (y - \bar{y})^i B_{k_{x,y}}) \quad (5.17)$$

where (\bar{x}, \bar{y}) describes the mass center of B_k : $\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}}$. Afterward, the normalized central moments are determined [Ope20a]:

$$nu_{ji} = \frac{mu_{ji}}{m_{00}^{((i+j)/2)+1}} \quad (5.18)$$

In the final step, the seven Hu moments are extracted as features [Hu62][Ope20a]:

$$\begin{aligned} hu_0 &= nu_{20} + nu_{02} \\ hu_1 &= (u_{20} - nu_{02})^2 + 4n_{11}^2 \\ hu_2 &= (nu_{30} - 3nu_{12})^2 + (3nu_{21} - nu_{03})^2 \\ hu_3 &= (nu_{30} + nu_{12})^2 + (nu_{21} + nu_{03})^2 \\ hu_4 &= (nu_{30} - 3nu_{12})(nu_{30} + nu_{12})[(nu_{30} + nu_{12})^2 - 3(nu_{21} + nu_{03})^2] \\ &\quad + (3nu_{21} - nu_{03})(nu_{21} + nu_{03})[3(nu_{30} + nu_{12})^2 - (nu_{21} + nu_{03})^2] \\ hu_5 &= (nu_{20} - nu_{02})[(nu_{30} + nu_{12})^2 - (nu_{21} + nu_{03})^2] + 4nu_{11}(nu_{30} + nu_{12})(nu_{21} + nu_{03}) \\ hu_6 &= (3nu_{21} - nu_{03})(nu_{21} + nu_{03})[3(nu_{30} + nu_{12})^2 - (nu_{21} + nu_{03})^2] \\ &\quad - (nu_{30} - 3nu_{12})(nu_{21} + nu_{03})[3(nu_{30} + nu_{12})^2 - (nu_{21} + nu_{03})^2] \end{aligned} \quad (5.19)$$

5.2.1.3 Feature Set 3 - Fingerprint Semantics Features

Semantics

The fingerprint semantics features FS_3 introduced in [HKD+14] are derived from standard fingerprint preprocessing techniques. In particular Gabor filters are often utilized to emphasize the ridge-valley-pattern of fingerprints within image data [Mal+09, pp. 135–140]. For the feature extraction a Gabor filter bank G_f with kernels using a step size of 11.25 degrees, resulting in $f \in [0, 15]$ is created, which is consistent with the step size for the orientation fields in [Wat+07, pp. 51–52]. This particular step size is selected because the evaluation is performed using NIST Biometric Image Software [Nat13] with the same step size. For other biometric algorithms, using different step sizes might be necessary. In addition to that, only one particular sinusoidal plane wave is used which potentially limits the application of the feature extraction to fingerprints with a similar frequency of the ridge-valley-pattern. Based on the Gabor filtering, two features are extracted in [HKD+14]: mean \bar{G}_k and standard deviation G_{σ_k} of the Gabor filtered block B_{kG} with the highest filter response. In particular, the standard deviation of the filtered block is used as an indicator for the maximum filter response. In order to be able to detect a ridge-valley-pattern within the image using the Gabor filter, the block size for those features is increased by a factor of 31 resulting in patches of $1550 \times 1550 \mu m$. Thus, for this feature set a sliding window approach of $50 \times 50 \mu m$ is used in order to maintain a semantically compatible feature space in comparison to the remaining features.

Limitations of the approach

At first, the maximum Gabor response for the block B_k is determined [HKD+14]:

$$G_{\sigma_k} = \max(B_{kG}) = \max(\text{Var}(G_f B_k)), \forall f \in [0, 15] \quad (5.20)$$

Besides the value for feature G_{σ_k} , the best-fitting orientation f is determined. This orientation is finally used to determine the average intensity value of the Gabor filtered block B_{kG} :

$$\overline{G_{kG}} = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n B_{kG_{i,j}} \quad (5.21)$$

In theory the value of $\overline{G_{kG}}$ should converge to a similar value range in areas covered with a fingerprint pattern due to the emphasized the ridge-valley-pattern.

5.2.1.4 Feature Set 4 - Benford's Law-based Features

Benford's Law

The fourth feature space FS_4 for the segregation of fingerprint data from the substrate data is motivated by Benford's law Distribution of most significant digits within a block [HDV13] (similar to [QZH10] for the DCT-coefficients of a JPEG compression). In particular the relative frequencies for the nine most significant digits d within a block B_k are determined as features:

$$NBL_d = \frac{H(B_k|d)}{n^2}, d \in [1, 9] \quad (5.22)$$

The function H determines the frequency of a specific digit d in B_k .

5.2.1.5 Feature Set 5 - Normalized Statistics Features

Normalized Statistics

In order to reduce the impact of the sensor parametrization, the minimum, maximum, span, median and average value features from the statistics feature set FS_1 from [HDV13] are normalized by either the mean value \bar{B} of a block B (local normalization) or the global mean value \bar{I} of the image I (global normalization). The first set of global mean normalized features is determined by dividing selected feature values from FS_1 by the global mean value \bar{I} :

$$\begin{aligned} B_{k_{min}normGrel} &= \frac{B_{k_{min}}}{\bar{I}} \\ B_{k_{max}normGrel} &= \frac{B_{k_{max}}}{\bar{I}} \\ B_{k_{span}normGrel} &= \frac{B_{k_{span}}}{\bar{I}} \\ \overline{B_{knormGrel}} &= \frac{\bar{B}_k}{\bar{I}} \\ \widetilde{B_{knormGrel}} &= \frac{\bar{B}_k}{\bar{I}} \end{aligned} \quad (5.23)$$

The motivation of this normalization is to express the value of the feature in relation to the entire data of the scan. Under the assumption that roughly half of the surface captured by a detailed scan is covered with fingerprint residue, the global average value \bar{I} should be in-between the values of fingerprint residue and the raw substrate material. Thus, the normalization should result in value ranges for the features which are almost independent of the substrate properties and the sensor parameterization.

The second set of global mean normalized features is determined by subtracting the global mean value \bar{I} from the feature value from FS_1 :

$$\begin{aligned} B_{kmin_{normGabs}} &= B_{kmin} - \bar{I} \\ B_{kmax_{normGabs}} &= B_{kmax} - \bar{I} \\ \widetilde{B_{knormGabs}} &= \widetilde{B_k} - \bar{I} \\ B_{knormGabs} &= \widetilde{B_k} - \bar{I} \end{aligned} \quad (5.24)$$

The span of values from FS_1 is not normalized because this feature already accounts for the specific substrate and parameterization properties. The results of the normalization is a global zero-mean normalization which is supposed to remove the impact of the substrate properties and the sensor parameterization from this feature space.

Besides the global normalization, a local normalization can be performed. This is reasonable for cases where a scan shows some sort of global gradients which influence the global mean value \bar{I} . The first locally normalized feature set is formed by dividing the feature value from FS_1 by the local average value of a block $\overline{B_k}$:

$$\begin{aligned} B_{kmin_{normLrel}} &= \frac{B_{kmin}}{\overline{B_k}} \\ B_{kmax_{normLrel}} &= \frac{B_{kmax}}{\overline{B_k}} \\ B_{kspan_{normLrel}} &= \frac{B_{kspan}}{\overline{B_k}} \\ \widetilde{B_{knormLrel}} &= \frac{\widetilde{B_k}}{\overline{B_k}} \end{aligned} \quad (5.25)$$

Here, the average value of the block is not normalized because the resulting feature would always have the value of 1. For the other features, the motivation is similar to the features summarized in Equation 5.23. In particular, the resulting features express by which extent the feature value deviates from the average value of the local block B_k .

The second locally normalized feature set is calculated by subtracting the local average value of a block $\overline{B_k}$ from the respective feature value:

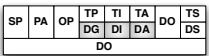
$$\begin{aligned} B_{kmin_{normLabs}} &= B_{kmin} - \overline{B_k} \\ B_{kmax_{normLabs}} &= B_{kmax} - \overline{B_k} \\ \widetilde{B_{knormLabs}} &= \widetilde{B_k} - \overline{B_k} \end{aligned} \quad (5.26)$$

In this local zero-mean normalization, the substrate and sensor parameterization influence is excluded. Similar to Equation 5.24 the span of values is exempt from the normalization because this particular feature can be considered as already normalized. In addition to that the average value is excluded because the resulting feature value would be always zero.

5.2.1.6 Sensor Data Preprocessing and Feature Extraction

Prior to the feature extraction the available sensor data, consisting of the intensity image I_I and the topography image I_T from the CWL sensor S_1 , is preprocessed in order emphasize particular properties of the fingerprint residue as introduced in [HDV13]. In particular various Sobel operators, as described e.g. in [Sze11, p. 104] and [Shi10, p. 57], are applied to the raw image data to highlight various gradients within the image. In addition to that, an unsharp masking $U(I)$ is applied to compensate global gradients throughout the image. The unsharp masking consists of a subtraction of a blurred version of the image I . The

Sensor Data
Processing
Pipeline



complete processing pipeline for the segregation of fingerprint and substrate data within the context of the introduced process model for digitized forensics from Section 3.1 and the signal processing pipeline from [Vie06, pp. 19–21] is illustrated in Figure 5.3. After the preprocessing of the raw sensor data, the features from the

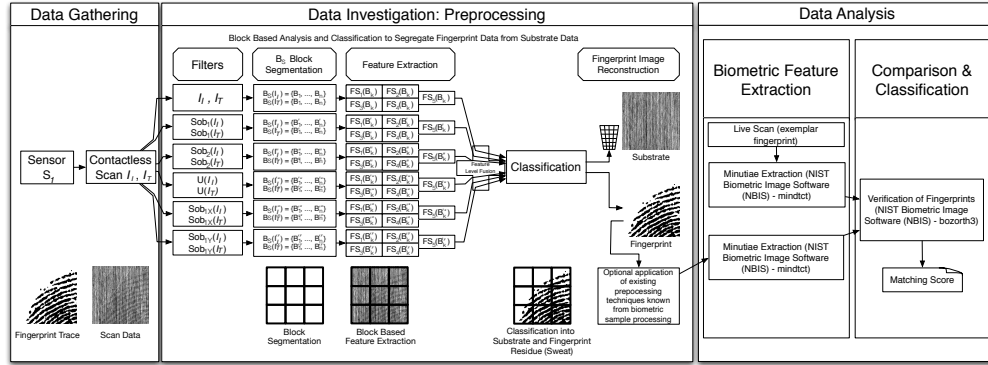


Figure 5.3: Latent Fingerprint Segregation Pipeline including Preprocessing Steps based on [HDV13] and [HKD+14] as Second-Tier Phases for the Data Gathering, Data Investigation and Data Analysis

previous paragraphs, as summarized in Table 5.1, are extracted for each resulting image. The final feature space is created by concatenating the set of features originating from each image. The set of images consists of the original intensity and topography images, the respective two-dimensional Sobel filtered images in first ($Sob_1(I)$) and second-order ($Sob_2(I)$), the first-order Sobel filtered images in X ($Sob_{1X}(I)$) and Y direction ($Sob_{1Y}(I)$) as well as the unsharp masked ($U(I)$) images. In total 12 images are used as the foundation for the extraction of the features from Table 5.1. Thus, a 600-dimensional feature vector is the result of the feature extraction within the data investigation phase.

This feature vector is then classified based on a trained model in order to decide whether a particular block of the acquired image contains fingerprint residue. Since the location of each block within the image I is known, it is possible to reconstruct a binary image on the foundation of the classifier’s decisions. Afterward, this image can be used by the latent fingerprint examiner for the analysis and comparison of the fingerprint pattern.

However, within the scope of this thesis an automated approach is used for the evaluation of the classification results. This is necessary to ensure reproducible evaluation results. Furthermore, the author of this thesis is no trained latent fingerprint examiner.

The evaluation is performed using the NIST Biometric Imaging Software [Nat13]. In particular mindtct is used to extract minutiae points from each reconstructed fingerprint as well as from the matching exemplar fingerprint captured by an optical live scanner. Afterward, Bozorth3 [Wat+08] is utilized to match the two fingerprint patterns within the verification mode. The limitation of this approach, in comparison to a manual comparison within the ACE-V process (see Section 2.1.1.1.2) by a latent fingerprint examiner, is the lack of flexibility regarding small differences between the two fingerprint patterns. Thus, it can be expected that the resulting matching rates indicate the lower bound of the performance of the proposed latent fingerprint pattern segregation technique. The advantage of this approach is the repeatability and reproducibility of the results, which

Feature Spaces from Preprocessed Images

Biometric Evaluation

	Feature	Number of Features	Definition
Feature Set 1 - Statistics Features	B_{min}	1	Equation 5.1
	B_{max}	1	Equation 5.2
	B_{span}	1	Equation 5.3
	$\overline{B_k}$	1	Equation 5.4
	$\widetilde{B_k}$	1	-
	$Var(B_k)$	1	Equation 5.5
	$v(B_k)$	1	Equation 5.6
	$w(B_k)$	1	Equation 5.7
	$MSE(B_k)$	1	Equation 5.8
	$ENT(B_k)$	1	Equation 5.9
Feature Set 2 - Structure Features	$Cov_{UL}(B_k)$	1	Equation 5.10
	$Cov_{LR}(B_k)$	1	Equation 5.11
	$LV(B_k)$	1	Equation 5.12
	$CV(B_k)$	1	Equation 5.13
	$LCV(B_k)$	1	Equation 5.14
	$CCV(B_k)$	1	Equation 5.15
Feature set 3 - Fingerprint Semantics Features	G_{σ_k}	1	Equation 5.20
	G_{kG}	1	Equation 5.21
Feature Set 4 - Benford's Law- based Features	NBL	9	Equation 5.22
Feature set 5 - Normalized Statistics Features	$B_{kminnormGrel}$	1	Equation 5.23
	$B_{kmaxnormGrel}$	1	Equation 5.23
	$B_{kspannormGrel}$	1	Equation 5.23
	$\overline{B_{knormGrel}}$	1	Equation 5.23
	$B_{knormGrel}$	1	Equation 5.23
	$B_{kminnormGabs}$	1	Equation 5.24
	$B_{kmaxnormGabs}$	1	Equation 5.24
	$\overline{B_{knormGabs}}$	1	Equation 5.24
	$B_{knormGabs}$	1	Equation 5.24
	$B_{kminnormLrel}$	1	Equation 5.25
	$B_{kmaxnormLrel}$	1	Equation 5.25
	$B_{kspannormLrel}$	1	Equation 5.25
	$B_{knormLrel}$	1	Equation 5.25
	$B_{kminnormLabs}$	1	Equation 5.26
	$B_{kmaxnormLabs}$	1	Equation 5.26
$B_{knormLabs}$	1	Equation 5.26	

Number of features for each image I: 50

Table 5.1: Combined Feature Space for each Image I based on [HDV13] and [HKD+14]

is not necessarily the case for the comparison carried out by human experts as summarized in Section 2.5.2.

5.2.2 Creation of Labeling Data

It is a necessity to gather ground truth data in order to create the labeling data for the two-class supervised learning approach. However, since a latent fingerprint cannot be accurately reproduced, the ground truth needs to be empirically determined. For that the differential scan approach from [HML+11] is utilized. Overall the question for the differential imaging is the nature of the interaction of the fingerprint residue with the substrate. In particular two different options are reasonable to assume:

- Additive relationship of the substrate and the fingerprint residue,
- Multiplicative relationship of the substrate and the fingerprint residue.

The additive relationship seems to be a reasonable assumption for non-porous substrates as the fingerprint residue is deposited on top of the substrate. Thus, within topography data, areas covered with fingerprint residue should appear closer to the sensor in comparison to the substrate. However, for the intensity data, such an assumption is hard to justify. The transparent fingerprint residue could act as an optical filter altering the signal response from the substrate which would likely be a form of a multiplicative relationship. On the other hand, light might be partially scattered and partially reflected from the surface of the fingerprint residue. If this is the case, the measured intensity value would be rather independent of the substrate properties. Thus, within the scope of this thesis an additive relationship is assumed for the topography and intensity data avoiding the need for two different differential imaging approaches.

The labeling data from the differential imaging approach is not necessarily accurate. Due to the image processing steps, including the binarization, some portions of the fingerprint might be labeled as background whereas some portions of the substrate might be labeled as fingerprint residue. Thus, for building models for an application in future forensic techniques, the validity of the labeling data should be confirmed. One potential approach for that is to treat the fingerprints with currently utilized means for the fingerprint enhancement, such as the fuming with Cyanoacrylate which is commonly known as super glue fuming. After photographing the enhanced trace, it would be possible to verify or improve the labeling data by comparing it to the scaled and aligned photo from the treated trace. Such an approach would be also suitable to verify the accuracy of the segregation of the trace from the substrate data. Nevertheless, the resulting patterns need to be aligned for the verification of the labeling data. However, due to the lack of such fuming equipment for the experiments in the scope of this thesis, such a verification remains future work.

5.3 Segregation of Fingerprint Traces from Substrate Data

The pattern recognition based segregation of fingerprint data from substrate data is evaluated within this section. The underlying raw data from the evaluation of the classifier as well as the biometric matching scores of successful segregation

Labeling Data
and Ground
Truth

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
			DO				

Potential Signal
Composition

Ground Truth
Approximation
using Differential
Imaging

attempts are included in Section A.3.

At first, the suitability of the available sensors is assessed in Section 5.3.1. Afterward, the experimental setup is described in Section 5.3.2. Subsequently, Section 5.3.3 contains the summary and discussion of the evaluation results for the pattern recognition based segregation of fingerprint data from substrate data.

5.3.1 Selection of the Most Suitable Available Sensor for the Digitization of Latent Fingerprints

Sensor Selection

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DO
						DS
						DO

In order to select the most suitable available sensor from Section 4.1, it is necessary to define particular requirements for the digitization of latent fingerprints. The following requirements should be met by a sensor for this use-case of digitized forensics:

1. General ability to acquire latent fingerprint residue,
2. Reproducible digitization results,
3. Possibility to automate the scan process,
4. Ability to perform coarse scans (resolution of less than 250 ppi / 10 pixels/mm),
5. Ability to perform detailed scans (resolution of at least 1000 ppi / 40 pixels/mm),
6. Possibility to acquire larger areas of a substrate within a coarse scan (at least 10 x 10 cm),
7. Reasonable scan duration for the acquisition of coarse and detailed scans.

The first requirement "general ability to acquire latent fingerprint residue" is an absolute necessity for a sensor in order to be applicable in digitized forensics. If the particular sensor is unable to detect any fingerprint residue, the sensor is unsuitable for gathering data for further analysis. The second requirement "reproducible digitization results" is also very important in forensics. However, the term reproducible is considered from a practical application and not from a scientific point of view, because all external influence factors and intrinsic noise cannot be avoided in a practical setup. Nevertheless, the essential information of the trace, i.e. the fingerprint pattern, must be accurately represented without any deviations from the ground truth of the physical trace. The third requirement "possibility to automate the scan process" is motivated by practical considerations. If an object contains multiple latent fingerprints, an automatic batch acquisition of all relevant substrate areas is advantageous. The fourth and fifth requirements "ability to perform coarse scans" and "ability to perform detailed scans" is motivated by the multi-staged digitization process described in Section 3.1.5 and Section 5.1. The sixth requirement "possibility to acquire larger areas of a substrate within a coarse scan", as well as the seventh requirement "reasonable scan duration for the acquisition of coarse and detailed scans", are motivated by practical considerations for the processing of various objects. The term "reasonable" implies that the overall processing time of an object containing traces should be comparable to currently utilized methods consisting of a preprocessing, potentially a dyeing process and some form of lifting

of the trace. The current processing duration with state-of-the-art techniques ranges from seconds to minutes in the case of the dusting with carbon powder to several hours or days for the utilization chemical agents.

The three available sensors are assessed regarding the requirements in Table 5.2. Depending on the substrate, the first requirement is fulfilled by all three sensors

	S_1	S_2	S_3
1. Latent Fingerprint Residue Acquirable	✓	✓	✓
2. Reproducible Results	✓	✓	✓
3. Process Automation	✓	(✓)	✓
4. Coarse Scans	✓	×	✓
5. Detailed Scans	✓	✓	×
6. Larger Scan Areas	✓	×	✓
7. Reasonable Scan Duration	○	○	×

Table 5.2: Comparison of the CWL (S_1), CLSM (S_2) and UV-VIS (S_3) Sensors Regarding the Requirements: ✓ Denotes a Fulfilled Requirement, ○ Is a Partially Fulfilled Requirement, × Indicates a Non-Fulfilled Requirement

as shown e.g. in [HKD+14] for S_1 , in [HiD15a] for S_2 and in [HMQ+13] for S_3 . All three sensors show reproducible results for the scan process, which is e.g. a necessity for determining aging tendencies in [Mer14].

The software of the FRT MicroProf 200 measurement device [FRT12] has a simple automation interface which is utilized by the DDPlusAcquire software described in Section 4.2.3. Thus, the scan process of the sensors S_1 and S_3 can be automated. For S_2 a simple automation is created within the scope of this thesis by means of wrapping the manufacturers .net control software for the CLSM by a custom-built application. However, this application is limited to the same set of acquisition parameters for multiple scans. Thus, the automation process cannot be fully customized.

The ability for coarse scans is only provided by S_1 and S_3 because the minimum resolution of S_2 is well in the region of detailed scans for latent fingerprints and cannot be further reduced during the digitization process. On the other hand, the ability for detailed scans is limited for S_3 because the native resolution is too low for such a scan. The sensors S_1 and S_2 can achieve sufficient resolutions for a biometric processing of the fingerprint patterns.

Larger scan areas can be acquired using S_1 and S_3 due to the properties of the FRT MicroProf 200. In particular the scan area is limited to 20 x 20 cm as summarized in Section 2.3.1.1. With the motorized measurement stage of S_2 in theory an acquisition of larger areas is also possible. However, due to the high resolutions of the resulting scans, the stitching process is usually computationally not feasible. The manufacturers stitching software is limited to a maximum of 560 scan images which results in a scan area of approximately 3.1 x 2.0 cm.

In terms of the reasonable scan duration the requirement is partially fulfilled by S_1 , as the scan process duration depends on the reflection properties of the substrate. The scan duration is acceptable for highly reflective substrates but on other substrates the acquisition of the same area with the same acquisition resolution results in a scan duration time increase by a factor of 20. The same limitation applies to S_3 . However, with identical acquisition resolutions the scan duration is approximately increased by a factor of 25 in comparison to S_1 . The

Purpose-Built
Sensor
Automation

Scan Area

Scan Duration

actual scan duration of S_2 significantly depends on the number of focal planes. In an ideal case, a scan of a latent fingerprint is as fast as with S_1 at a high acquisition resolution of 100 pixels/mm, but yielding a much higher resolution. However, as soon as the axial resolution and thus the number of focal planes is increased, the scan duration is significantly prolonged with S_2 .

Selected Sensor

The CWL sensor S_1 is selected for the evaluation of the latent fingerprint data segregation based on the assessment of those particular requirements. Given the available sensory, this particular sensor is considered the most suitable device for the digitization of the test samples within the data gathering phase in this thesis.

5.3.2 Experimental Setup for Evaluating the Segregation of Fingerprint Traces from Substrate Data

Experimental Setup

SP	PA	OP	TP	TI	TA	DO	TS	
			DG	DI	DA		DS	
			DO					

For evaluating the pattern recognition based segregation of fingerprint traces from substrate data, ten common substrate materials are used within the experimental setup, extending the eight substrate materials from [HKD+14]. The intention is to cover a broad range of porous, i.e. fingerprint-residue-absorbing, and non-porous substrates. Moreover, different surface structures and textures are represented within the evaluation as summarized in Table 5.3. In addition to the test samples summarized in Table 5.3, a set of 10 training samples is gathered for each substrate in a differential imaging approach to approximate the ground truth. The latent fingerprints in the test and training sets are created in so-called depletion series of ten fingerprints [DDB11]. In this procedure, the substrate is consecutively touched at different positions with the same finger. The result of this process is a decreasing amount and varying composition of the fingerprint residue forming the latent fingerprint. The resulting number of unique fingerprint patterns in the entire test set is too small for evaluating the biometric matching performance, but suitable for a forensic assessment of the traces using biometric matchers or manual verification. In order to cover some inter-person differences in the fingerprint residue composition, the fingerprints in the test set are collected from two or four different donors depending on the number of test samples for a particular substrate. For substrates with 50 test samples the latent fingerprints originate from two test subjects, whereas for substrates with 100 test samples four test subjects are involved. Furthermore, different fingerprint ages are covered due to the sequential digitization of the latent fingerprints. The test set size was chosen due to time constraints. The raw acquisition time is 119.5 days for the whole test and training data with a total of 900 scans using S_1 without taking any preparation of the samples into account. The average scan duration for a single sample in this setup is 3 hours, 11 minutes and 12 seconds.

Scan Duration

The fingerprints are applied with the help of a stencil mask placed on top of the substrate. This process allows for defining the scan areas for the detailed scans without visible fingerprint residue within the coarse scans as depicted in Figure 5.4 for M_8 . Each scan area is sized approximately 1.5 x 2.0 cm. Based on the coarse scan all fingerprints are manually selected and queued for the digitization as detailed scans with a resolution of 100 pixels/mm. The stencil mask is removed prior to the detailed scans in order to avoid artifacts within the resulting digitized latent fingerprints.

The acquisition of the training data differs slightly from this process. Due to the need for a ground truth, the training samples are acquired within a two-staged digitization process. At first the stencil mask is placed on top of the cleaned substrate on the measurement stage. After the coarse scan, ten positions are

Substrate	Abbrev.	Substrate Characteristics	Substrate Structure	Substrate Texture	Number of Test Samples	S_1 Measurement Frequency [Hz]
White Furniture Surface	M_1	Non-porous	Smooth	None	100	1000
Veneered Plywood (Beech)	M_2	Non-porous	Smooth	Textured	100	1000
Brushed Stainless Steel	M_3	Non-porous	Rough	None	100	1000
Aluminum Foil (Matte Side)	M_4	Non-porous	Rough	None	50	2000
“Golden-Oak” Veneer	M_5	Non-porous	Rough	Textured	50	1000
Non-metallic Matte Car Body Finish	M_6	Non-porous	Rough	None	50	1000
Metallic Car Body Finish	M_7	Non-porous	Multi-Layer	Metal Flakes	50	2000
Blued Metal	M_8	Porous	Rough	None	100	320
Ceramic Tile	M_9	Non-porous	Rough	None	50	1000
Copying Paper	M_{10}	Porous	Rough	None	50	320

Table 5.3: Substrate Materials and Number of Test Samples for the Segregation of Fingerprint Traces from Substrate Data

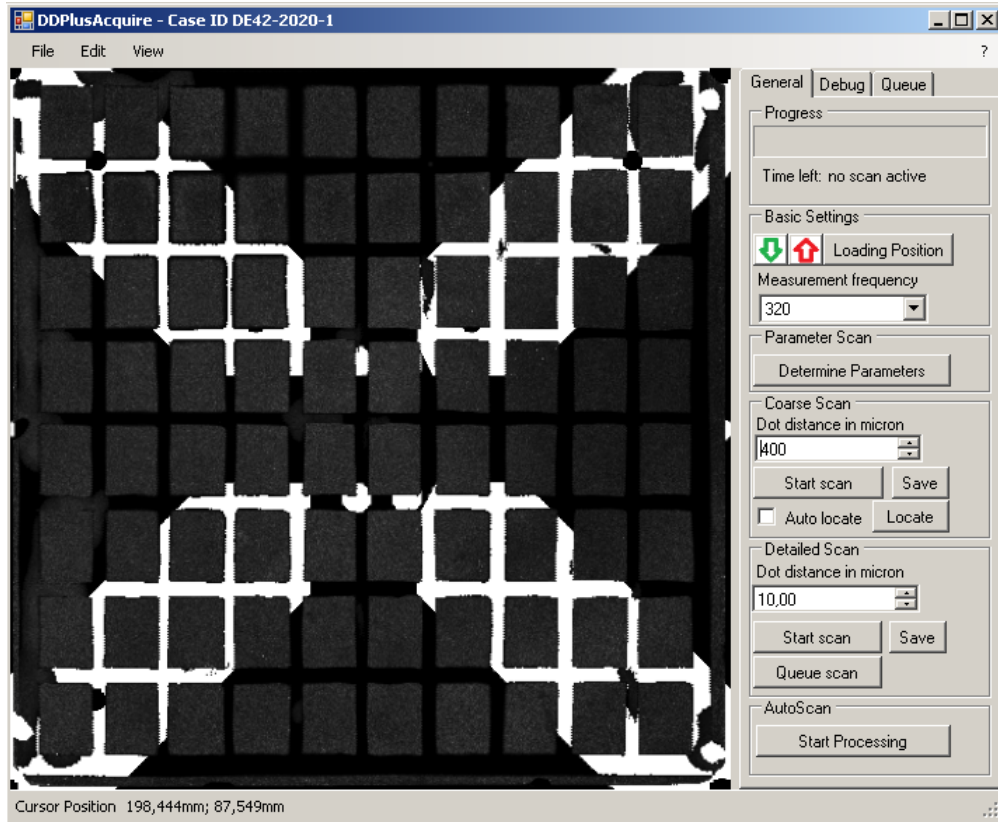


Figure 5.4: Coarse scan of blued metal M_8 with the stencil mask on top within DDPlusAcquire

selected for a detailed scan. The during the first digitization of detailed scans, each selected position does not contain any fingerprint residue or other contaminants. After the scans are completed, one depletion series of ten fingerprints is placed within the selected positions. Afterward, during the second digitization of detailed scans, the positions are scanned again. The area of each scan position is slightly smaller in comparison to the acquisition of the test samples because the stencil mask is not removed. Thus, each scan position must be defined within the respective bounding box of the stencil mask.

Ground Truth
Approximation

The ground truth for the labeling of the training data is created on the foundation of differential scans, as described in Section 5.2.2, by subtracting the scan prior to the deposition of the fingerprint residue from the scan with the fingerprint residue. Afterward, the resulting image is manually preprocessed and subsequently binarized for the extraction of the labels for each block.

Biometric
Evaluation

The classification results on the foundation of the test set are evaluated using the arbitrarily chosen biometric feature extraction and matching software NIST Biometric Image Software (NBIS) (version 4.0.1) [Nat13]. The reason for choosing this particular software suite is that it is available as free open source software which is suitable to determine a baseline performance. However, commercial fingerprint matching software might yield higher matching rates. The evaluation procedure is depicted in Figure 5.5. After the trace digitization, the block-based classification is performed using selected classifiers from the WEKA data mining software (version 3.6.6) [Hal+09]. In order to benchmark the classification results, the minutiae points (see Section 2.5.1) of the reconstructed fingerprint images

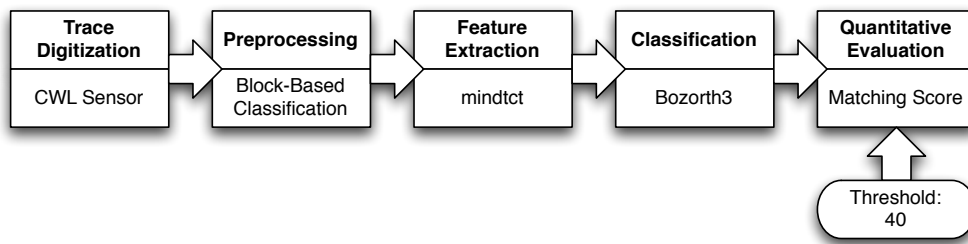


Figure 5.5: Biometric evaluation pipeline based on the biometric pipeline from [Vie06, pp. 19–21] as second-tier phases in digitized forensics for this application scenario

are extracted. Afterward, the biometric matcher Bozorth3 [Wat+08] is used in a verification setup to determine the matching scores based on one-to-one comparisons of a reconstructed fingerprint with the matching exemplar print captured using an optical Smith Heimann Biometrics live sensor (LS1 LITE-Xe) with an acquisition resolution of 500 ppi. This approach is necessary because the only available ground truth is the information about the finger which created a particular trace. There is no information about the amount of residue or the quality of the latent fingerprint. The biometric evaluation is performed using a threshold of 40 for the matching scores as suggested in [Wat+08, p. 21]. Any matching score of at least 40 is considered as a successful match and thus, a successful segregation of the fingerprint pattern from the substrate data.

5.3.3 Results for the complete feature space in a two-class supervised learning approach

The evaluation results for the two-class supervised learning based approach introduced in Section 5.2 are discussed in the following subsections. At first the raw classification performance is evaluated on the foundation of the labeled training set analogous to [HKD+14]. Afterward, deviating from the evaluation in [HKD+14], the non-labeled test set is evaluated using the biometric matching-based approach introduced in Section 5.3.2.

5.3.3.1 Cross-evaluation of the training data

The 2-fold cross validation of the classifiers for each substrate is performed to determine the error rates on the classifier level. This step is necessary since the data in the test sets is not labeled and thus, unsuitable for determining the raw classification performance. This evaluation step is a typical example for a task during the strategic preparation. As a result, the reliability of the classification approach for various substrates can be determined. The evaluation procedure using a 2-fold cross validation deviates from the evaluation process in [HKD+14]. In [HKD+14] two of the ten labeled samples are used for the training, whereas the remaining eight samples are used for testing. Thus, the number of training samples is significantly larger within the scope of this thesis. Nevertheless, the reported classification performance from [HKD+14] can be used for comparison with the achieved evaluation results in this thesis.

Based on the experiments in [HKD+14] the three classifiers SMO [Pla99], a Java implementation of a C4.5 decision tree [DHS00, p. 411] (J48) and Bagging [Bre96] from the WEKA data mining software (version 3.6.6) [Hal+09] are utilized. All

Cross Validation
of the Classifier

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DS	
DO							

classifiers are used with the standard settings within WEKA, without specifying any modified parameterizations. The training sets are equalized in terms of the number of instances for the two classes in order to avoid any bias within the trained models. As a result, the classification accuracy (see Section 2.4.1) is used to represent the performance of the classifiers.

5.3.3.1.1 Evaluation of Classification Performance on White Furniture Surface M_1

The white furniture surface is a smooth, non-porous, non-textured substrate material made of plastic. Due to those properties, it is considered as a rather cooperative material in terms of lifting latent fingerprint patterns from it. The evaluation of the classification performance for this particular substrate is summarized in Table 5.4. From the confusion matrices in Table 5.4 it can

	SMO		J48		Bagging	
Classification As:	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	446419	55081	451889	49611	462330	39170
Substrate (SM)	34574	466926	50609	450891	33068	468432
Accuracy [%]	91.0613		90.008		92.7978	

Table 5.4: 2-Fold Cross-Validation Results for White Furniture Substrate M_1 - Confusion Matrix and Classification Accuracy

be seen that the particular errors are roughly equally distributed for J48 and Bagging, whereas with the SMO classifier considerably more blocks containing fingerprint residue are misclassified as substrate material blocks. However, in terms of the accuracy the J48 classifier is outperformed by SMO. The best classification accuracy of 92.7978% is achieved using the Bagging ensemble classifier. In comparison to [HDV13], the classification performance is improved by 0.1 percent points for Bagging, but it decreased by 0.3 percent points for SMO and 0.9 percent points for J48. However, the classification performance of all classifiers is lower in comparison to [HKD+14]. The root cause for the difference can be either the different evaluation procedure or the extended feature space. Nevertheless, the classification performance can be considered as good for this particular substrate material.

5.3.3.1.2 Evaluation of Classification Performance on Veneered Plywood M_2

The veneered plywood substrate is a smooth, non-porous, but textured substrate material made of plastic. Due to those properties, it is considered as a slightly more challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The evaluation of the classification performance for this particular substrate is summarized in Table 5.5. The confusion matrices in Table 5.5 show that the errors are equally distributed within the J48 based evaluation. Using SMO and Bagging slightly more blocks with fingerprint residue are misclassified as substrate material blocks. The highest classification accuracy of 84.305% is achieved using the Bagging classifier followed by SMO (81.3138%) and J48 (79.4084%). In comparison to [HKD+14] and [HDV13], the classification achieves an improved accuracy for all evaluated classifiers.

Classification As:	SMO		J48		Bagging	
	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	365849	87394	360327	92916	379999	73244
Substrate (SM)	81994	371249	93744	359499	69029	384214
Accuracy [%]	81.3138		79.4084		84.305	

Table 5.5: 2-Fold Cross-Validation Results for Veneered Plywood M_2 - Confusion Matrix and Classification Accuracy

5.3.3.1.3 Evaluation of Classification Performance on Brushed Stainless Steel M_3

The brushed stainless steel substrate is a rough, non-porous, non-textured substrate material consisting of stainless steel. Due to those properties, it is considered as a moderately challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The surface structure likely has an impact on the deposition of fingerprint residue as well. The evaluation of the classification performance for this particular substrate is summarized in Table 5.6. From the confusion matrices in Table 5.6 it can

Classification As:	SMO		J48		Bagging	
	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	285571	91700	269338	107933	298070	79201
Substrate (SM)	93838	283433	108782	268489	86557	290714
Accuracy [%]	75.4105		71.2786		78.032	

Table 5.6: 2-Fold Cross-Validation Results for Brushed Stainless Steel M_3 - Confusion Matrix and Classification Accuracy

be seen that the particular errors are roughly equally distributed for SMO and J48, whereas the Bagging ensemble classifier detects more blocks containing no fingerprint residue as blocks with fingerprint residue. However, in terms of the accuracy the Bagging classifier performs best with an accuracy of 78.032%. The second-best result is achieved by the SMO classifier whereas the J48 performs almost seven percent points worse than the Bagging classifier. In comparison to [HKD+14], the classification performance is lower for all evaluated classifiers. On the other hand, the results for all classifiers are improved in comparison to [HDV13].

5.3.3.1.4 Evaluation of Classification Performance on Aluminum Foil (Matte Side) M_4

The matte side of aluminum foil is a rather smooth, non-porous, non-textured substrate material consists of aluminum. Due to those properties, it is considered as a rather cooperative material in terms of lifting latent fingerprint patterns from it. The evaluation of the classification performance for this particular substrate is summarized in Table 5.7. It can be seen that the classification performance is lower on M_4 in comparison to M_1 . From the confusion matrices in Table 5.7 it can be seen that the particular errors are roughly equally distributed for J48 only, whereas the SMO and Bagging ensemble classifier detect considerably more

	SMO		J48		Bagging	
Classification As:	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	377482	80659	355439	102702	389713	68428
Substrate (SM)	100239	357902	102284	355857	82382	375759
Accuracy [%]	80.2574		77.6285		83.5411	

Table 5.7: 2-Fold Cross-Validation Results for Aluminum Foil (Matte Side) M_4 - Confusion Matrix and Classification Accuracy

blocks containing no fingerprint residue as blocks with fingerprint residue. In comparison to [HKD+14], the classification performance is slightly improved for all three classifiers.

5.3.3.1.5 Evaluation of Classification Performance on Golden Oak Veneer M_5

The Golden Oak veneer substrate is a structured, non-porous, textured substrate material consisting of a plastic material. Due to those properties, it is considered as a challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The surface structure with several grooves has an impact on the deposition of fingerprint residue as well. The evaluation of the classification performance for this particular substrate is summarized in Table 5.8. From the confusion matrices in Table 5.8 it can be seen

	SMO		J48		Bagging	
Classification As:	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	442418	67050	356582	152886	423902	85566
Substrate (SM)	274833	234635	151423	358045	144985	364483
Accuracy [%]	66.4471		70.1346		77.3734	

Table 5.8: 2-Fold Cross-Validation Results for Golden Oak Veneer M_5 - Confusion Matrix and Classification Accuracy

that the particular errors are roughly equally distributed for the J48 classifier. However, using SMO and the Bagging ensemble classifiers significantly more blocks containing no fingerprint residue are detected as blocks with fingerprint residue. However, in terms of the accuracy, the Bagging classifier still performs best with an accuracy of 77.3734%. The worst performance is achieved by SMO with an accuracy of just 66.4471%. In comparison to [HKD+14], the achieved detection accuracy is significantly lower for all three classifiers.

5.3.3.1.6 Evaluation of Classification Performance on Non-Metallic Car Body Finish M_6

The non-metallic car body finish substrate is a structured, non-porous, non-textured surface finish. Due to those properties, it is considered as a moderately challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The evaluation of the classification performance for this particular substrate is summarized in Table 5.9. From the confusion matrices in Table 5.9 it can be seen that the particular errors are

Classification As:	SMO		J48		Bagging	
	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	396751	47669	370046	74374	400629	43791
Substrate (SM)	75279	369141	75826	368594	60896	383524
Accuracy [%]	86.1676		83.1016		88.2221	

Table 5.9: 2-Fold Cross-Validation Results for Non-Metallic Car Body Finish M_6 - Confusion Matrix and Classification Accuracy

roughly equally distributed for the J48 classifier. However, using SMO and the Bagging ensemble classifiers significantly more blocks containing no fingerprint residue are detected as blocks with fingerprint residue. Despite this observation, in terms of the accuracy the Bagging classifier still performs best with an accuracy of 88.2221%. The worst performance is achieved by J48 with an accuracy of 83.1016%. In comparison to [HKD+14], the achieved detection accuracy is slightly improved for all three classifiers.

5.3.3.1.7 Evaluation of Classification Performance on Metallic Car Body Finish M_7

The metallic car body finish substrate is a complex smooth, non-porous substrate material with a slight texture caused by the metallic flakes in the base color. The surface finish consists of a base color with metallic flakes covered by a transparent clear coat. Due to those properties, it is considered as a challenging material in terms of lifting latent fingerprint patterns from it using the contactless non-destructive sensory S_1 because multiple peaks can appear within the spectrum due to the clear coat. As a result of the substrate properties, the measured layer might be non-deterministic due to several external influence factors. The evaluation of the classification performance for this particular substrate is summarized in Table 5.10. From the confusion matrices in Table 5.10

Classification As:	SMO		J48		Bagging	
	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	193380	42076	164795	70661	197546	37910
Substrate (SM)	89838	145618	70987	164469	70021	165435
Accuracy [%]	71.9875		69.9205		77.0804	

Table 5.10: 2-Fold Cross-Validation Results for Metallic Car Body Finish M_7 - Confusion Matrix and Classification Accuracy

it can be seen that the particular errors are roughly equally distributed for the J48 classifier. However, using SMO and the Bagging ensemble classifiers significantly more blocks containing no fingerprint residue are detected as blocks with fingerprint residue. The highest detection accuracy is achieved by the Bagging classifier with an accuracy of 77.0804%. The worst performance is achieved by J48 with an accuracy of just 69.9205%. In comparison to [HKD+14], the achieved detection accuracy is significantly reduced for all three classifiers.

5.3.3.1.8 Evaluation of Classification Performance on Blued Metal M_8

Blued metal is a rough, porous, non-textured substrate material which is the result of chemically treating metal. Such surfaces are often found on firearms and hence, are quite important for forensic investigations. The substrate can absorb fingerprint residue. Furthermore, on very fresh fingerprints an increased blurring of the pattern can be observed. Due to those properties, it is considered as a very challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The evaluation of the classification performance for this particular substrate is summarized in Table 5.11. From the

	SMO		J48		Bagging	
Classification As:	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	390421	83339	364188	109572	408787	64973
Substrate (SM)	111213	362547	108706	365054	99620	374140
Accuracy [%]	79.4672		76.9632		82.6291	

Table 5.11: 2-Fold Cross-Validation Results for Blued Metal M_8 - Confusion Matrix and Classification Accuracy

confusion matrices in Table 5.11 it can be seen that the particular errors are roughly equally distributed for the J48 classifier. However, using SMO and the Bagging ensemble classifiers significantly more blocks containing no fingerprint residue are detected as blocks with fingerprint residue. The highest detection accuracy is achieved by the Bagging classifier with an accuracy of 82.6291%. The worst performance is achieved by J48 with an accuracy of just 76.9632%. In comparison to [HKD+14], the achieved detection accuracy is decreased by significantly for J48 and the Bagging classifier. The detection accuracy is marginally better for SMO in comparison to [HKD+14].

