An Optimal Parameters and Initial Values Selection Approach for a New Image Encryption Chaotic System

Sura Hasballah Shnawa, Emad Abdul Kareem and Sadiq A. Mehdi
Department of Computer Science, College of Education, Al-Mustansiriyah University, 10052 Baghdad, Iraq
suraahassaballah@gmail.com, mmimad72@uomustansiriyah.edu.iq, sadiqmehdi71@uomustansiriyah.edu.iq

Keywords: Image Encryption, 7D Chaotic System, Simulated Annealing, Chaos-based Cryptography, Hyperchaotic System, Security Analysis.

Abstract: With the rapid escalation of cybersecurity threats, the demand for robust and efficient encryption techniques to secure sensitive visual data has become increasingly critical. Conventional algorithms such as AES and DES, although widely used, exhibit limitations when applied to digital images due to their high computational overhead and inadequate adaptability to the intrinsic characteristics of visual content. This study introduces a novel image encryption scheme grounded in chaotic systems, incorporating an optimized selection mechanism for system parameters and initial conditions to enhance both security and computational performance. Leveraging the inherent properties of chaotic dynamics - such as extreme sensitivity to initial states and pseudo-random behavior - the proposed approach achieves high levels of confusion and diffusion. Experimental evaluations confirm that the encrypted images exhibit uniform histogram distributions, effectively concealing visual structures and thwarting statistical analysis. Entropy measurements ranged from 7.9993 to 7.9998, indicating an exceptionally high degree of randomness. Furthermore, correlation analysis revealed a substantial reduction in adjacent pixel correlation, with values between -0.0003 and -0.0025, signifying strong decorrelation and noise-like behavior in the encrypted outputs. The method also demonstrated strong resilience against differential attacks, achieving a 100% NPCR (Number of Pixels Change Rate), underscoring its sensitivity to minor input alterations. UACI (Unified Average Changing Intensity) values ranged from 33.48% to 33.50%, highlighting the algorithm’s effectiveness in uniformly diffusing changes throughout the image. In terms of efficiency, the proposed system outperforms traditional methods by offering reduced encryption and decryption times, rendering it highly suitable for contemporary digital environments where both security and performance are paramount.

1 INTRODUCTION

With the rapid advancement of digital communications, the instantaneous transmission of diverse data types - such as images, documents, speech, and video - over shared frequency bands has introduced a host of significant security vulnerabilities [1], [2], [3]. Digital images, in particular, are critical assets in various domains including information exchange, authentication, remote sensing, satellite imagery, medical diagnostics, and military operations. Their widespread use and inherent characteristics make them a prime target for cyberattacks, thereby necessitating robust cryptographic techniques to prevent unauthorized access [4], [5].

Encryption, as a core security mechanism, transforms digital content into an unreadable format that can only be reverted by an authorized party. This process is vital for preserving essential security attributes such as confidentiality, authenticity, integrity, and non-repudiation [6], [7]. However, the nature of multimedia files poses unique challenges: the large data volume, high redundancy, and strong correlations between neighboring pixels render conventional algorithms - like the Advanced Encryption Standard (AES) - inefficient, particularly in dynamic and resource-constrained environments [8], [9], [10], [11]. These limitations have spurred the exploration of alternative approaches better suited to the complex nature of image data. In this context, chaotic systems have emerged as a promising alternative for image encryption. Owing to their inherent properties - extreme sensitivity to initial conditions, pseudo-random behavior, and deterministic dynamics that paradoxically emulate randomness - chaotic systems naturally align with the cryptographic requirements for robust security [1], [12]. The inception of chaos theory in computational systems, pioneered by Edward Lorenz in 1963 [13], catalyzed significant research into chaos-based cryptosystems over the past decades. These systems harness properties such as high data resilience, sensitivity to minute perturbations, and noise-like signals to achieve effective diffusion and confusion mechanisms, which are critical for safeguarding data [7], [8]. Furthermore, high-dimensional chaotic functions, such as those derived from the logistic map, have been shown to provide enhanced resistance against cryptanalytic attacks by significantly expanding the key space and complicating the underlying system dynamics [13], [11], [14].

