Robust Steganography for Online Secure Communication with Binary Text Image in JPEG Compressed Domain

Zainalabideen Abdulsamad[1,2], Naseer Aljawad[3] and Athar Ali[3]
[1]*University of Buckingham, Hunter Street Str. 6, MK18 1EG Buckingham, United Kingdom*
[2]*University of Kufa, Najaf Road 115, 54001 Kufa, Iraq*
[3]*Applied Computing Department, University of Buckingham, Hunter Str. 6, MK18 1EG Buckingham, United Kingdom*
naseer.aljawad@buckingham.ac.uk, athar.ali@buckingham.ac.uk

Keywords: Imperceptibility, Robustness, Rich Texture Image, Texture Block, JPEG domain, Visual Artifact.

Abstract: This paper introduces a novel steganography method of secure communication to mitigate the perceptual degradation associated with the quantization process in JPEG compression, particularly when images are recompressed at standard quality levels by potential attackers. Our approach operates within the compressed domain, optimizing the selection of cover images based on the presence of high-texture blocks, thereby enhancing robustness and capacity while avoiding visual artifacts. This technique ensures a high Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) without the common compromise on visual quality. Additionally, our method allows for the retrieval of embedded messages without the need for the original image, making it highly applicable to real-time communication scenarios. Through extensive experimentation, we demonstrate that cover images containing over 80% textured blocks, with blocks selected for embedding having at least two non-zero quantized Discrete Cosine Transform (DCT) coefficients beyond the DC component, significantly improve PSNR values over existing methods while maintaining high payload capacity. The system exhibits robustness against JPEG recompression across a wide range of quality factors (42 to 99) and resilience to various image processing attacks, marking a significant advancement in the field of image compression and secure communication.

1 INTRODUCTION

The need for private and secure communication has become paramount in our ever-digital environment. The skill of concealing data inside a digital file is one alluring way to accomplish this. This technique, known as watermarking or steganography, provides a degree of protection and anonymity in the context of digital communication by enabling the hidden object conveyance of data through seemingly innocuous files. Digital steganography is the science, technique, or art of hiding digital information in a digital object so that no one other than the recipient can feel the actual existence of this information in the given media. The cover object and data can be in any format such as image, audio, video, or text [1]. Watermarking is the technology used to protect files from tampering and forgery. Copyright and property rights require watermarking techniques to indicate ownership and copyright of that file. Although the similarity between watermarking and steganography lies in the concept of hiding something in a digital file, for example, in a digital image, there are also differences between them. The main differences between watermarking and steganography are: 1) the amount of data in watermarking is limited, while steganography hides more data; 2) the robust watermarking technique makes the signature difficult to remove, while in robust steganography the secret message is difficult to detect; and 3) watermarking aims to protect the property, while in steganography it is to protect information[2], [3].

The usual image steganographic techniques are ineffective when used for online services since the images are usually heavily compressed using lossy compression techniques [4], [5], [6].

However, the most robust steganography methods need to send the cover image first before sending the stego image. But sending the same image multiple times gives a chance for the third party to detect the method. For that reason, creating robust steganography methods that do not need to send the cover image in advance is a challenge. In contrast, watermarking images are successful in resisting lossy compression and noise to some extent. However, it is limited in payload capacity since robustness and imperceptibility are the dominant considerations. Thus, it is challenging to present a method that achieves a trade-off between capacity, robustness, and imperceptibility[5], [7].

Therefore, in this paper, we propose a method that balances robustness capacity and imperceptibility.

The steganography and watermarking system can be applied in two domains: spatial and frequency. In both domains the same principle of steganography and watermarking is applied; that is to say, the secret message is embedded in the cover image. However, the way it is embedded is different from domain to domain and from one method to another, and the level of complexity and time is also different.

Several image steganography and invisible watermarking methods are proposed within the frequency domain. This is because the robustness factor supported by the frequency domain prompted researchers to develop their methods in this field. The proposed methods compete with one another in terms of robustness against attacks, quality of host image, and payload capacity. The coefficient values in the frequency domain then are exploited for embedding the secret message while maintaining the image quality. Changing the coefficient value of the frequency domain leads to a change in the image quality in the spatial domain. Some techniques use texture regions for the embedding process because they are robust against image processing manipulation. However, some techniques embed the binary bits in the non-textured regions of the image to increase the payload capacity. Some techniques use either low or high frequency to achieve robustness or high payload capacity. The low-frequency coefficients are more robust against image processing manipulation because they are quantized using low quantization factors. However, maintaining the perceptuality quality of the image by embedding within these coefficients is a challenge. On the other hand, embedding within high-frequency coefficients maintains the perceptuality of the host image but is not robust and may lead to a decreased compression ratio.