5.3.3.1.9 Evaluation of Classification Performance on Ceramic Tile M_9

The ceramic tile substrate is a structured, non-porous, non-textured substrate consisting of a glazed ceramic material. Due to those properties, it is considered as a moderately challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The evaluation of the classification performance for this particular substrate is summarized in Table 5.12. From the confusion matrices in Table 5.12 it can be seen that the

	SMO		J48		Bagging	
Classification As:	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	274049	75880	246979	102950	279471	70458
Substrate (SM)	88545	261384	102655	247274	80553	269376
Accuracy [%]	76.5059		70.6219		78.4226	

Table 5.12: 2-Fold Cross-Validation Results for Ceramic Tile M_9 - Confusion Matrix and Classification Accuracy

particular errors are roughly equally distributed for the J48 classifier. However,

using SMO and the Bagging ensemble classifiers more blocks containing no fingerprint residue are detected as blocks with fingerprint residue. The highest detection accuracy is achieved by the Bagging classifier with an accuracy of 78.4226%. The worst performance is achieved by J48 with an accuracy of just 70.6219%.

5.3.3.1.10 Evaluation of Classification Performance on Copying Paper M_{10}

The copying paper substrate is a structured, porous, non-textured substrate consisting of cellulose fibers. Due to those properties, it is considered as a very challenging material in terms of lifting latent fingerprint patterns from it using contact-less non-destructive sensory. The evaluation of the classification performance for this particular substrate is summarized in Table 5.13. From

Classification As:	SMO		J48		Bagging	
	FP	SM	FP	SM	FP	SM
Fingerprint (FP)	157659	56738	145467	68930	165608	48789
Substrate (SM)	56902	157495	69154	145243	58637	155760
Accuracy [%]	73.4978		67.7971		74.9469	

Table 5.13: 2-Fold Cross-Validation Results for Copying Paper M_{10} - Confusion Matrix and Classification Accuracy

the confusion matrices in Table 5.13 it can be seen that the particular errors are roughly equally distributed for the J48 and SMO classifiers. However, using the Bagging ensemble classifier more blocks containing no fingerprint residue are detected as blocks with fingerprint residue. The highest detection accuracy is achieved by the Bagging classifier with an accuracy of 74.9469%. The worst performance is achieved by J48 with an accuracy of just 67.7971%.

5.3.3.1.11 Summary and Conclusions of the Evaluation of the Classification Performance

Summarizing the evaluation of the classifiers in a 2-fold cross validation, it is quite obvious that the best results are achieved using the Bagging ensemble classifier. The worst results are achieved using the J48 decision tree, which is however, the easiest one to explain in terms of the decision-making process. Based the overall detection accuracy summarized in Table 5.14, it can be stated that the classification-based detection of fingerprint residue is in general possible, but yields different error rates depending on the substrate material. With respect to the biometric evaluation the best results can be expected for M_1 . The worst and least reliable results can be expected on M_3 , M_5 , M_7 , M_9 and M_{10} . Thus, especially a surface structure or multiple surface layers seem to impact the detection performance within the utilized experimental setup.

5.3.3.2 Biometric evaluation of unlabeled data

Before the reconstructed fingerprint images can be analyzed using biometric matching as a part of the data analysis phase, it is necessary to develop particular strategies for the interpretation of the classifier's decisions, which is a part of the

Biometric
Evaluation

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DS	
OO							

	SMO	J48	Bagging
M_1	91.0613	90.008	92.7978
M_2	81.3138	79.4084	84.305
M_3	75.4105	71.2786	78.032
M_4	80.2574	77.6285	83.5411
M_5	66.4471	70.1346	77.3734
M_6	86.1676	83.1016	88.2221
M_7	71.9875	69.9205	77.0804
M_8	79.4672	76.9632	82.6291
M_9	76.5059	70.6219	78.4226
M_{10}	73.4978	67.7971	74.9469

Table 5.14: Comparison of Classification Accuracy in Percent from the 2-Fold Cross-Validation Results for all Substrates

strategic preparation. The two classifiers J48 and Bagging provide confidence levels for the membership of a block in each of the specific classes as depicted in listing 5.1. With SMO such an additional information is not available. The listing in listing 5.1 consists of the header of the classification result file and the decision for each block of an image. In addition to that, an initial label is included within the file, in this experiment this label does not indicate the ground truth since the images in the test set are gathered without any ground truth due to the practical reason of the required acquisition times. The last two columns of each result vector contain the probabilities for each block to be a member of the first or the second class. Both values need to be interpreted in order to reconstruct the fingerprint image.

```
@attribute @attribute ID numeric
@attribute @attribute FPBLOCK {f,b}
@attribute FilteredClassifier_prob_0 numeric
@attribute FilteredClassifier_prob_1 numeric

@data
0.0 , b, 0.9896280436821216 , 0.01037195631787837 ,
1.0 , b, 0.9896280436821216 , 0.01037195631787837 ,
2.0 , b, 0.9896280436821216 , 0.01037195631787837 ,
3.0 , b, 0.9944442492157185 , 0.005555750784281532 ,
4.0 , b, 0.9944442492157185 , 0.005555750784281532 ,
5.0 , b, 0.9944442492157185 , 0.005555750784281532 ,
6.0 , b, 0.9944442492157185 , 0.005555750784281532 ,
```

Listing 5.1: Excerpt of a Classification Result File Determined on the Foundation of the Bagging Classifier; Header Describing the Data Fields - BlockID, Label from Ground Truth (if Available, Fixed to b for Substrate Block Otherwise), Probabilities for Class Assignments

Based on the dimensions of the original image, it is possible to determine the exact position of a result vector within a two-dimensional image. Each particular block represents one pixel of the reconstructed fingerprint image I_R . This particular image has a resolution of 500 ppi, which is compatible to the exemplar fingerprints

as well as the biometric feature extraction and matching within NBIS [Nat13]. There are several options to create the resulting fingerprint image. The intuitive option is to use the most probable class and assign either a low or a high intensity value. The result is the binary image I_{Raw} . The second option takes classification errors and uncertainty into consideration. In this case, the probability for a block representing fingerprint residue must exceed the probability for the block containing substrate by some margin. For the evaluation within the scope of this thesis, this margin is arbitrarily defined as 5 percent. As a result, a block is only considered as a fingerprint block if the probability for fingerprint residue within the block exceeds the probability of being a substrate-only block by five percent points. Besides this peculiarity, the resulting image $I_{Optimized}$ is a binary image as well.

The third option is the consideration of likelihood ratios (see Section 2.1.2.2). In this case the quotient between the probabilities is used to reconstruct an image. In particular two images I_{RLRa} , I_{RLRb} are determined:

$$I_{RLRa} = \bigcup \frac{P_A(B_k)}{P_B(B_k)} \quad (5.27)$$

$$I_{RLRb} = \bigcup \frac{P_B(B_k)}{P_A(B_k)} \quad (5.28)$$

With P_A and P_B representing the particular class probabilities for each block B_k . The two images are generated due to the fact that the reconstructed images are stored as 8-bit gray-scale JPG-files. If the dividend is larger than the divisor, the value is mapped to the range]1,255], otherwise the resulting value range is [0,1]. Thus, the values are mapped differently which results in a potentially unintended loss. Calculating both images, avoids this particular loss. In addition to that the classical likelihood ratio is determined by dividing the larger probability by the smaller one. However, this image is primarily intended to support a latent fingerprint examiner to determine particular areas with higher uncertainty. Thus, this particular image is probably not utilized for the biometric feature extraction and matching in practice.

The biometric evaluation is supposed to simulate the manual comparison process during the data analysis phase of the digitized forensics process. The sole indicator for the segregation performance is the number of successfully matched latent fingerprints. A high number of matches indicates a very good performance for the introduced approach. However, a low number of matches can originate from various factors:

- Low detection performance of the proposed pattern recognition based approach,
- Selection of an unsuitable sensor for digitizing latent fingerprints from a particular substrate,
- Low quality of the latent fingerprint.

In order to mitigate this uncertainty regarding the root cause for a low performance, the biometric feature extraction and matching is also performed on the foundation of the raw intensity image I_I scaled to a resolution of 500 ppi forming I_{orig} . If the matching performance on such raw images outperforms

Potential Root Causes of low Matching Rates

Selection of a Reference Performance Indicator

the matching performance on the reconstructed images from the classifier, it is a clear indicator for a low performance of the pattern recognition based approach, because the resulting sensor data and the quality of the latent fingerprints are sufficient for the matching. If the pattern recognition based approach performs better, the proposed approach is somewhat suitable.

In the following subsections, the biometric matching performance is compared for each of the ten evaluated substrate materials, classification algorithms and image reconstruction strategies.

5.3.3.2.1 Evaluation of Biometric Matching Performance on White Furniture Surface M_1

The biometric matching performance on the white furniture surface is quite low as summarized in Table 5.15. Based on the image reconstruction on the foundation of the results of the Bagging classifier no particular matches are achieved. However, with SMO and J48 the matching shows at least improved results in comparison to the matching on the foundation of the original intensity image I_{orig} .

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	I_{RLRa}	I_{RLRb}
SMO	4	12	10	0	10
J48		4	12	0	0
Bagging		0	0	0	0

Table 5.15: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_1

In comparison to [HKD+14] the achieved matching rates are much lower with 12 % successful matches for $I_{R_{raw}}$ from the SMO classifier based model and $I_{R_{optimized}}$ from the J48 classifier based model. No particular matches are achieved using the Bagging ensemble classifier based model. This is quite surprising because the classifier performed best in the 2-fold cross validation in Section 5.3.3.1. However, the classification errors seem to be located in the valleys of the ridge-valley-pattern of the fingerprint. Thus, the reconstructed image constitutes a region mask for the latent fingerprint instead of the anticipated reconstruction of the fingerprint pattern. Nevertheless, the tendency from [HKD+14] that the classification based approach is in general suitable for the fingerprint pattern reconstruction in contact-less non-destructive scans is confirmed.

Selected sections of a successfully matched sample and an unsuccessful reconstruction are illustrated in Figure 5.6 and Figure 5.7.

The sample in Figure 5.6 is successfully matched using the raw image ($I_{R_{raw}}$) and the $I_{R_{optimized}}$ reconstructed with the J48-based model. However, it is quite obvious that a ridge-valley pattern is also reconstructed by the Bagging classifier. Overall the reconstructed images are still rather noisy, which could increase the necessary effort for the comparison by a human expert. The unsuccessful matching result for the example depicted in Figure 5.7 is very surprising given the very clear ridge-valley pattern in the images reconstructed using the SMO-based model. Such a fingerprint quality is highly likely to be usable for forensic purposes. The ridge-valley-pattern resulting from the J48-based reconstruction is very noisy for this example, whereas the Bagging-based reconstruction seems to be hardly of value at all.

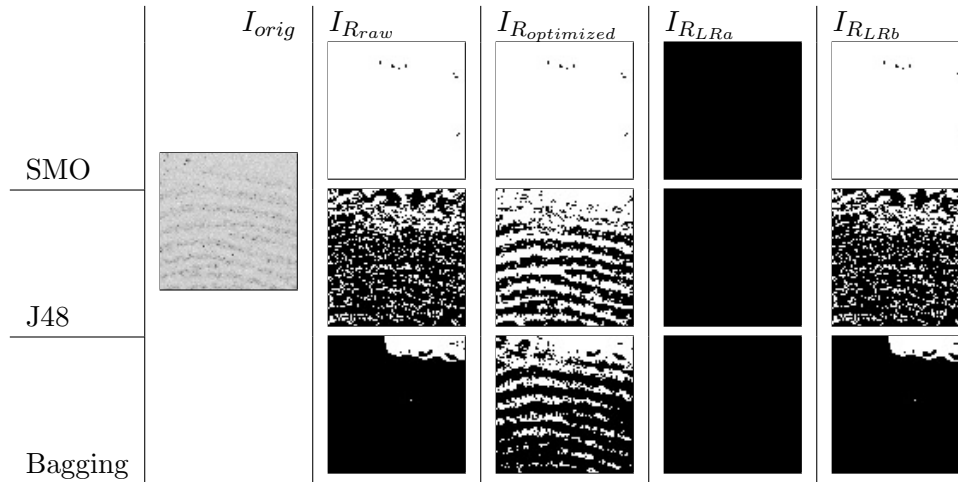


Figure 5.6: Illustration of a 4 by 4 mm section of a sample from M_1 successfully matched using $I_{R_{optimized}}$ with J48 and I_{orig} , second fingerprint of the depletion series

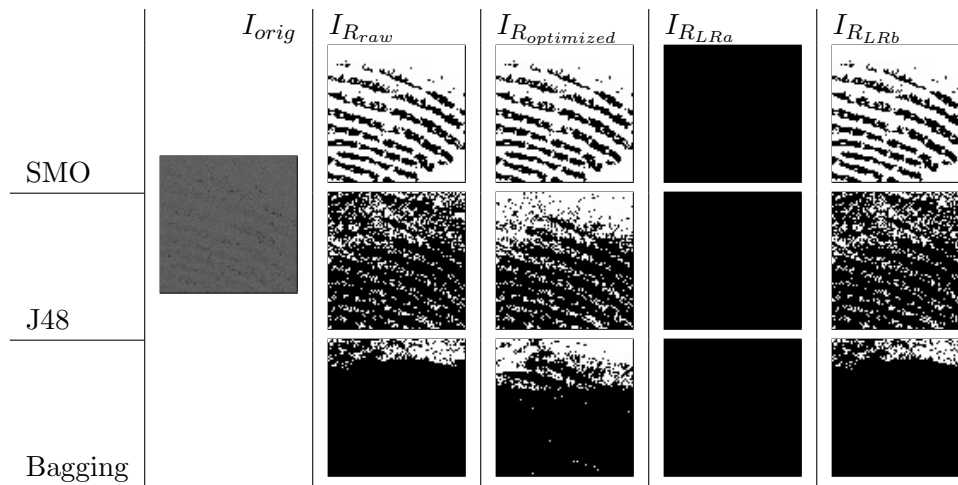


Figure 5.7: Illustration of a 4 by 4 mm section of a sample from M_1 which is not successfully matched using any evaluated image, ninth fingerprint of the depletion series

5.3.3.2.2 Evaluation of Biometric Matching Performance on Veneered Plywood M_2

The evaluation results on the veneered plywood substrate show a similar tendency for the Bagging classifier in comparison to those on the white furniture surface as summarized in Table 5.16. In particular no successful matches are possible on the foundation of the images reconstructed using Bagging classifier based model. However, for this particular substrate, no matches are achieved using reconstructed images from the J48 classifier based model either.

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	$I_{R_{LRa}}$	$I_{R_{LRb}}$
SMO	0	1	1	0	1
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.16: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_2

In comparison to [HKD+14] the matching performance is slightly better with one successful match using the SMO classifier based segregation of the fingerprint data. However, this single match indicates a success rate of just 1 % being achieved with $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRa}}$. The highest matching score of 56 is achieved using $I_{R_{raw}}$. Even though the overall performance is quite low, it still outperforms the matching performance on the original intensity image I_{orig} .

Selected sections of a successfully matched sample and an unsuccessful reconstruction are illustrated in Figure 5.8 and Figure 5.9.

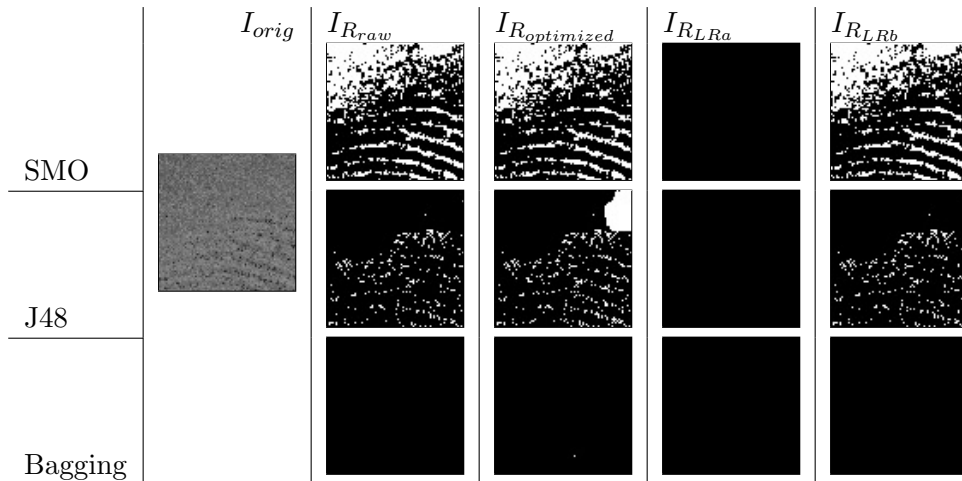


Figure 5.8: Illustration of a 4 by 4 mm section of a sample from M_2 successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ with SMO, eighth fingerprint of the depletion series

The sample in Figure 5.8 is successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ reconstructed on the foundation of the SMO-based model. However, the reconstruction is noisy especially in the substrate region in the upper left corner of the section. The reconstruction using the J48-based model shows a very noisy result which would probably be of no value for a latent fingerprint examiner. The classification using the Bagging-based model seems to fail completely for this sample. The unsuccessful matching result for the example depicted in Figure 5.9 is showing no usable ridge-valley pattern at all.

5.3.3.2.3 Evaluation of Biometric Matching Performance on Brushed Stainless Steel M_3

Despite the strong structure pattern caused by the brush marks, the biometric matching performance on brushed stainless steel is slightly better than the

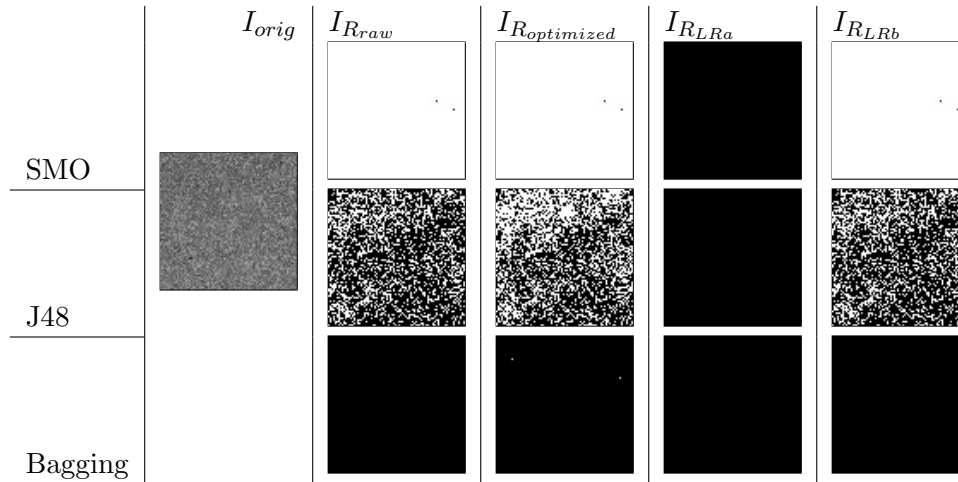


Figure 5.9: Illustration of a 4 by 4 mm section of a sample from M_2 which is not successfully matched using any evaluated image, fourth fingerprint of the depletion series

performance on the veneered plywood as summarized in Table 5.17. However, using the Bagging classifier model based reconstruction no particular matches are achieved. The best performance of up to 2 % successful matches is again

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	$I_{R_{LRa}}$	$I_{R_{LRb}}$
SMO	0	2	1	0	1
J48		0	1	0	0
Bagging		0	0	0	0

Table 5.17: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_3

achieved using the SMO classifier based reconstruction of the fingerprint pattern. With the J48 classifier model based reconstruction one successful biometric match is achieved for $I_{R_{optimized}}$. However, the relative number of successful matches is lower in comparison to [HKD+14].

Selected sections of a successfully matched sample and an unsuccessful reconstruction are illustrated in Figure 5.10 and Figure 5.11.

The sample in Figure 5.10 is successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ reconstructed on the foundation of the SMO-based model. It shows a good suppression of the substrate pattern and a low noise level within the ridge-valley-pattern. The reconstruction using the J48-based model shows a noisy result which might still be usable by a latent fingerprint examiner. The classification using the Bagging-based model seems to fail completely for this sample. However, the $I_{R_{optimized}}$ seems to depict at least a coarse region of the fingerprint pattern. The unsuccessful matching result for the example depicted in Figure 5.11 is showing a mixture of the fingerprint pattern and the low-frequency substrate pattern for the SMO-based reconstruction. A similar effect can be observed for the J48-based reconstruction which shows a high-frequency noise. Despite the influence of the substrate, which is still present in the reconstruction, the results from the SMO classifier might still be usable for a human latent fingerprint examiner.

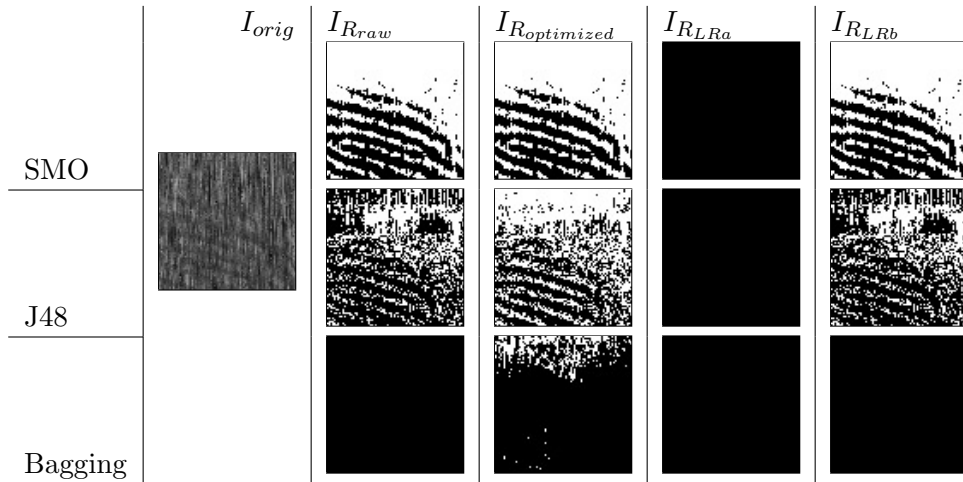


Figure 5.10: Illustration of a 4 by 4 mm section of a sample from M_3 successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ with SMO, third fingerprint of the depletion series

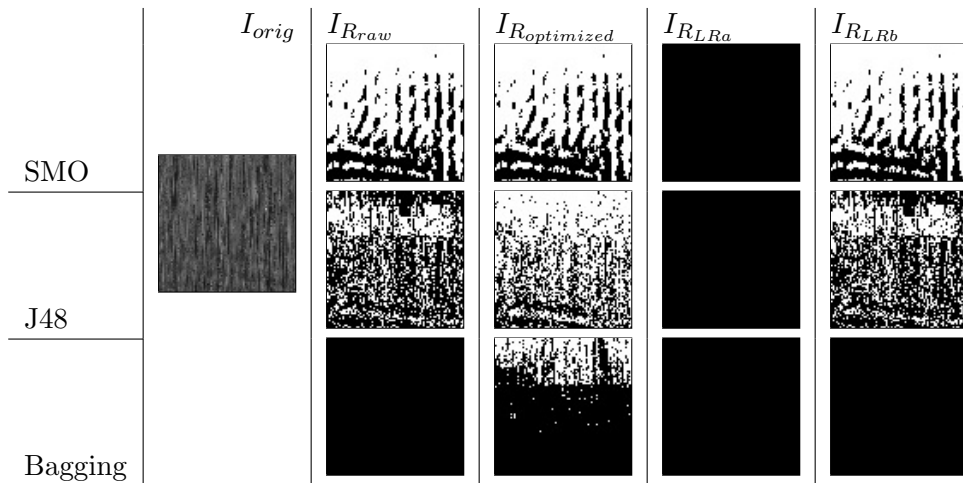


Figure 5.11: Illustration of a 4 by 4 mm section of a sample from M_3 which is not successfully matched using any evaluated image, ninth fingerprint of the depletion series

5.3.3.2.4 Evaluation of Biometric Matching Performance on Aluminum Foil (Matte Side) M_4

The aluminum foil substrate is more cooperative with the selected setup in the scope of digitized forensics as summarized in Table 5.18. One successful match is achieved using the original intensity image I_{orig} . However, similar to the other substrates, no successful matches are possible using the Bagging classifier model based reconstruction.

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	$I_{R_{LRa}}$	$I_{R_{LRb}}$
SMO	1	6	6	0	6
J48		2	4	0	1
Bagging		0	0	0	0

Table 5.18: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_4

Using the SMO classifier model based reconstruction six images are successfully matched. This performance of is on par with the white furniture surface because for M_4 only 50 samples are analyzed resulting in a successful matching rate of 12 %. For the J48 classifier model based reconstruction the most successful matches are achieved using $I_{R_{optimized}}$, yielding a successful match rate of 8 %. In comparison to [HKD+14] those results constitute a significant improvement because in [HKD+14] no successful matches are achieved using the classifier based fingerprint data segregation approach.

Selected sections of a successfully matched sample and an unsuccessful reconstruction are illustrated in Figure 5.12 and Figure 5.13.

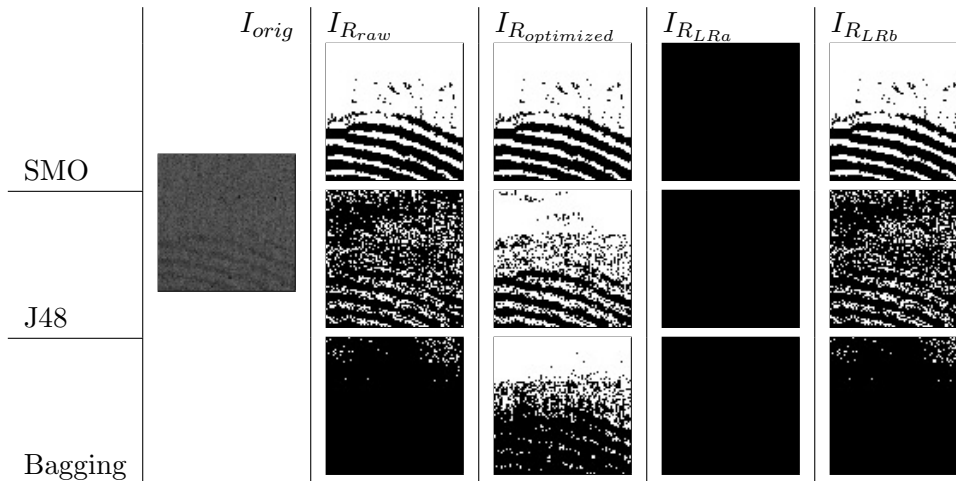


Figure 5.12: Illustration of a 4 by 4 mm section of a sample from M_4 successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$, $I_{R_{LRb}}$ with SMO and J48, as well as I_{orig} , first fingerprint of the depletion series

The sample depicted in Figure 5.12 is successfully matched using $I_{R_{raw}}$, $I_{R_{optimized}}$ and $I_{R_{LRb}}$ reconstructed on the foundation of the SMO-based and J48-based models. It shows a good quality of the ridge-valley-pattern for the SMO-based reconstruction and a rather high level of noise with the J48-based reconstruction. The $I_{R_{optimized}}$ resulting from the Bagging-classifier-based reconstruction shows a ridge-valley-pattern as well. However, this pattern is almost hidden in a high level of noise, thus, this reconstruction is likely to be hardly usable by a latent fingerprint examiner. The unsuccessful matching result for the example depicted in Figure 5.13 is showing an influence of the substrate structure within the reconstructed fingerprint pattern. In this example a low-frequency noise pattern can be observed for the SMO-based reconstruction whereas the J48-

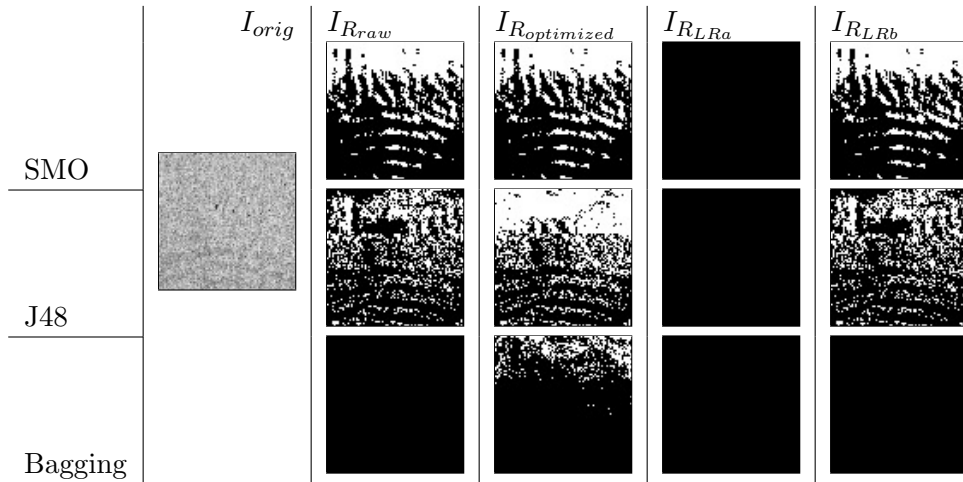


Figure 5.13: Illustration of a 4 by 4 mm section of a sample from M_4 which is not successfully matched using any evaluated image, tenth fingerprint of the depletion series

based reconstruction results in high-frequency noise in the image. The Bagging-classifier-based reconstruction does not produce any results usable for determining the feature points of the fingerprint pattern.

5.3.3.2.5 Evaluation of Biometric Matching Performance on Golden Oak Veneer M_5

No particular biometric matches are achieved on the golden oak veneer substrate as summarized in Table 5.19.

	I_{orig}	I_{Rraw}	$I_{Roptimized}$	I_{RLRa}	I_{RLRb}
SMO	0	0	0	0	0
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.19: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_5

This observation is in line with [HKD+14]. Thus, the extended feature space and extended training set does not result in any significant improvements. An example for the reconstruction of the fingerprint pattern on this substrate material is depicted in Figure 5.14. A fingerprint pattern is not visible in any of the reconstructed images. The suppression of the substrate structure worked to some extent using the SMO-based model. However, the noise pattern caused by the substrate in I_{orig} is just substituted with another pattern of noise. For the reconstruction using the J48-based model a large artifact is created in the selected section of the image. In addition to that, a high level of noise can be observed.

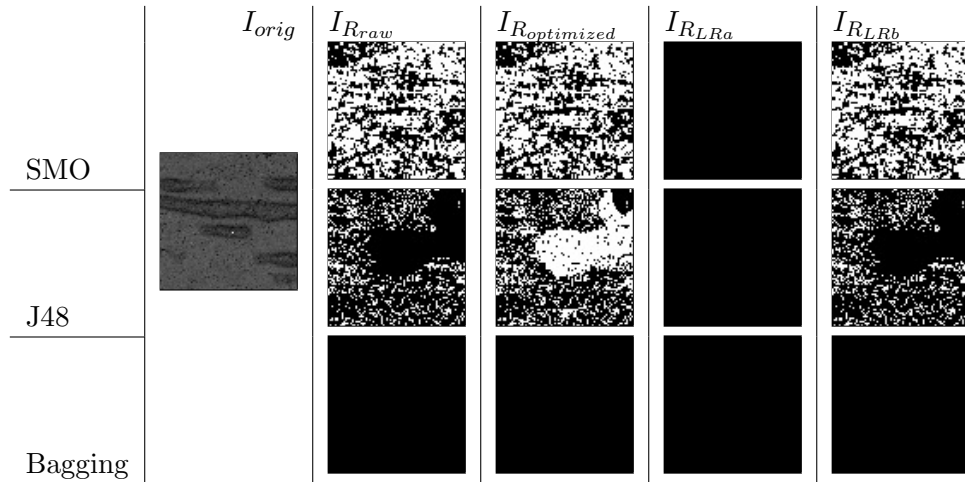


Figure 5.14: Illustration of a 4 by 4 mm section of a sample from M_5 which is not successfully matched using any evaluated image, fourth fingerprint of the depletion series

5.3.3.2.6 Evaluation of Biometric Matching Performance on Non-Metallic Car Body Finish M_6

No particular biometric matches are achieved on the non-metallic car body finish as summarized in Table 5.20.

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	$I_{R_{LRa}}$	$I_{R_{LRb}}$
SMO	0	0	0	0	0
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.20: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_6

In comparison to [HKD+14], this constitutes a degradation of the performance in the setup of this thesis, because in [HKD+14] at least one successful biometric match is achieved using the SMO and Bagging classifier based reconstructions. An example for the reconstruction of the fingerprint pattern on this substrate material is depicted in Figure 5.15. A fingerprint pattern is not visible in any of the reconstructed images. Furthermore, all reconstructed images contain a high level of noise.

5.3.3.2.7 Evaluation of Biometric Matching Performance on Metallic Car Body Finish M_7

No particular biometric matches are achieved on the metallic car body finish as summarized in Table 5.21.

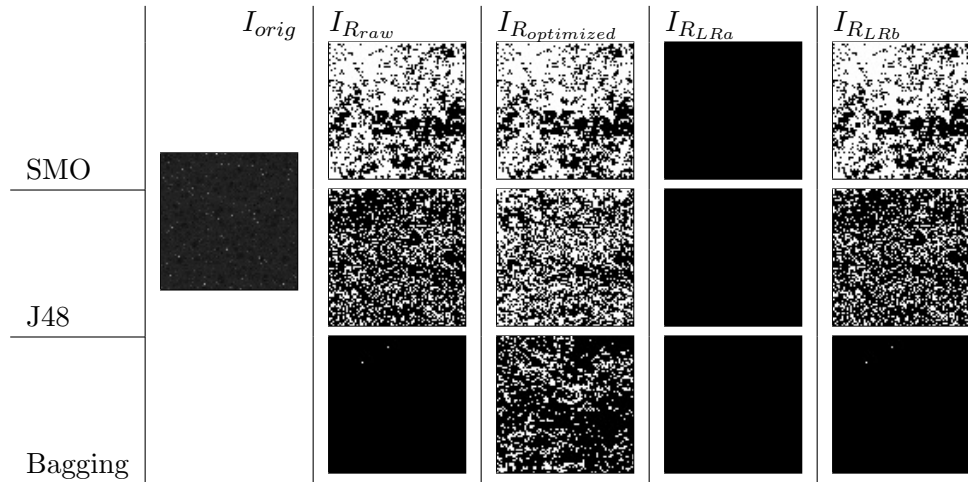


Figure 5.15: Illustration of a 4 by 4 mm section of a sample from M_6 which is not successfully matched using any evaluated image, seventh fingerprint of the depletion series

	I_{orig}	I_{Rraw}	$I_{Roptimized}$	I_{RLRa}	I_{RLRb}
SMO	0	0	0	0	0
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.21: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_7

This observation is in line with [HKD+14]. Thus, the extended feature space and extended training set does not result in any significant improvements. An example for the reconstruction of the fingerprint pattern on this substrate material is depicted in Figure 5.16. A fingerprint pattern is not visible in any of the reconstructed images. However, the J48-based reconstruction might show a ridge-valley-pattern which is hardly of any value, as it is superimposed by a high level of noise.

5.3.3.2.8 Evaluation of Biometric Matching Performance on Blued Metal M_8

No particular biometric matches are achieved on the blued metal surface as summarized in Table 5.22.

	I_{orig}	I_{Rraw}	$I_{Roptimized}$	I_{RLRa}	I_{RLRb}
SMO	0	0	0	0	0
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.22: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_8

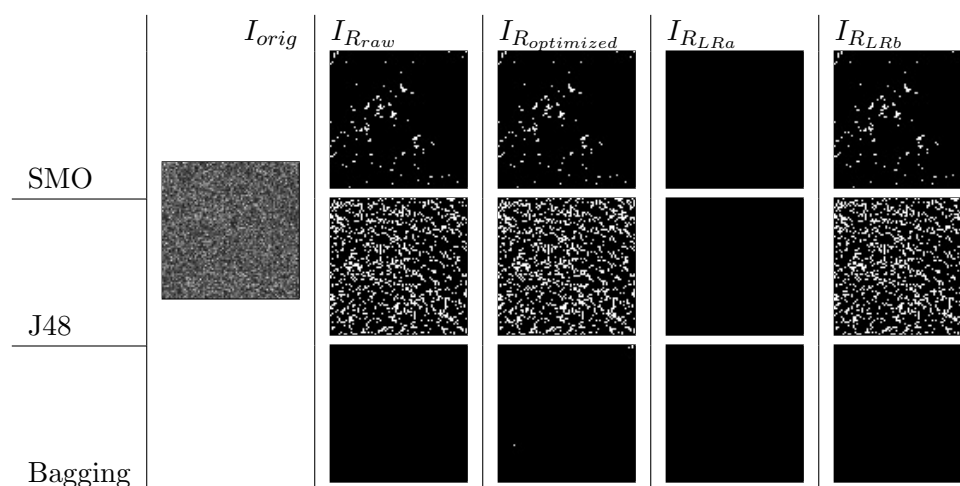


Figure 5.16: Illustration of a 4 by 4 mm section of a sample from M_7 which is not successfully matched using any evaluated image, fourth fingerprint of the depletion series

This observation is in line with [HKD+14]. Thus, the extended feature space and extended training set does not result in any significant improvements.

An example for the reconstruction of the fingerprint pattern on this substrate material is depicted in Figure 5.17. A fingerprint pattern is not visible in any of

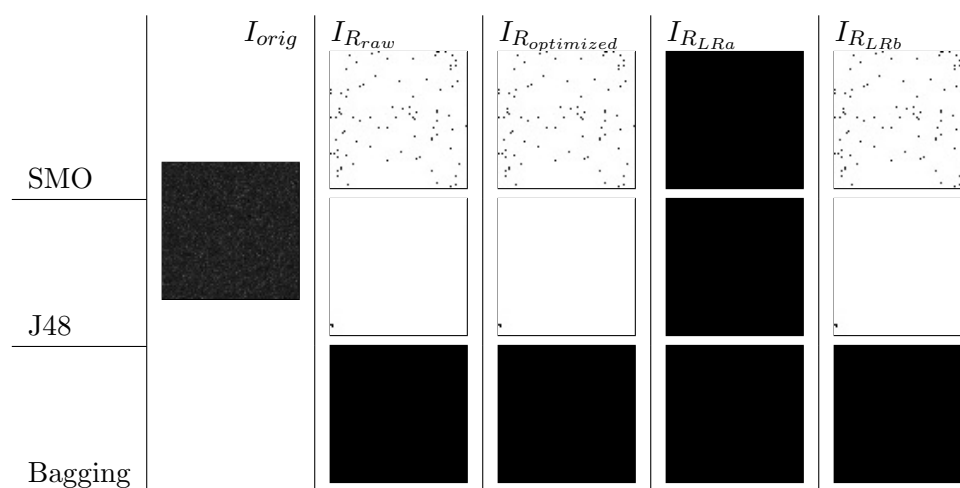


Figure 5.17: Illustration of a 4 by 4 mm section of a sample from M_8 which is not successfully matched using any evaluated image, second fingerprint of the depletion series

the reconstructed images. However, only a low level of noise can be observed. This can be either the result of an incorrect decision boundary of the trained models or of an unsuitable sensor which cannot detect any fingerprint residue after some time on this particular substrate at all.

5.3.3.2.9 Evaluation of Biometric Matching Performance on Ceramic Tile M_9

No particular biometric matches are achieved on the ceramic tile as summarized in Table 5.23.

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	$I_{R_{LRa}}$	$I_{R_{LRb}}$
SMO	0	0	0	0	0
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.23: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_9

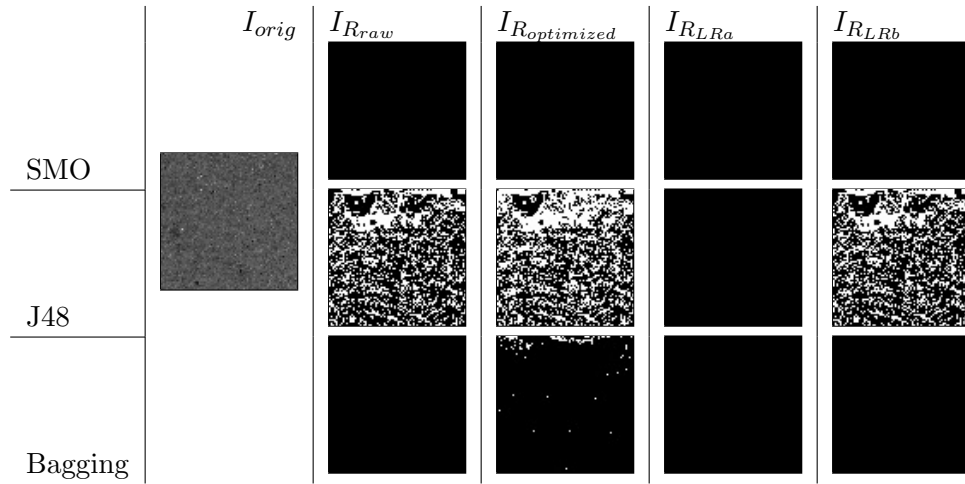


Figure 5.18: Illustration of a 4 by 4 mm section of a sample from M_9 which is not successfully matched using any evaluated image, second fingerprint of the depletion series

A fingerprint pattern is not visible in any of the reconstructed images depicted in Figure 5.18. However, the pattern reconstructed by the J48-based model might contain a ridge-valley pattern which is superimposed by a lot of noise. It is hard to determine whether such an image would be of any evidential value at all.

5.3.3.2.10 Evaluation of Biometric Matching Performance on Copying Paper M_{10}

No particular biometric matches are achieved on copying paper as summarized in Table 5.24.

	I_{orig}	$I_{R_{raw}}$	$I_{R_{optimized}}$	$I_{R_{LRa}}$	$I_{R_{LRb}}$
SMO	0	0	0	0	0
J48		0	0	0	0
Bagging		0	0	0	0

Table 5.24: Number of Fingerprint Matches for Latent Fingerprints Digitized from M_{10}

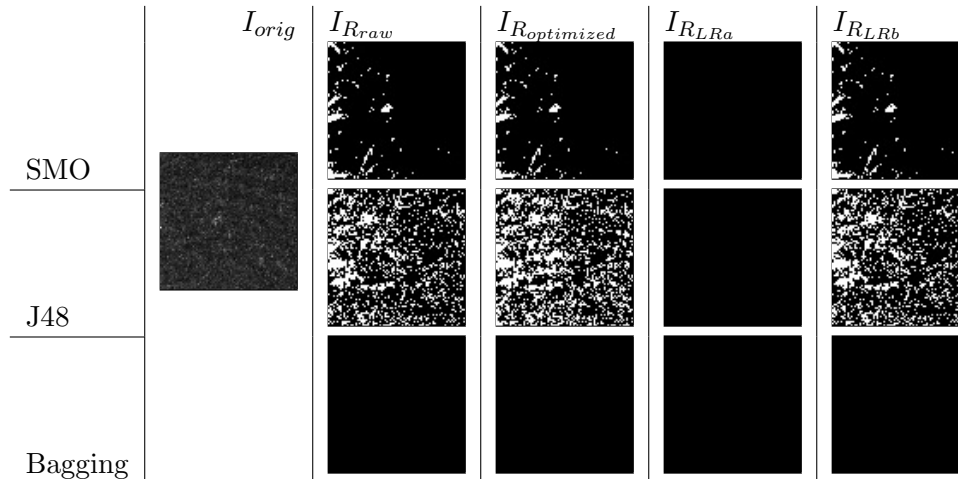


Figure 5.19: Illustration of a 4 by 4 mm section of a sample from M_10 which is not successfully matched using any evaluated image, second fingerprint of the depletion series

A fingerprint pattern is not visible in any of the reconstructed images depicted in Figure 5.19. Similar to the observation for M_9 in the previous paragraph, the pattern reconstructed by the J48-based model might also contain a ridge-valley pattern which is superimposed by a lot of noise.