In the current era of digital transformation, the need for secure and efficient cryptographic methods is more pronounced than ever. While traditional cryptographic techniques continue to serve as a foundational security layer, their inflexibility often limits their application in scenarios requiring dynamic and scalable protection frameworks. Recent studies have increasingly highlighted the potential of chaotic systems to bridge this gap, leveraging their unpredictability and acute sensitivity to initial conditions to overcome the inherent challenges of multimedia data encryption [15], [16], [17]. Early work in chaos-based image cryptography focused on obfuscation and diffusion mechanisms for concealing sensitive information. Notably, Fridrich introduced a general architecture for image encryption based on two-dimensional chaotic maps in 1998, influencing subsequent schemes [1]. Despite these advancements, the selection of system parameters and initial values remains acritical challenge. without a systematic optimization process, they often fail to meet the necessary sensitivity thresholds. Such suboptimal choices can lead to recurring patterns or vulnerabilities that undermine the security of the system [18]. Addressing this issue, Alvarez and Li (2006) emphasized the imperative of aligning the intrinsic properties of chaotic systems with the fundamental requirements of cryptography. They argued that the meticulous selection of initial values and system parameters is essential to maximize both obfuscation and diffusion during the encryption process [4]. In a similar vein, Chen et al. (2004) demonstrated that the use of multidimensional chaotic maps can significantly expand the available key space and increase system complexity, thereby effectively impeding quantitative analysis and differential attacks aimed at uncovering the original information [5].

To address the limitations inherent in existing chaos-based encryption schemes - particularly those stemming from arbitrary parameter selection and insufficient sensitivity - this work introduces a novel approach that combines a high-dimensional chaotic system with an automated parameter optimization mechanism. Specifically, we propose a new seven-dimensional (7D) autonomous chaotic system designed to exhibit complex dynamical behavior suitable for cryptographic applications. To maximize the randomness and unpredictability of the generated sequences, we integrate a Simulated Annealing (SA) algorithm for the systematic optimization of both system parameters and initial conditions. This hybrid methodology ensures that the generated chaotic sequences possess high Lyapunov exponents, entropy, and diffusion characteristics, thereby significantly enhancing the security of image encryption. Unlike prior approaches that rely on heuristic or manually tuned configurations, our method ensures a mathematically grounded, high-performance solution with resilience against statistical and differential attacks. The proposed system, therefore, represents a substantial step forward in designing robust and efficient cryptographic frameworks for secure image transmission in multimedia environments

2 RELATED WORK

Researchers focus on the chaotic systems of image encrypting and decryption processes.

One method integrates a 4D chaotic system with DNA coding. It involves two stages: first, pixel positions are rearranged using chaotic sequences; second, an XOR operation is applied between the scrambled image and DNA-coded data to produce the final encrypted image. The greatest entropy value is 7.9987, UACI of 33.0203 percent and NPCR of 99.6436%. N. N. Jasem and S. A. Mehdi [19] proposed a new cipher algorithm that exploits a hyper six-dimension chaotic system. The algorithm combines switching, randomization, XOR operations, diffusion in a number of phases to warrant robust cryptography. Shahna and Mohamed [19] proposed a grayscale image encryption method based on the Z-order curve and the Logistic Map. The image is first scrambled using the Z-order curve and then encrypted with a key stream generated from the Logistic Map. The method has an entropy of 7.9972, a UACI of 33.5124%, an NPCR of 99.6713%, and an encryption time of 0.52619 seconds. Budiman et al. [20] proposed an encryption scheme that combines two chaotic methods and two hash functions. The first approach relies on rotation and region-wise partitioning algorithms, which are based on plaintext and hash keys, to provide local encryption for each region of the image. The second approach uses a logistic map to implement overall image encryption. The proposed model consists of two stages: in the first stage, the chaotic method is applied to each region of the image to achieve confusion, while in the second stage, it is used to achieve diffusion. However, the researchers did not specify the encryption time for the proposed method.