2 LITERATURE REVIEW

Although our research work is concerning Steganography, we are in additional researching the watermarking techniques as both present similar digital signal imbedding concepts. In the evolving field of digital watermarking and steganography, researchers have continually sought to balance the imperceptibility, robustness, and payload capacity of their methods. This review synthesizes key contributions from the literature spanning over two decades, reflecting the progression from simple embedding techniques to complex hybrid systems that aim to optimize these critical attributes.

Initially, Lin et al. [8] study enhanced robustness and imperceptibility by employing a mathematical remainder concept for embedding in the luminance component's low-frequency texture blocks. The approach represented significant strides in watermarking technology but also highlighted the ongoing challenge of balancing capacity with image integrity. Further advancements were made by [9], [10]. Who employed Discrete Wavelet Transform (DWT) to improve image quality and robustness. Ansari et al. focused on embedding watermark bits by modifying the largest singular value within each block, a technique complemented by the latter's method, which introduced an embedding strength parameter and a relationship of DCT coefficients for robust watermarking against various attacks, including JPEG compression. An enhancement to the current steganography in the JPEG-compressed domain is proposed In [11]. The embedding process led to the maintenance of compression ratio and image distortion. They successfully created a stego image that closely resembled the original compressed image in some respects. However, they did not conduct a thorough investigation of its robustness against attacks. The quest for imperceptibility led [12] and [13] to explore blind and non-blind watermarking approaches respectively. DCT coefficient blocks for embedding, prioritizing high imperceptibility and partial robustness against specific attacks utilized by [12], while, the median principle for block selection, achieving robustness, particularly against JPEG compression was adopted by [13] . In a significant leap forward, a hybrid watermarking technique combining LSB and DWT methods present in [14]. The study aims to strike a balance between robustness against compression and noise attacks. However, like its predecessors, this method faced limitations regarding payload capacity and security aspects. Most recently, two studies have pushed the boundaries further by incorporating advanced DWT decompositions, SVD transformations, and novel embedding strategies as explained in [15] and [16]. In [15] focused on achieving high imperceptibility and robustness against a range of attacks through a sophisticated DWT and SVD-based nonblind approach, albeit with challenges in compression attack resilience for different quality factors and payload capacity. On the other hand, a steganography method targeting high texture areas in RGB images, leveraging maximum energy pixels for high-capacity embedding proposed in[16]. This method, while showcasing high-quality stego images, acknowledges the need for further development in robustness.

On the other hand. Some methods rely on deep learning rather than traditional approaches.

Hu et al [17]. utilize the noise vector to record the secret message and train the model to generate the non-modification stego image based on secret message information. The model is trained to embed and extract the hidden message from the stego image based on the noise vector. Most non-modification steganography methods show a high potential for hiding information. However, most non-modification steganography methods have produced a low stego image quality in showing which led to the detection and insufficient accuracy in extracting the secret message as pointed out in [18]. For that reason, an improvement by adding an attention mechanism to the GAN model is suggested in [21]. The GAN model is improved using enhanced training techniques. During the image generation process, the attention technique improves the image and removes any artifacts that may appear in the image background by improving the correlation coefficients between image units. The soft margin discriminator improves information extraction and addresses errors during image generation. However, the results of this study indicate progress in information retrieval and stego image quality. The payload capacity is constrained. In addition, no mention of robustness.

To achieve high payload capacity, the high dimensionality of the latent vector of a flow-based generative model is utilized in [19]. The study focused on the invertible recording between the latent vector and image space of the flow-based generative model with the lossless coding to embed and extract the secret message precisely. The hidden message encodes within a high-dimensional latent vector based on a location encoding algorithm to achieve high payload capacity. Despite that, the study achieves high payload capacity due to the utilization of the high dimension of the latent noise vector of the flow-based generative model which is larger than the GAN model. The secret message is retrieved due to the invertible of the flow-based generative. However, robustness is constrained, especially for JPEG compression. In addition, utilizing the latent vector for mapping the secret message without consideration of the effect of different elements' latent vectors on the image quality is a drawback of this method as pointed out by [20].

While a watermarking method against rotation and JPEG compression attacks is suggested in [21]. The method focused on learning the GAN model to embed the watermark in the host image and to improve the quality of the watermarked image within the training stage. The model applied attack simulation to make the extractor able to extract the watermark from an attacked image. However, the model succeeded in learning the watermarked image generator, stego image discriminator, and extractor to extract the watermark blindly. The study considers low embedding capacity, high complexity and not well enough robust against JPEG compression.