5.3.3.2.11 Summary and Conclusions of the Evaluation of the Biometric Matching Performance

The pattern recognition based approach is in general suitable to segregate latent fingerprint data from the substrate data since the classifier model based reconstruction of the fingerprint images outperforms the matching performance on the respective original intensity images. However, successful matches are only achieved on the white furniture surface M_1 , veneered plywood M_2 , brushed stainless steel M_3 , and aluminum foil M_4 . In comparison to the 2-fold cross validation results in Section 5.3.3.1, this result is quite surprising because it seems to be independent of the initial performance of the classifier. Furthermore, using the best performing Bagging classifier models no particular matches are achieved. From the nature of the biometric matches shown in Section A.3.2, it can be seen that the training using one depletion series from one test subject did not impact the matching performance for other persons or fingers as successful matches are achieved for all four test persons in the test setup. The particular amount of fingerprint residue seems to have a negligible impact in this test setup because matches are achieved for the first up to the eighth sample of a depletion series.

5.4 Feature Selection

Given the dimensionality of the feature space with 600 dimensions the occurrence of the effect known as the curse-of-dimensionality (see e.g. [DHS00, p. 168]) is likely. This particular effect describes the phenomenon of an increased complexity of the training and determination of decision boundaries in high-dimensional feature spaces. Within the training of the classifiers the rather long training time and memory requirements for the SMO classifier [Pla99] could be an indicator

Feature Selection

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DO	DS
						DO	

for the presence of the curse-of-dimensionality within this application scenario. Thus, a reduction of dimensionality of the feature space could be beneficial.

In order to achieve such a reduction of the dimensionality either features can be selected by removing redundant features, contradictory features or features with a low discriminatory power or by projecting the feature space into another feature space with a lower dimensionality. An example for the latter is the principle component analysis (PCA) (see e.g. [DHS00, p. 568]).

Since the classification models in this thesis are trained for each substrate separately, the approach of the feature selection by the removal of features is favored because it allows for creating a shared feature space by creating a superset of the selected features for each individual substrate. The result of this design decision is that the feature selection is not necessarily required for the training of models for new substrates. However, this assumption is only valid if the selection of substrate materials is more or less representative for the characteristics of all substrate materials within the designed initial feature space.

In particular the WEKA data mining software [Hal+09] using the AttributeSelectedClassifier with the CfsSubsetEval technique as the attribute evaluation, the Best-First search method [Hal98] and the J48/C4.5 decision tree are utilized in their default settings for performing the feature selection. As the result of the feature selection, the following features are selected for the dimensionality-deduced feature space:

1. Intensity image I_I value span B_{span} (Equation 5.3))
2. Intensity image I_I Skewness $v(B_k)$ (Equation 5.6)
3. Intensity image I_I Kurtosis $w(B_k)$ (Equation 5.7)
4. Intensity image I_I first Hu moment $Hu(B_k)$ (Equation 5.19)
5. Intensity image I_I second Hu moment $Hu(B_k)$ (Equation 5.19)
6. Intensity image I_I globally normalized (zero-mean) max value $B_{kmaxnormGabs}$ (Equation 5.24)
7. Intensity image I_I globally normalized (zero-mean) mean value $\overline{B_{knormGabs}}$ (Equation 5.24)
8. Intensity image I_I globally normalized (relative) value span $B_{kspannormGrel}$ (Equation 5.23)
9. Intensity image I_I locally normalized (zero-mean) min value $B_{kminnormLabs}$ (Equation 5.26)
10. Intensity image I_I globally normalized (relative) median value $\widetilde{B_{knormLrel}}$ (Equation 5.25)
11. Topography image I_T globally normalized (zero-mean) min value $B_{kminnormGabs}$ (Equation 5.24)
12. Topography image I_T globally normalized (zero-mean) max value $B_{kmaxnormGabs}$ (Equation 5.24)
13. Topography image I_T globally normalized (zero-mean) median value $\widetilde{B_{knormGabs}}$ (Equation 5.24)

14. Topography image I_T globally normalized (relative) min value $B_{kminnormLrel}$ (Equation 5.25)
15. Sobel filtered (x,y) intensity image $Sob_1(I_I)$ Mean-Squared Error $MSE(B_k)$ (Equation 5.8)
16. Sobel filtered (x,y) intensity image $Sob_1(I_I)$ globally normalized (zero-mean) min value $B_{kminnormGabs}$ (Equation 5.24)
17. Second-order Sobel filtered (x,y) intensity image $Sob_2(I_I)$ globally normalized (zero-mean) max $B_{kmaxnormGabs}$ (Equation 5.24)
18. Unsharp masked intensity image $U(I_I)$ Skewness $v(B_k)$ (Equation 5.6)
19. Unsharp masked intensity image $U(I_I)$ globally normalized (zero-mean) max value $B_{kmaxnormGabs}$ (Equation 5.24)
20. Unsharp masked intensity image $U(I_I)$ locally normalized (zero-mean) median value $B_{knormLabs}$ (Equation 5.26)
21. Sobel filtered (y) intensity image $Sob_{1Y}(I_T)$ Entropy $ENT(B_k)$ (Equation 5.9)

The feature selection results show that no features from the semantic feature space 3 in Section 5.2.1.3 and the Benford's Law based feature space 4 in Section 5.2.1.4 are selected and that most of the features originate from the normalized feature space 5 in Section 5.2.1.5. While the latter observation is reasonable, especially the omission of features intended to capture fingerprint properties is interesting. Obviously, the features do not contribute sufficiently towards the decision boundary. The reason for that can be potentially the lack of a proper ground truth, which might reduce the correlation between the feature and the intended property within a particular block.

The evaluation results for the best and the worst performing classifier are summarized in Table 5.25. It can be seen that the classification accuracy of the

Evaluation
Results

	Without Feature Selection		With Feature Selection	
	J48	Bagging	J48	Bagging
M_1	90.008	92.7978	91.0105	92.0091
M_2	79.4084	84.305	81.5417	83.409
M_3	71.2786	78.032	73.3	75.7388
M_4	77.6285	83.5411	80.173	82.071
M_5	70.1346	77.3734	67.7438	70.4785
M_6	83.1016	88.2221	82.0311	84.3106
M_7	69.9205	77.0804	70.6771	73.1769
M_8	76.9632	82.6291	78.6863	81.264
M_9	70.6219	78.4226	72.1939	74.6761
M_{10}	67.7971	74.9469	71.536	73.6515

Table 5.25: Comparison of Classification Accuracy in Percent from the 2-Fold Cross-Validation Results for all Substrates with and without the Feature Selection

Bagging classifier is lower for all substrates after reducing the feature space. This

effect is reasonable since this Bagging classifier is an ensemble classifier which could potentially benefit from more diverse feature subsets. The classification accuracy of the J48 decision tree is increased for most substrates with the exception of the "Golden-Oak" veneer M_5 and the non-metallic matte car body finish M_6 . This observation is reasonable as the feature selection is performed on the foundation of the J48 decision tree classifier. Thus, the feature space is optimized for this classification approach. However, the overall impact on the classification performance is quite low. Hence, the biometric evaluation is not repeated for the newly trained models.

5.5 Chapter Summary and Limitations

Summary of
 addressed
 Research
 Questions,
 Objectives and
 Contributions

This chapter describes the primary application scenario of this thesis addressing the validation of the introduced process model for digitized forensics within the scope of latent fingerprint analysis. At first, the potential processing pipeline for latent fingerprints in digitized forensics is outlined as potential second-tier phases for the data gathering in Section 5.1. This set of second-tier phases describe the trace specific processing of latent fingerprints with respect to the first-tier phases introduced in Section 3.1, addressing research question Q_4 . This process provides a coarse outline for achieving objective O_3 regarding the design of a novel signal processing and pattern recognition based pipeline for segregating latent fingerprint patterns from substrate data. Afterward, the scenario specific requirements regarding the sensory are assessed for three available sensors addressing research question Q_3 as a part of the strategic preparation. This is the foundation for achieving objective O_3 . Based on the selection of sensory and the definition of second-tier processing phases, a suitable classification scheme for the segregation of fingerprint patterns from the substrate data is designed, implemented and evaluated in Section 5.3 in order to address research question Q_5 . The selected two-class, substrate-dependent, supervised-learning based approach addresses the objective O_3 and shows an acceptable performance in the evaluation on the classifier level using a two-fold cross validation approach. The designed and utilized feature space represents the contribution C_5 . The subsequent biometric evaluation based on a test set specifically designed for this thesis in Section 5.3.3.2 indicates positive tendencies for rather cooperative substrates. This extensive evaluation represents the contribution C_6 of this thesis.

Limitations

The limitation to specific substrates could originate from the sensory, e.g. for porous substrates, the designed feature space, an inaccurate approximation of ground truth data for the training and the quality of the fingerprint patterns themselves. Especially the latter is not accounted for by the biometric matching algorithm utilized in this thesis. Thus, the results can be considered as a lower bound for the matching performance of a forensic expert. Due to the time constraints within the scope of a thesis, it is furthermore not possible to determine whether the classification approach achieves generalization for the segregation of the data. The multitude of fingerprint patterns, sweat compositions and amounts as well as potential contaminants and substrate properties in practice could require different decision boundaries within the trained models. Another limitation of the approach is currently the computational expensiveness, which potentially limits the extension of the training data. With training sets containing 400,000 to 1,000,000 feature vectors and a 600-dimensional feature space the training of a single model for one substrate could take up to one week using an Intel Core i5-4570T CPU using the SMO classifier [Pla99], while requiring

up to 28 GB of main memory space during the process. While the feature selection reduced the dimensionality of the feature space significantly, the impact on the classification performance is marginal. Furthermore, especially the features intended for the detection of fingerprint patterns are removed by the evaluated feature selection approach.

Application Scenario 2: Detection of Printed Latent Fingerprint Forgeries

This chapter addresses an exemplary issue of anti-forensics for the investigation of fingerprint-based evidence. The intention of this chapter is the analysis of a very specific sub-question in the analysis process of a specific trace type in order to verify that the two-tiered process modeling approach for digitized forensics introduced in Section 3.1 is suitable for such specific investigations as well. This chapter is structured as follows:

6.1	Fundamentals of Application Scenario 2: Forgery Creation and Subjective Analysis	141
6.1.1	Creation of Latent Fingerprints using Ink-Jet Printers and Artificial Sweat	141
6.1.2	Subjective Assessment and Data Gathering for Fingerprint Trace Forgery Detection	143
6.2	Feature Space Design for Fingerprint Trace Forgery Detection	144
6.2.1	Dot-Based Features	145
6.2.2	Crystalline Structure-Based Features	148
6.2.3	Benford's-Law-Based Features	149
6.3	Detection of Printed Latent Fingerprint Forgeries . .	150
6.3.1	Selection of the Most Suitable Available Sensor for the Detection of Printed Latent Fingerprint Forgeries	150
6.3.2	Experimental Setup for the Detection of Printed Latent Fingerprint Forgeries	151
6.3.3	Evaluation of the Three Feature Spaces	152
6.3.4	Evaluation of the Detection of Printed Latent Fingerprint Forgeries on Specific Substrate Materials . .	152
6.3.4.1	Evaluation of Dot Based Features	153
6.3.4.2	Evaluation of Crystalline Structure Based Features	153
6.3.4.3	Evaluation of Benford's Law Based Features .	154
6.3.4.4	Summary of the Evaluation of the Detection Performance on Individual Substrate Materials	155
6.3.5	Substrate-Independent Evaluation of the Detection of Printed Latent Fingerprint Forgeries	155

6.3.6 Fusion of the Three Feature Spaces 156

6.3.7 Summary of the Evaluation of the Three Feature Spaces for the Detection of Printed Latent Fingerprint Forgeries 157

6.3.8 Benchmarking of the Detector Robustness using StirTrace157

6.3.8.1 StirTrace Benchmarking of Sensor Characteristics 158

6.3.8.2 StirTrace Benchmarking of Smudgy Fingerprint Effects 159

6.3.8.3 StirTrace Benchmarking of Printer Characteristics 160

6.3.8.4 StirTrace Benchmarking of Acquisition Conditions 160

6.4 Feature Selection 163

6.5 Chapter Summary and Limitations 164

In order to address the issue of anti-forensics in the context of latent fingerprint investigation at first it is necessary to define genuine traces - called real latent fingerprints within the scope of this thesis.

Definition 6.1: Real Latent Fingerprint

A real latent fingerprint has been created by the contact of a finger with a substrate. This contact is leaving residue behind, which forms the latent fingerprint pattern.

Definition of Real Latent Fingerprints

Latent Fingerprint Forgeries

SP	PA	OP	TP	TI	TA	TS
		DG	DI	DA	DO	DS
DO						

Special challenges in forensics arise from forged and fabricated traces. Such traces could be used to mislead forensic experts, resulting in potentially erroneous conclusions. In the context of latent fingerprints such forgeries could be created by transferring a latent fingerprint from one object to another (fabricated evidence) or by creating it entirely artificially (forged evidence) [Wer94], whereas the latter is the focus of this chapter:

Definition 6.2: Latent Fingerprint Forgery

A latent fingerprint forgery or in short fingerprint forgery is an artificially created fingerprint pattern that is placed on a substrate. Fingerprint forgeries might be created using various chemical solutions to form the residue mimicking a real latent fingerprint.

Definition of Latent Fingerprint Forgeries

Forensic experts are trained to some extent to recognize fabricated or forged evidence. However, in order to detect forged evidence, experts usually pay attention for multiple identical traces which are highly unlikely in practice. The alternative of printing latent fingerprints allows for creating slightly different patterns and thus, avoiding raising any suspicion based on the training of the expert. Such a technique for printing latent fingerprints using artificial sweat has been proposed by Schwarz [Sch09] for the purpose of evaluating chemical preprocessing techniques for porous substrates. However, given the low requirements for recreating the technique based on off-the-shelf ink-jet printers it is possible to misuse the technique for tampering with crime scenes by placing forged traces. Thus, the detection of printed fingerprints is an important step during the analysis phase of the ACE-V model in the data analysis as described

in Section 3.1.7. A novel pattern recognition based approach is introduced and evaluated in this chapter addressing research question Q_6 to mitigate the risks arising from this forgery creation technique. With respect to [IR00, pp. 43 – 61], this particular detection constitutes an identification or determination of class characteristics.

As this second application scenario is intended for the validation of the applicability of the process model introduced in Section 3.1 as well, the processing steps are mapped to the first-tier phases of the model as well. The particularly involved phases are highlighted in Figure 6.1. The design, evaluation and extended

Q_6 : Detection of Forged Traces

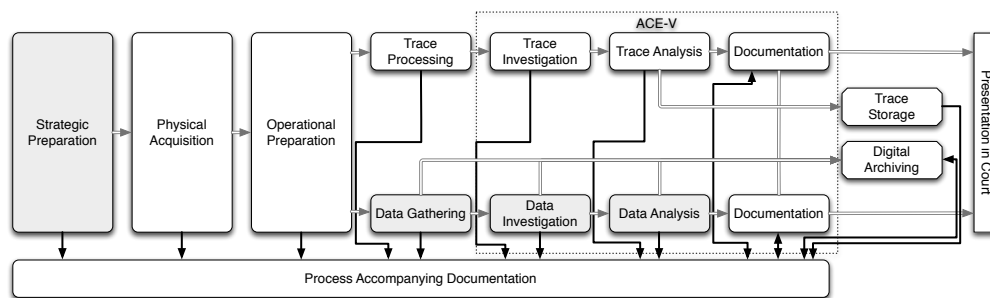


Figure 6.1: Overview of First-Tier Phases of the Novel Model of the Digitized Forensics Process, Phases Highlighted by Gray Shading are Addressed within this Chapter

benchmarking of the feature spaces and the trained models can be considered as individual second-tier phases of the strategic preparation. The actual application of the designed approach is primarily a second-tier phase for the data analysis as a part of the analysis phase of the ACE-V model supporting the latent fingerprint examiner. In addition to that, particular second-tier phases regarding the data gathering and the data investigation in the form of preprocessing are addressed by this chapter as well.

The contents of this chapter have been peer reviewed and published in part within the scope of the following publications as joint work with the co-authors Jana Dittmann, Stefan Kiltz, Claus Vielhauer and Jennifer Sturm (in descending order of the frequency of co-authorship): [DiH14], [HKS+12], [HiD15a], [HiD15b], [HKD13a], [Hil15], [HiD14], [HiD16] and [HKD+11].

6.1 Fundamentals of Application Scenario 2: Forgery Creation and Subjective Analysis

This section contains the fundamentals of this application scenario. At first the process of forging latent fingerprints using artificial sweat and ink-jet printers is analyzed towards the attack chain in Section 6.1.1. Afterward, the digitization and subjective assessment of the latent fingerprint forgeries is described in Section 6.1.2 as a preparation for the sensor selection and to design of particular detection features.

6.1.1 Creation of Latent Fingerprints using Ink-Jet Printers and Artificial Sweat

The general approach for creating latent fingerprint forgeries within the scope of this thesis is derived from the method proposed by Schwarz [Sch09]. In particular

a solution of water, sodium chloride and various amino acids is mixed to mimic some of the properties of the sweat forming latent fingerprint residue. In order to be able to print such forgeries, it is required that the resulting liquid is more or less compatible with common ink-jet printing technologies. Nowadays, two different drop-on-demand ink-jet printing technologies are utilized: bubble-jet and piezoelectric-electric print heads. Whereas the objective of both techniques is to deposit a small drop of ink on the substrate the printer is printing on, the two printing techniques are quite different.

Drop-on-Demand
Ink-Jet
Technologies

A bubble-jet printer heats the ink in the nozzle of the print head. This forms a bubble which shoots out a drop of ink resulting in its deposition on the substrate [LT88, pp. 335-345]. A piezoelectric printer uses a piezoelectric element in each nozzle. This element is deformed when an electric current is applied [LT88, pp. 332-334]. This deformation of the element shoots a drop of ink out of the nozzle. Each modern printer is equipped with a print head with several nozzles in order to create the patterns of ink on the substrate. Each manufacturer designs the printer for the specific properties of the ink, e.g. its viscosity. In addition to that, especially within bubble-jet printers, it is essential that the bubble can be formed within the nozzle in order to eject a drop of ink from it. Within the scope of the thesis, the properties of the artificial sweat are not compared with those of the manufacturer ink. Thus, it is possible that a specific printer might show incompatibilities resulting in a deteriorated printing result.

Potential
artifacts caused
by printing
defects

Printing defects, such as blocked nozzles, result in visible artifacts that could be exploited in order to detect the forged latent fingerprint. Due to the nature of ink-jet printers, gray shadings need to be created using a certain combination of microscopic ink drops and areas without ink. Depending on the distribution and relative amount of area covered by ink, various shades of gray can be created. This process is called halftoning (see e.g. [LT88, pp. 347-352]). Similar to that, different colors can be created based on typically four different ink colors in ink-jet printers. Due to this mechanism of the printer, ideally the digital template for the fingerprint forgery is provided in the form of a binary image. Otherwise, the resulting fingerprint forgery will not contain any continuous ridge line impression. Several attack chains are possible using artificial sweat [DiH14]. Figure 6.2 depicts the steps for the creation of the print sample to the final placement of the latent fingerprint forgery. The awareness about this attack chain is an important foundation for raising awareness and developing detection mechanisms within the phase of the strategic preparation (see Section 3.1.2). During the first step,

Printing Pipeline
for Creating
Latent
Fingerprints
using Artificial
Sweat

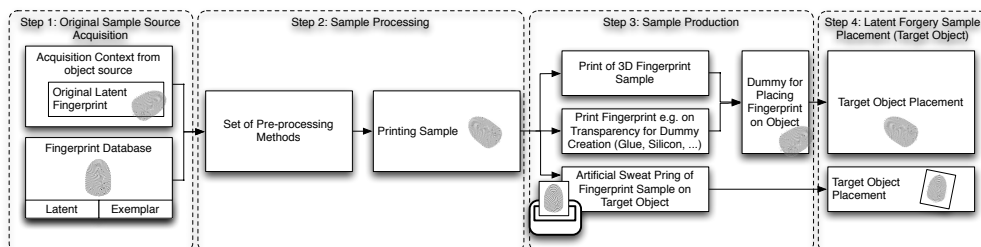


Figure 6.2: Full Context Attack Chain for Latent Fingerprint Forgeries Resketched from [DiH14] as a Foundation for the Strategic Preparation for Designing Detection Approaches

the fingerprint sample can either originate from a database containing latent or exemplar fingerprints or being lifted as a latent fingerprint from an object. During

the second step, the fingerprint needs to be preprocessed. Such preprocessing steps consist of a binarization of the image in order to avoid halftoning-patterns during the printing process and pattern enhancement or modification steps. The slight modification of the pattern is necessary if multiple printing samples should be derived from a single source sample. Otherwise, a number of identical latent fingerprints at the crime scene might raise suspicion during the investigation by a latent print examiner. After the print sample has been created, several options exist for the third step of the sample production. Within the scope of this thesis, the focus lies on the direct printing of latent fingerprint samples on objects using ink-jet printers and artificial sweat. However, it is also possible to create 3D fingerprint samples - e.g. for creating stamps using flexible filament in a 3D printer or by printing on a transparency using a laser printer as a production step for a latex, silicon or glue based dummy finger. Afterward the dummy finger or the 3D stamp could be used to stamp latent fingerprints with artificial sweat to arbitrary substrates. Those options are particularly relevant for placing latent fingerprints on non-planar surfaces where using a printer is impossible. For planar substrates the direct printing of artificial sweat is probably more reliable. Especially with compact mobile printers which can print on arbitrary surfaces, such as the PrinCube¹, a large number of variations of the same fingerprint pattern could in theory be placed at crime scenes.

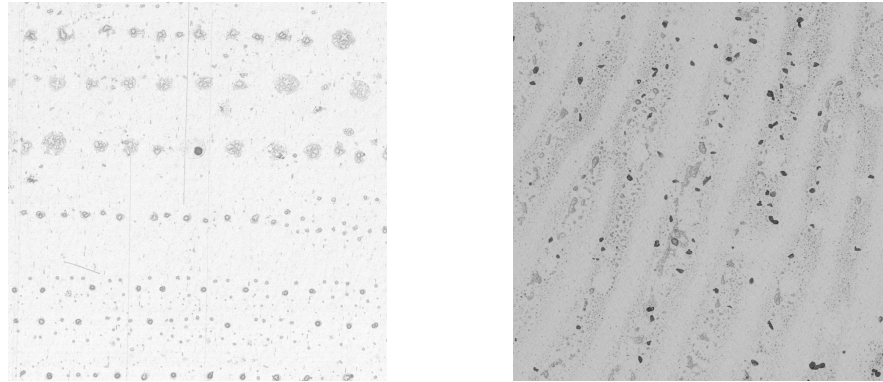
The fourth and last step of the attack chain consists of the placement of the target objects at the crime scene.

6.1.2 Subjective Assessment and Data Gathering for Fingerprint Trace Forgery Detection

For analyzing latent fingerprints towards potential indicators of a fingerprint forgery, it is necessary to acquire a small area of the latent fingerprint at a very high resolution. In addition to that, a non-destructive acquisition technique without the need for any preprocessing of the physical trace is desirable, because any processing might destroy particular properties of the forgery which can be utilized for its detection. Two different sensors are evaluated for the acquisition of the traces within the scope of this thesis, a chromatic-confocal sensor (FRT CWL600, S_1 : $S_{1T} = \{M_{2.2}, O_1, D_{Syntax_2}, D_{Semantics_3}\}$, $S_{1I} = \{M_{2.2}, O_1, D_{Syntax_2}, D_{Semantics_1}\}$) with a maximum lateral resolution of 12700 ppi and a confocal laser scanning microscope (Keyence VK-x 110 CLSM, S_2 : $S_{2T} = \{M_1, O_3, D_{Syntax_2}, D_{Semantics_3}\}$, $S_{2I} = \{M_1, O_3, D_{Syntax_2}, D_{Semantics_1}\}$, $S_{2C} = \{M_{2.2}, O_3, D_{Syntax_3}, D_{Semantics_2}\}$) with a 10x objective lens resulting in a resolution of roughly 20000 ppi. Those acquisition resolutions significantly exceed the currently recommended resolution of acquiring latent fingerprints specified at 1000 ppi. However, acquiring the full fingerprint at such a high resolution is, at least at the time of the creation of the thesis, impractical due to the resulting file sizes and the duration of the digitization process. Thus, only a small section of 2 by 2 millimeters (S_1) or 1.3 by 1 millimeters (S_2) is acquired for the analysis. The acquisition time with those settings using S_1 is roughly 70 minutes for reflective substrates. Particular scan results for a printed and a real latent fingerprint are depicted in Figure 6.3. In contrast to that, the acquisition using S_2 is rather fast, being completed usually in less than a minute. However, the acquisition of surface areas exceeding the scan area of a particular objective lens would require image stitching of multiple scans. The results from S_2 are depicted in Figure 6.4.

Digitization of
potential
Fingerprint
Forgeries

¹<https://www.indiegogo.com/projects/princube-the-world-s-smallest-mobile-color-printer>

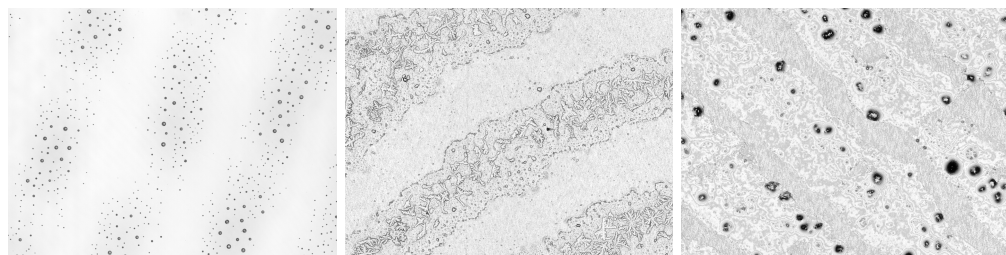


(a) Epson Piezoelectric Printer with Artificial Sweat

(b) Real Fingerprint with Natural Sweat

Figure 6.3: CWL (S_1) intensity data from fingerprints on an overhead transparency, 2 x 2 mm, 12700 ppi

Within the samples printed by an Epson piezoelectric ink-jet printer (Figure 6.3a



(a) Epson Piezoelectric Printer with Artificial Sweat

(b) Canon Bubble-Jet Printer with Artificial Sweat

(c) Real Fingerprint with Natural Sweat

Figure 6.4: CLSM (S_2) intensity data from fingerprints on an overhead transparency, 1.3 x 1 mm, 20000 ppi

and Figure 6.4a), the formation of dots of artificial sweat is quite dominant in the printing results. Real fingerprints usually form more continuous lines of deposited sweat as shown in (Figure 6.3b and Figure 6.4c). However, a pattern of dots is also visible, which might originate from skin cells and contaminants within the residue. The samples originating from the Canon Bubble-Jet ink-jet printer (Figure 6.4b) also show continuous lines of deposited sweat. In addition to that, crystals have formed within those lines. In empirical studies such crystals are characteristic for prints with artificial sweat, they can be also found within larger dots created by the piezoelectric ink-jet printer. However, some real latent fingerprint samples also show such crystals. In such cases, the donor usually had a low concentration of lipids in the sweat.

6.2 Feature Space Design for Fingerprint Trace Forgery Detection

For the feature extraction the two different observations of the occurrence of dots of different sizes [HKD+11] and the formation of crystalline structures [HKS+12], [HKD13a], [HiD15a] are exploited as content-dependent features. In addition to that, the samples are analyzed based on the distribution of gray

Forgery
Detection
Pipeline

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DS
DO						

values in the intensity images and height values in topography images, motivated by Benford’s law (see Section 2.4.4) as introduced in [HiD15b]. The design of the feature space and classification approach, including the training and/or evaluation is a part of the strategic preparation (see Section 3.1.2), whereas the final concept stretches from the data gathering over the data investigation to the data analysis phase.

6.2.1 Dot-Based Features

For the dot based features the pattern recognition pipeline after the sensing consists, as published in [HiD15a], of the steps depicted in Figure 6.5. In essence,

Dot-Based
Detection
Features

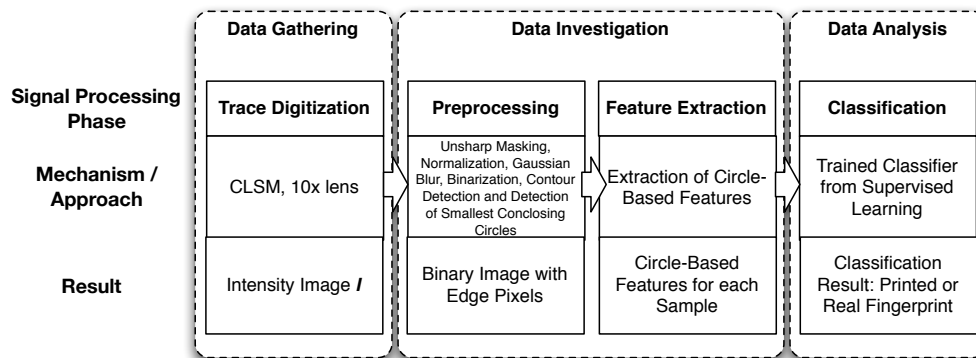


Figure 6.5: Signal Processing Pipeline for Circle-Based Features based on [HiD15a] as Second-Tier Phases of the novel Process Model for Digitized Forensics

the following processing steps are performed on the foundation of the intensity image I digitized by the CLSM S_2 :

- Preprocessing Step 1: Unsharp Masking,
- Preprocessing Step 2: Normalization,
- Preprocessing Step 3: Image Blurring,
- Preprocessing Step 4: Binarization using Otsu’s method [Ots79],
- Preprocessing Step 5: Contour detection,
- Preprocessing Step 6: Determination of Smallest Enclosing Circles,
- Feature Extraction Step 1: Extraction of statistical features based on the set of detected circles,

Depending on the point of view, the preprocessing steps 4-6 could also be considered as a part of the feature extraction because those steps are necessary to extract the information relevant for the feature space from the data. However, since all applied methods are fairly common image processing techniques, those steps are considered as preprocessing within the scope of this thesis.

In contrast to this approach for extracting circle-based features, the approach in [HKD+11] utilizes the Hough Circles algorithm for detecting the circles (preprocessing steps 5 and 6). However, the Hough Circles algorithm follows

a brute-force-attempt for the detection of the circles. Thus, it is rather slow in comparison to the detection of the Smallest Enclosing Circles. While the computational expensiveness is rather irrelevant for the acquisition using the CWL sensor S_1 , the feature extraction would significantly increase the processing time when the CLSM S_2 is used for the digitization of the samples.

The result of the Feature Extraction Step 3 is a set of detected circles $C: X \times Y \times R$. Each circle $c_i \in C$ is defined by its center point $(x_i, y_i) \in I_{x,y}$, $x_i \in X$, $y_i \in Y$ and its radius $r_i \in R$. Based on this set, the statistical features are extracted within step 4:

Number of circles $ncircles$ within an image I [HiD15a]:

$$ncircles = |C| \quad (6.1)$$

Mean circle radius $rmean$ of each circle c_i within C [HiD15a]:

$$rmean = \frac{1}{|C|} \cdot \sum_{i=0}^{|C|-1} r(c_i) \quad (6.2)$$

Here, the function r determines the radius of the circle c_i .

Standard deviation of the circle radii $rstddev$ [HiD15a]:

$$rstddev = \sqrt{\frac{1}{|C|} \sum_{i=0}^{|C|-1} (r(c_i) - rmean)^2} \quad (6.3)$$

Mean degree of filling $meanfill$ of the detected circles [HiD15a]:

$$meanfill = \frac{1}{|C|} \cdot \sum_{i=0}^{|C|-1} \frac{|F(x(c_i), y(c_i))|}{\pi \cdot r(c_i)^2} \quad (6.4)$$

The feature describes the set of pixels within the circle c_i with a center point (x, y) . The functions $x(c_i)$ and $y(c_i)$ determine the x and y coordinates of each circle c_i , whereas $F(x, y)$ employs a connected component labeling based approach starting at the center point of a circle to determine the number of connected pixels. The regular shape of the amino acid dots created by the ink-jet printers should result in a larger degree of filling in comparison to the rather irregularly shaped contaminants in real fingerprints.

Mean horizontal circle distance $hmean$ [HiD15a]:

$$hmean = \frac{1}{|C_c|} \cdot \sum_{i=0}^{|C_c|-1} |x(c_i) - x(c_{i+1})|, \quad (6.5)$$

$$C_c \subset C : \forall C_i \in C_c : x(c_i) - x(c_{i+1}) < 300\mu m,$$

$$y(c_i) - y(c_{i+1}) < 600\mu m$$

The nearest neighboring circle is determined for each detected circle. If the distance to the neighboring circle does not exceed a horizontal distance of $300\mu m$ and a vertical distance of $600\mu m$, the horizontal distance is recorded. Otherwise, the circle is excluded because no neighboring circle has been detected. The motivation for those distance thresholds is the geometry of the print head and the ridge-valley-pattern of the fingerprint, which could cause very large distances between dots of two adjacent ridges.

Mean vertical circle distance $vmean$ [HiD15a]:

$$vmean = \frac{1}{|C_c|} \cdot \sum_{i=0}^{|C_c|-1} |y(c_i) - y(c_{i+1})|, \quad (6.6)$$

$$C_c \subset C : \forall C_i \in C_c :$$

$$y(c_i) - y(c_{i+1}) < 300\mu m, x(c_i) - x(c_{i+1}) < 600\mu m$$

Analogous to the mean horizontal circle distance, the mean vertical circle distance is determined using thresholds for a maximum vertical distance of $300\mu m$ and maximum horizontal distance of $600\mu m$.

The probability density function for the circle radii results in 15 features $rpdf_1 \dots rpdf_{15}$. In essence those features represent a histogram of the number of observed radii for an empirically determined bucket size of $6\mu m$ normalized by the total number of detected circles within the I [**HiD15a**]:

$$\begin{aligned} rpdf_k &= \frac{|C_r|}{|C|}, C_r \subset C : \\ \forall c_i \in C_r \quad (k-1) \cdot 6\mu m &\leq r(c_i) < k \cdot 6\mu m, 1 \leq k \leq 15 \end{aligned} \quad (6.7)$$

The bucket number within the histogram of circle radii is indicated by k . The probability density function features are supposed to describe the actual distribution of circle radii within the acquired data.

Probability density functions are also used as features for the horizontal and vertical circle distances as defined in Equation 6.8 and Equation 6.9 [**HiD15a**]:

$$\begin{aligned} hpdf_k &= \frac{|C_h|}{|C|}, C_h \subset C : \forall c_i \in C_h \quad (k-1) \cdot 40\mu m \\ &\leq (x(c_i) - x(c_{i+1})) < k \cdot 40\mu m, 1 \leq k \leq 15 \end{aligned} \quad (6.8)$$

$$\begin{aligned} vpdf_k &= \frac{|C_v|}{|C|}, C_v \subset C : \forall c_i \in C_v \quad (k-1) \cdot 40\mu m \\ &\leq (y(c_i) - y(c_{i+1})) < k \cdot 40\mu m, 1 \leq k \leq 15 \end{aligned} \quad (6.9)$$

For Equation 6.8 and Equation 6.9 a bucket size of $40\mu m$ is used for determining the histogram.

The distance features are likely not rotation invariant because different thresholds need to be used for the horizontal and vertical dot distances due to the properties of fingerprint patterns. Thus, additionally the distances are determined using the nearest neighbor method for determining the mean distance between two neighboring dots [**HiD15a**]:

$$\begin{aligned} nnmean &= \frac{1}{|C|} \cdot \sum_{i=0}^{|C|-1} \\ &\quad \sqrt{(x(c_i) - x(c_l))^2 + (y(c_i) - y(c_l))^2}, \\ &\quad c_i, c_l \in C, \\ \forall c_i &: (x(c_i) - x(c_l))^2 + (y(c_i) - y(c_l))^2 \\ &< (x(c_i) - x(c'_l))^2 + (y(c_i) - y(c'_l))^2 \end{aligned} \quad (6.10)$$

The probability density function for the nearest neighbor distances is determined with a bucket size of $20\mu m$ [**HiD15a**]:

$$\begin{aligned} nnpdf_k &= \frac{|C_n|}{|C|}, C_n \subset C : \forall c_i \in C_n \\ (k-1) \cdot 20\mu m &\leq \sqrt{(x(c_i) - x(c_l))^2 + (y(c_i) - y(c_l))^2} \\ &< k \cdot 20\mu m, 1 \leq k \leq 15 \end{aligned} \quad (6.11)$$

For the nearest neighbor distances in Equation 6.10 and Equation 6.11 no particular threshold is used for excluding implausible neighbors of a circle.

6.2.2 Crystalline Structure-Based Features

Edge-based features for analyzing and quantifying the amount of crystalline structures

Based on the formation of crystalline structures within the dried artificial sweat of latent fingerprint forgeries, it is reasonable to assume that the presence of a large number of such crystals can be used as an indicator for the detection of such forgeries. However, certain sweat compositions might also lead to the formation of some crystalline structures in real latent fingerprints as well.

In [HKS+12] the crystalline structures are used to detect latent fingerprint forgeries. The corresponding signal processing pipeline based on intensity images I originating from the CLSM S_2 is depicted in Figure 6.6. During the preprocessing

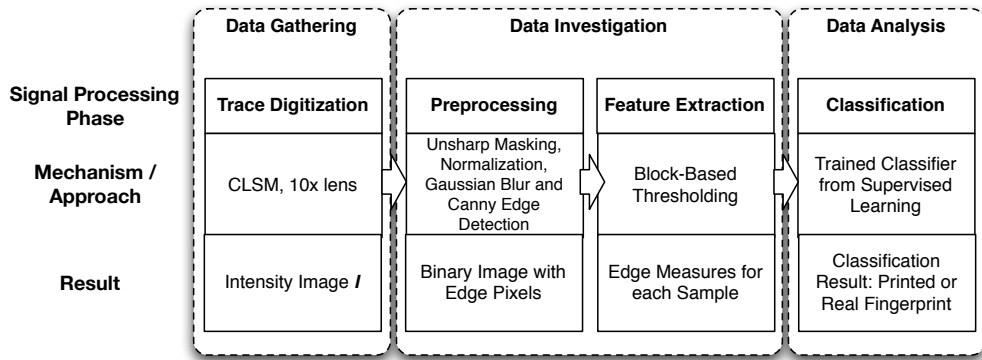


Figure 6.6: Signal Processing Pipeline for Crystalline Structure-Based Features based on [HKS+12] as Second-Tier Phases of the novel Process Model for Digitized Forensics

at first the intensity image I is blurred using a Gaussian blur in order to remove small artifacts such as measurement errors that would otherwise be detected as an edge within the image. The second step of the preprocessing consists of the application of Canny's edge detection algorithm [Can86] to detect edges within the image data. Based on the observation of the crystalline structures within the fingerprint forgeries originating from an ink-jet printer equipped with amino acid, the edge detection algorithm should yield a higher number of edge pixels in comparison to real latent fingerprints.

Afterward, the feature extraction is performed using a non-overlapping block based approach as specified in Equation 6.12 [HiD15a]:

$$\begin{aligned}
 E_\tau &= \frac{1}{k \cdot l} \cdot \sum_{b_x=0}^k \sum_{b_y=0}^l E_{(b_x, b_y)}^\tau, \\
 &\quad k = \lfloor \frac{X}{b} \rfloor, l = \lfloor \frac{Y}{b} \rfloor, b = 10 \\
 E_{(b_x, b_y)}^\tau &= \begin{cases} 1 & \text{if } \sum_{x=0}^b \sum_{y=0}^b I_{((b \cdot b_x + x), (b \cdot b_y + y))} > \tau \cdot b^2 \\ 0 & \text{otherwise} \end{cases} \quad (6.12)
 \end{aligned}$$

For the feature extraction a block size b of 10 by 10 pixels is used. The actual feature space is formed by using different thresholds τ for the relative number of edge pixels within a block. In total ten features E_τ within the range $0.05 \leq \tau \leq 0.5$ are derived for the image I . In essence E_τ contains the percentage of blocks with a number of edge pixels exceeding $\tau \times b^2$ pixels.

6.2.3 Benford's-Law-Based Features

Whereas the features based on amino acid dots in Section 6.2.1 and crystalline structures in Section 6.2.2 rely on visual properties of the printed fingerprint forgeries, the Benford's Law-Based feature space is purely based on the distribution of pixel values within the digitized image I . In [HiD15b] the finding of significantly different distributions between real and printed fingerprints are reported for CLSM S_2 scans. Here, the topography data follows the Benford distribution [Ben38] (see Section 2.4.4) pretty closely, whereas the intensity data shows the highest probability for the first digit six as depicted in Figure 6.7. The distributions are determined on the foundation of 3000 amino acid printed

Benford's-law-based features for detecting amino acid printed latent fingerprint forgeries

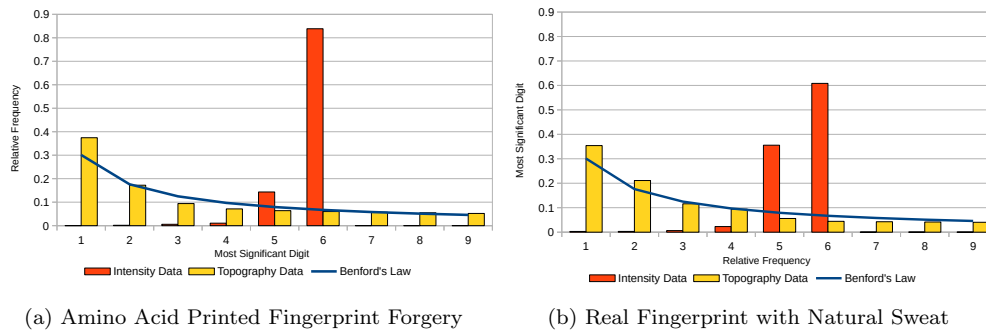


Figure 6.7: Distribution of the most significant digits in CLSM (S_2) intensity and topography data based on [HiD15b]

fingerprint forgeries and 3000 real latent fingerprints with natural sweat. This test set is used for the first time within the scope of [HKD13a], consisting of samples originating from three different substrates, namely overhead transparencies, compact disks and hard disk platters.

The signal processing pipeline for the classification of samples is depicted in Figure 6.8. The intensity image data I_I is not preprocessed before the feature

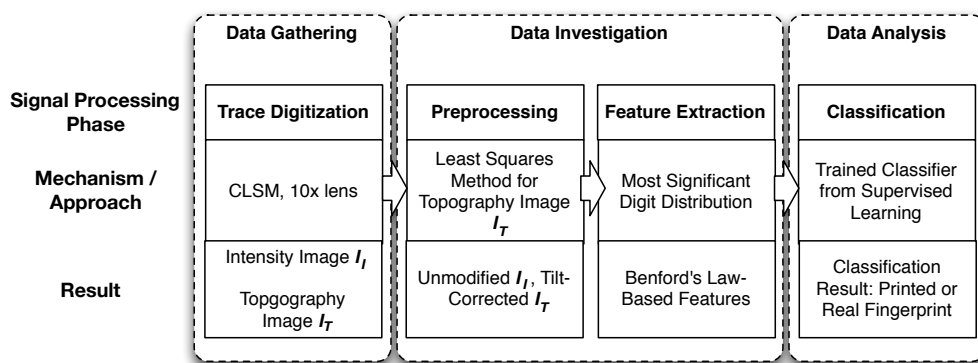


Figure 6.8: Signal Processing Pipeline for Benford's-Law-Based Features based on [HiD15b] as Second-Tier Phases of the novel Process Model for Digitized Forensics

extraction, whereas the topography image data I_T is preprocessed using the least-squares-method (see Section 2.3.5.1) in order to compensate any slightly tilted placement of the substrate on the measurement device.