Li et al. [21] A novel chaotic map is presented, which is based on a real-time variable logistic map with a randomly chosen decimal. This chaotic mapping is used to encrypt images. Several simulations indicate that the novel encryption technique may produce a securely encrypted image with low time complexity. The greatest entropy value is 7.9979, while the highest values of UACI and NPCR are 33.47 percent and 99.62%, respectively. While encryption speed is 0.0386 (second).

3 PROPOSED METHOD

We propose a new chaotic-based encryption scheme that utilizes an optimal parameter selection mechanism to enhance security and performance. The proposed approach integrates a chaotic map with a rigorous selection process for initial values, ensuring robustness against statistical and cryptanalytic attacks. By leveraging the advantages of chaotic behavior, our method achieves high sensitivity, diffusion, and confusion properties essential for secure image encryption, As Show in Figure 1 and Figure 2.

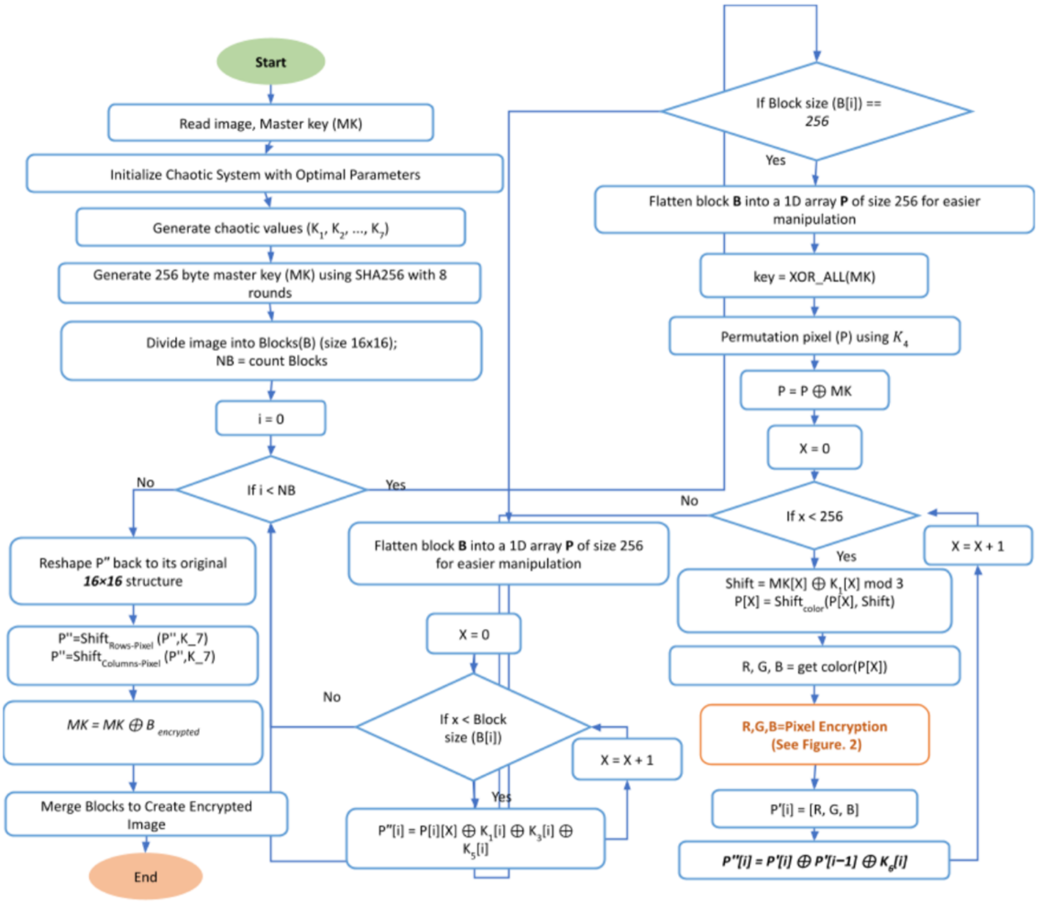

Start
Read image, Master key (MK)
Initialize Chaotic System with Optimal Parameters
Generate chaotic values (K1, K2, ..., K7)
Generate 256 byte master key (MK) using SHA256 with 8 rounds
Divide image into Blocks(B) (size 16x16); NB = count Blocks
i = 0
If i < NB
No
Yes
Reshape P" back to its original 16×16 structure
P"=Shift Rows-Pixel (P",K_7)
P"=Shift Columns-Pixel (P",K_7)
MK = MK ⊕ B encrypted
Merge Blocks to Create Encrypted Image
End
If Block size (B[i]) == 256
Yes
Flatten block B into a 1D array P of size 256 for easier manipulation
key = XOR_ALL(MK)
Permutation pixel (P) using K4
P = P ⊕ MK
X = 0
If x < 256
No
Yes
X = X + 1
Shift = MK[X] ⊕ K1[X] mod 3
P[X] = Shift color(P[X], Shift)
R, G, B = get color(P[X])
R,G,B=Pixel Encryption (See Figure. 2)
P'[i] = [R, G, B]
P"[i] = P'[i] ⊕ P'[i−1] ⊕ K6[i]
Flatten block B into a 1D array P of size 256 for easier manipulation
X = 0
If x < Block size (B[i])
No
Yes
X = X + 1
P"[i] = P[i][X] ⊕ K1[i] ⊕ K3[i] ⊕ K5[i]

Figure 1: Detailed diagram of the proposed image encryption algorithm encryption algorithm.