Bagheri et al. [22] focus on determining the suitable positions for hosting the watermark bits with consideration of the strength factor principle. They applied the embedding process in the hybrid of DWT and DCT domains. The host image is input to the R-CNN to find the strength factor for generating several important classes. The strength factor of each class is calculated based on the maximum importance coefficient of that class, which is mentioned on the predefined constant scale. The model tries to avoid embedding in the region which has important objects. The blocks which have lower importance are selected as candidate blocks for hosting the watermark bits. However, the strength factor for each block is guaranteed the hosting bit unchanged from attacks by increasing the difference between candidate coefficients. A voting algorithm applied to the fifteen extracted watermark bits increases the chance of extracting the right bits. The study is limited in the payload capacity. In addition, the study is robust against JEG attack for high-quality factors 70,80,90 as the study refers.

A model to find the appropriate areas to add the watermark in the image to achieve high imperceptibility is suggested by [23]. The model is trained through an optimization technique to analyze the image to obtain features of the regions, and then the optimal areas are selected using deep CNN. The feature inputs are used to choose the best region for hiding the watermark while a fitness function is used to address the optimal solution. After identifying the areas of interest in the wavelet sub band transform of the image, the fitness technique is used to hide the watermark in these areas of interest. The study demonstrates a high quality of the watermarked image compared with other existing studies by high PSNR and correlation coefficient. However, the cover image and fitness are necessary in the extraction process. In addition, the study needs to evaluate the complexity because it uses several techniques and mentions the robustness.

An autoencoder steganography method to hide the secret message by taking advantage of the latent space in the encoder offered in [24]. The method encodes both the message and the cover image by two different encoders that produce an equal-sized sample, then the cover image encoder decodes the two samples to generate the stego image, then the noise is added to obtain the required robustness, and the message retrieval process is done by the encoder message, and the method showed good performance in terms of robustness as well as short computational cost, while it lacked image quality preservation as is the case for the automatically trained encoder, and most importantly, it includes limited payload capacity, as the researcher indicated that the process of increasing the payload capacity leads to a decrease in the accuracy of message retrieval and affects the image quality as well.

Recently, Xu et al. [25] try to increase the payload capacity to 250 bits. The method is to pre-process the watermark and combine it with the reduced cover image. The two images are fed into the encoder network MUINT to generate a residual image. This residual image is then resized and added to the original cover image to generate the watermarked image. To obtain robustness, the study added noise to the watermarked image to simulate the attacks to learn the decoder to extract the watermark from the noisy watermarked image. However, the method considers higher payload capacity than the relevant previous studies and achieves robustness. The limitation of this study and the other relevant studies is to produce non-artifact images as mentioned by studies, even though the high quantity results in terms of PSNR and SSIM are obtained by most studies. In addition, the study has a limited payload capacity of only 250 bits.

This literature review highlights a continuous effort in the field to refine and balance the essential qualities of digital watermarking and steganography methods. Despite the significant progress made, the quest for an optimal balance between imperceptibility, robustness, and payload capacity remains a central challenge, driving ongoing research and innovation. Additionally, factors such as sending the original image during the extraction process or sending the stego or watermarked image as a spatial domain image are also considered in research. The authors in [7] mentioned that sending the original image within the stego or watermarked image is highly risky to be detected by an attacker. Also [26] emphasized that the time for extracting a message within the compressed domain is less because it only requires entropy decoding, while the frequency domain requires more calculations for the transformation process.

Even though the deep learning methods tried to present a new method to achieve robustness they lack in capacity or quality, visible artifact. Therefore, we propose to find an optimal host image, the best block for embedding, and the best coefficients within the block, apply an adaptive embedding method, work within the compressed domain, avoid sending the original image, and scramble the binary image. This is to increase payload capacity and achieve robustness, and imperceptibility. Additionally, it allows for a short time for extraction and ensures security when archiving.

3 IMAGE ANALYSIS AND THRESHOLDS

The analysis materials comprise different 16 colour images of 512 512 pixels were collected from the CVG–UGR [27] image databases. The result of an intensive analysis of the images in terms of compression and embedding shows the visual artifacts in most images. Following the JPEG compression process with a standard quality factor is a challenge in terms of the perceptibility of the visual artifact. The reason is that the quantization process in the smooth area of the image produces a visual artifact. In addition, embedding the secret bits in the smooth area leads to visual artifacts. The literature only mentions the visual artifact caused by the embedding process; therefore, researchers try to embed in the texture blocks to some extent. However, there is no mention of the visual artifact caused by compression by applied JPEG standard quality factor SQF.