The feature space is formed by the difference of the observed probability of a

most significant digit within $I = (x, y)$ and its distribution defined by Benford's law, based on [HiD15b]:

$$\begin{aligned}
 FB_d^I &= \left(\frac{1}{x \cdot y} \cdot \sum_{k=1}^x \sum_{l=1}^y MSD_{(k,l)}^d \right) - \log_{10} \left(1 + \frac{1}{d} \right), \\
 &\quad d \in [1, 9], I \in \text{intensity, topography}; \text{ with} \\
 MSD_{(k,l)}^d &= \begin{cases} 1 & \text{if } MSD(I_{k,l}) = d \\ 0 & \text{otherwise} \end{cases}
 \end{aligned} \tag{6.13}$$

Here, the function $MSD(I_{k,l})$ determines the most significant digit of a pixel (k,l) within an image I . The result of the feature extraction process are 9 features for the intensity data and 9 features for the topography data of a digitized sample.

6.3 Detection of Printed Latent Fingerprint Forgeries

The ability to detect latent fingerprint forgeries is important in forensic investigations in order to avoid errors and resulting convictions of innocent persons. An automated tool which can indicate the need for a more thorough investigation of a particular trace could support forensic experts within the scope of digitized forensics. However, in order to contribute to the forensic process, it is necessary that the particular false miss and false alarm rates are as low as possible because otherwise such a tool would be considered unreliable. The following subsections describe the evaluation of the proposed feature spaces towards their detection performance of printed latent fingerprint forgeries.

6.3.1 Selection of the Most Suitable Available Sensor for the Detection of Printed Latent Fingerprint Forgeries

In order to select the most suitable available sensor from Section 4.1 for the detection of latent fingerprint forgeries, it is necessary to define and assess particular requirements. The following requirements that should be met by a sensor for this use-case of digitized forensics are summarized in Table 6.1. The first

Cross Validation
of The Classifier

SP	PA	OP	TP	TI	TA	TS
			DG	DI	DA	DO
						DS
						DO

	S_1	S_2	S_3
1. Latent Fingerprint Residue Acquirable	✓	✓	✓
2. Reproducible Results	✓	✓	✓
3. Process Automation	✓	(✓)	✓
4. High Lateral Resolution Detailed Scans	✓	✓	✗
5. Fast Digitization Process	○	✓	✗

Table 6.1: Comparison of the CWL (S_1), CLSM (S_2) and UV-VIS (S_3) Sensors Regarding the Requirements for the Detection of Latent Fingerprint Forgeries: ✓ Denotes a Fulfilled Requirement, ○ Is a Partially Fulfilled Requirement, ✗ Indicates a Non-Fulfilled Requirement

three requirements are identical to the generic acquisition of latent fingerprints in Section 5.3.1, because those particular requirements are considered a necessity for the application in the context of digitized forensics. The fourth requirement "high lateral resolution detailed scans" is defined on the foundation of [KHD+11], which shows that a high acquisition resolution of at least 3200 ppi is necessary to recognize particular detection properties. Based on this threshold, S_1 and S_2

are in general suitable for the detection of latent fingerprint forgeries. The fifth requirement "fast digitization process" is important for such a confirmation process that a particular trace is not a forgery. In order to delay the digitization of the fingerprint as minimal as possible, a fast digitization of small areas at a high lateral resolution is advantageous. The requirement is fully fulfilled by S_2 with digitization times of a few minutes. For S_1 in [HKD+11] a scan duration of more than an hour is reported. Thus, the requirement is only partially fulfilled. The digitization using S_3 is too slow due to the high integration times of the spectrometer.

The CLSM sensor S_2 is selected for the evaluation of detection of printed latent fingerprint forgeries based on the assessment of those particular requirements. Given the available sensory, this particular sensor is considered the most suitable device for the digitization of the test samples within the data gathering phase since all particular requirements are fulfilled.

Selected Sensor

6.3.2 Experimental Setup for the Detection of Printed Latent Fingerprint Forgeries

In this thesis, the experimental setup for the detection of printed latent fingerprint forgeries from [HKD13a] is used. This particular data set is captured using the CLSM S_2 from three different highly cooperative substrate materials as summarized in Table 6.2. For the selection of the substrates three particular

Experimental Setup

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DO	DS
DO							

Source	Substrate Material			All
	Hard Disk Platter M_{1P}	Overhead Foil M_{2P}	Compact Disk M_{3P}	
Samples from real fingerprints	1000	1000	1000	3000
Samples from printed fingerprints	1000	1000	1000	3000
Total	2000	2000	2000	6000

Table 6.2: Overview Test Sample from the CLSM S_2 based on [HKD13a]

factors are crucial:

1. The ink-jet printer must be able to print directly on the particular substrate material,
2. The available sensory must be able to digitize the residue on the substrate,
3. No particular preprocessing should be necessary in order to render the residue on the substrate visible, i.e. no segregation of the fingerprint data from the substrate data is necessary.

For the printed fingerprints a Canon PIXMA iP4600² bubble jet ink-jet printer is used. This printer is capable of printing directly on compact disks using a special printing tray. This particular tray is utilized for printing on M_{1P} and

²<https://www.usa.canon.com/internet/portal/us/home/products/details/printers/support-inkjet-printer/ip-series/pixma-ip4600>

M_{3P} . In total, fingerprint patterns from all ten fingers of four test persons are used to create the 1000 samples per substrate material. The digitization process is partially automated by acquiring several scans relative to the center of the fingerprint pattern using S_2 with the 10x magnification objective lens. The z-Pitch is set to one micrometer. As a result of this sensor parameterization, each scan has a varying scan duration between 15 and 30 seconds.

Classifier
Selection and
Error Rates

The evaluation of the detection of printed latent fingerprint forgeries is performed using various classifiers from the WEKA data mining software (version 3.6.6) [Hal+09]. The classification is performed within a two-class supervised learning approach. The initial evaluation of the feature spaces utilizes a ten-fold cross validation to determine the detection performance of the trained classifier models. In line with [HKD13a], the false positive rate FPR, false negative rate FNR and accuracy ACC are used as quality metrics for the evaluation. The consideration of the two separate error rates is necessary in order to determine the false alarm rate which equals the FPR as well as the miss rate, which equals the FNR. This is necessary because the detection of potential latent fingerprint forgeries should trigger additional investigations steps which might be time-consuming. On the other hand, a missed detection of a fingerprint forgery might lead to the conviction of innocent persons. Thus, the three performance indicators are important to compare the evaluation results of different models and classifiers with each other. The half total error rate is additionally used in [HKD13a] for evaluating the performance. However, since this performance indicator is directly related to the classification accuracy, it is omitted within the scope of this thesis. The experimental setup consists of equal amounts of samples for the two classes of printed and real fingerprints. Thus, the particular classifier models should be bias-free. In addition to that, a proper ground truth label is assigned for each sample based on the known origin of the digitized trace.

Fusion and
Benchmarking

For the fusion of the feature spaces and the benchmarking of the classification approaches using StirTrace, the test data is separated into a set of training data containing 500 printed and 500 real samples for each of the three substrates. The remaining test data contains 500 printed and 500 real samples for each of the three substrates as well. However, the test and training data is gathered in two independent sessions in order to avoid any bias within the trained models.

6.3.3 Evaluation of the Three Feature Spaces

In [HKD13a] various classifiers are evaluated for a combination of the dot based features described in Section 6.2.1 and crystalline structure based feature described in Section 6.2.2. Based on those findings, the classifiers Multilayer Perceptron [Bau88], Logistic Model Tree [LHF05] and Dagging [TW97] show the best detection performances. In addition to that, the ensemble classifier RotationForest [RKA06] is used in [HiD15a]. The preprocessing of the test samples described in Section 6.3.2 for the feature extraction is performed as described in Section 6.2. The raw evaluation reports from WEKA are included in this thesis in Section A.4.

6.3.4 Evaluation of the Detection of Printed Latent Fingerprint Forgeries on Specific Substrate Materials

In order to evaluate the detection performance of the three feature spaces at first a cross validation is performed for each substrate material. This evaluation is supposed to avoid any bias caused by substrate properties and thus, should

allow for an assessment of the detection performance for each feature space in lab conditions.

6.3.4.1 Evaluation of Dot Based Features

The detection using the dot based features yields a very high accuracy for all four evaluated classifiers as summarized in Table 6.3. On the highly cooperative

	M_{1P}			M_{2P}			M_{3P}		
	FNR	FPR	ACC	FNR	FPR	ACC	FNR	FPR	ACC
LMT	0.4	0.1	99.75	0.1	0.3	99.8	0.8	0.7	99.25
MLP	0.5	0.5	99.5	0.2	0.2	99.8	0.8	1.2	99
DAG	0.7	0	99.65	0.1	1.2	99.35	0.5	0.2	99.65
RF	0.6	0.1	99.65	0.3	0.2	99.75	1.2	0.3	99.25

Table 6.3: Evaluation of Dot Based Features using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)

hard disk platter substrate material M_{1P} the best performance is achieved using the Logistic Model Tree (LMT) classifier [LHF05] with a detection accuracy of 99.75%. In addition to that, the false miss rate (FNR) is the lowest with 0.4%. The lowest false alarm rate (FPR) is zero using the Dagging (DAG) classifier [TW97].

On the overhead foil M_{2P} the best detection performance of 99.8% is achieved using LMT and the MultilayerPerceptron (MLP) [Bau88]. The lowest miss rate of 0.1% is achieved with LMT and DAG. The lowest false alarm rates of 0.2% are achieved using MLP and the RotationForest (RF) classifier [RKA06].

On the compact disk M_{3P} , the highest accuracy of 99.65% is achieved with the Dagging (DAG) classifier, which also has the lowest false miss rate (0.5%) and false alarm rate (0.2%).

6.3.4.2 Evaluation of Crystalline Structure Based Features

The detection using the crystalline structure based features yields a high to very high detection accuracy for all four evaluated classifiers as summarized in Table 6.4. On the highly cooperative hard disk platter substrate material M_{1P} the

	M_{1P}			M_{2P}			M_{3P}		
	FNR	FPR	ACC	FNR	FPR	ACC	FNR	FPR	ACC
LMT	1.8	0.5	98.85	0.6	0.2	99.6	2.2	2.8	97.5
MLP	1.8	0.7	98.75	1.0	0.3	99.35	1.9	2.9	97.6
DAG	1.1	8.9	95	2.8	3.1	97.05	4.2	37.6	79.1
RF	1.7	0.4	98.95	1.0	0.4	99.3	1.5	3.1	97.7

Table 6.4: Evaluation of Crystalline Structure Based Features using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)

best performance is achieved using the RotationForest (RF) classifier [RKA06]

with a detection accuracy of 98.95%. In addition to that, the lowest false alarm rate (FPR) of 0.4% is achieved using this classifier. The lowest false miss rate (FNR) 1.1% using the Dagging (DAG) classifier [TW97].

On the overhead foil M_{2P} the best detection performance of 99.6% is achieved using the Logistic Model Tree (LMT) classifier [LHF05]. This particular classifier also yields the lowest false miss rate (FNR) of 0.6% and false alarm rate (FPR) of 0% on this particular substrate material.

On the compact disk M_{3P} , the best performing classifier is RF, yielding a detection accuracy of 97.7%, which also has the lowest false miss rate (FNR) of 1.5%. The lowest false alarm rate (FPR) of 2.8% is achieved using LMT.

A significant outlier for this feature space is the performance of the Dagging classifier (DAG) [TW97]. On M_{1P} and M_{3P} the cross validation yields very high false alarm rates of 8.9% and 37.6%. Thus, this classifier cannot be considered a viable option for detecting latent fingerprint forgeries within the crystalline structure based feature space.

6.3.4.3 Evaluation of Benford’s Law Based Features

The detection using the Benford’s Law based features yields a high to very high detection accuracy for all four evaluated classifiers as summarized in Table 6.5. On the highly cooperative hard disk platter substrate material M_{1P} the highest

	M_{1P}			M_{2P}			M_{3P}		
	FNR	FPR	ACC	FNR	FPR	ACC	FNR	FPR	ACC
LMT	0.1	0.1	99.9	0.3	0.6	99.55	0.6	0.6	99.4
MLP	0.2	0.1	99.85	0.3	0.6	99.55	0.2	0	99.9
DAG	0.4	1.1	99.25	0.3	10.2	94.75	1.8	13	92.6
RF	0.3	0.1	99.8	0.4	0.2	97.7	0.6	0.2	99.6

Table 6.5: Evaluation of Benford’s Law Based Features using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)

detection accuracy is achieved using the Logistic Model Tree (LMT) classifier [LHF05] with a detection accuracy of 99.9%. This particular classifier also yields the lowest the false miss rate (FNR) of 0.1%. The lowest false alarm rate (FPR) is 0.1% for LMT, the MultilayerPerceptron (MLP) [Bau88] and RotationForest (RF) [RKA06] classifiers.

On the overhead foil M_{2P} the best detection performance of 99.55% is achieved using LMT and MLP. The lowest false miss rate of 0.3% is achieved with LMT, MLP and Dagging (DAG) [TW97] classifiers. The lowest false alarm rate of 0.2% is achieved using the RotationForest (RF) classifier.

On the compact disk M_{3P} , the highest accuracy of 99.9% is achieved with MLP, which also has the lowest false miss rate (0.2%) and false alarm rate (0%).

For the Benford’s Law based feature space a similar phenomenon as already described in Section 6.3.4.2 for the crystalline structure based features can be observed for the Dagging classifier. In particular on M_{2P} and M_{3P} the usage of this particular classifier results in high false alarm rates, which results in a false alarm for 10% of the evaluated samples of real fingerprints.

6.3.4.4 Summary of the Evaluation of the Detection Performance on Individual Substrate Materials

In summary all three feature spaces seem to be very suitable to detect printed latent fingerprint forgeries. However, for the crystalline structure and Benford's law based feature spaces the Dagging classifier has a tendency to yield large numbers of false alarms. Thus, this particular classifier seems to be unstable for detecting printed latent fingerprint forgeries within those feature spaces in any practical forensic application. Overall, the classification accuracy is at least 95% for all classifiers on the very cooperative hard disk platter surface M_{1P} . All classifiers with the exception of Dagging yield a classification accuracy of at least 97.5% on M_{2P} and M_{3P} . However, training a model for each substrate can be very time-consuming and also requires the selection of the proper classification model matching the substrate a latent fingerprint in question is present on. Thus, it is reasonable to investigate the performance of substrate independent models as well, which is discussed in Section 6.3.5.

6.3.5 Substrate-Independent Evaluation of the Detection of Printed Latent Fingerprint Forgeries

The substrate-independent evaluation results for the four selected classifiers are summarized in Table 6.6. The highest detection accuracy of 99.43% is achieved

	Dot Based Features			Crystalline Structure Based Features			Benford's Law Based Features		
	FNR	FPR	ACC	FNR	FPR	ACC	FNR	FPR	ACC
LMT	0.9	1.3	98.9	3.2	2.4	97.22	1.3	1.6	98.52
MLP	0.5	0.6	99.43	3.0	3.9	96.58	1.8	1.7	98.22
DAG	1.7	2.1	98.1	11.3	38.6	75.05	3.8	22.1	87.05
RF	0.8	0.4	99.42	2.5	3.0	97.25	1.0	0.9	99.05

Table 6.6: Substrate-Independent Evaluation of Features Spaces using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)

using the MultilayerPerceptron (MLP) [Bau88] within the dot based feature space. The model based on this particular classifier has also the lowest false miss rate (FNR) of 0.5%. The lowest false alarm rate (FPR) of 0.4% is achieved within the same feature space using the model based on the RotationForest (RF) classifier [RKA06]. The second-best performing feature space is the Benford's Law feature space with a detection accuracy of 99.05% using the RF based model. This particular classifier also yields the lowest false miss rates (1.0%) and false alarm rates (0.9%) in this feature space. The best performance in the crystalline structure based feature space is achieved using RF as well. However, the detection accuracy is only 97.25%. In terms of the lowest false miss rate (FNR) the RF based model achieves the best performance with an FNR of 2.5%. The lowest false alarm rate (FPR) of 2.4% is achieved with the Logistic Model Tree (LMT) classifier [LHF05].

Overall, the tendency regarding the error rates from the Dagging classifier based

model can be confirmed within the substrate-independent evaluation as well. In particular the false alarm rates within the crystalline structure based and Benford's law based feature spaces are very high with 38.6% and 22.1%.

The risk of over-fitting of the classifiers is assessed in [HKD13a]. In particular the evaluation based on the MultilayerPerceptron (MLP) [Bau88] and a combined feature space consisting of dot and crystalline structure based features, shows that the classification accuracy exceeds 99% with 1500 samples in the training data set. Even with just 60 training samples a classification accuracy of 92.3% is achieved. Thus, it can be inferred that the features capture the essential differences between real latent fingerprints and printed latent fingerprint forgeries pretty well. However, the test setup contains only samples originating from one particular printer. Hence, it is not possible to generalize the findings on the foundation of the test set. In order to achieve such a generalization, the experimental setup needs to be extended to cover several printers, artificial sweat compositions as well as additional substrate materials. This, however, is out of scope for a thesis and thus, remains future work.

6.3.6 Fusion of the Three Feature Spaces

In order to increase the robustness of the classification, it is reasonable to combine the three feature spaces into a combined classification scheme. In [Hil15] the following fusion approaches are considered on a theoretical level; the selected approach is highlighted in bold face:

1. **Feature level fusion,**
2. Multi-Algorithm fusion,
3. Decision level fusion.

Sensor Level
Fusion

A sensor level fusion and rank level fusion as additionally described e.g. in [RNJ06] in the context of biometric systems, is not considered because all samples are digitized using the CLSM S_2 . The sensor level fusion is not feasible because synchronizing two different sensors to capture the same part of a latent fingerprint sample with an exact alignment is very challenging. A rank level fusion would require a ranked list of the classification results. Since the detection of latent fingerprint forgeries is a two-class problem - a latent fingerprint is either a forgery or authentic - such a fusion approach is not applicable.

Feature Level
Fusion

For a feature level fusion according to [RNJ06] two potential options exist: either the features can be combined, resulting in a dimensionality equal to the source feature spaces or the feature spaces could be concatenated. Since the three feature spaces for the detection of latent fingerprint forgeries differ in their dimensionality and their semantics, the latter is the only viable option for a feature level fusion.

Multi-Algorithm
Fusion

A multi-algorithm fusion can be used in conjunction with classifiers utilizing different machine learning algorithms. However, in order to combine the decisions of each classifier to determine the final decision, the complexity of the classification scheme is significantly increased.

Decision Level
Fusion

In a decision level fusion the results of the classifier need to be combined, e.g. via a majority voting or by weighting according to their accuracy or confidence levels. The advantage of this approach, in comparison to the feature level fusion, is the reduced dimensionality of each classification problem. However, on the other hand, multiple classifiers need to be trained and evaluated.

In [Hil15] the feature level fusion is selected as a fusion approach. The performance evaluation of the four classifiers used in this thesis is summarized in Table 6.7. The fusion of the feature spaces by concatenating increases the

	FNR	FPR	ACC
LMT	0.4	0.3	99.65
MLP	0.2	0.1	99.82
DAG	0.9	0.1	99.48
RF	0.3	0.1	99.82

Table 6.7: Substrate-Independent Evaluation of Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)

detection accuracy in comparison to the separate feature spaces summarized in Table 6.6. In particular, the highest classification accuracy of 99.82% is achieved using the models based on the MultilayerPerceptron (MLP) [Bau88] and RotationForest (RF) [RKA06] classifiers. The false alarm rate (FPR) is 0.1% for MLP, RF and Dagging (DAG) [TW97]. The lowest false miss rate (FNR) of 0.2% is achieved using MLP. The differences of the classification performance in comparison to [Hil15] originate from a different evaluation method. In [Hil15] half of the samples are used for training, whereas the other half is used for the testing. For consistency with the previous subsections, the classifiers are evaluated using a ten-fold cross validation within the scope of this thesis. As a result more samples are used for the training, which results in a more accurate model as summarized in [HKD13a] for the evaluation of the potential overfitting.

6.3.7 Summary of the Evaluation of the Three Feature Spaces for the Detection of Printed Latent Fingerprint Forgeries

The pattern recognition based detection of printed latent fingerprint forgeries is a very suitable, highly accurate detection mechanism for digitized forensics based on the available test data. Overall, the detection process is very fast due to the fast sample acquisition with the CLSM S_2 and the low processing times for a single sample. From the individual feature spaces the best detection performance is consistently achieved with the dot based feature space. However, the detection performance using Benford's Law based features is only slightly worse. The fusion of the feature spaces resulted in a further improved detection accuracy with all evaluated classifiers.

6.3.8 Benchmarking of the Detector Robustness using StirTrace

The very high detection performance of printed latent fingerprint forgeries justifies a more thorough benchmarking in order to determine the limitations of the trained classification models. Within the scope of this thesis, the findings from [HiD15a], [Hil15] and [HiD16] are combined. Due to the nature of the benchmarking, the available data is split into two sets with an equal number of samples. Thus, the baseline accuracy for the classifiers from [Hil15] is used as the reference. The classification models are trained on one half of the available samples

Benchmarking
using StirTrace

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA		DS
DO							

without any additional preprocessing. In particular, the three models based on the classifiers Logistic Model Tree (LMT) [LHF05], MultilayerPerceptron (MLP) [Bau88] and RotationForest (RF) [RKA06] are evaluated. The Dagging classifier is excluded for two reasons - it resulted in elevated false alarm rates and it has been removed from newer versions of the WEKA data mining software [Hal+09]. After the training of the models, the second half of the samples are manipulated using StirTrace in order to benchmark the robustness of the combined feature space. In an ideal case, a specific filtering of the image does not result in differences of the overall detection accuracy. Any deteriorated detection accuracy is an indicator for limitations of the proposed detection approach. Any improvement can indicate a potential for additional preprocessing steps.

The 11 selected filters and parameters from StirTrace are summarized in Table 6.8.

Simulation Goals	StirTrace for Printed Fingerprint Context	Evaluated Parameterization
Sensor Characteristics	Random Additive Gaussian Noise	$L_N \in \{3, 6, 9, 12, 15\}$
Smudgy Fingerprint Effects	Median Cut Filtering: Simulation of smudgy fingerprints/merging amino acid dots	$L_M \in \{3, 5\}$
Printer Characteristics	Remove Lines and Columns: Simulation of printer characteristics	$R_m \in \{10, 20, 30, \dots, 100\}$, $C_m \in \{10, 20, 30, \dots, 100\}$
	Banding Artifacts	Replacement of random lines (width $50 \mu m$) with the median value of the image, $L_{NP} \in \{0.5\%, 1.0\%, 2.5\%\}$
	Stretching in X-Direction	$L_X \in \{1.035, 1.070, 1.105, 1.140, 1.175, 1.210, 1.280, 1.350\}$
	Shearing in Y-Direction	$L_Y \in \{0.05, 0.10, 0.15, 0.20, 0.25, 0.30\}$
Different Acquisition Conditions	Rotation: Simulation of rotation during the acquisition	$L_\phi \in \{-20, -15, -10, -5.5, -5, 7, 7.5, 13, 18, 20\}$ (in degrees)
	Cropping	$L_C \in \{25\%, 50\%, 75\%\}$ of the original size of I
	Rescaling	$L_S \in \{50\%, 75\%, 90\%, 110\%, 150\%, 200\%\}$ of the original size of I
	Sample Tilting	$I_T \in m \times n \times c \in \{(2,2,0), (2,3,0), (3,2,0), (10,15,0), (20,30,0), (0,0,100), (0,0,1000)\}$

Table 6.8: Selected Filters and Filter Parameters for the Benchmarking using StirTrace based on [HiD15a], [Hil15] and [HiD16] - in Sum 70 Filter-Parameter-Combinations are Selected for the Benchmarking

The evaluation for each category of simulation goals is discussed in the following subsections.

6.3.8.1 StirTrace Benchmarking of Sensor Characteristics

For the evaluation of sensor characteristics, the impact on the detection performance of printed latent fingerprint forgeries for the example of additive Gaussian noise is analyzed as summarized in Table 6.9. The best detection

Filter	Parameter	LMT	MLP	RF
Baseline Performance from [Hil15]	-	96.00	93.50	98.50
Additive Gaussian Noise	3	96.33	96.57	99.47
	6	97.00	70.67	99.90
	9	96.87	50.00	99.73
	12	86.93	50.00	88.10
	15	62.67	50.00	64.80

Table 6.9: Evaluation of the Detection Accuracy for Additive Gaussian Noise within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15]; best results highlighted in bold face (all accuracy values in %)

performance is consistently achieved using the RotationForest (RF) [RKA06] based model. Interestingly, the addition of a low amount of Gaussian noise ($L_N = 3$) helps to increase the detection performance for all three classifiers. The root cause for this effect is hard to determine, but it is likely that the noise improves the result of the preprocessing of the digitized samples and thus, minimizes the variance of the features. The best performance in this evaluation is achieved with RF at $L_N = 6$. However, the performance using the MultilayerPerceptron (MLP) [Bau88] based model is already significantly deteriorated at this particular level of noise. Furthermore, with a noise level of at least 9, the results of the MLP model are completely unreliable and represent just random chance. For RF and the Logistic Model Tree (LMT) [LHF05] based models, a drop in the detection accuracy can be observed at a noise level of 12 with an additional significant decreased accuracy at a level of 15.

Overall, it can be seen that the sample preprocessing and feature extraction are quite robust regarding low levels of noise. With higher noise levels, the performance significantly deteriorates. However, such noise levels are quite dominant within the image data, Thus, in practice only misconfigured, defective or inappropriate sensory can lead to such a severely degraded image quality.

6.3.8.2 StirTrace Benchmarking of Smudgy Fingerprint Effects

Smudgy fingerprints might lead to significant shifts within the feature space due to different spatial distributions of the fingerprint residue. The particular evaluation results from [Hil15] are summarized in Table 6.10. The limitation of

Filter	Parameter	LMT	MLP	RF
Baseline Performance from [Hil15]	-	96.00	93.50	98.50
Median	3	96.00	96.57	99.60
	5	95.60	97.20	98.23

Table 6.10: Evaluation of the Detection Accuracy for Median Cut Filtering within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15]; best results highlighted in bold face (all accuracy values in %)

this experiment is the filter size of the median blur based on the bit-depth of the digitized traces. In particular, a maximum of a 5×5 -pixel filter can be utilized.

The effect of such kind of filtering in conjunction with the very high lateral acquisition resolution of S_2 is probably resembling an additional preprocessing instead of the intended smudging of the fingerprint pattern. This assumption is backed by the observed detection accuracy in Table 6.10. Here, a median cut filtering with a filter size of 3×3 pixels results in an increased detection accuracy for the MLP and RF based models and an unaltered detection accuracy for LMT. In particular, for RF the detection accuracy is increased to 99.6% in comparison to the baseline performance of 98.5%. Thus, this benchmarking indicates further improvement potential within the processing pipeline for the detection of printed latent fingerprint forgeries.

For the filter size of 5×5 pixels the accuracy of the LMT and RF based detectors is slightly reduced in comparison to the baseline performance. In contrast to that, the performance of MLP is further increased to 97.2%.

6.3.8.3 StirTrace Benchmarking of Printer Characteristics

Specific printer characteristics and printing defects can have a significant impact on the appearance of a fingerprint sample. The selection of filters is suitable to simulate errors in the paper feed, the positioning of the print head as well as potential blocked nozzles within the print head. The benchmarking results for the specific filters and parameters for simulating printer characteristics are summarized in Table 6.11. It is quite obvious that the classification performance of all three classifiers is very constant for the removal of lines, columns, low probability banding and stretching in X-direction. For shearing of the samples in Y direction with $L_\gamma = 0.3$, a significant reduction of the classification accuracy can be observed for the RF based detector. In all other cases the performance of this particular detector is remarkably constant. Nevertheless, the results summarized in Table 6.11 indicate that the simulated printer characteristics only have a marginal impact on the detection performance.

6.3.8.4 StirTrace Benchmarking of Acquisition Conditions

Variations in the acquisition conditions are probably the most significant influence factor in digitized forensics. Thus, a Daubert challenge [DG01, pp. 1–4] assesses the existence and maintenance of standards for the application of a method. In addition to that, particular standards for forensic laboratories are specified within ISO/IEC17025 [ISO17], see Section 2.1.1.1.1. Nevertheless, not all potential influence factors during the data gathering process could be eliminated. As a result, it is crucial to benchmark the impact of acquisition influence factors during the strategic preparation. The results for this evaluation are summarized in Table 6.12. In comparison to the baseline performance, the LMT based model seems to be rather resistant against the rotation of a sample. This is not the case for the MLP and RF based models. With respect to the feature spaces, the result for this phenomenon is probably a different weighing of the features within the trained model, as especially the dot based features contain a subset of rotation-dependent features. The results for the cropping of the sample are reasonable, as the reduction of the digitized area leads to a potentially higher impact of local variations of the fingerprint residue. Similarly, a significant reduction of the scan resolution results in a lower detection accuracy.

For the tilting simulation in [HiD16] the feature extraction is performed within StirTrace. As a result, only one particular image of S_2 is processed for the feature extraction. In particular, the intensity image I_I is used for the feature extraction

Filter	Parameter	LMT	MLP	RF
Baseline Performance from [Hil15]	-	96.00	93.50	98.50
Removal of Lines	10	97.13	97.57	99.60
	20	96.63	98.30	99.67
	30	95.93	98.60	99.73
	40	96.00	98.07	99.33
	50	96.00	97.10	99.37
	60	96.00	96.63	99.77
	70	96.00	96.93	99.30
	80	95.87	98.03	99.33
	90	96.00	97.00	99.23
	100	95.93	97.83	99.73
Removal of Columns	10	96.57	98.47	99.20
	20	96.37	97.70	99.40
	30	96.10	98.13	99.70
	40	95.83	96.93	99.83
	50	96.03	97.90	99.27
	60	95.80	97.93	99.87
	70	95.83	97.87	99.77
	80	95.83	96.83	99.27
	90	95.60	98.00	99.50
	100	95.87	96.77	99.63
Banding	0.005	97.57	98.53	99.57
	0.01	97.93	98.03	98.77
	0.025	96.80	97.80	93.67
X-Stretching	1.035	94.97	96.57	99.67
	1.07	95.07	96.20	99.60
	1.105	94.53	95.53	99.47
	1.14	94.20	95.50	99.40
	1.175	94.23	96.03	99.60
	1.21	93.90	95.43	99.40
	1.28	93.40	94.23	98.97
	1.35	92.67	93.20	98.80
Y-Shearing	0.05	95.53	94.23	96.60
	0.1	97.20	93.60	98.37
	0.15	97.63	98.33	98.10
	0.2	96.93	97.50	97.40
	0.25	91.50	85.53	93.70
	0.3	97.77	93.37	81.50

Table 6.11: Evaluation of the Detection Accuracy for the Simulation of Printer Characteristics within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15]; best results highlighted in bold face (all accuracy values in %)

Filter	Parameter	LMT	MLP	RF
Baseline Performance from [Hil15]	-	96.00	93.50	98.50
Rotation	-20	95.80	92.13	76.53
	-15	95.57	93.00	75.60
	-10	96.40	97.73	77.30
	-5.5	93.83	90.30	88.30
	-5	92.97	93.07	84.87
	7	95.30	83.47	85.37
	7.5	93.53	74.40	83.30
	13	97.10	91.97	79.23
	18	96.37	93.60	77.80
	20	95.87	73.03	74.63
Cropping	25	60.07	74.10	48.07
	50	87.57	83.70	52.57
	75	98.63	98.03	90.37
Rescaling	50	55.37	60.30	50.00
	75	97.77	97.53	77.20
	90	97.97	99.10	99.40
	110	93.63	95.70	99.43
	150	84.40	83.67	92.03
	200	68.23	70.63	80.60
Sample Tilting*	(2,2,0)	96.87	97.40	96.93
	(2,3,0)	96.83	97.13	97.00
	(3,2,0)	96.77	97.03	96.93
	(10,15,0)	95.37	50.00	96.23
	(20,30,0)	81.47	50.00	96.57
	(0,0,100)	99.47	84.03	95.20
	(0,0,1000)	50.00	50.00	95.43

Table 6.12: Evaluation of the Detection Accuracy for the Simulation of Acquisition Conditions within the Combined Feature Space using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), Dagging (DAG), RotationForest (RF) from [Hil15] and [HiD16]; best results highlighted in bold face, (* feature extraction exclusively performed on I_I of S_2 , all accuracy values in %)

for the training data and the simulated trace data. As a result, in [HiD16] a different baseline performance of 96.6% for LMT, 97.83% for MLP and 96.96% for RF is achieved. As a learned lesson from the simulation, it can be seen in Table 6.12 that differences in the placement of the sample underneath the sensor based on the evaluation of the fused feature space for I_I from S_2 in [HiD16] are negligible for small gradients (tilted plane parameters (2,2,0), (2,3,0) and (3,2,0)) for all three classifiers. The highest classification accuracy for those particular parameterizations of StirTrace is achieved using the MultilayerPerceptron (MLP) based classification model. However, with stronger gradients or a significant shift of values (0,0,1000) the MLP based model produces results by random chance. For the smaller shift of values (0,0,100) the best performance is achieved with the Logistic Model Tree (LMT) based classification model. However, overall the most consistent and stable detection results are achieved using the RotationForest (RF) based model, which achieves a detection accuracy of at least 95.2% within the evaluated sample tilting simulation parameters.

6.4 Feature Selection

The concatenation of the feature vectors inevitably increases the dimensionality of the classification problem. While this is apparently not yet an issue in this application scenario, a feature selection could also help to remove redundant or contradictory features and thus, simplify the decision boundaries within the feature space. Besides the fusion of the feature spaces, a feature selection is performed and evaluated in [Hil15]. In particular, the feature selection is performed using the WEKA data mining software [Hal+09] with the CfsSubsetEval technique in combination with the Best-First algorithm [Hal98] in its default settings to find non-correlated features and select them using a greedy hill-climbing approach. As a result, the following features are selected for the reduced feature space:

- Number of circles $ncircles$ (Equation 6.1)
- Standard deviation of the circle radii $rstddev$ (Equation 6.3)
- Mean vertical circle distance $vmean$ (Equation 6.6)
- Mean nearest neighbor distance $nnmean$ (Equation 6.10)
- Probability of circle radii between 0 and 6 μm $rpdf_1$ (Equation 6.7)
- Probability for horizontal circle distances $hpdf_2$, $hpdf_3$, $hpdf_5$ (40-80, 80-120, 160-200 μm) (Equation 6.8)
- Probability for vertical circle distances $vpdf_2$, $vpdf_3$, $vpdf_5$ (40-80, 80-120, 160-200 μm) (Equation 6.9)
- Probability for nearest neighbor distances $nnpdf_2$, $nnpdf_3$ (20-40, 40-60 μm) (Equation 6.11)
- Probability of the most significant digit 3 of the intensity image I_I (Equation 6.13)
- Probability of the most significant digit 8 of the intensity image I_I (Equation 6.13)

Feature Selection

SP	PA	OP	TP	TI	TA	DO	TS
			DG	DI	DA	DS	
DO							

- Probability of the most significant digit 1 of the topography image I_T (Equation 6.13)

It is worth noticing that none of the crystalline structure-based features from Section 6.2.2 are selected by the algorithm.

Alternatives to this approach are classifier-based feature subset evaluation, with a similar optimization problem to solve, as well as transformations of the feature space, such as a principal component analysis (PCA) [DHS00, p. 568], which projects the feature space to an eigenvector-based feature space of lower dimensionality.

The evaluation results for three selected classifiers are summarized in Table 6.13. Two observations can be made based on the evaluation results. First of all, it

	Without Feature Selection			With Feature Selection		
	FNR	FPR	ACC	FNR	FPR	ACC
LMT	0.4	0.3	99.65	0.0	6.8	96.6
MLP	0.2	0.1	99.82	0.0	6.2	96.9
RF	0.3	0.1	99.82	0.0	3.0	98.5

Table 6.13: Substrate-Independent Evaluation of Combined Feature Space with an without Feature Selection using the Classifiers Logistic Model Tree (LMT), MultilayerPerceptron (MLP), RotationForest (RF) - FNR Indicates the Miss Rate, FPR is the False Alarm Rate, ACC the Overall Accuracy; best results highlighted in bold face (all values in %)

is obvious that the best detection accuracy is reduced from 99.82% to 98.5%. While this decrease of the accuracy seems rather low, the effects of the feature selection are quite significant as the false alarm rate is increased by a factor of 30. The second observation is the reduction of the false miss rate to 0% for all three classifiers. This puts the lower accuracy into another perspective as no particular printed latent fingerprint forgeries are missed by the trained models. In conjunction with the intention of raising additional attention for a more detailed analysis if indicators of anti-forensics are detected, this detection feature space could be preferred in comparison to the full feature space.

6.5 Chapter Summary and Limitations

Summary of
addressed
Research
Questions,
Objectives and
Contributions

The application scenario in this chapter addresses an aspect of anti-forensics in latent fingerprint processing by analyzing latent fingerprints forged by means of ink-jet printers equipped with artificial sweat. In order to answer the research question \mathcal{Q}_6 regarding supporting the detection of forged traces using novel technology, at first the available sensory is assessed in Section 6.3.1 as a part of the strategic preparation of the model introduced in Section 3.1. Based on the selected sensory, a pattern recognition based approach is designed, implemented and evaluated to address the objective \mathcal{O}_4 of this thesis. In line with this objective, three particular detection feature spaces are introduced in Section 6.2, representing the contribution \mathcal{C}_7 . Based on those feature spaces, supervised-learning based learning techniques are utilized to create models for the detection of such latent fingerprint forgeries. The evaluation of the trained models, including the systematic simulation of influence factors using StirTrace (\mathcal{C}_4), represents

the contribution \mathcal{C}_8 . While all those steps are second-tier phases of the strategic preparation phase, the application of the trained models represents a second-tier phase of the data analysis.

The main limitation of the presented detection approach is its limited scope. In particular, only one printer and artificial sweat composition is analyzed within the experiments. Thus, it is not determined whether the trained models achieve the necessary generalization for detecting all potential kinds of printed latent fingerprints. Furthermore, the set of four test subjects probably does not cover the multitude of different sweat compositions and potential contaminants for real latent fingerprints. However, the classification performance shows a remarkable robustness against various simulated influence factors. This observation would merit a more extensive evaluation in order to determine whether the approach could be utilized by forensic laboratories to assist latent fingerprint examiners during the challenging task of the forgery detection. The feature selection can reduce the false miss rate to zero but increases the false alarm rate significantly. Thus, the choice of the utilized feature space depends on the particular goal of the application of the detection method.

Limitations

Potential Future Implications

The purpose of this chapter is the reflection of already conducted research with respect to the process model for digitized forensics introduced in [Section 3.1](#) as well as other aspects of this thesis. The concepts of digitized forensics constitute an evolution of forensic investigations instead of a revolution. The intention is the formalization of the utilization of novel computer based techniques in forensics without neglecting the challenges that arise from such a transition in the generally accepted procedures. However, since the validation of the digitized forensics process is solely performed on the example of latent fingerprints as one specific type of trace evidence, it is necessary to briefly analyze the processing and investigation of other types of traces as well. This is necessary in order to confirm the applicability of the model resulting from an inductive modeling approach. Though, the applicability to the processing of selected other types of traces is no proof of the achievement of a universally applicable process model either. However, with more and more domains which can be mapped to the model introduced in this thesis, the level of confidence regarding its applicability to other investigation processes can be increased.

This chapter briefly sheds light on the application of the novel process model to other types of traces in [Section 7.1](#). Furthermore, other application fields of the benchmarking approach introduced in [Section 4.3](#) are discussed in [Section 7.2](#). Subsequently, the potential impact of digitized forensics on future forensic investigations is outlined in [Section 7.3](#). The latter is not intended as a summary of future research directions rather than an assessment of the potential impact of this thesis on forensic investigations in general.

7.1 Application of the Novel Process Model of Digitized Forensics to Other Types of Trace Evidence

The sensors which are utilized for the two application scenarios within this thesis have been successfully utilized for the domains of fiber analysis [[ADV15](#)], the analysis of toolmarks on bullet casings [[FVH+13](#)] and within locks [[Cla+12](#)] as well as handwriting traces [[SKV17](#)]. The overall investigation process is very similar to the approach in the first application scenario in this thesis in [Chapter 5](#), as various pattern recognition based processing approaches are evaluated to either perform an individualization or identification. Thus, common processing steps

along a pattern recognition pipeline consist of the initial digitization of the trace, some sort of preprocessing, followed by a feature extraction and final classification phase. Naturally, those processing steps can be mapped as second-tier phases to the first-tier phases of data gathering, data investigation and data analysis within the process model introduced in Section 3.1.

In addition to that, a similar method of analyzing traces with specific sensors is e.g. utilized in nuclear forensics analyzing radionuclides [Kip+20], the forensic analysis of chemicals such as narcotics [SGN17] or even the medical imaging of mummified corpses using non-destructive computer tomography [Jan+02].

7.2 Extension of the Artifact Simulation of StirTrace to other Applications

StirTrace for
Benchmarking
Latent
Fingerprint Age
Estimation

Even though StirTrace is primarily intended for the benchmarking in the context of latent fingerprint forgery detection, it can be applied to other forensic purposes as well. A closely related topic in digitized forensics is the age estimation of latent fingerprints as described in [Mer14]. Since the approach relies on the degradation of the sample over time, a particular sensor and environment conditions are likely to have an impact on the detection performance. In [MHD15] StirTrace is used to benchmark the robustness of the short-term age estimation scheme based on degradation series of intensity images captured by a Chromatic White Light sensor (S_1). All particular artifacts from Table 4.1 are simulated with the exception of the removal of lines and columns, the replacement of lines, shearing in Y direction and stretching in X direction because those artifacts are originating from printer characteristics, which are unlikely to occur within authentic latent fingerprints. In addition to that, the rotation of the samples is omitted because the feature space is designed to be rotation-invariant. Thus, any observed deviation of the results in conjunction with the rotation simulation is caused by the interpolation rather than the quantization of the sample during the data gathering.

StirTrace in
Media Forensics

In media forensics StirTrace is applied and extended for benchmarking detectors for morphed face images [HNM+17], [NMH+18]. In this context StirTrace is used as a post-processing for morphed images in order to evaluate the detection robustness against intentionally created artifacts. In particular the rotation, median cut filtering, removal of lines and columns, the stretching in X direction, re-scaling, cropping and the addition of Gaussian, uniform and salt&pepper noise are evaluated using StirTrace. As an extension of StirTrace a double scaling, a downscaling followed by an upscaling to reduce artifacts from the morphing process, is implemented. Additionally, a specific filter is implemented for simulating a crucial step of the passport creation process: the cropping of the face image to standards compliant with international travel documents and the scaling to an image resolution commonly found in passports. In addition to that this so-called passport scaled image is compressed to a size of 15 kB in order to fit in the data group 2 in the microchip embedded into the passport [ICA015, pp. 33-37].

7.3 Potential Impact on Forensic Investigations

The potential impact of digitized forensics on future forensic investigations is two-fold. At first a novel method needs to be assessed according to the Daubert

factors [DG01, p. 3], in particular the existence and maintenance of standards for the utilization of a technique or method as well as the known or potential rate of error. Furthermore, the method needs to be accepted in the relevant domain by being peer reviewed. After such a novel technique has been established as sufficiently reliable and accepted, secondly the techniques need to be integrated into the standards and guidelines for forensic investigations. Especially with requirements regarding novel, potentially expensive sensory, more traditional processing techniques and modern processing techniques will probably coexist for quite some time. The major advantage of the digitization of traces is the possibility of performing a load balancing of the trace analysis by forwarding the data to forensic experts with a lower load level or shorter backlog. Furthermore, a digital transfer of the traces might help to reduce context information available to the forensic expert, which might cause any bias in the decision-making process. With the availability of contact-less, non-destructive sensory and storage facilities minimizing the degradation of traces, it is also possible to conserve traces for future investigations, e.g. within the context of so-called cold-cases which cannot be solved immediately. Thus, novel digitization techniques could help to preserve the ability of utilizing novel, more advanced processing techniques once they become available.

In this chapter, the scientific results of this thesis are discussed with respect to the research questions, objectives and contributions introduced in [Chapter 1](#). At first, the specific contributions of this thesis to the scientific community are summarized in [Section 8.1](#). Afterward, the achieved contributions are assessed with respect to the initial objectives of the thesis in [Section 8.2](#). The achieved contributions of this thesis are reflected against the initial research questions in [Section 8.3](#). Subsequently, in [Section 8.4](#), lessons learned and concluding remarks of this thesis are summarized.

8.1 Summary of Contributions

This section briefly summarizes the contributions achieved within the scope of this thesis.

C_1 A novel process model for forensics in the physical and digital domain as a foundation for modeling forensic application scenarios from a scientific point of view as well as a coarse guideline for forensic investigations in the future.

The main contribution of this thesis is the novel process model for digitized forensics in [Section 3.1](#). The process model combines aspects from best practices in forensic investigations with particular requirement from a computer science-based IT-security perspective.

C_2 Formalization of Error, Loss and Uncertainty with respect to sensor data syntax and semantics in digitized forensics.

The formalization of error, loss and uncertainty within the scope of digitized forensics is a novel contribution of this thesis. Whereas the loss is divided into intentional loss and unintentional loss during the digitization process and the processing of the digitized data, the uncertainty and errors are defined within the scope of probabilistic decisions in forensic investigations. Any unintentional loss can cause uncertainty which might eventually lead to errors in the formulation and evaluation of intermediate or final hypotheses of the forensic investigation.

C_3 A novel approach for creating a bijective link between a physical trace and its digital representations.

The contribution in [Section 4.2](#) addresses a major gap in terms of the authenticity of the digitized traces in digitized forensics and computational forensics. Without such an approach the sole options are organizational measures which can be tampered with easily due to the media discontinuity caused by the digitization.

\mathcal{C}_4 A benchmarking solution for simulating sensor and trace influences in image sensor data.

The benchmarking solution StirTrace introduced in [Section 4.3](#) is not novel in a narrow sense, as most of the functionality is provided by the StirMark [\[PAK98\]](#) framework as well. However, due to the limitations of StirMark regarding image size and bit-depth, it cannot be adequately applied to the domain of digitized forensics. Furthermore, as described in [Section A.1](#) the evaluation module of StirTrace can be used to extract features directly without the need to save the modified images. A limitation of this approach is the reproducibility for all artifacts with a random element, such as noise, because the noise pattern will vary with each application of StirTrace.

\mathcal{C}_5 A novel feature space for segregating latent fingerprints from substrate data as part of a signal processing pipeline in fingerprint recognition.

The novel feature space for the segregation of latent fingerprint data from substrate data is the major contribution of the first application scenario in [Chapter 5](#) within this thesis. Based on the evaluation of the classification performance in a two-fold cross-validation, the feature space can be considered suitable for the pattern recognition problem. However, the detection performance should be further improved in order to reduce the uncertainty connected to the application of the feature space for extracting latent fingerprint patterns from arbitrary substrates.

\mathcal{C}_6 Biometrics based evaluation of the segregation of latent fingerprints from substrate data.

The biometrics based evaluation of the reconstructed latent fingerprint patterns is an estimator for the performance of forensic experts in [Section 5.3.3.2](#). The evaluation results indicate the general suitability of the pattern recognition based segregation approach, but also indicate a significant demand for improvements.

\mathcal{C}_7 Three feature spaces for the pattern recognition based detection of fingerprint forgeries based on printed amino acid.

The three feature spaces for the detection of artificial sweat printed latent fingerprint forgeries in [Section 6.2](#) are designed to express particular features of the printed forgeries as well as those of real latent fingerprints in high-resolution scans. Each individual feature space shows slightly different results in terms of the suitability for the four evaluated classifiers. Overall, the best result of a detection accuracy of 99.43% for dot based features is achieved using the Multilayer perceptron [\[Bau88\]](#) classifier, whereas for crystalline structure based and Benford's law based features the RotationForest [\[RKA06\]](#) classifier performs best with a detection accuracy of 97.25% and 99.05%.

\mathcal{C}_8 Benchmarking and fusion of feature spaces for the detection of latent fingerprint forgeries based on printed amino acid.

With the very promising detection accuracy based on the separate feature spaces, the fusion of the feature spaces is a reasonable approach to further reduce the error rates. In particular, a feature space fusion by concatenation of the feature vectors in Section 6.3.6 supports this assumption. In the combined feature space the detection accuracy is further increased to 99.82% for the Multilayer perceptron [Bau88] and RotationForest [RKA06] classifier. Within the StirTrace-based benchmarking in Section 6.3.8, the limitations of the trained models are identified as strong noise levels, strong shearing, rotation, cropping and significant scaling of the digitized image data. Furthermore, the benchmarking approach is suitable to identify different behaviors of the classification approaches.

8.2 Summary of the Results Addressing the Objectives

This section summarizes whether and how the objectives of the thesis as defined in Chapter 1 are addressed by the research results.

\mathcal{O}_1 Creation of a novel universal process model for digitized forensics for all types of traces on the foundation of existing process models from forensics and digital forensics and its exemplary validation for the domain of latent fingerprint processing.

The process model for digitized forensics is introduced in Section 3.1. The specific objective of achieving a universal applicability to different trace types is accomplished by adopting the two-tiered approach for modeling forensic processes from [BC04] - a trace independent first-tier of universal phases for the forensic process is introduced. The trace-specific second-tier of processing phases is used as a validation method for the process model within the scope of the exemplary selected application scenario of latent fingerprint processing and analysis in Chapter 5 and the specific detection of forged latent fingerprints in Chapter 6. The validation by example method shows that the universal model for digitized forensics created by the analysis of existing models from different forensic disciplines using an inductive modeling approach is indeed applicable for this particular scope. Furthermore, particular common ground with other forensic disciplines summarized in Section 7.1 indicates the achievement of this particular objective. However, as the second-tier of phases is trace-dependent, such phases need to be created and mapped to the first-tier phases in order to complete the process model for a specific domain. Nevertheless, due to the shared first-tier of phases a general evaluation method for novel forensic approaches in digitized forensics could be derived.

\mathcal{O}_2 Design and implementation of selected supporting tools for digitized forensics addressing current research gaps in the context of \mathcal{O}_1 .

Particular challenges connected to digitized forensics are identified in Section 3.3 with respect to the authenticity of the digitized traces and the reproducibility of the scan process. The issue authenticity is addressed by designing and

implementing a tool to create a bijective link between the physical trace and its digital representations in [Section 4.2](#). This particular approach utilizes the peculiarities of the chain-of-custody by extending it with information about the digitization processes and creating a machine-readable version of the recorded information. With the help of digital signatures, the contents of the machine-readable QR codes are verifiable in terms of the authenticity of the data contents. The authenticity of the evidence is ensured by the sealed evidence bag and the records contained in the chain-of-custody. Similarly, in the digital domain, the digitized traces can be stored with metadata pointing to the physical object including digital signatures allowing for a verification of the data authenticity. The potential issue of the reproducibility is addressed by the StirTrace benchmarking framework in [Section 4.3](#). This particular framework allows for analyzing the impact of different artifacts from the trace and the acquisition process on pattern recognition based processing methods within the scope of digitized forensics as part of the strategic preparation. However, this approach is only suitable to simulate the influence of variations in the digital representation of a trace. Further aspects of the reproducibility include a proper storage of the physical traces in order to slow down or even stop degradation processes.

③ Design, implementation and evaluation of a novel signal processing and pattern recognition based pipeline for segregating latent fingerprint patterns from substrate data within a subset of \mathcal{O}_1 .

The first application scenario in [Chapter 5](#) is dedicated to this particular objective. The design consists of an analysis of suitable sensory, the design of a feature space and strategies for reconstructing biometric images from the classifier's output in order to allow for a biometric comparison of the fingerprint patterns. The implementation of the feature extraction uses C++ and OpenCV [[Ope20b](#)] in order to create ARFF files for the WEKA data mining software [[Hal+09](#)]. The combined feature space, consisting of five different sub-feature-spaces, has a dimensionality of 600 resulting from the features and specific preprocessing techniques creating various variations of the original scan data prior to the feature extraction. Within a purpose-built wrapper for WEKA written in Java, the training, evaluation and classification is performed using three selected classifiers for supervised learning. The selection of the classifiers is performed on the foundation of the evaluation results in [[HKD+14](#)] the three best performing classifiers are selected for an in-depth evaluation with extended training and test sets. In total 700 unlabeled latent fingerprint samples are collected from ten substrates involving up to four different donors per substrate material. In addition to that, ten training samples utilizing a differential imaging approach to approximate ground truth data for labeling are acquired. The collection of this test data took 119.5 days of raw scan time without considering the time for preparing the samples and scans. The evaluation in a two-fold cross-validation and training of the classifier models for the three classifiers took another three months on a computer equipped with an Intel Core i5-4570T CPU. The evaluation of the classifier models in the cross-validation approach achieved accuracy ranges from 66.4471% to 92.7978%. The lowest accuracy for the overall best performing Bagging ensemble classifier [[Bre96](#)] is 74.9469% in the evaluated two-class classification problem. However, the promising classification performance is not reflected in the results of the biometric evaluation. This, observation is especially true for the Bagging ensemble classifier which does not

lead to a single biometric match within the reconstructed images. For the other classifiers between 0% and 12% of the samples can be successfully matched using an off-the-shelf biometric matcher from the NIST biometric imaging software [Nat13]. Those results indicate the general suitability of the approach as the matching results of the reconstructed images outperform the results of the non-processed intensity data, but also show the need for further evaluations in order to determine the root cause for the low matching rates.

The whole process for the segregation of latent fingerprint patterns from the substrate data can be mapped to the novel process model introduced in Section 3.1. Thus, the applicability of the novel model is successfully shown within this objective.

\mathbb{O}_4 Design, implementation and evaluation of a novel pattern recognition based approach for detecting latent fingerprint forgeries based on printed amino acid within a subset of \mathbb{O}_1 .

The second application scenario in Chapter 6 is dedicated to this particular objective. The design consists of an analysis of suitable sensory and the design of three feature spaces in order to allow for recognizing latent fingerprint forgeries using models created by supervised learning. The implementation of the feature extraction uses C++ and OpenCV [Ope20b] in order to create ARFF files for the WEKA data mining software [Hal+09]. Within a purpose-built wrapper for WEKA written in Java, the training, evaluation and classification is performed using three selected classifiers for supervised learning. In particular the training set consists of 1500 real and 1500 printed fingerprint samples captured by a Confocal Laser Scanning Microscope. The evaluation of the detection performance is carried out using an independent set of another 1500 real and 1500 printed fingerprint samples. The fingerprint patterns are taken from four different test subjects. The detection accuracy of the best performing Multilayer perceptron [Bau88] classifier is as high as 99.82%. Additionally, the impact of various artifacts and acquisition conditions is systematically evaluated using the StirTrace framework.

The whole process for the detection of latent fingerprint forgeries can be mapped to the novel process model introduced in Section 3.1. Thus, the applicability of the novel model is successfully shown within this objective as well.

8.3 Summary of the Results Addressing the Research Questions

This section provides an overview of the specific contributions of this thesis to address each research question.

\mathbb{Q}_1 How could a generic digitized forensic investigation be formalized as a process and validated for the selected domain of latent fingerprints?

This thesis introduces a novel process model for digitized forensics. The investigation process is formalized by adopting the fundamental idea of the modeling approach from [BC04] using two tiers of phases to describe the digitized forensic process in Section 3.1, a trace independent first-tier of universal phases for the forensic process is introduced. The set of first-tier phases covers the

strategic preparation for increasing the forensic readiness, the actual investigation of the crime scene, including the acquisition of items potentially bearing relevant traces, the processing steps in the physical and digital domain at the forensic laboratory, the documentation and the archiving of items of evidence. The process model is created using an inductive modeling approach by analyzing and integrating aspects of existing and accepted process models and standards from the domains of latent fingerprint analysis, accreditation of forensic laboratories, incident response and digital forensics. The resulting model is designed to address the whole domain of criminalistics as defined in [IR00, pp. 10 – 12]. The two application scenarios within Chapter 5 and Chapter 6 illustrate that the modeling approach using two tiers of phases is suitable for deriving a second tier of trace specific phases under the canon of the trace-independent first-tier of phases.

Q₂ Which novel challenges need to be addressed within digitized forensic investigations, in particular with respect to latent fingerprints?

The novel challenges connected to the digitization of forensic investigations are summarized in Section 3.3. The particular focus of this thesis regarding the challenges are the peculiarities of the digitization process as the major aspect of digitized forensics. Instead of relying on organizational measures to ensure the evidential value within the scope of computational forensics, in the newly defined domain of digitized forensics the arising challenges are addressed by technical means from the perspective of computer science. First and foremost, the issues of integrity and authenticity during and after the digitization of a trace are addressed by this thesis. For the digitization process an awareness regarding the properties, limitation and results of a particular sensor device must be known. For that, syntax and semantics as well as sensor errors and noise are considered in Section 3.2. Furthermore, the potential gap of the chain-of-custody created by the transition from physical to digitized traces is addressed by creating a QR code based linking approach as described in Section 4.2. Within the context of latent fingerprints a sensor needs to be capable to digitize information relevant for the fingerprint pattern without altering the properties of the trace as described in Section 5.3.1. The idea of this digitization is to avoid any concurrency situation between different types of traces present on the same object. Furthermore, the storage conditions of the physical trace prior and after the digitization need to be suitable to minimize the degradation of the unprocessed traces. The relevant aspects of the chain-of-custody for physical evidence as well as the protection of the integrity and authenticity of digitized traces can be considered sufficiently addressed by the state of the art at the time of writing this thesis.

Q₃ Which requirements need to be fulfilled by metrology sensory for an application in digitized forensics and what is the impact syntax and semantics of the captured sensor data related to error, loss and uncertainty?

The particular requirements for the sensory are assessed on a trace-independent level in Section 3.2 with application-specific requirements being assessed in Section 5.3.1 and Section 6.3.1 for the two application scenarios within this thesis. The aspects of syntax and semantics of sensor data are covered in Section 3.2.1. The aspect of loss is analyzed from the data point of view focusing on the sensor data and the following preprocessing in Section 3.2.2. In particular the relevant

information regarding a trace should be captured by a sensor and retained by the preprocessing, any unessential information should be removed in order to simplify the forensic investigation. In contrast to this intended loss, basically representing a data reduction, any unintended loss might lead to uncertainty and eventually potential errors. Based on the nature of decision-making in forensic investigations, the terms uncertainty and error are defined from a probabilistic point of view in [Section 3.2.2](#). With respect to the first application scenario in [Chapter 5](#) particular unintended loss can be observed for the selected sensory in conjunction with porous substrates as the fingerprint residue is absorbed by the substrate over time. As the classification errors of the trained models can be considered as an intermediate processing step for the biometric comparison of the traces, the particular accuracy during the classifier evaluation can be considered as a source of uncertainty. Regarding the errors during the biometric matching, no particular false matches are observed but depending on the substrate very high false non-match errors occur. With respect to the second application scenario in [Chapter 6](#) no particular unintended loss is observed due to the selection of cooperative substrates. The final error rates for the detection of latent fingerprint forgeries are very low within the experiments with independent training and test sets. The extended systematic benchmarking using StirTrace indicates significantly increased error rates for strong noise levels, strong shearing, rotation, cropping and significant scaling of the digitized image data.

Q_4 How could and should latent fingerprints be captured and analyzed within a digitized forensics process using signal processing and pattern recognition to ensure an accurate digital representation of the physical trace?

The particular capturing process for latent fingerprints within the scope of digitized forensics is described in [Section 5.1](#) consisting of profile scans for the parameter detection, coarse scans for the localization of potential fingerprints and detailed scans as the foundation for the biometric comparison. In addition to that, additional scans for narrowing down the list of potentially relevant fingerprint traces might be performed prior to the detailed scan. The particular sensory for representing the latent fingerprint trace as accurately as possible is assessed in [Section 5.3.1](#).

Q_5 Which classification scheme suits a pattern recognition based fingerprint-substrate segregation best?

This research question is discussed in [Section 5.2](#) considering the learning strategies of supervised, unsupervised and reinforcement learning as well as different numbers of classes. For the evaluation either two-class or one-class classification schemes are considered for supervised learning. In addition to that, clustering is a potentially suitable approach as well, which has the advantage of not requiring a time-consuming training phase. For the evaluation the two-class classification supervised learning scheme is selected because it allows for independently assessing the performance of the model which can be considered as prior odds for the uncertainty of the reconstructed fingerprint patterns. This uncertainty is expressed by likelihood ratio based image reconstructions in [Section 5.3.3.2](#). However, due to the lack of proper ground truth for the training of the classifiers, it is hard to determine whether the selected approach

is the best option. In particular a one-class classification could circumvent the immediate need for ground truth labels as the models could be trained solely on the foundation of surface data. However, for the evaluation of the resulting classification models, the ground truth data for latent fingerprints would be necessary anyway in order to determine the prior odds for uncertainty. Another open issue in this context is the question of generalization of the trained models. The training data originates from a depletion series from only one test subject. Even though successful biometric matches are achieved for all test subjects in the test data, it is not possible to estimate whether the trained models would work similarly for larger populations.

Q_6 How and in which way could the new technology support the detection of forged fingerprint traces?

The detection of forged latent fingerprint traces is addressed in the second application scenario described in [Chapter 6](#). In particular, the digitization of a small fraction of the fingerprint pattern in question using a Confocal Laser Scanning Microscope seems to be sufficient for the proposed pattern recognition based detection approach. The detection approach utilizes three different feature spaces which yield a very high detection accuracy of up to 99.82% for completely independent training and test sets. The false positive (or false alarm) rate using a Multilayer perceptron [[Bau88](#)] is as low as 0.1% with a false negative (false miss) rate of 0.2%. This very positive detection performance justifies the extended benchmarking using simulated artifacts in [Section 6.3.8](#) using StirTrace which indicates significantly increased error rates for strong noise levels, strong shearing, rotation, cropping and significant scaling of the digitized image data. Overall, the performance is very good and should be evaluated with a further extended test set.

8.4 Concluding Remarks and Lessons Learned

Within the two application scenarios of this thesis the introduced model for digitized forensics could be successfully applied by creating task and trace-specific second-tier phases under the canon of the trace type-independent first-tier phases. A comparison of the two application scenarios is summarized in [Table 8.1](#). Both application scenarios share the requirement for a contact-less sensor capable of acquiring fingerprint residue. However, due to the assessment of microscopic details for detecting latent fingerprint forgeries, the second application scenario demands for a higher acquisition resolution of at least 3200 ppi whereas a resolution of 500 ppi is sufficient for a biometric comparison of fingerprint patterns. Both application scenarios fit the concept of the two-tiered process model with second-tier phases during the strategic preparation, data gathering, data investigation and data analysis phases. The feature spaces are tailored for the specific application scenarios. A main difference is the availability of a reliable ground truth for the training of the classifiers. In the first application scenario for the segregation of fingerprint and substrate patterns only an approximated ground truth is available by using differential scans. For the latent fingerprint forgery detection the ground truth can be easily determined by the known origin of a sample. Both application scenarios utilize a two-class supervised learning approach with independent test and training sets. The selection of classifiers is based on a broad evaluation in [[HKD13a](#)] for the second application scenario,

	Application Scenario 1 Fingerprint Segregation	Application Scenario 2 Fingerprint Forgery Detection
Sensor Requirements	Able to detect fingerprint residue, contact-less, large scan area, resolution at least 500 ppi, selected sensor: FRT CWL sensor S_1	Able to detect fingerprint residue, contact-less, resolution at least 3200 ppi, selected sensor: Keyence VK-x 110 CLSM with 10x lens S_2
2 nd tier phases	Profile scan (DG), coarse scan (DG), time series (DG), detailed scan (DG), image filtering (DI), block segmentation (DI), feature extraction (DI), classification (DI), fingerprint image reconstruction (DI), biometric feature extraction (DA), biometric comparison&classification (DA); model training (SP)	Trace digitization (DG), preprocessing (DI), feature extraction (DI), classification (DA); model training (SP)
Feature spaces	Statistics, structure features, Benford's law-based, fingerprint semantics, normalized statistics	Dot-based, crystalline structure-based, Benford's law-based
Ground Truth	Approximated by differential scan	Based on origin
Classification scheme	two-class supervised learning, independent test and training sets	two-class supervised learning, independent test and training sets
Utilized Classifiers	SMO [Pla99], J48 (Java implementation of a C4.5 decision tree [DHS00, p. 411]), Bagging [Bre96]	Multilayer Perceptron [Bau88], Logistic Model Tree [LHF05], Dagging [TW97], RotationForest [RKA06]
Number of substrates in test set	10	3
Number of test samples	700 unlabeled + 100 labeled	6.000 labeled (+ simulation with StirTrace)
Technology Readiness Level	3	4

Table 8.1: Comparison of the Two Application Scenarios

whereas three classifiers are arbitrarily selected for the first application scenario. The reason for the latter is the required training time. As a result three classifiers are selected based on the underlying classification principle. A total of ten substrates is evaluated for the first application scenario, whereas only three substrates are evaluated for the second application scenario. The reason for the latter are the limitations of the utilized printer which is required to be able to print directly on the substrate. Due to the required acquisition time a total of 800 fingerprint samples is acquired within the experimental setup of the first application scenario. In the second application scenario 6.000 samples are acquired and additionally processed using StirTrace. Based on the achieved classification accuracies the achieved technology readiness level¹ for the first application scenario is 3 (experimental proof of concept). For the second application scenario the technology readiness level is at least 4 (technology validate in lab).

Lessons Learned
from Application
Scenario 1

The evaluation in [Chapter 5](#) shows that the performance of a classifier cannot be directly projected to achievable results in terms of a forensic investigation. The evaluation of 700 latent fingerprint samples from 10 different substrate materials resulted in a classification problem with literally hundreds of millions of blocks and feature vectors yielded only a small number of successful biometric matches. However, at least for some substrates, a manual comparison of the samples by latent fingerprint examiners might yield better results. The feature selection for the 600-dimensional feature space has removed all designed semantic features as well as the features derived from Benford's Law. As the resulting features originate from the original images as well as the particular preprocessing results, the selected preprocessing likely has a positive impact on the discriminatory power of some of the features. However, the overall accuracy of the detection approach is almost not affected by the feature selection. Though, this could at least help to minimize the computational expensiveness of the training of the models in the selected supervised learning-based approaches. Overall, the approach needs a more detailed investigation including a proper source of ground truth data.

Lessons Learned
from Application
Scenario 2

The second application scenario in [Chapter 6](#) indicates a very high detection accuracy for the designed feature spaces. The feature selection reduced the dimensionality of the feature space and resulted in a decreased detection accuracy. However, the false miss rate in the reduced feature space is zero for all three evaluated classifiers. Using the StirTrace benchmarking, the 3,000 test samples are virtually expanded to a test set of 210,000 samples by applying 70 filter-parameter-combinations. While the results from the evaluation are still very promising, the approach does not necessarily achieve generalization as only one particular printer model is used in the experimental setup.

¹https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trL_en.pdf, last accessed 10/11/2020

Due to the limited scope of a PhD thesis, not all aspects of a topic can be addressed in detail. Within this thesis such limitations apply regarding the selected application scenarios from one specific domain, the size of the test sets as well as the evaluation approaches. With a multi-disciplinary, cross-sectional topic of forensic science, computer science as well as physics and metrology, only a small portion of the field could be covered. Furthermore, due to the nature of this thesis being focused on the computer science aspects of forensic investigations, aspects of other scientific domains are not covered in detail. This section gives an outline of potential future research directions towards the process model, sensors and sensor data preprocessing, latent fingerprint investigation and the detection of latent fingerprint forgeries.

9.1 Future Research Directions Regarding the Process Model

With the initial step of creating a first tier of phases for the organization of digitized forensic investigations, the foundation for further research is created. The exemplary validation for the domain of latent fingerprint investigations supports the claim of a universally applicable process model for digitized forensics in the sense of criminalistics. However, it is still necessary to investigate other domains in detail in order to determine whether all second-tier phases can be logically mapped to the phases defined in the first tier. Any discrepancies would require an updated version of the process model which might cause incompatibilities with other trace type investigation procedures.

The compatibility with additional dimensions of process models, such as the model of Kiltz et al. [KHA+09] in Section 2.1.1.2.6 should be analyzed as well. A major open issue in the context of digitized forensics is the shift in required storage conditions for the physical traces in order to avoid or minimize the degradation of a trace over a long period of time. This would require extensive experiments from a physics and chemical point of view.

A more immediate issue is the acceptance of novel processing techniques in court. Especially discussions with latent fingerprint examiners revealed that they tend to bring the physically or chemically preprocessed traces to court hearings to prove the authenticity of the evidence. Especially in a transition period, the traces might be processed using traditional methods after the contact-less digitization to show

the validity of the results of the novel methods. The question here is whether police agencies and forensic laboratories are willing to invest the additional effort in order to establish the foundation for the acceptance of novel techniques. This is especially an issue considering the backlogs present in various forensic disciplines. From a more practical point of view other means to protect a chain-of-custody such as the utilization of blockchain technologies in conjunction with tamper-proof-timestamps as suggested by Prof. Ntalianis in his review of this thesis should be investigated. For the sake of data retention times and data protection regulations the data protected in such a blockchain should be limited to the relevant meta-data.

9.2 Future Research Directions Regarding Sensory and Sensor Data Preprocessing

From perspective of sensory multiple future research directions arise. For the experiments within the scope of this thesis three different sensors were available. However, it is an open question whether the underlying measurement principles are the most suited for the investigated application scenario. Especially with respect to porous substrates this is probably not the case. Furthermore, the particular lateral resolution of the UV-VIS-reflection spectrometer is too low for the reliable analysis of level-2 features of latent fingerprints. The experiments in [Mak+15] and [HMQ+13] show promising results for some substrates which are considered challenging for the CWL-sensor utilized in Chapter 5. Here, other optics might improve the lateral resolution. However, this might even further increase the scan duration of a fingerprint sample also increasing the exposure to UV radiation. An alternative approach is the application of models from compressive sensing, as described in [Jas13] for the application of the domain of face biometrics, to increase the resolution of the resulting data. However, such an approach needs to be extensively evaluated to determine whether the calculated information is representing the investigated trace appropriately.

Even though the focus of the application scenarios in this thesis is on pattern recognition-based processing of the scan data, other methods, e.g. image processing techniques, might yield similar or even better results. Here, a benchmarking of different approaches seems to be a logical direction for further research. In conjunction with that, particular confidence levels of the image processing techniques should be determined as well.

The potential impact of particular sensors on different trace types should be investigated in order to be able to assess the trace concurrency as suggested by Prof. Ntalianis in his review of this thesis. In particular factors such as survival-rules for traces in relation to sensory as well as a potential ranking of traces (best-traces-for-custody rules) should be evaluated in this context.

9.3 Future Research Directions Regarding Latent Fingerprint Investigation

The directions for further research regarding the latent fingerprint investigation are basically outlined by the limitations of this thesis. In particular different classification approaches such as an one-class classifier or substrate independent models should be evaluated. Furthermore, the feature space needs to be improved in order to reduce the error rates for the fingerprint pattern reconstruction. In

line with that, additional image analysis techniques should be investigated as suggested by Prof. Jassim in his review for this thesis. The major issue for the training remains the acquisition of realistic data with a proper ground truth. Within a broader scope of the thesis a simulation of latent fingerprint scans was considered as a potential approach to get a ground truth. However, this approach was discarded because it would inevitably raise the question of the representativity of the resulting data. Another option would be the creation of test sets using artificial sweat and ink-jet printers as used in [Chapter 6](#). However, due to observed printing defects the reproducibility would be limited and furthermore no variations in the amount and composition of the fingerprint residue would occur. Within the limited scope of the evaluation, it is also not possible to determine whether the trained models achieve a generalization for the classification problem at hand. Thus, a significantly extended test set would be necessary in order to provide reliable estimates for the performance in practice. The second major limitation is the evaluation methodology for the quality of the reconstructed fingerprint data. As the author of this thesis is not a trained latent fingerprint examiner and due to the lack of ground truth, employing biometric matching techniques is the only feasible assessment technique. However, in future work latent fingerprint examiners should analyze the results in order to determine the actual error rates.

9.4 Future Research Directions Regarding the Detection of Latent Fingerprint Forgeries

The directions for further research regarding the detection of latent fingerprint forgeries are also primarily driven by the limitations of the evaluation of the application scenario in [Chapter 6](#). In particular, multiple printers and multiple artificial sweat compositions should be analyzed in future work to evaluate whether the trained models for the detection achieved sufficient generalization of the decision boundaries within the feature space. Moreover, other sources of latent fingerprint forgeries should be assessed as well. Since the proposed approach is designed as an assisting analysis tool, an open issue is the appropriate presentation of the decision of the detection algorithm. The intended behavior of the forensic expert would be a more detailed investigation of the trace in order to confirm the suspected forgery rather than an immediate exclusion of the latent fingerprint in question.

This appendix contains supplemental materials of the thesis. In particular the software design of the StirTrace [HiD16] benchmarking framework is described in Section A.1. The current state of the items for the formal definition of sensors is contained in Section A.2. The particular raw data from the WEKA data mining software [Hal+09] and the biometric matching using the NIST Biometric Imaging Software [Nat13] for the application scenario in Chapter 5 are contained in Section A.3. Subsequently, the raw classification results for the evaluation within the scope of the application scenario in Chapter 6 are presented in Section A.4.

A.1 Software Architecture of StirTrace

The benchmarking framework StirTrace¹ is designed to be extendable regarding different evaluation goals. StirTrace is written in C++, QT4.8² and utilizes OpenCV 2.4 [Ope20b] for image processing. The overall software architecture is depicted in Figure A.1. By its very nature, the core part of StirTrace is the

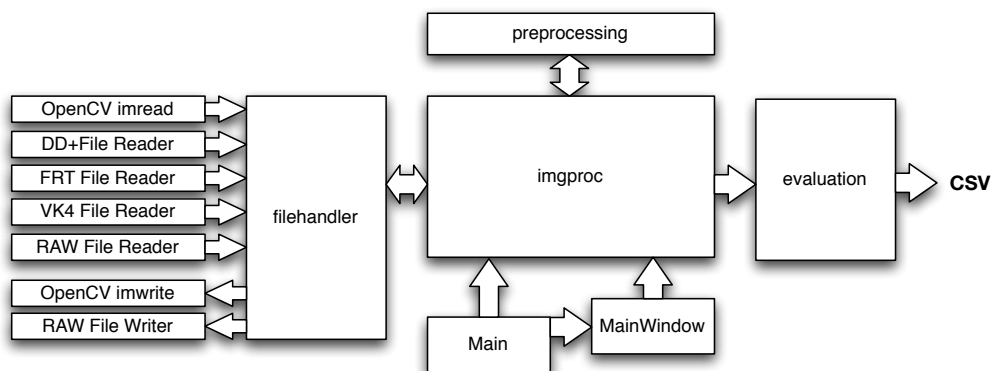


Figure A.1: Software Architecture of StirTrace

image processing block (imgproc). This block is either initialized via command line parameters supplied to the main block or by specifying parameters in an embedded graphical user interface (MainWindow). With the parameterization of imgproc, the signal processing pipeline is specified in terms of the data source

¹<https://sourceforge.net/projects/stirtrace/>

²<https://doc.qt.io/archives/qt-4.8/>

(filehandler), preprocessing (currently unused), specific image manipulation techniques and either the storage of the manipulated image via the file handler or the evaluation and feature extraction using the evaluation block. The image manipulation techniques in the `imgproc` module can be utilized either separately or in combination with each other.

File Handler

The file handler is intended to provide an abstract interface for various image formats and the relevant metadata, particularly the scale of the image I . In particular, the standard image formats supported by OpenCV, as well as sensory-specific scan data can be read by the file handler. The latter was re-implemented according to the format documentation or based on reverse engineering within the scope of this thesis. In addition to that, a manufacturer-independent image format in conjunction with metadata is designed and implemented within the scope of the research. The latter, as well as the standard image formats supported by OpenCV, can be used to export the processed images as well.

Evaluation
Module

The evaluation module is intended to minimize the amount of generated data by performing the feature extraction within StirTrace. In doing so, no manipulated image data is permanently stored. Instead, only the relevant feature values are recorded within comma separated value (CSV) files. The major advantage of this approach is the significant minimization of the required amount of data to be written. Thus, the evaluation is sped up significantly. The disadvantage of this approach is the lack of exact reproducibility in conjunction with any image manipulation technique with a random element.

A.2 Formal Definition of Sensors

- M - measurement principle
 - M_1 mono chromatic
 - M_2 multi chromatic
 - * $M_{2,1}$ UV Radiation
 - * $M_{2,2}$ Visible Light
 - * $M_{2,3}$ Near Infrared (NIR)
- O - Mode of operation
 - O_1 Point sensor
 - O_2 Line sensor
 - O_3 Area sensor
 - O_4 Volume sensor
- D_{Syntax} Syntax of the resulting data
 - D_{Syntax_0} Single value
 - D_{Syntax_1} One-dimensional array of values
 - D_{Syntax_2} Two-dimensional array of values
 - D_{Syntax_3} Three-dimensional array of values
- $D_{Semantics}$ Syntax of the resulting data
 - $D_{Semantics_1}$ Light intensity data

- $D_{Semantics_2}$ Color data
- $D_{Semantics_3}$ Distance/height data
- $D_{Semantics_4}$ Room-coordinates
- $D_{Semantics_5}$ Spectral data

A.3 Supplemental Material for the Segregation of Fingerprint Traces from Substrate Data

A.3.1 Classifier Outputs for the 2-Fold Cross Validation

The following subsections contain the results of the two-fold cross validation of the three evaluated classifiers for each of the substrates. The class label f represents a block with fingerprint residue, whereas the class label b represents a block with the substrate not covered by fingerprint residue. The particular ground truth is estimated based on the differential scan method as described in Section 5.2.

A.3.1.1 White Furniture Surface M_1

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      913345          91.0613 %
Incorrectly Classified Instances    89655           8.9387 %
Kappa statistic                    0.8212
Mean absolute error                0.0894
Root mean squared error            0.299
Relative absolute error            17.8774 %
Root relative squared error        59.7953 %
Total Number of Instances          1003000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.89    0.069    0.928     0.89    0.909     0.911    f
                0.931    0.11    0.894     0.931    0.912     0.911    b
Weighted Avg.    0.911    0.089    0.911     0.911    0.911     0.911
=== Confusion Matrix ===

      a      b  <-- classified as
446419  55081 |      a = f
 34574  466926 |      b = b
    
```

Listing A.1: WEKA Classifier Output for the 2-Fold Cross Validation on M_1 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      902780          90.008 %
Incorrectly Classified Instances    100220           9.992 %
Kappa statistic                    0.8002
Mean absolute error                0.1032
Root mean squared error            0.3083
Relative absolute error            20.6406 %
Root relative squared error        61.6523 %
Total Number of Instances          1003000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.901    0.101    0.899     0.901    0.9       0.882    f
                0.899    0.099    0.901     0.899    0.9       0.882    b
Weighted Avg.    0.9     0.1     0.9       0.9     0.9       0.882
=== Confusion Matrix ===

      a      b  <-- classified as
451889  49611 |      a = f
 50609  450891 |      b = b
    
```

Listing A.2: WEKA Classifier Output for the 2-Fold Cross Validation on M_1 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      930762          92.7978 %
Incorrectly Classified Instances    72238           7.2022 %
Kappa statistic                    0.856
Mean absolute error                 0.1067
Root mean squared error             0.2264
Relative absolute error             21.3326 %
Root relative squared error         45.2722 %
Total Number of Instances          1003000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.922    0.066    0.933     0.922   0.928     0.983    f
                 0.934    0.078    0.923     0.934   0.928     0.983    b

=== Confusion Matrix ===
      a      b  <-- classified as
462330  39170 |      a = f
 33068  468432 |      b = b

```

Listing A.3: WEKA Classifier Output for the 2-Fold Cross Validation on M_1 using Bagging

A.3.1.2 Veneered Plywood (Beech) M_2

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      737098          81.3138 %
Incorrectly Classified Instances    169388          18.6862 %
Kappa statistic                    0.6263
Mean absolute error                 0.1869
Root mean squared error             0.4323
Relative absolute error             37.3724 %
Root relative squared error         86.4551 %
Total Number of Instances          906486
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.807    0.181    0.817     0.807   0.812     0.813    f
                 0.819    0.193    0.809     0.819   0.814     0.813    b

=== Confusion Matrix ===
      a      b  <-- classified as
365849  87394 |      a = f
 81994  371249 |      b = b

```

Listing A.4: WEKA Classifier Output for the 2-Fold Cross Validation on M_2 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      719826          79.4084 %
Incorrectly Classified Instances    186660          20.5916 %
Kappa statistic                    0.5882
Mean absolute error                 0.2086
Root mean squared error             0.4431
Relative absolute error             41.7192 %
Root relative squared error         88.6168 %
Total Number of Instances          906486
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.795    0.207    0.794     0.795   0.794     0.772    f
                 0.793    0.205    0.795     0.793   0.794     0.772    b

=== Confusion Matrix ===
      a      b  <-- classified as
360327  92916 |      a = f
 93744  359499 |      b = b

```

Listing A.5: WEKA Classifier Output for the 2-Fold Cross Validation on M_2 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

```

```

Correctly Classified Instances      764213      84.305 %
Incorrectly Classified Instances    142273      15.695 %
Kappa statistic                    0.6861
Mean absolute error                0.2125
Root mean squared error            0.3243
Relative absolute error            42.5099 %
Root relative squared error        64.8592 %
Total Number of Instances          906486
===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.838	0.152	0.846	0.838	0.842	0.933	f
	0.848	0.162	0.84	0.848	0.844	0.933	b
Weighted Avg.	0.843	0.157	0.843	0.843	0.843	0.933	

```

===== Confusion Matrix =====
      a      b  <-- classified as
379999  73244 |      a = f
69029   384214 |      b = b

```

Listing A.6: WEKA Classifier Output for the 2-Fold Cross Validation on M_2 using Bagging

A.3.1.3 Brushed Stainless Steel M_3

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

```

Correctly Classified Instances	569004	75.4105 %
Incorrectly Classified Instances	185538	24.5895 %
Kappa statistic	0.5082	
Mean absolute error	0.2459	
Root mean squared error	0.4959	
Relative absolute error	49.179 %	
Root relative squared error	99.1756 %	
Total Number of Instances	754542	

```

===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.757	0.249	0.753	0.757	0.755	0.754	f
	0.751	0.243	0.756	0.751	0.753	0.754	b
Weighted Avg.	0.754	0.246	0.754	0.754	0.754	0.754	

```

===== Confusion Matrix =====
      a      b  <-- classified as
285571  91700 |      a = f
93838   283433 |      b = b

```

Listing A.7: WEKA Classifier Output for the 2-Fold Cross Validation on M_3 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

```

Correctly Classified Instances	537827	71.2786 %
Incorrectly Classified Instances	216715	28.7214 %
Kappa statistic	0.4256	
Mean absolute error	0.2903	
Root mean squared error	0.5231	
Relative absolute error	58.0643 %	
Root relative squared error	104.6267 %	
Total Number of Instances	754542	

```

===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.714	0.288	0.712	0.714	0.713	0.702	f
	0.712	0.286	0.713	0.712	0.712	0.702	b
Weighted Avg.	0.713	0.287	0.713	0.713	0.713	0.702	

```

===== Confusion Matrix =====
      a      b  <-- classified as
269338  107933 |      a = f
108782  268489 |      b = b

```

Listing A.8: WEKA Classifier Output for the 2-Fold Cross Validation on M_3 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

```

Correctly Classified Instances	588784	78.032 %
Incorrectly Classified Instances	165758	21.968 %

```

Kappa statistic                0.5606
Mean absolute error            0.3003
Root mean squared error       0.3832
Relative absolute error       60.0622 %
Root relative squared error   76.6466 %
Total Number of Instances     754542
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.79    0.229   0.775     0.79   0.782     0.87     f
                0.771   0.21    0.786     0.771 0.778     0.87     b
Weighted Avg.    0.78    0.22    0.78      0.78   0.78      0.87
=== Confusion Matrix ===

      a      b  <-- classified as
298070 79201 |      a = f
 86557 290714 |      b = b

```

Listing A.9: WEKA Classifier Output for the 2-Fold Cross Validation on M_3 using Bagging

A.3.1.4 Aluminum Foil M_4

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances  735384                80.2574 %
Incorrectly Classified Instances 180898                19.7426 %
Kappa statistic                0.6051
Mean absolute error            0.1974
Root mean squared error       0.4443
Relative absolute error       39.4852 %
Root relative squared error   88.8653 %
Total Number of Instances     916282
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.824   0.219   0.79      0.824   0.807     0.803     f
                0.781   0.176   0.816     0.781   0.798     0.803     b
Weighted Avg.    0.803   0.197   0.803     0.803   0.802     0.803
=== Confusion Matrix ===

      a      b  <-- classified as
377482  80659 |      a = f
100239 357902 |      b = b

```

Listing A.10: WEKA Classifier Output for the 2-Fold Cross Validation on M_4 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances  711296                77.6285 %
Incorrectly Classified Instances 204986                22.3715 %
Kappa statistic                0.5526
Mean absolute error            0.2273
Root mean squared error       0.4623
Relative absolute error       45.4545 %
Root relative squared error   92.4523 %
Total Number of Instances     916282
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.776   0.223   0.777     0.776   0.776     0.754     f
                0.777   0.224   0.776     0.777   0.776     0.754     b
Weighted Avg.    0.776   0.224   0.776     0.776   0.776     0.754
=== Confusion Matrix ===

      a      b  <-- classified as
355439 102702 |      a = f
102284 355857 |      b = b

```

Listing A.11: WEKA Classifier Output for the 2-Fold Cross Validation on M_4 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances  765472                83.5411 %
Incorrectly Classified Instances 150810                16.4589 %
Kappa statistic                0.6708
Mean absolute error            0.2311
Root mean squared error       0.3366

```

```

Relative absolute error          46.2201 %
Root relative squared error      67.323 %
Total Number of Instances        916282
===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.851	0.18	0.825	0.851	0.838	0.921	f
	0.82	0.149	0.846	0.82	0.833	0.921	b
Weighted Avg.	0.835	0.165	0.836	0.835	0.835	0.921	

```

===== Confusion Matrix =====

```

a	b	<-- classified as
389713	68428	a = f
82382	375759	b = b

Listing A.12: WEKA Classifier Output for the 2-Fold Cross Validation on M_4 using Bagging

A.3.1.5 Golden-Oak Veneer M_5

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

```

Correctly Classified Instances	677053	66.4471 %
Incorrectly Classified Instances	341883	33.5529 %
Kappa statistic	0.3289	
Mean absolute error	0.3355	
Root mean squared error	0.5792	
Relative absolute error	67.1059 %	
Root relative squared error	115.8498 %	
Total Number of Instances	1018936	