The result from our experiment shows that the smooth area in the carrier image causes visual artifacts in terms of compression and embedding. On the other hand, rich texture images have high quality after the compression and embedding process in terms of fewer visual artifacts and less reduction in the PSNR value compared to non-rich texture images. Studying and warily evaluating the image using the quantization procedure, we discovered that the quantized macroblock is the only one with a non-zero quantized DC value and all other quantized DCT coefficients are zeros. This results in the flat macroblock following dequantization processes. The reason is the error between quantization and dequantization. Flat macroblock means all values within the block are equal. However, this block before quantization had a low variation over values.

A rich texture image is an image with a lot of details while a non-texture image is when the image looks smooth or has smooth parts. For example, Lenan's shoulder in Lena's image is considered a smooth part which case visual artifact that is changed by the quantization process.

The experiment is run for several thresholds to find the best values for T1 and T2 in terms of quality and robustness. T1 is to determine the proportion of texture blocks within the image. According to the results, an image with more than 80% texture blocks is considered as a rich texture image when the threshold T2 value is 2. The outcome indicates that, at least in part, there is no correlation between robustness or quantity measurements (PSNR and SSIM) and a higher threshold. As a result, there is no justification for selecting a higher threshold because the payload capacity will be constrained below it. Threshold T2 value (2) can balance the factors like robustness, payload capacity and visual artifact. The experiment extends to select the best candidate quantized DCT within texture blocks in terms of robustness and quality.

4 THE PROPOSED SYSTEM

The proposed system is to select an optimal cover image content with a high texture block that follows the standard JPEG process. And to embed the message bits in the texture block within the selected image. As shown in Figure 1, steps 5 to 9 within the box are the proposed system for embedding while the rest outside the box is related to the JPEG process. To ensure security, the embedded watermark or binary text image is scrambled using the Arnold transformation. That is mean without precise info about the scrambling procedure the scrambling binary text image cannot be mended.

4.1 Embedding Algorithm Steps

The embedding procedure is conducted in the following sequence of steps:

Step 1. Select the image from the data set.

Step 2. Convert the carrier RGB image into YCbCr colour space and divide each component of YCbCr (luminance and two chrominances) into non-overlapping blocks with a size of 8by8 blocks called macroblocks.

Step 3. Apply the DCT transform to each macroblock to get the DCT macroblock coefficients. (in row way).

Step 4. Apply the quantized operation to the DCT macroblock coefficients (with SQF). The output is called quantized DCT macroblock coefficients.

Step 5. Select the quantized DCT macroblock from the three components. (Luminance and two chrominances).

Step 6. If the number of non-zero quantized DCT coefficients in the block is lower than two discard this macroblock, go to Step 5, otherwise address the block as texture block and go to Step 7.

Step 7. If the number of texture blocks is equal to or greater than 80% out of the total blocks in the image, address the image as a rich texture image, and go to Step 8 otherwise discard this image and go to Step 1.

Step 8. Select the texture block that contains at least two non-zero quantized DCT coefficients apart from the DC coefficient, two of them are the candidate coefficients for embedding.

Step 9. Perform embedding operations in the block as follows:

$$NDCT = \begin{cases} ODCT, & Wi = 1 \; and \; ODCT \; is \; odd \\ ODCT + 1, & Wi = 1 \; and \; ODCT \; is \; even \\ ODCT + 1, & Wi = 0 \; and \; ODCT \; is \; even' \\ ODCT, & Wi = 0 \; and \; ODCT \; is \; odd \end{cases}$$

where old quantized DCT is the selected quantized DCT before embedding, NDCT is the quantized DCT after embedding and Wi is the corresponding watermarking bit. Each time two watermarking bits Wi and Wi+1 are embedded in two quantized DCT (2,1) and DCT (2,2) respectively. (The two quantized DCT (2,1) and DCT (2,2) should be non-zero before and after embedding as well as the sign of the coefficient is maintained(

Step 10. Repeat Steps 8 to 9 to embed all watermark bits.

Step 11. Finally, the entropy encoding stage is applied to encode the quantized macroblocks DCT coefficients into bitstreams. Image JPEG file format.