```

===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.868	0.539	0.617	0.868	0.721	0.664	f
	0.461	0.132	0.778	0.461	0.579	0.664	b
Weighted Avg.	0.664	0.336	0.697	0.664	0.65	0.664	

```

===== Confusion Matrix =====

```

a	b	<-- classified as
442418	67050	a = f
274833	234635	b = b

Listing A.13: WEKA Classifier Output for the 2-Fold Cross Validation on M_5 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

```

Correctly Classified Instances	714627	70.1346 %
Incorrectly Classified Instances	304309	29.8654 %
Kappa statistic	0.4027	
Mean absolute error	0.3014	
Root mean squared error	0.5323	
Relative absolute error	60.2898 %	
Root relative squared error	106.463 %	
Total Number of Instances	1018936	

```

===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.7	0.297	0.702	0.7	0.701	0.698	f
	0.703	0.3	0.701	0.703	0.702	0.698	b
Weighted Avg.	0.701	0.299	0.701	0.701	0.701	0.698	

```

===== Confusion Matrix =====

```

a	b	<-- classified as
356582	152886	a = f
151423	358045	b = b

Listing A.14: WEKA Classifier Output for the 2-Fold Cross Validation on M_5 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

```

Correctly Classified Instances	788385	77.3734 %
Incorrectly Classified Instances	230551	22.6266 %
Kappa statistic	0.5475	
Mean absolute error	0.3143	
Root mean squared error	0.3894	
Relative absolute error	62.8687 %	
Root relative squared error	77.889 %	
Total Number of Instances	1018936	

```

===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.832   0.285   0.745     0.832   0.786     0.859     f
                0.715   0.168   0.81      0.715   0.76      0.859     b
Weighted Avg.  0.774   0.226   0.778     0.774   0.773     0.859
===== Confusion Matrix =====
      a      b  <-- classified as
423902 85566 |      a = f
144985 364483 |      b = b

```

Listing A.15: WEKA Classifier Output for the 2-Fold Cross Validation on M_5 using Bagging

A.3.1.6 Non-Metallic Matte Car Body Finish M_6

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      765892           86.1676 %
Incorrectly Classified Instances    122948           13.8324 %
Kappa statistic                    0.7234
Mean absolute error                 0.1383
Root mean squared error             0.3719
Relative absolute error             27.6648 %
Root relative squared error         74.3839 %
Total Number of Instances          888840
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.893   0.169   0.841     0.893   0.866     0.862     f
                0.831   0.107   0.886     0.831   0.857     0.862     b
Weighted Avg.  0.862   0.138   0.863     0.862   0.862     0.862
===== Confusion Matrix =====
      a      b  <-- classified as
396751 47669 |      a = f
75279 369141 |      b = b

```

Listing A.16: WEKA Classifier Output for the 2-Fold Cross Validation on M_6 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      738640           83.1016 %
Incorrectly Classified Instances    150200           16.8984 %
Kappa statistic                    0.662
Mean absolute error                 0.1753
Root mean squared error             0.3999
Relative absolute error             35.0572 %
Root relative squared error         79.9791 %
Total Number of Instances          888840
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.833   0.171   0.83      0.833   0.831     0.813     f
                0.829   0.167   0.832     0.829   0.831     0.813     b
Weighted Avg.  0.831   0.169   0.831     0.831   0.831     0.813
===== Confusion Matrix =====
      a      b  <-- classified as
370046 74374 |      a = f
75826 368594 |      b = b

```

Listing A.17: WEKA Classifier Output for the 2-Fold Cross Validation on M_6 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      784153           88.2221 %
Incorrectly Classified Instances    104687           11.7779 %
Kappa statistic                    0.7644
Mean absolute error                 0.1822
Root mean squared error             0.2925
Relative absolute error             36.4454 %
Root relative squared error         58.4973 %
Total Number of Instances          888840
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class

```

```

                0.901    0.137    0.868    0.901    0.884    0.953    f
                0.863    0.099    0.898    0.863    0.88    0.953    b
Weighted Avg.  0.882    0.118    0.883    0.882    0.882    0.953
===== Confusion Matrix =====
      a      b  <-- classified as
400629 43791 |      a = f
 60896 383524 |      b = b
    
```

Listing A.18: WEKA Classifier Output for the 2-Fold Cross Validation on M_6 using Bagging

A.3.1.7 Metallic Car Body Finish M_7

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      338998      71.9875 %
Incorrectly Classified Instances    131914      28.0125 %
Kappa statistic                    0.4398
Mean absolute error                 0.2801
Root mean squared error             0.5293
Relative absolute error             56.0249 %
Root relative squared error        105.8536 %
Total Number of Instances          470912
===== Detailed Accuracy By Class =====
      TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
      0.821    0.382    0.683     0.821    0.746     0.72     f
      0.618    0.179    0.776     0.618    0.688     0.72     b
Weighted Avg.  0.72     0.28     0.729     0.72     0.717     0.72
===== Confusion Matrix =====
      a      b  <-- classified as
193380 42076 |      a = f
 89838 145618 |      b = b
    
```

Listing A.19: WEKA Classifier Output for the 2-Fold Cross Validation on M_7 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      329264      69.9205 %
Incorrectly Classified Instances    141648      30.0795 %
Kappa statistic                    0.3984
Mean absolute error                 0.3039
Root mean squared error             0.5335
Relative absolute error             60.7859 %
Root relative squared error        106.6934 %
Total Number of Instances          470912
===== Detailed Accuracy By Class =====
      TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
      0.7      0.301    0.699     0.7     0.699     0.694     f
      0.699    0.3     0.699     0.699   0.699     0.694     b
Weighted Avg.  0.699    0.301    0.699     0.699   0.699     0.694
===== Confusion Matrix =====
      a      b  <-- classified as
164795 70661 |      a = f
 70987 164469 |      b = b
    
```

Listing A.20: WEKA Classifier Output for the 2-Fold Cross Validation on M_7 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      362981      77.0804 %
Incorrectly Classified Instances    107931      22.9196 %
Kappa statistic                    0.5416
Mean absolute error                 0.3081
Root mean squared error             0.3935
Relative absolute error             61.6285 %
Root relative squared error        78.7064 %
Total Number of Instances          470912
===== Detailed Accuracy By Class =====
      TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
      0.839    0.297    0.738     0.839    0.785     0.848     f
      0.703    0.161    0.814     0.703    0.754     0.848     b
Weighted Avg.  0.771    0.229    0.776     0.771    0.77     0.848
    
```

```

===== Confusion Matrix =====
      a      b  <-- classified as
197546 37910 |      a = f
 70021 165435 |      b = b

```

Listing A.21: WEKA Classifier Output for the 2-Fold Cross Validation on M_7 using Bagging

A.3.1.8 Blued Metal M_8

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      752968                79.4672 %
Incorrectly Classified Instances    194552                20.5328 %
Kappa statistic                    0.5893
Mean absolute error                 0.2053
Root mean squared error             0.4531
Relative absolute error             41.0655 %
Root relative squared error         90.6262 %
Total Number of Instances          947520
===== Detailed Accuracy By Class =====
              TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.  0.824  0.235    0.778    0.824    0.801    0.795    f
                0.765  0.176    0.813    0.765    0.788    0.795    b
Weighted Avg.  0.795  0.205    0.796    0.795    0.794    0.795

===== Confusion Matrix =====
      a      b  <-- classified as
390421 83339 |      a = f
111213 362547 |      b = b

```

Listing A.22: WEKA Classifier Output for the 2-Fold Cross Validation on M_8 using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      729242                76.9632 %
Incorrectly Classified Instances    218278                23.0368 %
Kappa statistic                    0.5393
Mean absolute error                 0.2334
Root mean squared error             0.4689
Relative absolute error             46.6766 %
Root relative squared error         93.7797 %
Total Number of Instances          947520
===== Detailed Accuracy By Class =====
              TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.  0.769  0.229    0.77    0.769    0.769    0.75    f
                0.771  0.231    0.769    0.771    0.77    0.75    b
Weighted Avg.  0.77    0.23    0.77    0.77    0.77    0.75

===== Confusion Matrix =====
      a      b  <-- classified as
364188 109572 |      a = f
108706 365054 |      b = b

```

Listing A.23: WEKA Classifier Output for the 2-Fold Cross Validation on M_8 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      782927                82.6291 %
Incorrectly Classified Instances    164593                17.3709 %
Kappa statistic                    0.6526
Mean absolute error                 0.2392
Root mean squared error             0.3435
Relative absolute error             47.8424 %
Root relative squared error         68.7062 %
Total Number of Instances          947520
===== Detailed Accuracy By Class =====
              TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.  0.863  0.137    0.804    0.863    0.832    0.913    f
                0.79    0.174    0.852    0.79    0.82    0.913    b
Weighted Avg.  0.826  0.174    0.828    0.826    0.826    0.913

===== Confusion Matrix =====
      a      b  <-- classified as

```



```
408787 64973 | a = f
99620 374140 | b = b
```

Listing A.24: WEKA Classifier Output for the 2-Fold Cross Validation on M_8 using Bagging

A.3.1.9 Ceramic Tile M_9

```
2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      535433          76.5059 %
Incorrectly Classified Instances    164425          23.4941 %
Kappa statistic                    0.5301
Mean absolute error                 0.2349
Root mean squared error            0.4847
Relative absolute error             46.9881 %
Root relative squared error        96.9413 %
Total Number of Instances         699858
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.783   0.253   0.756     0.783   0.769     0.765     f
                0.747   0.217   0.775     0.747   0.761     0.765     b
Weighted Avg.   0.765   0.235   0.765     0.765   0.765     0.765

=== Confusion Matrix ===

      a      b  <-- classified as
274049 75880 | a = f
 88545 261384 | b = b
```

Listing A.25: WEKA Classifier Output for the 2-Fold Cross Validation on M_9 using SMO

```
2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      494253          70.6219 %
Incorrectly Classified Instances    205605          29.3781 %
Kappa statistic                    0.4124
Mean absolute error                 0.2978
Root mean squared error            0.5268
Relative absolute error             59.5517 %
Root relative squared error        105.3504 %
Total Number of Instances         699858
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.706   0.293   0.706     0.706   0.706     0.702     f
                0.707   0.294   0.706     0.707   0.706     0.702     b
Weighted Avg.   0.706   0.294   0.706     0.706   0.706     0.702

=== Confusion Matrix ===

      a      b  <-- classified as
246979 102950 | a = f
102655 247274 | b = b
```

Listing A.26: WEKA Classifier Output for the 2-Fold Cross Validation on M_9 using J48

```
2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      548847          78.4226 %
Incorrectly Classified Instances    151011          21.5774 %
Kappa statistic                    0.5685
Mean absolute error                 0.3071
Root mean squared error            0.3854
Relative absolute error             61.4204 %
Root relative squared error        77.0851 %
Total Number of Instances         699858
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.799   0.23   0.776     0.799   0.787     0.867     f
                0.77   0.201  0.793     0.77   0.781     0.867     b
Weighted Avg.   0.784   0.216  0.784     0.784   0.784     0.867

=== Confusion Matrix ===

      a      b  <-- classified as
279471 70458 | a = f
 80553 269376 | b = b
```

Listing A.27: WEKA Classifier Output for the 2-Fold Cross Validation on M_9 using Bagging

A.3.1.10 Copying Paper M_{10}

```

2-Fold Cross-validation results for weka.classifiers.functions.SMO
Classifier: weka.classifiers.functions.SMO

Correctly Classified Instances      315154                73.4978 %
Incorrectly Classified Instances    113640                26.5022 %
Kappa statistic                    0.47
Mean absolute error                 0.265
Root mean squared error             0.5148
Relative absolute error             53.0045 %
Root relative squared error        102.9606 %
Total Number of Instances          428794
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.735   0.265   0.735     0.735   0.735     0.735    f
                0.735   0.265   0.735     0.735   0.735     0.735    b
Weighted Avg.   0.735   0.265   0.735     0.735   0.735     0.735
=== Confusion Matrix ===

      a      b  <-- classified as
157659  56738 | a = f
 56902 157495 | b = b

```

Listing A.28: WEKA Classifier Output for the 2-Fold Cross Validation on M_{10} using SMO

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      290710                67.7971 %
Incorrectly Classified Instances    138084                32.2029 %
Kappa statistic                    0.3559
Mean absolute error                 0.3246
Root mean squared error             0.5536
Relative absolute error             64.912 %
Root relative squared error        110.7185 %
Total Number of Instances          428794
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.678   0.323   0.678     0.678   0.678     0.668    f
                0.677   0.322   0.678     0.677   0.678     0.668    b
Weighted Avg.   0.678   0.322   0.678     0.678   0.678     0.668
=== Confusion Matrix ===

      a      b  <-- classified as
145467  68930 | a = f
 69154 145243 | b = b

```

Listing A.29: WEKA Classifier Output for the 2-Fold Cross Validation on M_{10} using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      321368                74.9469 %
Incorrectly Classified Instances    107426                25.0531 %
Kappa statistic                    0.4989
Mean absolute error                 0.3313
Root mean squared error             0.4056
Relative absolute error             66.2699 %
Root relative squared error        81.1272 %
Total Number of Instances          428794
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.772   0.273   0.739     0.772   0.755     0.836    f
                0.727   0.228   0.761     0.727   0.744     0.836    b
Weighted Avg.   0.749   0.251   0.75     0.749   0.749     0.836
=== Confusion Matrix ===

      a      b  <-- classified as
165608  48789 | a = f
 58637 155760 | b = b

```

Listing A.30: WEKA Classifier Output for the 2-Fold Cross Validation on M_{10} using Bagging

A.3.2 Successful Matches and Matching Scores from the Biometric Evaluation

This section contains the biometric matching results of the NIST Biometric Imaging Software [Nat13] using the reconstructed latent fingerprint patterns. The particular threshold for the matching score is set to 40 according to the rule of thumb for a true match in [Wat+08, p. 21]. All matching scores of less than 40 are omitted and considered as unsuccessful biometric matches.

A.3.2.1 White Furniture Surface M_1

```

71 /mnt/diss/digidak/data/unimd_amsl_48/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu/J48/orig//Scan31_r0_10.FRT-orig.jpg.xyt
49 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/orig//Scan11_r0_10.FRT-orig.jpg.xyt
84 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/orig//Scan22_r0_10.FRT-orig.jpg.xyt
56 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/J48/orig//Scan11_r0_10.FRT-orig.jpg.xyt

```

Listing A.31: Bozorth3 matching scores on M_1 for the original image

```

75 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan13_r0_10.FRT-raw.jpg.xyt
83 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan15_r0_10.FRT-raw.jpg.xyt
73 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan17_r0_10.FRT-raw.jpg.xyt
89 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan23_r0_10.FRT-raw.jpg.xyt
69 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan25_r0_10.FRT-raw.jpg.xyt
40 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan26_r0_10.FRT-raw.jpg.xyt
45 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/raw//Scan28_r0_10.FRT-raw.jpg.xyt
47 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/raw//Scan13_r0_10.FRT-raw.jpg.xyt
40 /mnt/diss/digidak/data/unimd_amsl_3/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/raw//Scan3_r0_10.FRT-raw.jpg.xyt
47 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/raw//Scan24_r0_10.FRT-raw.jpg.xyt
57 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/raw//Scan25_r0_10.FRT-raw.jpg.xyt
44 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/raw//Scan27_r0_10.FRT-raw.jpg.xyt

```

Listing A.32: Bozorth3 matching scores on M_1 for the raw SMO classifier output

```

90 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/optimized//Scan13_r0_10.FRT-optimized.jpg
  .xyt
90 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/optimized//Scan15_r0_10.FRT-optimized.jpg
  .xyt
69 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/optimized//Scan17_r0_10.FRT-optimized.jpg
  .xyt
76 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/optimized//Scan23_r0_10.FRT-optimized.jpg
  .xyt
67 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/optimized//Scan25_r0_10.FRT-optimized.jpg
  .xyt
48 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/optimized//Scan28_r0_10.FRT-optimized.jpg
  .xyt
44 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/optimized//Scan13_r0_10.FRT-optimized.jpg
  .xyt
49 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/optimized//Scan24_r0_10.FRT-optimized.jpg
  .xyt
61 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/optimized//Scan25_r0_10.FRT-optimized.jpg
  .xyt
49 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/optimized//Scan27_r0_10.FRT-optimized.jpg
  .xyt

```

Listing A.33: Bozorth3 matching scores on M_1 for the optimized SMO classifier output

```

90 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/LRb//Scan13_r0_10.FRT-LRb.jpg.xyt
90 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/LRb//Scan15_r0_10.FRT-LRb.jpg.xyt
69 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/LRb//Scan17_r0_10.FRT-LRb.jpg.xyt
76 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/LRb//Scan23_r0_10.FRT-LRb.jpg.xyt
67 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/LRb//Scan25_r0_10.FRT-LRb.jpg.xyt
48 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/SMO/LRb//Scan28_r0_10.FRT-LRb.jpg.xyt
44 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/LRb//Scan13_r0_10.FRT-LRb.jpg.xyt
49 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/LRb//Scan24_r0_10.FRT-LRb.jpg.xyt
61 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/LRb//Scan25_r0_10.FRT-LRb.jpg.xyt
49 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/SMO/LRb//Scan27_r0_10.FRT-LRb.jpg.xyt

```

Listing A.34: Bozorth3 matching scores on M_1 for the LRb SMO classifier output

```

86 /mnt/diss/digidak/data/unimd_amsl_0/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu/J48/optimized//Scan14_r0_10.FRT-optimized.jpg.xyt
48 /mnt/diss/digidak/data/unimd_amsl_48/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu/J48/optimized//Scan32_r0_10.FRT-optimized.jpg.xyt
77 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/optimized//Scan12_r0_10.FRT-optimized.jpg
  .xyt
71 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/optimized//Scan14_r0_10.FRT-optimized.jpg
  .xyt
48 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/optimized//Scan15_r0_10.FRT-optimized.jpg
  .xyt
52 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/optimized//Scan22_r0_10.FRT-optimized.jpg
  .xyt
46 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/optimized//Scan24_r0_10.FRT-optimized.jpg
  .xyt
41 /mnt/diss/digidak/data/unimd_amsl_1/ri.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/neu2_uni_md_amsl_1/J48/optimized//Scan26_r0_10.FRT-optimized.jpg
  .xyt
52 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/J48/optimized//Scan11_r0_10.FRT-optimized.jpg.
  xyt
44 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/J48/optimized//Scan12_r0_10.FRT-optimized.jpg.
  xyt
55 /mnt/diss/digidak/data/unimd_amsl_3/lt.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/J48/optimized//Scan13_r0_10.FRT-optimized.jpg.
  xyt
45 /mnt/diss/digidak/data/unimd_amsl_48/rm.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  moebeloberflaeche/uni_md_amsl_3_48/J48/optimized//Scan26_r0_10.FRT-optimized.jpg.
  xyt

```

Listing A.35: Bozorth3 matching scores on M_1 for the optimized J48 classifier output

A.3.2.2 Veneered Plywood (Beech) M_2

```

56 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  furnier/xmas/SMO/raw//Scan28_r0_11.FRT-raw.jpg.xyt

```

Listing A.36: Bozorth3 matching scores on M_2 for the raw SMO classifier output

```

46 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  furnier/xmas/SMO/optimized//Scan28_r0_11.FRT-optimized.jpg.xyt

```

Listing A.37: Bozorth3 matching scores on M_2 for the optimized SMO classifier output

```

46 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
  furnier/xmas/SMO/LRb//Scan28_r0_11.FRT-LRb.jpg.xyt

```

Listing A.38: Bozorth3 matching scores on M_2 for the LRb SMO classifier output

A.3.2.3 Brushed Stainless Steel M_3

```
63 /mnt/diss/digidak/data/unimd_amsl1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
edelstahl/10_uni_md_amsl1/SMO/raw//Scan3_r0_10.FRT-raw.jpg.xyt
45 /mnt/diss/digidak/data/unimd_amsl1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
edelstahl/testset/SMO/raw//Scan42_r0_10.FRT-raw.jpg.xyt
```

Listing A.39: Bozorth3 matching scores on M_3 for the raw SMO classifier output

```
69 /mnt/diss/digidak/data/unimd_amsl1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
edelstahl/10_uni_md_amsl1/SMO/optimized//Scan3_r0_10.FRT-optimized.jpg.xyt
```

Listing A.40: Bozorth3 matching scores on M_3 for the optimized SMO classifier output

```
69 /mnt/diss/digidak/data/unimd_amsl1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
edelstahl/10_uni_md_amsl1/SMO/LRb//Scan3_r0_10.FRT-LRb.jpg.xyt
```

Listing A.41: Bozorth3 matching scores on M_3 for the LRb SMO classifier output

```
43 /mnt/diss/digidak/data/unimd_amsl1/ri.jpg.xyt /mnt/diss/digidak/lka_like_testset/
edelstahl/neu/J48/optimized//Scan1_r0_10.FRT-optimized.jpg.xyt
```

Listing A.42: Bozorth3 matching scores on M_3 for the optimized J48 classifier output

A.3.2.4 Aluminum Foil M_4

```
48 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/J48/orig//Scan1_r0_10.FRT-orig.jpg.xyt
```

Listing A.43: Bozorth3 matching scores on M_4 for the original image

```
66 /mnt/diss/digidak/data/unimd_amsl0/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-0-ri/SMO/raw//Scan1_r0_10.FRT-raw.jpg.xyt
51 /mnt/diss/digidak/data/unimd_amsl0/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-0-ri/SMO/raw//Scan5_r0_10.FRT-raw.jpg.xyt
109 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/raw//Scan1_r0_10.FRT-raw.jpg.xyt
49 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/raw//Scan2_r0_10.FRT-raw.jpg.xyt
47 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/raw//Scan3_r0_10.FRT-raw.jpg.xyt
73 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/raw//Scan7_r0_10.FRT-raw.jpg.xyt
```

Listing A.44: Bozorth3 matching scores on M_4 for the raw SMO classifier output

```
64 /mnt/diss/digidak/data/unimd_amsl0/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-0-ri/SMO/optimized//Scan1_r0_10.FRT-optimized.jpg.xyt
70 /mnt/diss/digidak/data/unimd_amsl0/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-0-ri/SMO/optimized//Scan5_r0_10.FRT-optimized.jpg.xyt
104 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/optimized//Scan1_r0_10.FRT-optimized.jpg.xyt
52 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/optimized//Scan2_r0_10.FRT-optimized.jpg.xyt
60 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/optimized//Scan3_r0_10.FRT-optimized.jpg.xyt
62 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/optimized//Scan7_r0_10.FRT-optimized.jpg.xyt
```

Listing A.45: Bozorth3 matching scores on M_4 for the optimized SMO classifier output

```
64 /mnt/diss/digidak/data/unimd_amsl0/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-0-ri/SMO/LRb//Scan1_r0_10.FRT-LRb.jpg.xyt
70 /mnt/diss/digidak/data/unimd_amsl0/rm.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-0-ri/SMO/LRb//Scan5_r0_10.FRT-LRb.jpg.xyt
104 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/LRb//Scan1_r0_10.FRT-LRb.jpg.xyt
52 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/LRb//Scan2_r0_10.FRT-LRb.jpg.xyt
60 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/LRb//Scan3_r0_10.FRT-LRb.jpg.xyt
62 /mnt/diss/digidak/data/unimd_amsl1/li.jpg.xyt /mnt/diss/digidak/lka_like_testset/
aluminium/uni-md-amsl-1_li_lm/SMO/LRb//Scan7_r0_10.FRT-LRb.jpg.xyt
```

Listing A.46: Bozorth3 matching scores on M_4 for the LRb SMO classifier output

```

44 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/raw//Scan1_r0_10.FRT-raw.jpg.xyt
48 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/raw//Scan2_r0_10.FRT-raw.jpg.xyt

```

Listing A.47: Bozorth3 matching scores on M_4 for the raw J48 classifier output

```

101 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/optimized//Scan1_r0_10.FRT-optimized.jpg.xyt
102 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/optimized//Scan2_r0_10.FRT-optimized.jpg.xyt
79 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/optimized//Scan3_r0_10.FRT-optimized.jpg.xyt
41 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/optimized//Scan4_r0_10.FRT-optimized.jpg.xyt

```

Listing A.48: Bozorth3 matching scores on M_4 for the optimized J48 classifier output

```

43 /mnt/diss/digidak/data/unimd_amsl_1/li.jpg.xyt /mnt/diss/digidak/1ka_like_testset/
    aluminium/uni-md-amsl-1.li_lm/J48/LRb//Scan2_r0_10.FRT-LRb.jpg.xyt

```

Listing A.49: Bozorth3 matching scores on M_4 for the LRb J48 classifier output

A.3.3 Feature Selection Classifier Outputs for the 2-Fold Cross Validation

The following subsections contain the results of the two-fold cross validation of the two evaluated classifiers for the reduced feature space for each of the substrates. The class label f represents a block with fingerprint residue, whereas the class label b represents a block with the substrate not covered by fingerprint residue. The particular ground truth is estimated based on the differential scan method as described in Section 5.2.

A.3.3.1 White Furniture Surface M_1

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      912835          91.0105 %
Incorrectly Classified Instances    90165           8.9895 %
Kappa statistic                     0.8202
Mean absolute error                 0.1124
Root mean squared error             0.2684
Relative absolute error             22.4749 %
Root relative squared error         53.6826 %
Total Number of Instances          1003000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.909    0.088    0.911     0.909    0.91       0.946    f
                0.912    0.091    0.909     0.912    0.91       0.946    b
Weighted Avg.   0.91     0.09     0.91     0.91     0.91       0.946
=== Confusion Matrix ===

      a      b  <-- classified as
455701  45799 | a = f
 44366  457134 | b = b

```

Listing A.50: WEKA Classifier Output for the 2-Fold Cross Validation on M_1 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      922851          92.0091 %
Incorrectly Classified Instances    80149           7.9909 %
Kappa statistic                     0.8402
Mean absolute error                 0.1148
Root mean squared error             0.2383
Relative absolute error             22.9594 %
Root relative squared error         47.6596 %
Total Number of Instances          1003000
=== Detailed Accuracy By Class ===

```

```

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.913   0.073   0.926     0.913   0.92       0.979     f
                0.927   0.087   0.915     0.927   0.921     0.979     b
Weighted Avg.  0.92     0.08     0.92      0.92    0.92      0.979
===== Confusion Matrix =====
                a      b  <-- classified as
458073  43427 |      a = f
 36722  464778 |      b = b
    
```

Listing A.51: WEKA Classifier Output for the 2-Fold Cross Validation on M_1 using Bagging

A.3.3.2 Veneered Plywood (Beech) M_2

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      739164          81.5417 %
Incorrectly Classified Instances    167322          18.4583 %
Kappa statistic                    0.6308
Mean absolute error                 0.2196
Root mean squared error             0.3759
Relative absolute error             43.9115 %
Root relative squared error         75.1759 %
Total Number of Instances          906486
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.814   0.184   0.816     0.814   0.815     0.868     f
                0.816   0.186   0.815     0.816   0.816     0.868     b
Weighted Avg.  0.815     0.185     0.815     0.815   0.815     0.868
===== Confusion Matrix =====
                a      b  <-- classified as
369162  84081 |      a = f
 83241  370002 |      b = b
    
```

Listing A.52: WEKA Classifier Output for the 2-Fold Cross Validation on M_2 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      756091          83.409 %
Incorrectly Classified Instances    150395          16.591 %
Kappa statistic                    0.6682
Mean absolute error                 0.2214
Root mean squared error             0.3334
Relative absolute error             44.2891 %
Root relative squared error         66.6863 %
Total Number of Instances          906486
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.829   0.161   0.837     0.829   0.833     0.926     f
                0.839   0.171   0.831     0.839   0.835     0.926     b
Weighted Avg.  0.834     0.166     0.834     0.834   0.834     0.926
===== Confusion Matrix =====
                a      b  <-- classified as
375963  77280 |      a = f
 73115  380128 |      b = b
    
```

Listing A.53: WEKA Classifier Output for the 2-Fold Cross Validation on M_2 using Bagging

A.3.3.3 Brushed Stainless Steel M_3

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      553079          73.3 %
Incorrectly Classified Instances    201463          26.7 %
Kappa statistic                    0.466
Mean absolute error                 0.3206
Root mean squared error             0.4431
Relative absolute error             64.1264 %
Root relative squared error         88.6221 %
Total Number of Instances          754542
===== Detailed Accuracy By Class =====
    
```

```

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.746   0.28    0.727     0.746   0.737     0.783    f
                0.72    0.254  0.739     0.72    0.729     0.783    b
Weighted Avg.  0.733   0.267   0.733     0.733   0.733     0.783
===== Confusion Matrix =====
                a      b  <-- classified as
281570  95701 |      a = f
105762 271509 |      b = b

```

Listing A.54: WEKA Classifier Output for the 2-Fold Cross Validation on M_3 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      571481                75.7388 %
Incorrectly Classified Instances    183061                24.2612 %
Kappa statistic                    0.5148
Mean absolute error                 0.3205
Root mean squared error             0.4006
Relative absolute error             64.0905 %
Root relative squared error         80.122 %
Total Number of Instances          754542
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.756   0.241   0.758     0.756   0.757     0.845    f
                0.759   0.244   0.756     0.759   0.758     0.845    b
Weighted Avg.  0.757   0.243   0.757     0.757   0.757     0.845
===== Confusion Matrix =====
                a      b  <-- classified as
285062  92209 |      a = f
 90852 286419 |      b = b

```

Listing A.55: WEKA Classifier Output for the 2-Fold Cross Validation on M_3 using Bagging

A.3.3.4 Aluminum Foil M_4

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      734611                80.173 %
Incorrectly Classified Instances    181671                19.827 %
Kappa statistic                    0.6035
Mean absolute error                 0.2454
Root mean squared error             0.3879
Relative absolute error             49.0741 %
Root relative squared error         77.5766 %
Total Number of Instances          916282
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.823   0.219   0.79     0.823   0.806     0.855    f
                0.781   0.177   0.815   0.781   0.798     0.855    b
Weighted Avg.  0.802   0.198   0.802   0.802   0.802     0.855
===== Confusion Matrix =====
                a      b  <-- classified as
376829  81312 |      a = f
100359 357782 |      b = b

```

Listing A.56: WEKA Classifier Output for the 2-Fold Cross Validation on M_4 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      752002                82.071 %
Incorrectly Classified Instances    164280                17.929 %
Kappa statistic                    0.6414
Mean absolute error                 0.2453
Root mean squared error             0.3503
Relative absolute error             49.0651 %
Root relative squared error         70.0624 %
Total Number of Instances          916282
===== Detailed Accuracy By Class =====
                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.839   0.198   0.809   0.839   0.824     0.908    f

```


Weighted Avg.	0.802	0.161	0.833	0.802	0.817	0.908	b
Confusion Matrix	0.821	0.179	0.821	0.821	0.821	0.908	
====							
	a	b	<-- classified as				
384421	73720		a = f				
90560	367581		b = b				

Listing A.57: WEKA Classifier Output for the 2-Fold Cross Validation on M_4 using Bagging

A.3.3.5 Golden-Oak Veneer M_5

2-Fold Cross-validation results for weka.classifiers.trees.J48							
Classifier: weka.classifiers.trees.J48							
Correctly Classified Instances	690266				67.7438 %		
Incorrectly Classified Instances	328670				32.2562 %		
Kappa statistic		0.3549					
Mean absolute error		0.3741					
Root mean squared error		0.4794					
Relative absolute error		74.8289 %					
Root relative squared error		95.8829 %					
Total Number of Instances	1018936						
==== Detailed Accuracy By Class ====							
	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.74	0.385	0.658	0.74	0.696	0.717	f
	0.615	0.26	0.703	0.615	0.656	0.717	b
Weighted Avg.	0.677	0.323	0.68	0.677	0.676	0.717	
==== Confusion Matrix ====							
	a	b	<-- classified as				
376762	132706		a = f				
195964	313504		b = b				

Listing A.58: WEKA Classifier Output for the 2-Fold Cross Validation on M_5 using J48

2-Fold Cross-validation results for weka.classifiers.meta.Bagging							
Classifier: weka.classifiers.meta.Bagging							
Correctly Classified Instances	718131				70.4785 %		
Incorrectly Classified Instances	300805				29.5215 %		
Kappa statistic		0.4096					
Mean absolute error		0.3767					
Root mean squared error		0.4345					
Relative absolute error		75.3383 %					
Root relative squared error		86.8968 %					
Total Number of Instances	1018936						
==== Detailed Accuracy By Class ====							
	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.768	0.358	0.682	0.768	0.722	0.779	f
	0.642	0.232	0.734	0.642	0.685	0.779	b
Weighted Avg.	0.705	0.295	0.708	0.705	0.704	0.779	
==== Confusion Matrix ====							
	a	b	<-- classified as				
391132	118336		a = f				
182469	326999		b = b				

Listing A.59: WEKA Classifier Output for the 2-Fold Cross Validation on M_5 using Bagging

A.3.3.6 Non-Metallic Matte Car Body Finish M_6

2-Fold Cross-validation results for weka.classifiers.trees.J48							
Classifier: weka.classifiers.trees.J48							
Correctly Classified Instances	729125				82.0311 %		
Incorrectly Classified Instances	159715				17.9689 %		
Kappa statistic		0.6406					
Mean absolute error		0.2228					
Root mean squared error		0.3838					
Relative absolute error		44.5505 %					
Root relative squared error		76.7624 %					
Total Number of Instances	888840						
==== Detailed Accuracy By Class ====							
	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.86	0.219	0.797	0.86	0.827	0.847	f

Weighted Avg.	0.781	0.14	0.848	0.781	0.813	0.847	b
==== Confusion Matrix ====	0.82	0.18	0.822	0.82	0.82	0.847	
	a	b	← classified as				
382161	62259		a = f				
97456	346964		b = b				

Listing A.60: WEKA Classifier Output for the 2-Fold Cross Validation on M_6 using J48

2-Fold Cross-validation results for weka.classifiers.meta.Bagging							
Classifier: weka.classifiers.meta.Bagging							
Correctly Classified Instances	749386		84.3106 %				
Incorrectly Classified Instances	139454		15.6894 %				
Kappa statistic			0.6862				
Mean absolute error			0.2258				
Root mean squared error			0.3351				
Relative absolute error			45.1528 %				
Root relative squared error			67.0126 %				
Total Number of Instances	888840						
==== Detailed Accuracy By Class ====							
	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.897	0.211	0.81	0.897	0.851	0.916	f
	0.789	0.103	0.885	0.789	0.834	0.916	b
Weighted Avg.	0.843	0.157	0.847	0.843	0.843	0.916	
==== Confusion Matrix ====							
	a	b	← classified as				
398635	45785		a = f				
93669	350751		b = b				

Listing A.61: WEKA Classifier Output for the 2-Fold Cross Validation on M_6 using Bagging

A.3.3.7 Metallic Car Body Finish M_7

2-Fold Cross-validation results for weka.classifiers.trees.J48							
Classifier: weka.classifiers.trees.J48							
Correctly Classified Instances	332827		70.6771 %				
Incorrectly Classified Instances	138085		29.3229 %				
Kappa statistic			0.4135				
Mean absolute error			0.3495				
Root mean squared error			0.4655				
Relative absolute error			69.8983 %				
Root relative squared error			93.1002 %				
Total Number of Instances	470912						
==== Detailed Accuracy By Class ====							
	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.779	0.365	0.681	0.779	0.726	0.742	f
	0.635	0.221	0.741	0.635	0.684	0.742	b
Weighted Avg.	0.707	0.293	0.711	0.707	0.705	0.742	
==== Confusion Matrix ====							
	a	b	← classified as				
183324	52132		a = f				
85953	149503		b = b				

Listing A.62: WEKA Classifier Output for the 2-Fold Cross Validation on M_7 using J48

2-Fold Cross-validation results for weka.classifiers.meta.Bagging							
Classifier: weka.classifiers.meta.Bagging							
Correctly Classified Instances	344599		73.1769 %				
Incorrectly Classified Instances	126313		26.8231 %				
Kappa statistic			0.4635				
Mean absolute error			0.3492				
Root mean squared error			0.4203				
Relative absolute error			69.8462 %				
Root relative squared error			84.0585 %				
Total Number of Instances	470912						
==== Detailed Accuracy By Class ====							
	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.794	0.33	0.706	0.794	0.747	0.807	f
	0.67	0.206	0.765	0.67	0.714	0.807	b
Weighted Avg.	0.732	0.268	0.735	0.732	0.731	0.807	
==== Confusion Matrix ====							

```

a      b  <-- classified as
186870 48586 | a = f
77727 157729 | b = b
    
```

Listing A.63: WEKA Classifier Output for the 2-Fold Cross Validation on M_7 using Bagging

A.3.3.8 Blued Metal M_8

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      745568          78.6863 %
Incorrectly Classified Instances    201952          21.3137 %
Kappa statistic                    0.5737
Mean absolute error                 0.2525
Root mean squared error             0.4116
Relative absolute error             50.4925 %
Root relative squared error         82.3118 %
Total Number of Instances          947520
=== Detailed Accuracy By Class ===

              TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
              0.824   0.25    0.767     0.824   0.795     0.821    f
              0.75    0.176  0.81      0.75    0.779     0.821    b
Weighted Avg. 0.787   0.213  0.788     0.787   0.787     0.821
=== Confusion Matrix ===

      a      b  <-- classified as
390398 83362 | a = f
118590 355170 | b = b
    
```

Listing A.64: WEKA Classifier Output for the 2-Fold Cross Validation on M_8 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      769993          81.264 %
Incorrectly Classified Instances    177527          18.736 %
Kappa statistic                    0.6253
Mean absolute error                 0.255
Root mean squared error             0.3564
Relative absolute error             50.9953 %
Root relative squared error         71.2847 %
Total Number of Instances          947520
=== Detailed Accuracy By Class ===

              TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
              0.847   0.222  0.792     0.847   0.819     0.9      f
              0.778   0.153  0.836     0.778   0.806     0.9      b
Weighted Avg. 0.813   0.187  0.814     0.813   0.812     0.9
=== Confusion Matrix ===

      a      b  <-- classified as
401387 72373 | a = f
105154 368606 | b = b
    
```

Listing A.65: WEKA Classifier Output for the 2-Fold Cross Validation on M_8 using Bagging

A.3.3.9 Ceramic Tile M_9

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      505255          72.1939 %
Incorrectly Classified Instances    194603          27.8061 %
Kappa statistic                    0.4439
Mean absolute error                 0.3374
Root mean squared error             0.4584
Relative absolute error             67.4896 %
Root relative squared error         91.6803 %
Total Number of Instances          699858
=== Detailed Accuracy By Class ===

              TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
              0.761   0.317  0.706     0.761   0.732     0.755    f
              0.683   0.239  0.741     0.683   0.711     0.755    b
Weighted Avg. 0.722   0.278  0.723     0.722   0.722     0.755
=== Confusion Matrix ===
    
```

```

      a      b  <-- classified as
266200 83729 | a = f
110874 239055 | b = b

```

Listing A.66: WEKA Classifier Output for the 2-Fold Cross Validation on M_9 using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      522627          74.6761 %
Incorrectly Classified Instances    177231          25.3239 %
Kappa statistic                     0.4935
Mean absolute error                  0.3399
Root mean squared error              0.4134
Relative absolute error              67.9853 %
Root relative squared error          82.6755 %
Total Number of Instances           699858
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.775   0.281   0.734     0.775   0.754     0.823     f
                0.719   0.225   0.761     0.719   0.739     0.823     b
Weighted Avg.   0.747   0.253   0.748     0.747   0.747     0.823
=== Confusion Matrix ===

      a      b  <-- classified as
271073 78856 | a = f
 98375 251554 | b = b

```

Listing A.67: WEKA Classifier Output for the 2-Fold Cross Validation on M_9 using Bagging

A.3.3.10 Copying Paper M_{10}

```

2-Fold Cross-validation results for weka.classifiers.trees.J48
Classifier: weka.classifiers.trees.J48

Correctly Classified Instances      306742          71.536 %
Incorrectly Classified Instances    122052          28.464 %
Kappa statistic                     0.4307
Mean absolute error                  0.3445
Root mean squared error              0.4552
Relative absolute error              68.9004 %
Root relative squared error          91.0488 %
Total Number of Instances           428794
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.735   0.304   0.707     0.735   0.721     0.761     f
                0.696   0.265   0.724     0.696   0.71     0.761     b
Weighted Avg.   0.715   0.285   0.716     0.715   0.715     0.761
=== Confusion Matrix ===

      a      b  <-- classified as
157485 56912 | a = f
 65140 149257 | b = b

```

Listing A.68: WEKA Classifier Output for the 2-Fold Cross Validation on M_{10} using J48

```

2-Fold Cross-validation results for weka.classifiers.meta.Bagging
Classifier: weka.classifiers.meta.Bagging

Correctly Classified Instances      315813          73.6515 %
Incorrectly Classified Instances    112981          26.3485 %
Kappa statistic                     0.473
Mean absolute error                  0.3421
Root mean squared error              0.4167
Relative absolute error              68.4124 %
Root relative squared error          83.3302 %
Total Number of Instances           428794
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.754   0.281   0.729     0.754   0.741     0.819     f
                0.719   0.246   0.745     0.719   0.732     0.819     b
Weighted Avg.   0.737   0.263   0.737     0.737   0.736     0.819
=== Confusion Matrix ===

      a      b  <-- classified as
161649 52748 | a = f

```

60233 154164 | b = b

Listing A.69: WEKA Classifier Output for the 2-Fold Cross Validation on M_{10} using Bagging

A.4 Evaluation of the Detection of Printed Latent Fingerprint Forgeries

The following subsections contain the results of the ten-fold cross validation of the evaluations performed in Chapter 6. The class label 0 represents latent fingerprint forgery created by an ink-jet printer equipped with artificial sweat, whereas the class label 1 represents a scan of a genuine real latent fingerprint. The particular ground truth is assigned based on the experimental setup.

A.4.1 Evaluation of the Detection using Dot Based Features using LMT

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1995          99.75 %
Incorrectly Classified Instances    5             0.25 %
Kappa statistic                    0.995
Mean absolute error                 0.0042
Root mean squared error             0.0444
Relative absolute error             0.8446 %
Root relative squared error         8.8728 %
Total Number of Instances          2000
===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.999	0.004	0.996	0.999	0.998	1	1
	0.996	0.001	0.999	0.996	0.997	1	0
Weighted Avg.	0.998	0.003	0.998	0.998	0.997	1	

```

===== Confusion Matrix =====

 a  b  <-- classified as
999  1 | a = 1
 4 996 | b = 0

```

Listing A.70: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{1P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1996          99.8 %
Incorrectly Classified Instances    4             0.2 %
Kappa statistic                    0.996
Mean absolute error                 0.004
Root mean squared error             0.0401
Relative absolute error             0.7963 %
Root relative squared error         8.0159 %
Total Number of Instances          2000
===== Detailed Accuracy By Class =====

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.997	0.001	0.999	0.997	0.998	1	1
	0.999	0.003	0.997	0.999	0.998	1	0
Weighted Avg.	0.998	0.002	0.998	0.998	0.998	1	

```

===== Confusion Matrix =====

 a  b  <-- classified as
997  3 | a = 1
 1 999 | b = 0

```

Listing A.71: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{2P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1985          99.25 %
Incorrectly Classified Instances     15           0.75 %
Kappa statistic                     0.985
Mean absolute error                  0.0139
Root mean squared error              0.0796
Relative absolute error              2.7737 %
Root relative squared error          15.917 %
Total Number of Instances           2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.993    0.008    0.992     0.993    0.993     0.999     1
                 0.992    0.007    0.993     0.992    0.992     0.999     0
=== Confusion Matrix ===

  a  b  <-- classified as
993  7  |  a = 1
 8 992 |  b = 0

```

Listing A.72: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{3P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      5934          98.9 %
Incorrectly Classified Instances     66           1.1 %
Kappa statistic                     0.978
Mean absolute error                  0.0138
Root mean squared error              0.0936
Relative absolute error              2.7689 %
Root relative squared error          18.7171 %
Total Number of Instances           6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.987    0.009    0.991     0.987    0.989     0.997     1
                 0.991    0.013    0.987     0.991    0.989     0.997     0
                 0.989    0.011    0.989     0.989    0.989     0.997
=== Confusion Matrix ===

  a  b  <-- classified as
2960 40 |  a = 1
 26 2974 |  b = 0

```

Listing A.73: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.2 Evaluation of the Detection using Crystalline Structure Based Features using LMT

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1977          98.85 %
Incorrectly Classified Instances     23           1.15 %
Kappa statistic                     0.977
Mean absolute error                  0.0181
Root mean squared error              0.1044
Relative absolute error              3.6172 %
Root relative squared error          20.8789 %
Total Number of Instances           2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.995    0.018    0.982     0.995    0.989     0.993     1
                 0.982    0.005    0.995     0.982    0.988     0.993     0
                 0.989    0.012    0.989     0.989    0.988     0.993
=== Confusion Matrix ===

  a  b  <-- classified as
995  5  |  a = 1
18 982 |  b = 0

```

Listing A.74: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{1P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1992          99.6 %
Incorrectly Classified Instances    8             0.4 %
Kappa statistic                    0.992
Mean absolute error                 0.0119
Root mean squared error             0.0679
Relative absolute error             2.3862 %
Root relative squared error         13.5874 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.998   0.006   0.994     0.998   0.996     1         1
                0.994   0.002   0.998     0.994   0.996     1         0
Weighted Avg.   0.996   0.004   0.996     0.996   0.996     1
=== Confusion Matrix ===

  a  b  <-- classified as
998  2 |  a = 1
  6 994 |  b = 0

```

Listing A.75: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1950          97.5 %
Incorrectly Classified Instances    50            2.5 %
Kappa statistic                    0.95
Mean absolute error                 0.0393
Root mean squared error             0.1411
Relative absolute error             7.8513 %
Root relative squared error         28.2216 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.972   0.022   0.978     0.972   0.975     0.993     1
                0.978   0.028   0.972     0.978   0.975     0.994     0
Weighted Avg.   0.975   0.025   0.975     0.975   0.975     0.993
=== Confusion Matrix ===

  a  b  <-- classified as
972 28 |  a = 1
 22 978 | b = 0

```

Listing A.76: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      5833          97.2167 %
Incorrectly Classified Instances    167           2.7833 %
Kappa statistic                    0.9443
Mean absolute error                 0.0435
Root mean squared error             0.1487
Relative absolute error             8.7027 %
Root relative squared error         29.738 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.968   0.024   0.976     0.968   0.972     0.995     1
                0.976   0.032   0.968     0.976   0.972     0.995     0
Weighted Avg.   0.972   0.028   0.972     0.972   0.972     0.995
=== Confusion Matrix ===

  a  b  <-- classified as
2904 96 |  a = 1
  71 2929 | b = 0

```

Listing A.77: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.3 Evaluation of the Detection using Benford's Law Based Features using LMT

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1998          99.9 %
Incorrectly Classified Instances    2             0.1 %
Kappa statistic                    0.998
Mean absolute error                 0.0028
Root mean squared error            0.028
Relative absolute error             0.5541 %
Root relative squared error        5.5957 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.999   0.001   0.999     0.999   0.999     1         1
                0.999   0.001   0.999     0.999   0.999     1         0
Weighted Avg.   0.999   0.001   0.999     0.999   0.999     1
=== Confusion Matrix ===

  a  b  <-- classified as
999  1 | a = 1
  1 999 | b = 0

```

Listing A.78: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{1P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1991          99.55 %
Incorrectly Classified Instances    9             0.45 %
Kappa statistic                    0.991
Mean absolute error                 0.0054
Root mean squared error            0.0642
Relative absolute error             1.0827 %
Root relative squared error        12.8373 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.994   0.003   0.997     0.994   0.995     0.998     1
                0.997   0.006   0.994     0.997   0.996     0.999     0
Weighted Avg.   0.996   0.005   0.996     0.996   0.995     0.999
=== Confusion Matrix ===

  a  b  <-- classified as
994  6 | a = 1
  3 997 | b = 0

```

Listing A.79: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      1988          99.4 %
Incorrectly Classified Instances    12            0.6 %
Kappa statistic                    0.988
Mean absolute error                 0.0098
Root mean squared error            0.07
Relative absolute error             1.9698 %
Root relative squared error        14.0053 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.994   0.006   0.994     0.994   0.994     0.999     1
                0.994   0.006   0.994     0.994   0.994     0.999     0
Weighted Avg.   0.994   0.006   0.994     0.994   0.994     0.999
=== Confusion Matrix ===

  a  b  <-- classified as
994  6 | a = 1
  6 994 | b = 0

```

Listing A.80: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint


```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      5911          98.5167 %
Incorrectly Classified Instances    89            1.4833 %
Kappa statistic                    0.9703
Mean absolute error                0.0164
Root mean squared error            0.1133
Relative absolute error            3.2789 %
Root relative squared error        22.6507 %
Total Number of Instances         6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.984   0.013   0.987     0.984   0.985     0.994     1
                0.987   0.016   0.984     0.987   0.985     0.994     0
Weighted Avg.   0.985   0.015   0.985     0.985   0.985     0.994
=== Confusion Matrix ===

  a  b  <-- classified as
2951 49 |  a = 1
 40 2960 |  b = 0
    
```

Listing A.81: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using LMT, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.4 Evaluation of the Detection using Dot Based Features using MultilayerPerceptron

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1990          99.5 %
Incorrectly Classified Instances    10            0.5 %
Kappa statistic                    0.99
Mean absolute error                0.0065
Root mean squared error            0.0698
Relative absolute error            1.2954 %
Root relative squared error        13.9681 %
Total Number of Instances         2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.995   0.005   0.995     0.995   0.995     1         1
                0.995   0.005   0.995     0.995   0.995     1         0
Weighted Avg.   0.995   0.005   0.995     0.995   0.995     1
=== Confusion Matrix ===

  a  b  <-- classified as
995  5 |  a = 1
 5 995 |  b = 0
    
```

Listing A.82: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{1P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1996          99.8 %
Incorrectly Classified Instances    4             0.2 %
Kappa statistic                    0.996
Mean absolute error                0.0024
Root mean squared error            0.0376
Relative absolute error            0.4743 %
Root relative squared error        7.5222 %
Total Number of Instances         2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.998   0.002   0.998     0.998   0.998     1         1
                0.998   0.002   0.998     0.998   0.998     1         0
Weighted Avg.   0.998   0.002   0.998     0.998   0.998     1
=== Confusion Matrix ===

  a  b  <-- classified as
998  2 |  a = 1
 2 998 |  b = 0
    
```

Listing A.83: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{2P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1980          99 %
Incorrectly Classified Instances    20            1 %
Kappa statistic                     0.98
Mean absolute error                 0.0097
Root mean squared error             0.0921
Relative absolute error             1.9315 %
Root relative squared error         18.4107 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.988    0.008    0.992     0.988   0.99       1         1
                 0.992    0.012    0.988     0.992   0.99       1         0
Weighted Avg.   0.99     0.01     0.99      0.99    0.99       1

=== Confusion Matrix ===

  a  b  <-- classified as
988 12 | a = 1
 8 992 | b = 0

```

Listing A.84: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_3P using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      5966          99.4333 %
Incorrectly Classified Instances    34            0.5667 %
Kappa statistic                     0.9887
Mean absolute error                 0.0066
Root mean squared error             0.0706
Relative absolute error             1.3111 %
Root relative squared error         14.1221 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.994    0.005    0.995     0.994   0.994     1         1
                 0.995    0.006    0.994     0.995   0.994     1         0
Weighted Avg.   0.994    0.006    0.994     0.994   0.994     1

=== Confusion Matrix ===

  a  b  <-- classified as
2981 19 | a = 1
 15 2985 | b = 0

```

Listing A.85: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.5 Evaluation of the Detection using Crystalline Structure Based Features using MultilayerPerceptron

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1975          98.75 %
Incorrectly Classified Instances    25            1.25 %
Kappa statistic                     0.975
Mean absolute error                 0.0172
Root mean squared error             0.1018
Relative absolute error             3.4318 %
Root relative squared error         20.3539 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.993    0.018    0.982     0.993   0.988     0.994     1
                 0.982    0.007    0.993     0.982   0.987     0.994     0
Weighted Avg.   0.988    0.013    0.988     0.988   0.987     0.994

=== Confusion Matrix ===

  a  b  <-- classified as
993  7 | a = 1
18 982 | b = 0

```

Listing A.86: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_1P using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1987          99.35 %
Incorrectly Classified Instances    13            0.65 %
Kappa statistic                    0.987
Mean absolute error                0.0098
Root mean squared error            0.0735
Relative absolute error            1.9595 %
Root relative squared error        14.6986 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.997   0.01    0.99       0.99   0.994     0.999     1
                0.99   0.003   0.997     0.99   0.993     0.999     0
Weighted Avg.   0.994   0.007   0.994     0.994  0.993     0.999

=== Confusion Matrix ===

  a  b  <-- classified as
997  3  |  a = 1
10 990 |  b = 0

```

Listing A.87: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1952          97.6 %
Incorrectly Classified Instances    48            2.4 %
Kappa statistic                    0.952
Mean absolute error                0.0337
Root mean squared error            0.1369
Relative absolute error            6.7336 %
Root relative squared error        27.3768 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.971   0.019   0.981     0.971  0.976     0.992     1
                0.981   0.029   0.971     0.981  0.976     0.992     0
Weighted Avg.   0.976   0.024   0.976     0.976  0.976     0.992

=== Confusion Matrix ===

  a  b  <-- classified as
971  29 |  a = 1
19 981 |  b = 0

```

Listing A.88: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      5795          96.5833 %
Incorrectly Classified Instances    205           3.4167 %
Kappa statistic                    0.9317
Mean absolute error                0.0449
Root mean squared error            0.1588
Relative absolute error            8.9864 %
Root relative squared error        31.7606 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.961   0.03    0.97       0.961  0.966     0.993     1
                0.97   0.039   0.962     0.97   0.966     0.993     0
Weighted Avg.   0.966   0.034   0.966     0.966  0.966     0.993

=== Confusion Matrix ===

  a  b  <-- classified as
2884 116 |  a = 1
89 2911 |  b = 0

```

Listing A.89: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.6 Evaluation of the Detection using Benford's Law Based Features using MultilayerPerceptron

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1997          99.85 %
Incorrectly Classified Instances    3             0.15 %
Kappa statistic                    0.997
Mean absolute error                0.0018
Root mean squared error            0.0333
Relative absolute error            0.3628 %
Root relative squared error        6.6698 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.999   0.002   0.998     0.999   0.999     1         1
                0.998   0.001   0.999     0.998   0.998     1         0
Weighted Avg.   0.999   0.002   0.999     0.999   0.998     1
=== Confusion Matrix ===

  a  b  <-- classified as
999  1 | a = 1
  2 998 | b = 0

```

Listing A.90: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{1P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1991          99.55 %
Incorrectly Classified Instances    9             0.45 %
Kappa statistic                    0.991
Mean absolute error                0.0049
Root mean squared error            0.0571
Relative absolute error            0.9745 %
Root relative squared error        11.4156 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.994   0.003   0.997     0.994   0.995     1         1
                0.997   0.006   0.994     0.997   0.996     1         0
Weighted Avg.   0.996   0.005   0.996     0.996   0.995     1
=== Confusion Matrix ===

  a  b  <-- classified as
994  6 | a = 1
  3 997 | b = 0

```

Listing A.91: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      1998          99.9 %
Incorrectly Classified Instances    2             0.1 %
Kappa statistic                    0.998
Mean absolute error                0.0029
Root mean squared error            0.0334
Relative absolute error            0.5876 %
Root relative squared error        6.6727 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                1       0.002   0.998     1       0.999     0.999     1
                0.998   0       1       0.998   0.999     0.999     0
Weighted Avg.   0.999   0.001   0.999     0.999   0.999     0.999
=== Confusion Matrix ===

  a  b  <-- classified as
1000  0 | a = 1
  2 998 | b = 0

```

Listing A.92: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      5893          98.2167 %
Incorrectly Classified Instances    107           1.7833 %
Kappa statistic                    0.9643
Mean absolute error                 0.0236
Root mean squared error             0.1211
Relative absolute error             4.7162 %
Root relative squared error         24.2249 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.983   0.018   0.982     0.983   0.982     0.995     1
                0.982   0.017   0.983     0.982   0.982     0.995     0
Weighted Avg.   0.982   0.018   0.982     0.982   0.982     0.995

=== Confusion Matrix ===

  a    b  <-- classified as
2948  52 |   a = 1
 55 2945 |   b = 0
    
```

Listing A.93: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using MultilayerPerceptron, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.7 Evaluation of the Detection using Dot Based Features using Dagging

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1993          99.65 %
Incorrectly Classified Instances     7            0.35 %
Kappa statistic                    0.993
Mean absolute error                 0.0059
Root mean squared error             0.0643
Relative absolute error             1.19 %
Root relative squared error         12.8608 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                1       0.007   0.993     1       0.997     0.996     1
                0.993   0       1         0.993   0.996     0.996     0
Weighted Avg.   0.997   0.004   0.997     0.997   0.996     0.996

=== Confusion Matrix ===

  a    b  <-- classified as
1000  0 |   a = 1
 7 993 |   b = 0
    
```

Listing A.94: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{1P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1987          99.35 %
Incorrectly Classified Instances    13           0.65 %
Kappa statistic                    0.987
Mean absolute error                 0.0111
Root mean squared error             0.0724
Relative absolute error             2.21 %
Root relative squared error         14.4845 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.988   0.001   0.999     0.988   0.993     0.999     1
                0.999   0.012   0.988     0.999   0.994     0.999     0
Weighted Avg.   0.994   0.007   0.994     0.994   0.993     0.999

=== Confusion Matrix ===

  a    b  <-- classified as
988  12 |   a = 1
 1 999 |   b = 0
    
```

Listing A.95: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{2P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1993      99.65 %
Incorrectly Classified Instances    7         0.35 %
Kappa statistic                    0.993
Mean absolute error                 0.012
Root mean squared error             0.0635
Relative absolute error             2.4 %
Root relative squared error         12.6965 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.  0.998    0.005    0.995     0.998   0.997     0.999     1
                0.995    0.002    0.998     0.995   0.996     0.999     0

=== Confusion Matrix ===

  a  b  <-- classified as
998  2  |  a = 1
 5 995 |  b = 0

```

Listing A.96: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_3P using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      5886      98.1 %
Incorrectly Classified Instances    114       1.9 %
Kappa statistic                    0.962
Mean absolute error                 0.0225
Root mean squared error             0.1261
Relative absolute error             4.4933 %
Root relative squared error         25.2138 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.  0.979    0.017    0.983     0.979   0.981     0.992     1
                0.983    0.021    0.979     0.983   0.981     0.992     0

=== Confusion Matrix ===

  a  b  <-- classified as
2938 62 |  a = 1
 52 2948 | b = 0

```

Listing A.97: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.8 Evaluation of the Detection using Crystalline Structure Based Features using Dagging

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1900      95 %
Incorrectly Classified Instances    100       5 %
Kappa statistic                    0.9
Mean absolute error                 0.0526
Root mean squared error             0.2164
Relative absolute error             10.52 %
Root relative squared error         43.2759 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.  0.911    0.011    0.988     0.911   0.948     0.963     1
                0.989    0.089    0.917     0.989   0.952     0.963     0

=== Confusion Matrix ===

  a  b  <-- classified as
911  89 |  a = 1
 11 989 |  b = 0

```

Listing A.98: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_1P using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1941          97.05 %
Incorrectly Classified Instances    59            2.95 %
Kappa statistic                    0.941
Mean absolute error                0.032
Root mean squared error            0.1589
Relative absolute error            6.39 %
Root relative squared error        31.7774 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.969   0.028   0.972     0.969   0.97       0.983     1
                0.972   0.031   0.969     0.972   0.971     0.983     0
Weighted Avg.   0.971   0.03    0.971     0.971   0.97       0.983

=== Confusion Matrix ===

  a  b  <-- classified as
969 31 |  a = 1
 28 972 |  b = 0

```

Listing A.99: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1582          79.1 %
Incorrectly Classified Instances    418           20.9 %
Kappa statistic                    0.582
Mean absolute error                0.2313
Root mean squared error            0.3996
Relative absolute error            46.26 %
Root relative squared error        79.915 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.624   0.042   0.937     0.624   0.749     0.894     1
                0.958   0.376   0.718     0.958   0.821     0.894     0
Weighted Avg.   0.791   0.209   0.828     0.791   0.785     0.894

=== Confusion Matrix ===

  a  b  <-- classified as
624 376 |  a = 1
 42 958 |  b = 0

```

Listing A.100: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      4503          75.05 %
Incorrectly Classified Instances    1497          24.95 %
Kappa statistic                    0.501
Mean absolute error                0.2467
Root mean squared error            0.461
Relative absolute error            49.3333 %
Root relative squared error        92.2012 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.614   0.113   0.844     0.614   0.711     0.839     1
                0.887   0.386   0.697     0.887   0.78      0.839     0
Weighted Avg.   0.751   0.25    0.771     0.751   0.746     0.839

=== Confusion Matrix ===

  a  b  <-- classified as
1843 1157 |  a = 1
 340 2660 |  b = 0

```

Listing A.101: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.9 Evaluation of the Detection using Benford's Law Based Features using Dagging

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1985          99.25 %
Incorrectly Classified Instances    15            0.75 %
Kappa statistic                    0.985
Mean absolute error                 0.0077
Root mean squared error             0.0743
Relative absolute error             1.55 %
Root relative squared error         14.8661 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.989   0.004   0.996     0.989   0.992     0.996     1
                0.996   0.011   0.989     0.996   0.993     0.996     0
Weighted Avg.   0.993   0.008   0.993     0.993   0.992     0.996

=== Confusion Matrix ===

  a  b  <-- classified as
989 11 | a = 1
 4 996 | b = 0

```

Listing A.102: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{1P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1895          94.75 %
Incorrectly Classified Instances    105           5.25 %
Kappa statistic                    0.895
Mean absolute error                 0.0515
Root mean squared error             0.2122
Relative absolute error             10.29 %
Root relative squared error         42.4429 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.898   0.003   0.997     0.898   0.945     0.972     1
                0.997   0.102   0.907     0.997   0.95      0.972     0
Weighted Avg.   0.948   0.053   0.952     0.948   0.947     0.972

=== Confusion Matrix ===

  a  b  <-- classified as
898 102 | a = 1
 3 997 | b = 0

```

Listing A.103: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      1852          92.6 %
Incorrectly Classified Instances    148           7.4 %
Kappa statistic                    0.852
Mean absolute error                 0.0847
Root mean squared error             0.2483
Relative absolute error             16.95 %
Root relative squared error         49.6568 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.87    0.018   0.98      0.87    0.922     0.968     1
                0.982   0.13    0.883    0.982   0.93      0.968     0
Weighted Avg.   0.926   0.074   0.931    0.926   0.926     0.968

=== Confusion Matrix ===

  a  b  <-- classified as
870 130 | a = 1
18 982 | b = 0

```

Listing A.104: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint


```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      5223      87.05 %
Incorrectly Classified Instances    777       12.95 %
Kappa statistic                    0.741
Mean absolute error                 0.13
Root mean squared error             0.3264
Relative absolute error             26 %
Root relative squared error         65.2728 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.779   0.038   0.954     0.779   0.857     0.936     1
                0.962   0.221   0.813     0.962   0.881     0.936     0
Weighted Avg.   0.871   0.13    0.883     0.871   0.869     0.936

=== Confusion Matrix ===

  a    b  <-- classified as
2336  664 |    a = 1
 113 2887 |    b = 0
    
```

Listing A.105: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using Dagging, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.10 Evaluation of the Detection using Dot Based Features using RotationForest

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1993      99.65 %
Incorrectly Classified Instances     7         0.35 %
Kappa statistic                    0.993
Mean absolute error                 0.0092
Root mean squared error             0.0552
Relative absolute error             1.8341 %
Root relative squared error         11.0393 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.999   0.006   0.994     0.999   0.997     0.999     1
                0.994   0.001   0.999     0.994   0.996     0.999     0
Weighted Avg.   0.997   0.004   0.997     0.997   0.996     0.999

=== Confusion Matrix ===

  a    b  <-- classified as
 999   1 |    a = 1
   6 994 |    b = 0
    
```

Listing A.106: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{1P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1995      99.75 %
Incorrectly Classified Instances     5         0.25 %
Kappa statistic                    0.995
Mean absolute error                 0.0098
Root mean squared error             0.0499
Relative absolute error             1.9559 %
Root relative squared error         9.9751 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.998   0.003   0.997     0.998   0.998     1         1
                0.997   0.002   0.998     0.997   0.997     1         0
Weighted Avg.   0.998   0.003   0.998     0.998   0.997     1

=== Confusion Matrix ===

  a    b  <-- classified as
 998   2 |    a = 1
   3 997 |    b = 0
    
```

Listing A.107: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{2P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1985          99.25 %
Incorrectly Classified Instances     15           0.75 %
Kappa statistic                     0.985
Mean absolute error                 0.0243
Root mean squared error             0.0812
Relative absolute error              4.8556 %
Root relative squared error         16.2339 %
Total Number of Instances           2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.997   0.012   0.988     0.997   0.993     0.999     1
                0.988   0.003   0.997     0.988   0.992     0.999     0

=== Confusion Matrix ===

  a  b  <-- classified as
997  3  |  a = 1
12 988 |  b = 0

```

Listing A.108: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on M_{3P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      5965          99.4167 %
Incorrectly Classified Instances     35           0.5833 %
Kappa statistic                     0.9883
Mean absolute error                 0.0242
Root mean squared error             0.0804
Relative absolute error              4.8379 %
Root relative squared error         16.0876 %
Total Number of Instances           6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.996   0.008   0.992     0.996   0.994     1         1
                0.992   0.004   0.996     0.992   0.994     1         0

=== Confusion Matrix ===

  a  b  <-- classified as
2988 12 |  a = 1
23 2977 |  b = 0

```

Listing A.109: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.11 Evaluation of the Detection using Crystalline Structure Based Features using RotationForest

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1979          98.95 %
Incorrectly Classified Instances     21           1.05 %
Kappa statistic                     0.979
Mean absolute error                 0.0217
Root mean squared error             0.099
Relative absolute error              4.3401 %
Root relative squared error         19.7902 %
Total Number of Instances           2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.996   0.017   0.983     0.996   0.99     0.996     1
                0.983   0.004   0.996     0.983   0.989     0.996     0

=== Confusion Matrix ===

  a  b  <-- classified as
996  4  |  a = 1
17 983 |  b = 0

```

Listing A.110: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{1P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1986          99.3 %
Incorrectly Classified Instances    14            0.7 %
Kappa statistic                    0.986
Mean absolute error                0.0249
Root mean squared error            0.0884
Relative absolute error            4.9833 %
Root relative squared error        17.6862 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.996   0.01    0.99       0.99   0.993     0.999    1
                0.99   0.004   0.996     0.99   0.993     0.999    0
Weighted Avg.   0.993   0.007   0.993     0.993  0.993     0.999

=== Confusion Matrix ===

  a  b  <-- classified as
996  4  |  a = 1
10 990 |  b = 0

```

Listing A.111: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1954          97.7 %
Incorrectly Classified Instances    46            2.3 %
Kappa statistic                    0.954
Mean absolute error                0.0557
Root mean squared error            0.1401
Relative absolute error            11.148 %
Root relative squared error        28.0253 %
Total Number of Instances          2000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.969   0.015   0.985     0.969  0.977     0.997    1
                0.985   0.031   0.969     0.985  0.977     0.997    0
Weighted Avg.   0.977   0.023   0.977     0.977  0.977     0.997

=== Confusion Matrix ===

  a  b  <-- classified as
969  31 |  a = 1
15 985 |  b = 0

```

Listing A.112: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      5835          97.25 %
Incorrectly Classified Instances    165           2.75 %
Kappa statistic                    0.945
Mean absolute error                0.0626
Root mean squared error            0.153
Relative absolute error            12.515 %
Root relative squared error        30.5979 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.97   0.025   0.975     0.97   0.972     0.995    1
                0.975   0.03    0.97      0.975  0.973     0.995    0
Weighted Avg.   0.973   0.028   0.973     0.973  0.972     0.995

=== Confusion Matrix ===

  a  b  <-- classified as
2910  90 |  a = 1
75 2925 |  b = 0

```

Listing A.113: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.12 Evaluation of the Detection using Benford's Law Based Features using RotationForest

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1996          99.8 %
Incorrectly Classified Instances    4             0.2 %
Kappa statistic                    0.996
Mean absolute error                0.0055
Root mean squared error            0.0389
Relative absolute error            1.105 %
Root relative squared error        7.7748 %
Total Number of Instances          2000
===== Detailed Accuracy By Class =====

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.999   0.003   0.997     0.999   0.999     0.998     1
                0.997   0.001   0.999     0.997   0.998     0.998     1
Weighted Avg.   0.998   0.002   0.998     0.998   0.998     0.998     1
===== Confusion Matrix =====

  a   b  <-- classified as
999  1 | a = 1
  3 997 | b = 0

```

Listing A.114: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{1P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1994          99.7 %
Incorrectly Classified Instances    6             0.3 %
Kappa statistic                    0.994
Mean absolute error                0.0098
Root mean squared error            0.0528
Relative absolute error            1.9576 %
Root relative squared error        10.5511 %
Total Number of Instances          2000
===== Detailed Accuracy By Class =====

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.998   0.004   0.996     0.998   0.997     0.997     1
                0.996   0.002   0.998     0.996   0.996     0.997     1
Weighted Avg.   0.997   0.003   0.997     0.997   0.997     0.997     1
===== Confusion Matrix =====

  a   b  <-- classified as
998  2 | a = 1
  4 996 | b = 0

```

Listing A.115: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{2P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      1992          99.6 %
Incorrectly Classified Instances    8             0.4 %
Kappa statistic                    0.992
Mean absolute error                0.0142
Root mean squared error            0.0579
Relative absolute error            2.8403 %
Root relative squared error        11.5855 %
Total Number of Instances          2000
===== Detailed Accuracy By Class =====

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.998   0.006   0.994     0.998   0.996     0.996     1
                0.994   0.002   0.998     0.994   0.996     0.996     1
Weighted Avg.   0.996   0.004   0.996     0.996   0.996     0.996     1
===== Confusion Matrix =====

  a   b  <-- classified as
998  2 | a = 1
  6 994 | b = 0

```

Listing A.116: WEKA Classifier Output for the 10-Fold Cross Validation of Crystalline Structure Based Features on M_{3P} using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      5943          99.05 %
Incorrectly Classified Instances    57            0.95 %
Kappa statistic                    0.981
Mean absolute error                 0.0262
Root mean squared error            0.094
Relative absolute error             5.2313 %
Root relative squared error        18.8001 %
Total Number of Instances         6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.991   0.01    0.99       0.99   0.991     0.999    1
                0.99   0.009  0.991     0.99   0.99      0.999    0
Weighted Avg.   0.991   0.01    0.991     0.99   0.99      0.999

=== Confusion Matrix ===

  a    b  <-- classified as
2973  27 |   a = 1
  30 2970 |   b = 0
    
```

Listing A.117: WEKA Classifier Output for the 10-Fold Cross Validation of Dot Based Features on all substrate materials combined using RotationForest, class label 0 indicates a printed fingerprint, class label 1 indicates a real fingerprint

A.4.13 Evaluation of the Detection using the Combined Feature Space

```

10-fold cross-validation results for weka.classifiers.trees.LMT
Classifier: weka.classifiers.trees.LMT

Correctly Classified Instances      5979          99.65 %
Incorrectly Classified Instances    21            0.35 %
Kappa statistic                    0.993
Mean absolute error                 0.005
Root mean squared error            0.0518
Relative absolute error             1.0031 %
Root relative squared error        10.3566 %
Total Number of Instances         6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.997   0.004  0.996     0.997  0.997     1         real
                0.996   0.003  0.997     0.996  0.996     1         printed
Weighted Avg.   0.997   0.004  0.997     0.997  0.996     1

=== Confusion Matrix ===

  a    b  <-- classified as
2991   9 |   a = real
  12 2988 |   b = printed
    
```

Listing A.118: WEKA Classifier Output for the 10-Fold Cross Validation of the Concatenated Feature Space on all substrate materials combined using LMT

```

10-fold cross-validation results for weka.classifiers.functions.MultilayerPerceptron
Classifier: weka.classifiers.functions.MultilayerPerceptron

Correctly Classified Instances      5989          99.8167 %
Incorrectly Classified Instances    11            0.1833 %
Kappa statistic                    0.9963
Mean absolute error                 0.002
Root mean squared error            0.0396
Relative absolute error             0.4074 %
Root relative squared error        7.9293 %
Total Number of Instances         6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
                0.999   0.002  0.998     0.999  0.998     1         real
                0.998   0.001  0.999     0.998  0.998     1         printed
Weighted Avg.   0.998   0.002  0.998     0.998  0.998     1

=== Confusion Matrix ===

  a    b  <-- classified as
2996   4 |   a = real
  7 2993 |   b = printed
    
```

Listing A.119: WEKA Classifier Output for the 10-Fold Cross Validation of the Concatenated Feature Space on all substrate materials combined using MultilayerPerceptron

```

10-fold cross-validation results for weka.classifiers.meta.Dagging
Classifier: weka.classifiers.meta.Dagging

Correctly Classified Instances      5969          99.4833 %
Incorrectly Classified Instances    31            0.5167 %
Kappa statistic                    0.9897
Mean absolute error                 0.0062
Root mean squared error             0.0648
Relative absolute error             1.2367 %
Root relative squared error         12.9589 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.999    0.009    0.991     0.999   0.995     0.998    real
                0.991    0.001    0.999     0.991   0.995     0.998    printed
=== Confusion Matrix ===

  a    b  <-- classified as
2997  3  |  a = real
 28 2972 |  b = printed

```

Listing A.120: WEKA Classifier Output for the 10-Fold Cross Validation of the Concatenated Feature Space on all substrate materials combined using Dagging

```

10-fold cross-validation results for weka.classifiers.meta.RotationForest
Classifier: weka.classifiers.meta.RotationForest

Correctly Classified Instances      5989          99.8167 %
Incorrectly Classified Instances    11            0.1833 %
Kappa statistic                    0.9963
Mean absolute error                 0.0091
Root mean squared error             0.047
Relative absolute error             1.8171 %
Root relative squared error         9.4072 %
Total Number of Instances          6000
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
Weighted Avg.   0.999    0.003    0.997     0.999   0.998     1         real
                0.997    0.001    0.999     0.997   0.998     1         printed
=== Confusion Matrix ===

  a    b  <-- classified as
2998  2  |  a = real
 9 2991 |  b = printed

```

Listing A.121: WEKA Classifier Output for the 10-Fold Cross Validation of the Concatenated Feature Space on all substrate materials combined using RotationForest

Bibliography

- [FRE14] Bob Goodlatte et al., ed. *Federal Rules of Evidence*. 2014. URL: <https://www.uscourts.gov/sites/default/files/Rules%20of%20Evidence>. (cit. on pp. 5, 32, 61).
- [ADV15] Christian Arndt., Jana Dittmann., and Claus Vielhauer. “Spectral Fiber Feature Space Evaluation for Crime Scene Forensics - Traditional Feature Classification vs. BioHash Optimization”. In: *Proceedings of the 10th International Conference on Computer Vision Theory and Applications - Volume 2: VISAPP, (VISIGRAPP 2015)*. INSTICC. SciTePress, 2015, pp. 293–302. ISBN: 978-989-758-089-5. DOI: 10.5220/0005270402930302 (cit. on p. 167).
- [Ash99] David R. Ashbaugh. *Ridgeology: Modern Evaluative Friction Ridge Identification*. Forensic Identification Support Section, Royal Canadian Mounted Police. 1999. URL: <http://onin.com/fp/ridgeology.pdf> (cit. on pp. 45, 46).
- [Bar19] Elaine Barker. *Recommendation for Key Management: Part 1 – General*. NIST Special Publication 800-57 r5. 2019. URL: <https://doi.org/10.6028/NIST.SP.800-57pt1r5-draft> (cit. on p. 77).
- [Bau88] E. B. Baum. “On the capabilities of multilayer perceptrons”. In: *Journal of Complexity* 4.3 (1988), pp. 193–215. ISSN: 0885-064X. DOI: [http://dx.doi.org/10.1016/0885-064X\(88\)90020-9](http://dx.doi.org/10.1016/0885-064X(88)90020-9). URL: <http://www.sciencedirect.com/science/article/pii/0885064X88900209> (cit. on pp. xxii, 43, 44, 152–159, 172, 173, 175, 178, 179).
- [BC04] Nicole Lang Beebe and Jan Guynes Clark. “A Hierarchical, Objectives-Based Framework for the Digital Investigations Process”. In: *Proceedings of The Digital Forensic Research Conference*. Baltimore, MD: DFRWS, 2004, pp. 1–17. URL: https://dfrws.org/sites/default/files/session-files/paper-a_hierarchical_objectives-based_framework_for_the_digital_investigations_process.pdf (cit. on pp. 27, 54, 55, 68, 173, 175).
- [Ben38] Frank Benford. “The Law of Anomalous Numbers”. In: *Proceedings of the American Philosophical Society* 78.4 (1938), pp. 551–572 (cit. on pp. 41, 45, 149).
- [Bhu01] Bharat Bhushan. “Modern Tribology Handbook”. In: ed. by Bharat Bhushan. Vol. One. CRC Press, 2001. Chap. Surface Roughness Analysis and Measurement Techniques, pp. 49–119. ISBN: 0-8493-8403-6 (cit. on pp. 38, 100).

- [Ble+17] Stephen Bleay, Vaughn Sears, Rory Downham, Helen Bandey, Andrew Gibson, Valerie Bowman, Lesley Fitzgerald, Tomasz Ciuksza, Jona Ramadani, and Chris Selway. *Fingerprint Source Book v2.0*. second edition. CAST Publication 081/17. Home Office Centre for Applied Science and Technology (CAST), 2017. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/700212/fingerprint-source-book-v2-second-edition.pdf (cit. on p. 6).
- [BF04] Paul Blythe and Jessica Fridrich. “Secure Digital Camera”. In: *Proceedings of Digital Forensic Research Workshop (DFRWS)*. 2004, pp. 17–19 (cit. on p. 4).
- [Bre96] Leo Breiman. “Bagging predictors”. In: *Machine Learning* 24.2 (1996), pp. 123–140 (cit. on pp. xxi, 43, 44, 113, 174, 179).
- [BB08] Wilhelm Burger and Mark J. Burge. “Geometric Operations”. In: *Digital Image Processing: An Algorithmic Introduction using Java*. London: Springer London, 2008, pp. 375–428. ISBN: 978-1-84628-968-2. DOI: 10.1007/978-1-84628-968-2_16. URL: https://doi.org/10.1007/978-1-84628-968-2_16 (cit. on p. 88).
- [Can86] J Canny. “A computational approach for edge detection”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 8 (1986), pp. 679–698 (cit. on p. 148).
- [CS03] Brian Carrier and Eugene H. Spafford. “Getting Physical with the Digital Investigation Process”. In: *International Journal of Digital Evidence* 2.2 (2003), pp. 1–20 (cit. on pp. 6, 24–26, 55).
- [Cas02] Eoghan Casey. “Error, Uncertainty and Loss in Digital Evidence”. In: *International Journal of Digital Evidence* 1.2 (2002). URL: <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf> (cit. on pp. 2, 65).
- [CHA18] W. Chaidee, K. Horapong, and V. Areekul. “Filter Design Based on Spectral Dictionary for Latent Fingerprint Pre-enhancement”. In: *2018 International Conference on Biometrics (ICB)*. 2018, pp. 23–30. DOI: 10.1109/ICB2018.2018.00015 (cit. on p. 7).
- [CE14] C. Champod and M. Espinoza. “Forgeries of Fingerprints in Forensic Science”. English. In: *Handbook of Biometric Anti-Spoofing*. Advances in Computer Vision and Pattern Recognition. Springer, 2014, pp. 13–34. ISBN: 978-1-4471-6523-1. DOI: 10.1007/978-1-4471-6524-8_2. URL: http://dx.doi.org/10.1007/978-1-4471-6524-8_2 (cit. on pp. 7, 11).
- [CC09] Christophe Champod and Paul Chamberlain. “Handbook of Forensic Science”. In: ed. by Jim Fraser and Robin Williams. Routledge, 2009. Chap. Fingerprints, pp. 57–83. ISBN: 9781843927327. DOI: 10.4324/9781843927327.ch3 (cit. on pp. 19, 46).
- [Cha+04] Christophe Champod, Chris Lennard, Pierre Margot, and Milutin Stoilovic. *Fingerprints and Other Ridge Skin Impressions*. 1st ed. CRC Press, 2004. ISBN: 0-415-27175-4 (cit. on p. 45).

- [CCG07] Sharat Chikkerur, Alexander N. Cartwright, and Venu Govindaraju. “Fingerprint enhancement using STFT analysis”. In: *Pattern Recognition* 40.1 (2007), pp. 198–211. ISSN: 0031-3203. DOI: <https://doi.org/10.1016/j.patcog.2006.05.036>. URL: <http://www.sciencedirect.com/science/article/pii/S0031320306002457> (cit. on p. 96).
- [CJ18] Tarang Chugh and Anil K. Jain. “Fingerprint Presentation Attack Detection: Generalization and Efficiency”. In: *CoRR* abs/1812.11574 (2018). arXiv: 1812.11574. URL: <http://arxiv.org/abs/1812.11574> (cit. on p. 7).
- [Cic+12] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. *Computer Security Incident Handling Guide*. NIST Special Publication 800-61 r2, <http://dx.doi.org/10.6028/NIST/SP.800-61r2>. 2012 (cit. on pp. 20–22, 56).
- [Cla+12] Eric Clausing, Christian Kraetzer, Jana Dittmann, and Claus Vielhauer. “A first approach for digital representation and automated classification of toolmarks on locking cylinders using confocal laser microscopy”. In: *Optics and Photonics for Counterterrorism, Crime Fighting, and Defence VIII*. Ed. by Colin Lewis and Douglas Burgess. Vol. 8546. International Society for Optics and Photonics. SPIE, 2012, pp. 60–72. DOI: 10.1117/12.971454. URL: <https://doi.org/10.1117/12.971454> (cit. on p. 167).
- [CFD13] Nathan S. Claxton, Thomas J. Fellers, and Michael W. Davidson. *LASER SCANNING CONFOCAL MICROSCOPY*. 2013. URL: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.328.3562> (cit. on pp. 35, 36).
- [CF18] IAPR Technical Committee on Computational Forensics. *Computational Forensics*. last accessed 08/07/2018. 2018. URL: <https://sites.google.com/site/compforgroup/> (cit. on p. 2).
- [Cos98] Louis Costa. “Open Systems Interconnect (OSI) Model”. In: *JALA: Journal of the Association for Laboratory Automation* 3.1 (1998), pp. 28–35. DOI: 10.1177/221106829800300108. eprint: <https://doi.org/10.1177/221106829800300108>. URL: <https://doi.org/10.1177/221106829800300108> (cit. on p. 30).
- [Cra+07] Nicole J. Crane, Edward G. Bartick, Rebecca Schwartz Perlman, and Scott Huffman. “Infrared Spectroscopic Imaging for Noninvasive Detection of Latent Fingerprints”. In: *Journal of Forensic Sciences* 52.1 (2007), pp. 48–53. ISSN: 1556-4029. DOI: 10.1111/j.1556-4029.2006.00330.x (cit. on p. 7).
- [DiH14] Jana Dittmann and Mario Hildebrandt. “Context analysis of artificial sweat printed fingerprint forgeries: Assessment of properties for forgery detection”. In: *2nd International Workshop on Biometrics and Forensics*. 2014, pp. 1–6. DOI: 10.1109/IWBF.2014.6914246 (cit. on pp. 141, 142).

- [DG01] Lloyd Dixon and Brian Gill. *Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases Since the Daubert Decision*. RAND Institute for Civil Justice, 2001. ISBN: 0-8330-3088-4 (cit. on pp. 5, 15, 32, 33, 51, 55, 56, 58, 61, 65, 66, 81, 97, 98, 160, 169).
- [ICAO15] *Doc 9303 - Machine Readable Travel Documents, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*. 7th ed. International Civil Aviation Organization, 2015. ISBN: 978-92-9249-798-9. URL: https://www.icao.int/publications/Documents/9303/p10_cons_en.pdf (cit. on p. 168).
- [DDB11] A.J. Dominick, Niamh Daéid, and Stephen Bleay. “The recoverability of fingerprints on nonporous surfaces exposed to elevated temperatures”. In: *Journal of Forensic Identification* 61 (Sept. 2011), pp. 520–536 (cit. on p. 110).
- [Dro+11] Itiel E. Dror, Christophe Champod, Glenn Langenburg, David Charlton, Heloise Hunt, and Robert Rosenthal. “Cognitive issues in fingerprint analysis: Inter- and intra-expert consistency and the effect of a ‘target’ comparison”. In: *Forensic Science International* 208.1 (2011), pp. 10–17. ISSN: 0379-0738. DOI: <https://doi.org/10.1016/j.forsciint.2010.10.013>. URL: <http://www.sciencedirect.com/science/article/pii/S0379073810004706> (cit. on p. 47).
- [Dub+08] Satish Kumar Dubey, Dalip Singh Mehta, Arun Anand, and Chandra Shakher. “Simultaneous topography and tomography of latent fingerprints using full-field swept-source optical coherence tomography”. In: *Journal of Optics A: Pure and Applied Optics* 10.1 (2008), pp. 015307–015315 (cit. on p. 7).
- [DHS00] Richard o. Duda, Peter E. Hart, and David G. Stork. *Pattern Classification, 2nd Edition*. Wiley, 2000. ISBN: 978-0-471-05669-0 (cit. on pp. xxi, xxii, 40, 41, 43–45, 97, 113, 133, 134, 164, 179).
- [EB17] Jude Ezeobiejese and Bir Bhanu. “Latent Fingerprint Image Segmentation Using Deep Neural Network”. In: *Deep Learning for Biometrics*. Ed. by Bir Bhanu and Ajay Kumar. Cham: Springer International Publishing, 2017, pp. 83–107. ISBN: 978-3-319-61657-5. DOI: [10.1007/978-3-319-61657-5_4](https://doi.org/10.1007/978-3-319-61657-5_4). URL: https://doi.org/10.1007/978-3-319-61657-5_4 (cit. on p. 98).
- [FVH+13] Robert Fischer, Claus Vielhauer, Mario Hildebrandt, Stefan Kiltz, and Jana Dittmann. “Ballistic examinations based on 3D data: a comparative study of probabilistic Hough Transform and geometrical shape determination for circle-detection on cartridge bottoms”. In: *Media Watermarking, Security, and Forensics 2013*. Ed. by Adnan M. Alattar, Nasir D. Memon, and Chad D. Heitzenrater. Vol. 8665. International Society for Optics and Photonics. SPIE, 2013, pp. 134–145. DOI: [10.1117/12.2004283](https://doi.org/10.1117/12.2004283). URL: <https://doi.org/10.1117/12.2004283> (cit. on p. 167).