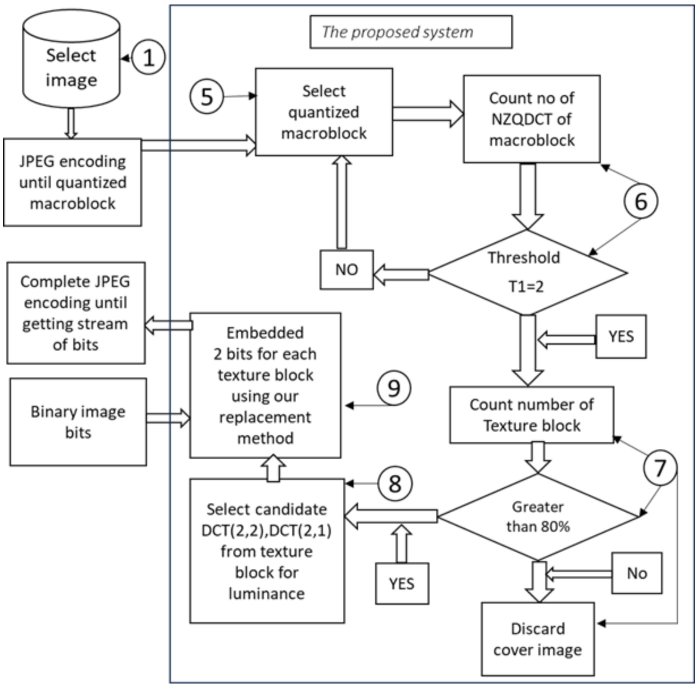
The proposed system
Select image
1
JPEG encoding until quantized macroblock
5
Select quantized macroblock
Count no of NZQDCT of macroblock
6
Threshold T1=2
NO
YES
Complete JPEG encoding until getting stream of bits
Embedded 2 bits for each texture block using our replacement method
9
Binary image bits
Count number of Texture block
7
8
Select candidate DCT(2,2),DCT(2,1) from texture block for luminance
Greater than 80%
YES
No
Discard cover image

Figure 1: The proposed system of selecting rich texture images and embedding process.

4.2 Retrieved Algorithm Steps

The retrieving part of the proposed system is very simple, and it does not need any other information from the original host image. The watermarking bits are retrieved from the compressed image JPEG file format (bitstream) by using the following steps:

Step 1. Decode the stream of bits (compressed image JPEG file format) into de-quantized DCT macroblock coefficients.

Step 2. Select the de-quantized DCT macroblock.

Step 3. If the block is the texture block which contains at least three non-zero quantized DCT coefficients, two of which are the candidate coefficients for extracting, go to Step 4 otherwise discard the macroblock and repeat Step 2.

Step 4. Perform retrieving operations in the block as follows:

$$Wi = \begin{cases} 1, & \text{quantized DCT is odd} \\ 0, & \text{quantized DCT is even} \end{cases}$$

where quantized DCT is the candidate quantized DCT coefficients from the block and Wi is the corresponding scrambling watermarking bit.

Step 5. Repeat Steps 3 and 4 to retrieve all scrambling watermark bits. Finally restore the original watermark by applying the inverse Arnold transformation to the scrambled watermark.

5 PERFORMANCE EVALUATION AND EXPERIMENTAL DISCUSSION

To evaluate the proposed method, the same 16 colour images are investigated images referred to in the previous section 3. While a double binary image IEEE logo with the size of 64×64 bits as the watermark image 128x64 bits. However, four colour images including Lena, Baboon, F16, and Fruit with a size of 512×512 pixels are selected to discuss the proposed system results with other studies in the paper. This is because most studies use these images in their experiment. The proposed system selects the Fruit and Baboon images as the host images and discards Lena and F16. This is because the Baboon and Fruit images are rich texture images, and the percentage of texture blocks is greater or equal to 80%. As we explained in section 3.

5.1 Robustness of the Proposed System

Different types of attacks are investigated in the following experiment to evaluate the robustness of the proposed system. The experiment investigated the spatial host images within the payload capacity of 8192 bits. The Normalized Correlation (NC) value is used to deliver unbiased decisions for the reliability of the proposed system. Figure 2 shows the NC values of extracted watermarks from the host images Lena, Baboon, F16, and Fruit in terms of JPEG compression attack with different quality factors. The NC value 0.99 is considered equal to 1. The missing NC value is related to the inverse operation of the DCT when the host image is converted from the frequency domain to the spatial domain. Results show that the watermark retrieved has approximately full NC values with quality factors starting from 48% up to 99%, the watermark retrieved has average NC values around 0.90 for a quality factor 42% up to 47% and the watermark retrieved has average NC values over 0.80 for a quality factor 35% up to 42%. However, it is difficult to recognize a watermark retrieved within a quality factor of 35% up to 41%. In addition, a watermark retrieved with lower than 35% cannot be recognized and has an NC value lower than 80. Furthermore, the result shows that a rich texture image such as Baboon and Fruit has the highest average NC values over all random quality factors.

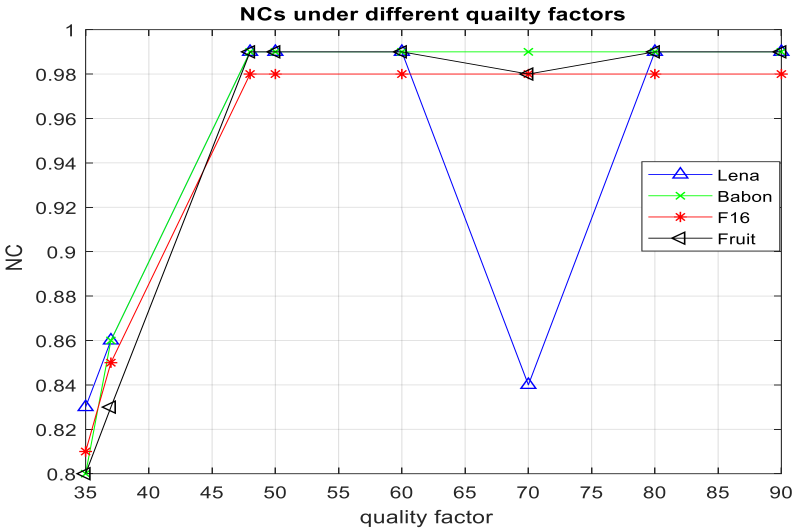

Figure 2: The NC values of the proposed system against JPEG compression for different quality factors.

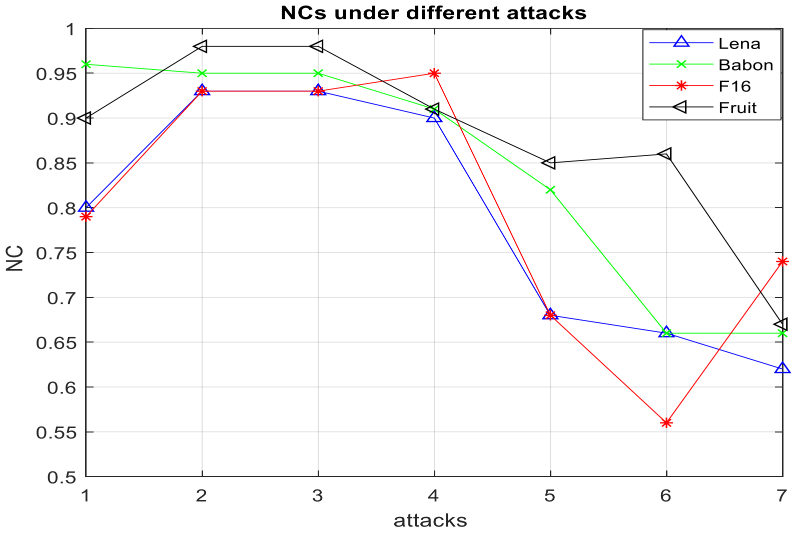

Figure 3: The NC values of the proposed system of common image processing attacks: 1) Salt and Pepper, 2) Emotion, 3) Sharp, 4) Gaussian, 5) Histogram, 6) Rotation 0.15, 7) Rotation 0.25.

The result from Figure 3 shows that the Baboon and Fruit images have the highest NC values for most types of attacks while Lena and F16 come later. The average PSNR due to attacks for images Baboon and Fruit (24.1 and 28.9) are lower than both images Lena and F16 (31.2 and 30.4). The average NC value of Baboon and Fruit is 0.84 overall image processing attacks. However, the average NC value for Lena is 0.78 and for F16 is 0.77. In addition, the retrieved watermark is more recognizable for these images within this type of attack. In addition, as shown in Figure 3 the watermark retrieved from both images Baboon and Fruit have the highest total average of NC values too. This is because these images are considered rich texture images with over 80% of texture blocks. As we mentioned in section 3 our investigation that rich texture images are robust against compression.

As a result, the proposed system can achieve acceptable robustness against random quality factors from 42 to 99 and against image processing attacks to some extent by selecting rich texture images such as Baboon and Fruit. The proposed system is considered limited in terms of rotation and histogram attack. This is because of the high reduction in the PSNR of host images due to the rotation attack. However, the NC values for images Baboon and Fruit are acceptable with rotation attack 0.15 degree (0.80 and 0.85) respectively and the NC values for Fruit image against histogram equalization is NC value 0.85.

5.1 The Proposed System Compared to Other Studies

The proposed system is compared with the existing methods as shown in Table 1. The result is that the proposed system provides a high payload capacity compared to the other methods, and the existing methods produce a lower quality (PSNR) compared to the proposed system except [12], [13], [14],[25] studies, as shown in the table. The reason is that the proposed system makes less change to the coefficient value within the embedding process and selects a rich texture image that supports more texture blocks for embedding. However, other methods apart from [12], [13], [14], [25] studies significantly alter the coefficient value through the embedding process.