- [FSC09] National Research Council Committee on Identifying the Needs of the Forensic Sciences Community. *Strengthening Forensic Science in the United States: A Path Forward*. The National Academies Press, 2009. ISBN: 9780309131308. URL: http://www.nap.edu/openbook.php?record_id=12589 (cit. on pp. 1, 3, 4, 32, 66, 67).
- [Fri13] Jessica Fridrich. “Sensor Defects in Digital Image Forensic”. In: *Digital Image Forensics: There is More to a Picture than Meets the Eye*. Ed. by Husrev Taha Sencar and Nasir Memon. New York, NY: Springer New York, 2013, pp. 179–218. ISBN: 978-1-4614-0757-7. DOI: 10.1007/978-1-4614-0757-7_6. URL: https://doi.org/10.1007/978-1-4614-0757-7_6 (cit. on p. 4).
- [Gar09] Simson L. Garfinkel. “Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools”. In: *The International Journal of Digital Crime and Forensics* Volume 1.Issue 1 (2009) (cit. on p. 75).
- [Ger20] German eForensics GmbH. *How EVISCAN works*. 2020. URL: <https://www.eviscan.com/en/eviscan/how-eviscan-works/> (cit. on p. 7).
- [Ges14] Alexander Geschonneck. *Computer-Forensik*. 6th Edition. dpunkt.verlag GmbH, 2014. ISBN: 978-3-86490-133-1 (cit. on p. 6).
- [FRT12] Fries Research & Technology GmbH. *MicroProf*. 2012. URL: [hhttps://web.archive.org/web/20120429063437/http://www.frt-gmbh.com/en/products/microprof/microprof/microprof.html](https://web.archive.org/web/20120429063437/http://www.frt-gmbh.com/en/products/microprof/microprof/microprof.html) (cit. on pp. 35, 37, 72, 78, 109).
- [FRT14a] Fries Research & Technology GmbH. *Chromatic White Light Sensor FRT CWL*. 2014. URL: <https://web.archive.org/web/20140517030400/http://www.frt-gmbh.com/en/chromatic-white-light-sensor-frt-cwl.aspx> (cit. on pp. 34, 35, 72).
- [FRT14b] Fries Research & Technology GmbH. *Thin Film Sensor FRT FTR*. 2014. URL: <https://web.archive.org/web/20141111113407/http://www.frt-gmbh.com/en/thin-film-sensor-frt-ftr.aspx> (cit. on pp. 37, 72, 74).
- [Hal+09] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H. Witten. “The WEKA Data Mining Software: An Update”. In: *SIGKDD Explorations* 11.1 (2009), pp. 10–18 (cit. on pp. 42–45, 112, 113, 134, 152, 158, 163, 174, 175, 185).
- [Hal98] Mark A. Hall. “Correlation-based Feature Subset Selection for Machine Learning”. PhD thesis. Hamilton, New Zealand: University of Waikato, 1998 (cit. on pp. 134, 163).
- [HUPU13] Jutta Hämmerle-Uhl, Michael Pober, and Andreas Uhl. “Towards a Standardised Testsuite to Assess Fingerprint Matching Robustness: The StirMark Toolkit - Cross-Feature Type Comparisons”. In: *Communications and Multimedia Security*. Vol. 8099. Lecture Notes in Computer Science. 2013, pp. 3–17. ISBN: 978-3-642-40778-9 (cit. on pp. 81, 85).

- [Hei27] W. Heisenberg. “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik”. In: *Zeitschrift für Physik* 43.3 (1927), pp. 172–198. ISSN: 0044-3328. DOI: 10.1007/BF01397280. URL: <https://doi.org/10.1007/BF01397280> (cit. on p. 64).
- [HiD15a] M. Hildebrandt and J. Dittmann. “StirTraceV2.0: Enhanced Benchmarking and Tuning of Printed Fingerprint Detection”. In: *IEEE Transactions on Information Forensics and Security* 10.4 (2015), pp. 833–848. ISSN: 1556-6021. DOI: 10.1109/TIFS.2015.2405412 (cit. on pp. 72, 81, 83–88, 95, 109, 141, 144–148, 152, 157, 158).
- [HiD16] M. Hildebrandt and J. Dittmann. “StirTraceV3.0 and printed fingerprint detection: Simulation of acquisition condition tilting and its impact to latent fingerprint detection feature spaces for crime scene forgeries”. In: *2016 4th International Conference on Biometrics and Forensics (IWBF)*. 2016, pp. 1–6. DOI: 10.1109/IWBF.2016.7449695 (cit. on pp. 72, 82–84, 89, 90, 141, 157, 158, 160, 162, 163, 185).
- [HML+11] M. Hildebrandt, R. Merkel, M. Leich, S. Kiltz, J. Dittmann, and C. Vielhauer. “Benchmarking contact-less surface measurement devices for fingerprint acquisition in forensic investigations: Results for a differential scan approach with a chromatic white light sensor”. In: *2011 17th International Conference on Digital Signal Processing (DSP)*. 2011, pp. 1–6. DOI: 10.1109/ICDSP.2011.6004969 (cit. on pp. 53, 65, 95, 107).
- [Hi15] Mario Hildebrandt. “Feature space fusion and feature selection for an enhanced robustness of the fingerprint forgery detection for printed artificial sweat”. In: *2015 IEEE International Conference on Multimedia Expo Workshops (ICMEW)*. 2015, pp. 1–6. DOI: 10.1109/ICMEW.2015.7169865 (cit. on pp. 141, 156–159, 161–163).
- [HiD14] Mario Hildebrandt and Jana Dittmann. “From StirMark to StirTrace: Benchmarking Pattern Recognition Based Printed Fingerprint Detection”. In: *Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security. IH&MMSec '14*. Salzburg, Austria: Association for Computing Machinery, 2014, 71–76. ISBN: 9781450326476. DOI: 10.1145/2600918.2600926. URL: <https://doi.org/10.1145/2600918.2600926> (cit. on pp. 72, 81, 82, 84–86, 141).
- [HiD15b] Mario Hildebrandt and Jana Dittmann. “Benford’s Law based detection of latent fingerprint forgeries on the example of artificial sweat printed fingerprints captured by confocal laser scanning microscopes”. In: *Media Watermarking, Security, and Forensics 2015*. Ed. by Adnan M. Alattar, Nasir D. Memon, and Chad D. Heitzenrater. Vol. 9409. International Society for Optics and Photonics. SPIE, 2015, pp. 77–86. DOI: 10.1117/12.2077531. URL: <https://doi.org/10.1117/12.2077531> (cit. on pp. 141, 145, 149, 150).

- [HDV13] Mario Hildebrandt, Jana Dittmann, and Claus Vielhauer. “Statistical Latent Fingerprint Residue Recognition in Contact-Less Scans to Support Fingerprint Segmentation”. In: *Proceedings of 18th International Conference on Digital Signal Processing (DSP)*. IEEE, 2013, pp. 1–6 (cit. on pp. 95, 98–101, 103–106, 114, 115).
- [HDV17] Mario Hildebrandt, Jana Dittmann, and Claus Vielhauer. “Capture and Analysis of Latent Marks”. In: *Handbook of Biometrics for Forensic Science*. Ed. by Massimo Tistarelli and Christophe Champod. Cham: Springer International Publishing, 2017, pp. 19–35. ISBN: 978-3-319-50673-9. DOI: 10.1007/978-3-319-50673-9_2. URL: https://doi.org/10.1007/978-3-319-50673-9_2 (cit. on pp. 6, 45).
- [HKD11] Mario Hildebrandt, Stefan Kiltz, and Jana Dittmann. “Automatisierte Lokalisierung und Erfassung von Fingerspuren”. In: *D-A-CH security 2011*. Ed. by Peter Schartner and Jürgen Taeger. syssec, 2011, pp. 422–434. ISBN: 978-3-00-034960-7 (cit. on pp. 53, 58).
- [HKD13b] Mario Hildebrandt, Stefan Kiltz, and Jana Dittmann. “Digitized forensics: retaining a link between physical and digital crime scene traces using QR-codes”. In: *Proc. SPIE 8667*. SPIE, 2013. DOI: 10.1117/12.2004548. URL: <https://doi.org/10.1117/12.2004548> (cit. on pp. 53, 54, 72, 75–80).
- [HKD13a] Mario Hildebrandt, Stefan Kiltz, and Jana Dittmann. “Printed fingerprints at crime scenes: a faster detection of malicious traces using scans of confocal microscopes”. In: *Media Watermarking, Security, and Forensics 2013*. Ed. by Adnan M. Alattar, Nasir D. Memon, and Chad D. Heitzenrater. Vol. 8665. International Society for Optics and Photonics. SPIE, 2013, pp. 73–84. DOI: 10.1117/12.2004507. URL: <https://doi.org/10.1117/12.2004507> (cit. on pp. 141, 144, 149, 151, 152, 156, 157, 178).
- [HKG+11] Mario Hildebrandt, Stefan Kiltz, Ina Grossmann, and Claus Vielhauer. “Convergence of Digital and Traditional Forensic Disciplines: A First Exemplary Study for Digital Dactyloscopy”. In: *Proceedings of the Thirteenth ACM Multimedia Workshop on Multimedia and Security*. MM&Sec ’11. Buffalo, New York, USA: ACM, 2011, pp. 1–8. ISBN: 978-1-4503-0806-9. DOI: 10.1145/2037252.2037254. URL: <http://doi.acm.org/10.1145/2037252.2037254> (cit. on pp. 3, 53, 54).
- [HKD+11] Mario Hildebrandt, Stefan Kiltz, Jana Dittmann, and Claus Vielhauer. “Malicious Fingerprint Traces: A Proposal for an Automated Analysis of Printed Amino Acid Dots Using Houghcircles”. In: *Proceedings of the Thirteenth ACM Multimedia Workshop on Multimedia and Security*. MM & Sec ’11. Buffalo, New York, USA: ACM, 2011, pp. 33–40. ISBN: 978-1-4503-0806-9. DOI: 10.1145/2037252.2037260. URL: <http://doi.acm.org/10.1145/2037252.2037260> (cit. on pp. 141, 144, 145, 151).

- [HDV+11] Mario Hildebrandt, Jana Dittmann, Claus Vielhauer, and Marcus Leich. “Optical techniques: using coarse and detailed scans for the preventive acquisition of fingerprints with chromatic white-light sensors”. In: *Technologies for Optical Countermeasures VIII*. Ed. by David H. Titterton and Mark A. Richardson. Vol. 8187. International Society for Optics and Photonics. SPIE, 2011, pp. 148–156. DOI: [10.1117/12.897701](https://doi.org/10.1117/12.897701). URL: <https://doi.org/10.1117/12.897701> (cit. on pp. 53, 58, 95).
- [HDP+11] Mario Hildebrandt, Jana Dittmann, Matthias Pocs, Michael Ulrich, Ronny Merkel, and Thomas Fries. “Privacy Preserving Challenges: New Design Aspects for Latent Fingerprint Detection Systems with Contact-Less Sensors for Future Preventive Applications in Airport Luggage Handling”. In: *Biometrics and ID Management*. Ed. by Claus Vielhauer, Jana Dittmann, Andrzej Drygajlo, Niels Christian Juul, and Michael C. Fairhurst. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 286–298. ISBN: 978-3-642-19530-3 (cit. on pp. 53, 58, 95, 96).
- [HKS+12] Mario Hildebrandt, Stefan Kiltz, Jennifer Sturm, Jana Dittmann, and Claus Vielhauer. “High-resolution printed amino acid traces: a first-feature extraction approach for fingerprint forgery detection”. In: *Media Watermarking, Security, and Forensics 2012*. Ed. by Nasir D. Memon, Adnan M. Alattar, and Edward J. Delp III. Vol. 8303. International Society for Optics and Photonics. SPIE, 2012, pp. 152–162. DOI: [10.1117/12.909072](https://doi.org/10.1117/12.909072). URL: <https://doi.org/10.1117/12.909072> (cit. on pp. 141, 144, 148).
- [HMQ+13] Mario Hildebrandt, Andrey Makrushin, Kun Qian, and Jana Dittmann. “Visibility Assessment of Latent Fingerprints on Challenging Substrates in Spectroscopic Scans”. In: *Communications and Multimedia Security*. Ed. by Bart De Decker, Jana Dittmann, Christian Kraetzer, and Claus Vielhauer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 200–203. ISBN: 978-3-642-40779-6 (cit. on pp. 109, 182).
- [HKD+14] Mario Hildebrandt, Stefan Kiltz, Jana Dittmann, and Claus Vielhauer. “An enhanced feature set for pattern recognition based contrast enhancement of contact-less captured latent fingerprints in digitized crime scene forensics”. In: *Media Watermarking, Security, and Forensics 2014*. Ed. by Adnan M. Alattar, Nasir D. Memon, and Chad D. Heitzenrater. Vol. 9028. International Society for Optics and Photonics. SPIE, 2014, pp. 78–92. DOI: [10.1117/12.2039074](https://doi.org/10.1117/12.2039074). URL: <https://doi.org/10.1117/12.2039074> (cit. on pp. 95, 99, 101–103, 105, 106, 109, 110, 113–118, 122, 124, 125, 127–131, 174).
- [HNM+17] Mario Hildebrandt, Tom Neubert, Andrey Makrushin, and Jana Dittmann. “Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps”. In: *2017 5th International Workshop on Biometrics and Forensics (IWBF)*. 2017, pp. 1–6. DOI: [10.1109/IWBF.2017.7935087](https://doi.org/10.1109/IWBF.2017.7935087) (cit. on p. 168).

- [HRL11] Eric H. Holder, Laurie O. Robinson, and John H. Laub, eds. *The Fingerprint Sourcebook*. U.S. Department of Justice, NIJ, 2011 (cit. on pp. 2, 4, 6, 16, 18, 22, 24, 25, 33, 37, 38, 47–49, 51, 56, 60).
- [HJ04] Lin Hong and Anil Jain. “Fingerprint Enhancement”. In: *Automatic Fingerprint Recognition Systems*. Ed. by Nalini Ratha and Ruud Bolle. New York, NY: Springer New York, 2004, pp. 127–143. ISBN: 978-0-387-21685-0. DOI: 10.1007/0-387-21685-5_7. URL: https://doi.org/10.1007/0-387-21685-5_7 (cit. on p. 96).
- [Hu62] Ming-Kuei Hu. “Visual pattern recognition by moment invariants”. In: *Information Theory, IRE Transactions on* 8.2 (1962), pp. 179–187. ISSN: 0096-1000. DOI: 10.1109/TIT.1962.1057692 (cit. on pp. 101, 102).
- [Huh+09] D. Huhnlein, U. Korte, L. Langer, and A. Wiesmaier. “A Comprehensive Reference Architecture for Trustworthy Long-Term Archiving of Sensitive Data”. In: *2009 3rd International Conference on New Technologies, Mobility and Security*. 2009, pp. 1–5. DOI: 10.1109/NTMS.2009.5384830 (cit. on p. 63).
- [IL92] Wayne Iba and Pat Langley. “Induction of One-Level Decision Trees”. In: *Machine Learning Proceedings 1992*. Ed. by Derek Sleeman and Peter Edwards. San Francisco (CA): Morgan Kaufmann, 1992, pp. 233–240. ISBN: 978-1-55860-247-2. DOI: <https://doi.org/10.1016/B978-1-55860-247-2.50035-8>. URL: <http://www.sciencedirect.com/science/article/pii/B9781558602472500358> (cit. on p. 44).
- [IR00] Keith Inman and Norah Rudin. *Principles and Practice of Criminalistics: The Profession of Forensic Science (Protocols in Forensic Science)*. CRC Press, 2000. ISBN: 978-0849381270 (cit. on pp. 2–6, 30, 60, 99, 141, 176).
- [Int06] International Organization for Standardization. *Information Technology — Automatic Identification and Data Capture Techniques — QR Code 2005 Bar Code Symbology Specification*. ISO/IEC 18004:2006. 2006 (cit. on p. 76).
- [ISO17] International Organization for Standardization. *General requirements for the competence of testing and calibration laboratories*. Third edition. 17025:2017(E). ISO/IEC, Nov. 2017 (cit. on pp. 16, 18, 55, 61, 65, 67, 160).
- [JCD07] A. K. Jain, Y. Chen, and M. Demirkus. “Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29.1 (2007), pp. 15–27. ISSN: 1939-3539. DOI: 10.1109/TPAMI.2007.250596 (cit. on p. 46).
- [Jan+02] Roel J. Jansen, Martin Poulus, Wijnbren Taconis, and Jaap Stoker. “High-resolution spiral computed tomography with multiplanar reformatting, 3D surface- and volume rendering: a non-destructive method to visualize ancient Egyptian mummification techniques”. In: *Computerized Medical Imaging and Graphics* 26.4 (2002), pp. 211–216. ISSN: 0895-6111. DOI: <https://doi.org/10.1016/>

- S0895-6111(02)00015-0. URL: <http://www.sciencedirect.com/science/article/pii/S0895611102000150> (cit. on p. 168).
- [Jas13] Sabah A. Jassim. “Face Recognition from Degraded Images – Super Resolution Approach by Non-adaptive Image-Independent Compressive Sensing Dictionaries”. In: *Communications and Multimedia Security*. Ed. by Bart De Decker, Jana Dittmann, Christian Kraetzer, and Claus Vielhauer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 217–232. ISBN: 978-3-642-40779-6 (cit. on p. 182).
- [Kay09] David H. Kaye. “Identification, individualization and uniqueness: What’s the difference?†”. In: *Law, Probability and Risk* 8.2 (July 2009), pp. 85–94. ISSN: 1470-8396. DOI: 10.1093/lpr/mgp018. eprint: <https://academic.oup.com/lpr/article-pdf/8/2/85/2773682/mgp018.pdf>. URL: <https://doi.org/10.1093/lpr/mgp018> (cit. on p. 5).
- [KEY20] KEYENCE International Belgium. *Shape Measurement Laser Microscope - VK-X110*. 2020. URL: https://www.keyence.eu/products/measure-sys/3d-measure/vk-x100_x200/models/vk-x110/ (cit. on pp. 36, 37, 72, 73).
- [KVL11] Tobias Kiertscher, Claus Vielhauer, and Marcus Leich. “Automated Forensic Fingerprint Analysis: A Novel Generic Process Model and Container Format”. In: *Biometrics and ID Management*. Ed. by Claus Vielhauer, Jana Dittmann, Andrzej Drygajlo, Niels Christian Juul, and Michael C. Fairhurst. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 262–273. ISBN: 978-3-642-19530-3 (cit. on pp. 75, 78, 79).
- [Kil20] Stefan Kiltz. “A Data-Centric Examination Approach (DCEA) for a qualitative determination of loss, error and uncertainty in digital and digitised forensics”. PhD Thesis, to be reviewed at Otto-von-Guericke-University, Faculty of Computer Science. 2020 (cit. on pp. 53, 65).
- [KHA+09] Stefan Kiltz, Mario Hildebrandt, Robert Altschaffel, Jana Dittmann, Claus Vielhauer, and Carsten Schulz. “Sicherstellung von gelöschtem Schadcode anhand von RAM-Analysen und Filecarving mit Hilfe eines forensischen Datenmodells”. In: *Sichere Wege in der vernetzten Welt, 11. Deutscher IT-Sicherheitskongress*. in German. SecuMedia, 2009, pp. 473–488 (cit. on pp. 28–30, 51, 53–55, 61, 181).
- [KHD+11] Stefan Kiltz, Mario Hildebrandt, Jana Dittmann, Claus Vielhauer, and Christian Kraetzer. “Printed fingerprints: a framework and first results towards detection of artificially printed latent fingerprints for forensics”. In: *Image Quality and System Performance VIII*. Ed. by Susan P. Farnand and Frans Gaykema. Vol. 7867. International Society for Optics and Photonics. SPIE, 2011, pp. 300–314. DOI: 10.1117/12.872329. URL: <https://doi.org/10.1117/12.872329> (cit. on p. 150).

- [Kip+20] Ruth Kips, Rachel Lindvall, Naomi Marks, Viktor Gluchsenko, Ayako Okubo, Yoshiki Kimura, Ogawa Jumpei, Evá Kovács-Széles, and Csaba Tobi. “Joint Sample Analysis on Selected Uranium Ore Concentrates and Nuclear Forensics Library Exercise”. In: *International Conference on Nuclear Security: Sustaining and Strengthening Efforts*. Vienna, Austria: International Atomic Energy Agency, 2020 (cit. on p. 168).
- [KC13] Alex C. Kot and Hong Cao. “Image and Video Source Class Identification”. In: *Digital Image Forensics: There is More to a Picture than Meets the Eye*. Ed. by Husrev Taha Sencar and Nasir Memon. New York, NY: Springer New York, 2013, pp. 157–178. ISBN: 978-1-4614-0757-7. DOI: 10.1007/978-1-4614-0757-7_5. URL: https://doi.org/10.1007/978-1-4614-0757-7_5 (cit. on p. 4).
- [Kra13] Christian Kraetzer. “Statistical pattern recognition for audio-forensics - empirical investigations on the application scenarios audio steganalysis and microphone forensics”. PhD thesis. Otto-von-Guericke-Universität Magdeburg, 2013. URL: <http://dx.doi.org/10.25673/3967> (cit. on pp. 4, 33).
- [Kri+19] Ram P. Krish, Julian Fierrez, Daniel Ramos, Fernando Alonso-Fernandez, and Josef Bigun. “Improving automated latent fingerprint identification using extended minutia types”. In: *Information Fusion* 50 (2019), pp. 9–19. ISSN: 1566-2535. DOI: <https://doi.org/10.1016/j.inffus.2018.10.001>. URL: <http://www.sciencedirect.com/science/article/pii/S1566253517308096> (cit. on p. 48).
- [LHF05] Niels Landwehr, Mark Hall, and Eibe Frank. “Logistic Model Trees”. In: *Machine Learning* 95.1-2 (2005), pp. 161–205 (cit. on pp. xxi, 43, 44, 152–155, 158, 159, 179).
- [Li+13] Hong xia Li, Jing Cao, Jie qing Niu, and Yun gang Huang. “Study of UV imaging technology for noninvasive detection of latent fingerprints”. In: *International Symposium on Photoelectronic Detection and Imaging 2013: Laser Sensing and Imaging and Applications*. Ed. by Farzin Amzajerjian, Astrid Aksnes, Weibiao Chen, Chunqing Gao, Yongchao Zheng, and Cheng Wang. Vol. 8905. International Society for Optics and Photonics. SPIE, 2013, pp. 422–427. DOI: 10.1117/12.2034451. URL: <https://doi.org/10.1117/12.2034451> (cit. on p. 6).
- [LFK18] Jian Li, Jianjiang Feng, and C.-C. Jay Kuo. “Deep convolutional neural network for latent fingerprint enhancement”. In: *Signal Processing: Image Communication* 60 (2018), pp. 52–63. ISSN: 0923-5965. DOI: <https://doi.org/10.1016/j.image.2017.08.010>. URL: <http://www.sciencedirect.com/science/article/pii/S0923596517301492> (cit. on p. 98).
- [LM02] R. Lienhart and J. Maydt. “An extended set of Haar-like features for rapid object detection”. In: *Proceedings. International Conference on Image Processing*. Vol. 1. 2002, pp. I–I. DOI: 10.1109/ICIP.2002.1038171 (cit. on p. 101).

- [Lin+06] Shih-Schön Lin, Konstantin M. Yemelyanov, Jr. Edward N. Pugh, and Nader Engheta. “Polarization-based and specular-reflection-based noncontact latent fingerprint imaging and lifting”. In: *Journal of the Optical Society of America A* 23.9 (2006), pp. 2137–2153. DOI: 10.1364/JOSAA.23.002137. URL: <http://josaa.osa.org/abstract.cfm?URI=josaa-23-9-2137> (cit. on p. 6).
- [LYJ98] Lin Hong, Yifei Wan, and A. Jain. “Fingerprint image enhancement: algorithm and performance evaluation”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 20.8 (1998), pp. 777–789. ISSN: 1939-3539. DOI: 10.1109/34.709565 (cit. on p. 96).
- [LT88] William J. Lloyd and Howard H. Taub. “Output Hardcopy Devices”. In: ed. by Robert C. Durbeck and Sol Sherr. San Diego: Academic Press, Inc., 1988. Chap. Ink Jet Printing, pp. 311–370. ISBN: 0-12-225040-0 (cit. on p. 142).
- [LI17] Steven P. Lund and Hari Iyer. “Likelihood Ratio as Weight of Forensic Evidence: A Closer Look”. In: *Journal of Research of National Institute of Standards and Technology* 122 (2017). DOI: <https://doi.org/10.6028/jres.122.027> (cit. on pp. 30–32).
- [MHF+12] Andrey Makrushin, Mario Hildebrandt, Robert Fischer, Tobias Kiertscher, Jana Dittmann, and Claus Vielhauer. “Advanced techniques for latent fingerprint detection and validation using a CWL device”. In: *Proc. SPIE 8436*. SPIE, 2012 (cit. on pp. 95, 98).
- [Mak+15] Andrey Makrushin, Kun Qian, Claus Vielhauer, and Tobias Scheidat. “Forensic analysis: on the capability of optical sensors to visualize latent fingerprints on rubber gloves”. In: *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*. 2015, pp. 1–6. DOI: <https://doi.org/10.1109/IWBF.2015.7110229> (cit. on p. 182).
- [Mal+09] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer Professional Computing. Springer London, 2009. ISBN: 9781848822542. DOI: <https://doi.org/10.1007/978-1-84882-254-2> (cit. on pp. 45, 46, 49, 102).
- [Mat+16] K. Matsumoto, Y. Tajima, R. Saito, M. Nakata, H. Sato, T. Kovacs, and K. Takadama. “Learning classifier system with deep autoencoder”. In: *2016 IEEE Congress on Evolutionary Computation (CEC)*. 2016, pp. 4739–4746 (cit. on p. 98).
- [McE10] Tom McEwen. *The Role and Impact of Forensic Evidence in the Criminal Justice System, Final Report*. Tech. rep. Institute for Law and Justice, Inc., 2010. URL: <https://www.ncjrs.gov/pdffiles1/nij/grants/236474.pdf> (cit. on p. 93).
- [Mer14] Ronny Merkel. “New solutions for an old challenge - chances and limitations of optical, non-invasive acquisition and digital processing techniques for the age estimation of latent fingerprints”. PhD thesis. Otto-von-Guericke-Universität Magdeburg, 2014. URL: <http://dx.doi.org/10.25673/4091> (cit. on pp. 68, 96, 109, 168).

- [MHD15] Ronny Merkel, Mario Hildebrandt, and Jana Dittmann. “Application of stirtrace benchmarking for the evaluation of latent fingerprint age estimation robustness”. In: *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*. 2015, pp. 1–6. DOI: [10.1109/IWBF.2015.7110221](https://doi.org/10.1109/IWBF.2015.7110221) (cit. on p. 168).
- [Mer+12] Ronny Merkel, Stefan Gruhn, Jana Dittmann, Claus Vielhauer, and Anja Bräutigam. “On non-invasive 2D and 3D Chromatic White Light image sensors for age determination of latent fingerprints”. In: *Forensic Science International* 222.1 (2012), pp. 52–70. ISSN: 0379-0738. DOI: <https://doi.org/10.1016/j.forsciint.2012.05.001>. URL: <http://www.sciencedirect.com/science/article/pii/S0379073812002095> (cit. on p. 3).
- [Mik+05] Aravind K. Mikkilineni, Osman Arslan, Pei ju Chiang, Roy M. Kumontoy, Jan P. Allebach, and George T. c. “Printer forensics using svm techniques”. In: *Proceedings of the IS&T’s NIP21: International Conference on Digital Printing Technologies*. 2005, pp. 223–226 (cit. on p. 82).
- [MSH08] Michael B. Mukasey, Jeffrey L. Sedgwick, and David W. Hagg. *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. NIJ Special Report 219941, [Online] available: <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>. National Institute of Justice. 2008 (cit. on pp. 22–25, 56).
- [Mur12] Kevin P. Murphy. *Machine Learning: A Probabilistic Perspective*. The MIT Press, 2012. ISBN: 978-0-262-01802-9 (cit. on p. 43).
- [Nat13] National Institute of Standards and Technology. *NIST Biometric Image Software*. 2013. URL: <http://www.nist.gov/itl/iad/ig/nbis.cfm> (cit. on pp. 102, 105, 112, 121, 175, 185, 197).
- [NMH+18] Tom Neubert, Andrey Makrushin, Mario Hildebrandt, Christian Kraetzer, and Jana Dittmann. “Extended StirTrace benchmarking of biometric and forensic qualities of morphed face images”. In: *IET Biometrics* 7.4 (2018), pp. 325–332. ISSN: 2047-4946. DOI: [10.1049/iet-bmt.2017.0147](https://doi.org/10.1049/iet-bmt.2017.0147) (cit. on p. 168).
- [NPP33] Jerzy Neyman, Egon Sharpe Pearson, and Karl Pearson. “On the problem of the most efficient tests of statistical hypotheses”. In: *Philosophical Transactions of the Royal Society of London, Series A, Containing Papers of a Mathematical or Physical Character* 231 (694-703 1933), 289–337. DOI: <https://doi.org/10.1098/rsta.1933.0009> (cit. on p. 31).
- [NT16] K. Ntalianis and N. Tsapatsoulis. “Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks”. In: *IEEE Transactions on Emerging Topics in Computing* 4.1 (2016), pp. 156–174. ISSN: 2168-6750. DOI: [10.1109/TETC.2015.2400135](https://doi.org/10.1109/TETC.2015.2400135) (cit. on p. 4).
- [Off06] Office of the Inspector General. *A Review of the FBI’s Handling of the Brandon Mayfield Case*. Tech. rep. U.S. Department of Justice: Washington, 2006. URL: <https://oig.justice.gov/special/s0601/exec.pdf> (cit. on pp. 2, 46).

- [Ope20a] OpenCV dev team. *Image Moments - OpenCV 2.4.13.7 documentation*. last accessed 02/08/2020. 2020. URL: <https://docs.opencv.org/2.4/doc/tutorials/imgproc/shapedescriptors/moments/moments.html> (cit. on p. 102).
- [Ope20b] OpenCV dev team. *Image Moments - OpenCV 2.4.13.7 documentation*. last accessed 02/08/2020. 2020. URL: <https://docs.opencv.org/2.4/index.html> (cit. on pp. 174, 175, 185).
- [Org20a] Organization of Scientific Area Committees. *Firearms & Toolmarks Subcommittee*. last accessed 04/11/2020. 2020. URL: <https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/firearms-toolmarks-subcommittee> (cit. on p. 61).
- [Org20b] Organization of Scientific Area Committees. *Friction Ridge Subcommittee*. last accessed 04/11/2020. 2020. URL: <https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/friction-ridge-subcommittee> (cit. on p. 61).
- [Org20c] Organization of Scientific Area Committees. *Materials (Trace) Subcommittee*. last accessed 04/11/2020. 2020. URL: <https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/materials-trace-subcommittee> (cit. on p. 61).
- [Ots79] N. Otsu. “A threshold selection method from gray level histograms”. In: *IEEE Trans. Systems, Man and Cybernetics* 9 (Mar. 1979), pp. 62–66 (cit. on p. 145).
- [PPJ02] S. Pankanti, S. Prabhakar, and A. K. Jain. “On the individuality of fingerprints”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 24.8 (2002), pp. 1010–1025. ISSN: 0162-8828. DOI: 10.1109/TPAMI.2002.1023799 (cit. on p. 3).
- [PAK98] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. “Attacks on Copyright Marking Systems”. English. In: *Information Hiding*. Vol. 1525. Lecture Notes in Computer Science. 1998, pp. 218–238. ISBN: 978-3-540-65386-8 (cit. on pp. 81, 84, 172).
- [Pla99] John C. Platt. “Fast Training of Support Vector Machines Using Sequential Minimal Optimization”. In: *Advances in Kernel Methods: Support Vector Learning*. Cambridge, MA, USA: MIT Press, 1999, 185–208. ISBN: 0262194163 (cit. on pp. xxii, 43, 113, 133, 136, 179).
- [QZH10] Ghulam Qadir, Xi Zhao, and Anthony T. S. Ho. “Estimating JPEG2000 compression for image forensics using Benford’s Law”. In: *Proc. SPIE 7723*. 2010 (cit. on p. 103).
- [RCG02] Mark Reith, Clint Carr, and Gregg Gunsch. “An Examination of Digital Forensic Models”. In: *International Journal of Digital Evidence* 1.3 (2002), pp. 1–12 (cit. on pp. 23, 24).
- [RKA06] Juan J. Rodriguez, Ludmila I. Kuncheva, and Carlos J. Alonso. “Rotation Forest: A New Classifier Ensemble Method”. In: *IEEE Trans. Pattern Anal. Mach. Intell.* 28 (10 2006), pp. 1619–1630. ISSN: 0162-8828 (cit. on pp. xxii, 43, 45, 152–155, 157–159, 172, 173, 179).

- [RNJ06] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. “Levels of Fusion in Biometrics”. English. In: *Handbook of Multibiometrics*. Vol. 6. International Series on Biometrics. Springer US, 2006, pp. 59–90. ISBN: 978-0-387-22296-7. DOI: 10.1007/0-387-33123-9_3. URL: http://dx.doi.org/10.1007/0-387-33123-9_3 (cit. on p. 156).
- [SI14] R. Saranya and M. G. Indu. “An Effective Method for Forensic Latent Fingerprint Enhancement and Dictionary Construction”. In: *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)* 3.4 (2014), pp. 13–17 (cit. on p. 7).
- [SKV17] Tobias Scheidat, Michael Kalbitz, and Claus Vielhauer. “Biometric authentication based on 2D/3D sensing of forensic handwriting traces”. English. In: *IET Biometrics* 6 (4 2017), 316–324(8). ISSN: 2047-4938. URL: <https://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2016.0127> (cit. on p. 167).
- [Sch+11] Harald Schneider, Thomas Sommerer, Steve Rand, and Peter Wiegand. “Hot flakes in cold cases”. In: *International Journal of Legal Medicine* 128 (2011), pp. 543–548. URL: <https://doi.org/10.1007/s00414-011-0548-7> (cit. on p. 62).
- [Sch09] Lothar Schwarz. “An Amino Acid Model for Latent Fingerprints on Porous Surfaces”. In: *Journal of Forensic Sciences* 54.6 (2009), pp. 1323–1326 (cit. on pp. 7, 140, 141).
- [SKB06] Donald E. Shelton, Young S. Kim, and Gregg Barak. “A Study of Juror Expectations and Demands Concerning Scientific Evidence: Does the ‘CSI Effect’ Exist?” In: *Vanderbilt Journal of Entertainment & Technology Law* 9.2 (2006), pp. 331–368 (cit. on p. 1).
- [She08] Hon. Donald E. Shelton. “The ‘CSI Effect’: Does It Really Exist?” In: *National Institute of Justice Journal* 259 (2008), pp. 1–8 (cit. on p. 1).
- [Shi10] Frank Y. Shih. “Image Enhancement”. In: *Image Processing and Pattern Recognition*. John Wiley & Sons, Ltd, 2010. Chap. 3, pp. 40–62. ISBN: 9780470590416. DOI: 10.1002/9780470590416.ch3. eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470590416.ch3>. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470590416.ch3> (cit. on pp. 39, 104).
- [SGN17] G.B. Slepchenko, T.M. Gindullina, and S.V. Nekhoroshev. “Capabilities of the electrochemical methods in the determination of narcotic and psychotropic drugs in forensic chemistry materials”. In: *Journal of Analytical Chemistry* 7 (2017), pp. 703–709. ISSN: 1608-3199. DOI: <https://doi.org/10.1134/S1061934817070127> (cit. on p. 168).
- [Smi12] Smithsonian. *Ten Inventions Inspired by Science Fiction*. 2012. URL: <http://www.smithsonianmag.com/science-nature/ten-inventions-inspired-by-science-fiction-128080674/> (cit. on p. 1).

- [Sri10] Sargur N. Srihari. “Computing the Scene of a Crime”. In: *IEEE Spectr.* 47.12 (Dec. 2010), pp. 38–43. ISSN: 0018-9235. DOI: 10.1109/MSPEC.2010.5644777. URL: <http://dx.doi.org/10.1109/MSPEC.2010.5644777> (cit. on p. 2).
- [SSG13] Jessica L. Staymates, Matthew E. Staymates, and Greg Gillen. “Evaluation of a drop-on-demand micro-dispensing system for development of artificial fingerprints”. In: *Anal. Methods* 5 (1 2013), pp. 180–186. DOI: 10.1039/C2AY26167G. URL: <http://dx.doi.org/10.1039/C2AY26167G> (cit. on p. 7).
- [Sus+13] Susan M. Ballou et al. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. NIST Interagency/Internal Report (NISTIR) - 7928. U.S. Department of Commerce, 2013. DOI: <http://dx.doi.org/10.6028/NIST.IR.7928> (cit. on pp. 2, 30).
- [SWG20] SWGDAM. *Scientific Working Group on DNA Analysis Methods*. last accessed 04/11/2020. 2020. URL: <https://www.swgdam.org/> (cit. on p. 61).
- [Sze11] Richard Szeliski. *Computer Vision: Algorithms and Applications*. London: Springer London, 2011. ISBN: 978-1-84882-935-0. DOI: 10.1007/978-1-84882-935-0_3. URL: https://doi.org/10.1007/978-1-84882-935-0_3 (cit. on pp. 39, 40, 48, 104).
- [Tao+12] X. Tao, X. Chen, X. Yang, and J. Tian. “Fingerprint recognition with identical twin fingerprints”. In: *PloS one* 7.4 (2012). DOI: <https://doi.org/10.1371/journal.pone.0035704> (cit. on p. 5).
- [TW97] Kai Ming Ting and Ian H. Witten. “Stacking Bagged and Dagged Models”. In: *Proceedings of the Fourteenth International Conference on Machine Learning. ICML '97*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1997, 367–375. ISBN: 1558604863 (cit. on pp. xxi, 43, 44, 152–154, 157, 179).
- [Ule+12] Bradford T. Ulery, R. Austin Hicklin, JoAnn Buscaglia, and Maria Antonia Roberts. “Repeatability and Reproducibility of Decisions by Latent Fingerprint Examiners”. In: *PloS one* 7.3 (2012). DOI: <https://dx.doi.org/10.1371/journal.pone.0032800> (cit. on pp. 46, 47).
- [Vie06] Claus Vielhauer. *Biometric User Authentication for it Security - From Fundamentals to Handwriting*. Springer, Boston, MA, 2006. ISBN: 978-0-387-28094-3. DOI: <https://doi.org/10.1007/0-387-28094-4> (cit. on pp. 38, 47, 105, 113).
- [Wat+07] Craig I. Watson, Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet, and Kenneth Ko. *User’s Guide to NIST Biometric Image Software (NBIS)*. National Institute of Standards and Technology. 2007. DOI: <https://doi.org/10.6028/NIST.IR.7392> (cit. on p. 102).
- [Wat+08] Craig I. Watson, Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet, and Kenneth Ko. *User’s Guide to Export Controlled Distribution of NIST Biometric Image Software (NBIS-EC)*. National Institute of Standards and Technology. 2008 (cit. on pp. 105, 113, 197).

- [Web02] Andrew R. Webb. *Statistical Pattern Recognition*. Second Edition. John Wiley & Sons Ltd, 2002. ISBN: 0-470-84514-7 (cit. on pp. xxii, 41–43).
- [Wer94] Pat A. Wertheim. “Detection of Forged and Fabricated Latent Prints”. In: *Journal of Forensic Identification* 44.6 (1994), pp. 652–681 (cit. on p. 140).
- [Xu+17] M. Xu, J. Feng, J. Lu, and J. Zhou. “Latent fingerprint enhancement using Gabor and minutia dictionaries”. In: *2017 IEEE International Conference on Image Processing (ICIP)*. 2017, pp. 3540–3544. DOI: 10.1109/ICIP.2017.8296941 (cit. on p. 7).
- [Yan+03] Jianwei Yang, Lifeng Liu, Tianzi Jiang, and Yong Fan. “A modified Gabor filter design method for fingerprint image enhancement”. In: *Pattern Recognition Letters* 24.12 (2003), pp. 1805–1817. ISSN: 0167-8655. DOI: [https://doi.org/10.1016/S0167-8655\(03\)00005-9](https://doi.org/10.1016/S0167-8655(03)00005-9). URL: <http://www.sciencedirect.com/science/article/pii/S0167865503000059> (cit. on p. 96).
- [YFJ11] S. Yoon, J. Feng, and A. K. Jain. “Latent fingerprint enhancement via robust orientation field estimation”. In: *2011 International Joint Conference on Biometrics (IJCB)*. 2011, pp. 1–8. DOI: 10.1109/IJCB.2011.6117482 (cit. on p. 7).
- [Zha+17] Mengqiu Zhang, Gang Li, ShaoHui Wang, Zhigang Fu, Yang Guan, and Ling Lin. “The influence of different integration time on stoichiometric analysis in near infrared grating spectrometers”. In: *Infrared Physics & Technology* 86 (2017), pp. 130–134. ISSN: 1350-4495. DOI: <https://doi.org/10.1016/j.infrared.2017.08.018>. URL: <http://www.sciencedirect.com/science/article/pii/S1350449517304632> (cit. on p. 35).

Index

- ACE-V, 18
- Artificial Sweat, 141
- Bagging Ensemble Classifier, 44
- Benford's Law, 45
- Benford's Law-based Features, 103, 149
- Bifurcation, 46
- C4.5 Decision Tree, 43
- Chain-of-Custody, 30
- Chromatic White Light Sensor, 34, 72
- CLSM, 35, 73
- Coarse Scan, 58
- Confocal Laser Scanning Microscope, 35, 73
- Cross Validation, 43
- Crystalline Structure-Based Features, 148
- CWL Sensor, 34, 72
- Dagging Ensemble Classifier, 44
- Data Analysis, 60
- Data Gathering, 57
- Data Investigation, 59
- Daubert Factors, 33
- Detailed Scan, 59
- Digital Assets, 20
- Dot-Based Features, 145
- Drop-on-Demand Ink-Jet, 142
- Error, 66
- Error Rates (Biometrics), 49
- Error Rates (Pattern Recognition), 41
- Feature Selection, 133, 163
- Federal Rules of Evidence, 32
- Final Documentation, 62
- Fingerprint Ridge, 48
- Fingerprint Semantics Features, 102
- Fingerprint Valley, 48
- FTR Sensor, 37, 74
- Gabor Filtering, 40
- Ground Truth, 42, 107
- Halftoning, 142
- Intensity Image, 36
- J48 Decision Tree, 43
- Labeling Data, 107
- Latent Fingerprint Forgery, 140
- Least-Squares-Method, 39
- Likelihood Ratio, 31
- Likelihood Ratio-based Reconstructed Fingerprint Image I_{RLRa} , 121
- Likelihood Ratio-based Reconstructed Fingerprint Image I_{RLRb} , 121
- Logistic Model Trees, 44
- Loss, 65
- Minutiae Point, 46
- Multilayer Perceptron, 44
- Nonporous Substrate, 37
- Normalized Statistics Features, 103
- Operational Preparation, 57
- Optimized Reconstructed Fingerprint Image $I_{R_{optimized}}$, 121
- Physical Acquisition, 56
- Porous Substrate, 37
- Process Accompanying Documentation, 61
- Raw Reconstructed Fingerprint Image $I_{R_{raw}}$, 121
- Real Latent Fingerprint, 140
- Reconstructed Fingerprint Image I_R , 120
- Ridge Ending, 46
- RotationForest Ensemble Classifier, 45

Segregation Feature Space 1, 99
Segregation Feature Space 2, 101
Segregation Feature Space 3, 102
Segregation Feature Space 4, 103
Segregation Feature Space 5, 103
Semantics, 64
SMO Classifier, 43
Sobel Operators, 39
Statistics Features, 99
StirTrace, 81, 185
Structure Features, 101
Substrate Properties, 37
Surface Structure, 38
Surface Texture, 38
Syntax, 64

Topography Image, 36
Trace Analysis, 61
Trace Investigation, 61
Trace Processing, 61

Uncertainty, 66
Unsharp Masking, 39