5.2 Robustness and Functional Advantages

Even though the study [25] has a higher PSNR but lacks visual artifacts, there is no guarantee for generating a non-visual artifact watermarked image, as the author mentions. The proposed system idea is to deliver a non-visual artefact watermarked or stego image based on selecting a rich texture image. In addition, the study [25] proves robustness against jpeg compression for only quality factor QF(50) while our proposed for different quality factors. The study [21] has a robustness value (BER=0.08) for JPEG attacks with QF(50), while the proposed system has (0.0). The method in [19], has robustness (NC=0.80) against JPEG attacks for only QF (90), however, our proposed system has (NC=1) for QF(50 up to 99). In [22] the robustness is discussed against JPEG only for QF (70,80 and 90). In addition, The method in [14] showed a robustness against JPEG compression with QF (55,75 and 95) only. Although [12], [13] studies have a high PSNR compared to the proposed system. However, the proposed system has a higher payload capacity than the two studies. The proposed system proves robustness against JPEG compression with different quality factors while there is no reference to this type of robustness in the [12]. In addition, the proposed system does not need the original image in the retrieving process while [13] needs the original image.

Table 1: The comparison between the proposed system and other studies in terms of the PSNR and capacity.

Methods	Capacity, (bits)	PSNR(DB)
[25]	250	N\A
[24]	100	33
[14]	2048	30-40
[12]	1024	45
[13]	512	43
[10]	4096	33.2
[8]	1024	31.4
Proposed system	8192	35.13

The proposed system is better than Lin et al. [8] study in terms of PSNR and capacity for four images Lena, Baboon, F16 and Fruit. However, the robustness in [8] is greater when compared to our method. In addition, the extracted part of the [8] study needs two key parameters. However, the extracted part of the proposed system does not need any further information. The proposed system achieves the same robustness for a jpeg compression attack with a random quality factor greater than 42%.

6 CONCLUSIONS

It is concluded that the rich host image recommended by the proposed system achieves high imperceptibility, avoids visual artifacts, and has a greater payload capacity range (1-8192) compared to other studies. It also has high robustness against JPEG compression for random quality factors (42-99), with acceptable robustness against common image processing attacks except for rotation higher than 0.20 degrees and histogram. In the extraction process, the proposed system needs only a run-length encoding process to retrieve the secret message, it works in a compressed domain. The binary text image is used as the secret message for steganography while the binary image logo for watermarking. This is because the binary text image or logo can be noticed in case of any modification. The number of characters in the binary text image is based on the font size used.

In the state of the arts. The proposed system outperforms most old and recent studies including traditional and deep learning as shown in Table 1. In comparison with deep learning steganography or watermarking methods, the proposed system is better than [25], and [24] in payload capacity and non-visual artefacts. And better than [19], and [21] in robustness against JPEG compression. Even though the study [22] works in a non-blind strategy, the proposed system works as blind and showing robustness against JPEG only for higher QF.

The proposed system is tested in real-world applications such as email and Facebook. The stego image is uploaded within Facebook and by email, and the binary text image is retrieved truly from the receiver side. As a result, the proposed system can be used in these online applications to exchange vital information in secure communication.

The limitations of the proposed system are robustness against rotation and histogram equalization. The traditional way of selecting the rich texture image as a cover image and selecting texture for embedding. The payload capacity.

For future work, more real-world applications need to be investigated. An investigation of the Deep learning technique to create a model in terms of selecting a rich texture image and selecting a texture block. Increasing the payload capacity and robustness against random noise and histogram.

REFERENCES

[1] A. Z. Al-Othmani, A. A. Manaf, and A. M. Zeki, "A survey on steganography techniques in real time audio signals and evaluation," Int. J. Comput. Sci. Issues IJCSI, vol. 9, no. 1, p. 30, 2012.

[2] M. B. Pope, M. Warkentin, E. Bekkering, and M. BSchmidt, "Digital Steganography—An Introduction to Techniques and Tools," Commun. Assoc. Inf. Syst., vol. 30, no. 1, Art. no. 1, 2012.

[3] N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in International Workshop on Information Hiding, Springer, 1998, pp. 273-289.

[4] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," Information, vol. 11, no. 2, Art. no. 2, 2020.

[5] A. Bahrushin, G. Bahrushina, and R. Bazhenov, "Robust to JPEG Compression Image Watermarking Scheme Based on Even-Odd Modulation and Error-Correcting Codes," in 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), IEEE, 2018, pp. 1-6.

[6] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, and N. Yu, "Robust adaptive steganography based on generalized dither modulation and expanded embedding domain," Signal Process., vol. 168, p. 107343, 2020.

[7] J. Zhang, X. Zhao, and X. He, "Robust JPEG steganography based on the robustness classifier," EURASIP J. Inf. Secur., vol. 2023, no. 1, p. 11, Dec. 2023, [Online]. Available: https://doi.org/10.1186/s13635-023-00148-x.

[8] S. D. Lin, S.-C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," Comput. Stand. Interfaces, vol. 32, no. 1, Art. no. 1, Jan. 2010, doi: 10.1016/j.csi.2009.06.004.

[9] I. A. Ansari, M. Pant, and C. W. Ahn, "ABC optimized secured image watermarking scheme to find out the rightful ownership," Optik, vol. 127, no. 14, pp. 5711-5721, 2016.

[10] M. Moosazadeh and G. Ekbatanifard, "An improved robust image watermarking method using DCT and YCoCg-R color space," Optik, vol. 140, pp. 975-988, 2017.

[11] R. A. Watheq, F. Almasalha, and M. H. Qutqut, "A new steganography technique using JPEG images," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 11, Art. no. 11, 2018.

[12] R. R. Kishore, "A novel and efficient blind image watermarking in transform domain," Procedia Comput. Sci., vol. 167, pp. 1505-1514, 2020.

[13] S. Sharma, J. J. Zou, and G. Fang, "A Novel Signature Watermarking Scheme for Identity Protection," in 2020 Digital Image Computing: Techniques and Applications (DICTA), Nov. 2020, pp. 1-5, [Online]. Available: https://doi.org/10.1109/DICTA51227.2020.9363396.

[14] S. E. Ghrare, A. A. M. Alamari, and H. A. Emhemed, "Digital Image Watermarking Method Based on LSB and DWT Hybrid Technique," in 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), IEEE, 2022, pp. 465-470.

[15] M. Begum et al., "Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness," Algorithms, vol. 17, no. 1, Art. no. 1, Jan. 2024, [Online]. Available: https://doi.org/10.3390/a17010032.

[16] R. Shmueli, D. Mishra, T. Shmueli, and O. Hadar, "A novel technique for image steganography based on maximum energy seam," Multimed. Tools Appl., Feb.

2024, [Online]. Available: https://doi.org/10.1007/s11042-024-18476-6.

[17] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," IEEE Access, vol. 6, pp. 38303-38314, 2018.

[18] C. Yu, D. Hu, S. Zheng, W. Jiang, M. Li, and Z. Zhao, "An improved steganography without embedding based on attention GAN," Peer--Peer Netw. Appl., vol. 14, no. 3, pp. 1446-1457, May 2021, doi: 10.1007/s12083-020-01033-x.

[19] Z. Zhou et al., "Secret-to-image reversible transformation for generative steganography," IEEE Trans. Dependable Secure Comput., 2022, Accessed: Jun. 08, 2024, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9931463/.

[20] Z. Zhou et al., "Latent vector optimization-based generative image steganography for consumer electronic applications," IEEE Trans. Consum Electron., vol. 70, no. 1, pp. 4357-4366, 2024.

[21] I. Hamamoto and M. Kawamura, "Neural watermarking method including an attack simulator against rotation and compression attacks," IEICE Trans. Inf. Syst., vol. 103, no. 1, pp. 33-41, 2020.

[22] M. Bagheri, M. Mohrekesh, N. Karimi, S. Samavi, S. Shirani, and P. Khadivi, "Image watermarking with region of interest determination using deep neural networks," in 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, 2020, pp. 1067-1072.

[23] S. Ingaleshwar, N. V. Dharwadkar, and J. D., "Water chaotic fruit fly optimization-based deep convolutional neural network for image watermarking using wavelet transform," Multimed. Tools Appl., vol. 82, no. 14, pp. 21957-21981, Jun. 2023, [Online]. Available: https://doi.org/10.1007/s11042-020-10498-0.

[24] T. Bui, S. Agarwal, N. Yu, and J. Collomosse, "Rosteals: Robust steganography using autoencoder latent space," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2023, pp. 933-942.

[25] R. Xu et al., "InvisMark: Invisible and Robust Watermarking for AI-generated Image Provenance," Nov. 19, 2024, arXiv: arXiv:2411.07795, [Online]. Available: https://doi.org/10.48550/arXiv.2411.07795.

[26] M. Fallahpour and D. Megías, "Flexible image watermarking in JPEG domain," in 2016 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), IEEE, 2016, pp. 311-316.

[27] "CVG - UGR - Image database," Accessed: Mar. 29, 2025, [Online]. Available: https://ccia.ugr.es/cvg/dbimagenes/.