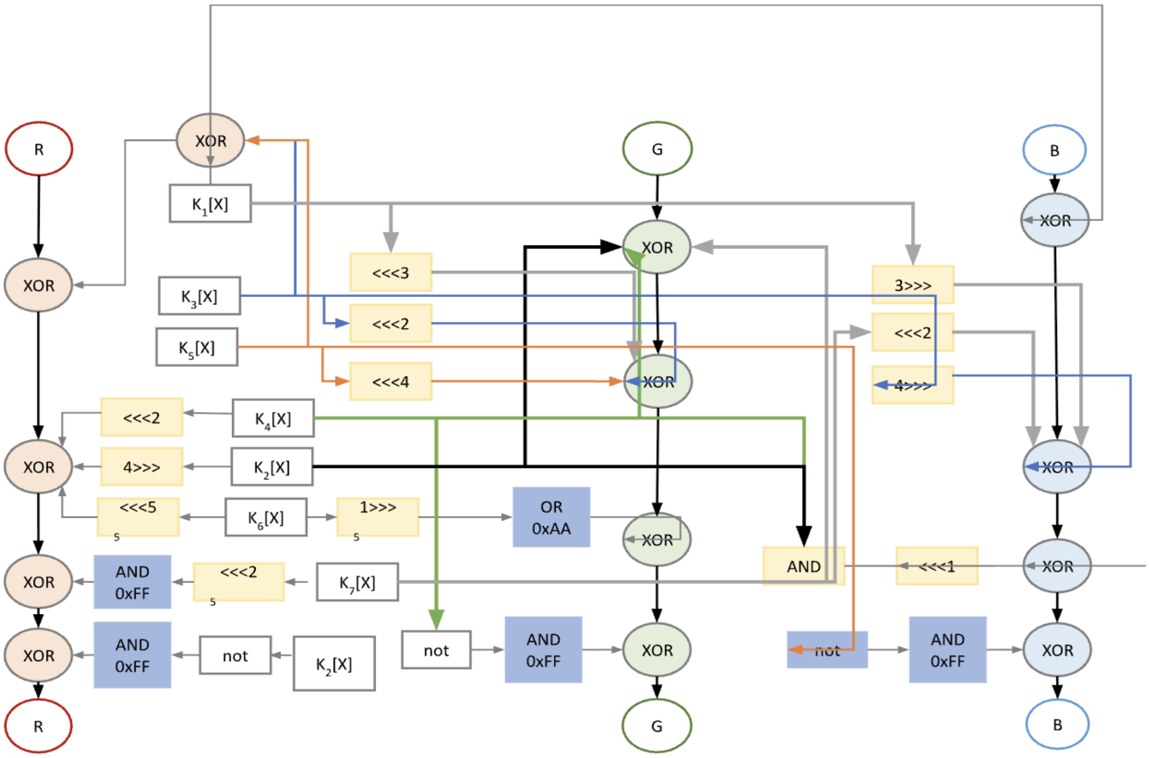


Figure 2: Schematic diagram of the pixel encrypting scheme of the proposed image encryption algorithm.

3.1 A New 7D-Chaotic System

The focal goal is to generate a mathematical model that represents a new chaotic system. The new 7D autonomous system is shown below (1):

$$\frac{dx_1}{dt} = -a\,x_1 + b\,x_2 + c\,x_4 - d\,x_3x_5 - x_3x_7$$
$$\frac{dx_2}{dt} = -e\,x_2 + f\,x_1 - g\,x_5 - h\,x_1x_3 + c\,x_3x_4$$
$$\frac{dx_3}{dt} = -i\,x_3 + d\,x_5 + g\,x_7 + x_1x_2 - x_2x_4$$
$$\frac{dx_4}{dt} = -x_4 + x_5 + d\,x_6 - j\,x_2x_3 - k\,x_5x_7 \qquad (1)$$
$$\frac{dx_5}{dt} = -h\,x_5 + d\,x_1 - d\,x_3 + x_2x_7 + x_6x_7$$
$$\frac{dx_6}{dt} = -\,l\,x_6 - x_2 + x_5 + m\,x_1x_7 - n\,x_3x_4$$
$$\frac{dx_7}{dt} = -\,e\,x_7 + j\,x_3 - dx_5 + h\,x_1x_2 + x_4x_5.$$

Where the system statuses are $x\_1, x\_2, x\_3, x\_4, x\_5, x\_6, x\_7$ and the system positive parameters are $a, b, c, d, e, f, g, h, i, j, k, l, m$ and n.

The proposed system Eq.(1) exhibit a chaotic system based on a strange attractor when system parameter values are selected as:

$$a = 15, b = 13, c = 0.4, d = 0.5, e = 14, f = 38, g = 1.5, h = 2, i = 6, j = 3, k = 5, l = 15.1, m = 30 \text{ and } n = 4.$$

We take the initial conditions as:

$$x\_1\ (0) = 5, x\_2\ (0) = 0.7, x\_3\ (0) = 3, x\_4\ (0) = 10, x\_5\ (0) = 0.2, x\_6\ (0) = 0.1 \text{ and } x\_7\ (0) = 0.6.$$

3.2 Optimal Generator for Chaotic Parameter

Simulated Annealing (SA) algorithm is used as one of the metaheuristic search techniques to find optimal solutions in nonlinear dynamical systems. In this work, SA is applied to optimize the parameters of a complex chaotic system, by optimizing chaos indices such as Lyapunov exponent, entropy, eigen variance, and space coverage.

The Simulated Annealing algorithm is based on the principle of gradual cooling of acceptance rates, so that random modifications that improve performance or even some worse modifications are accepted according to a specified probability, which prevents stopping at local minimum. The main steps are:

A) Initialization of the system:
1) Choose initial values for the system parameters and initial conditions.
2) Calculate initial values for chaos indices.

B) Random update of parameters:
1) Slightly modify the values of the parameters using a random distribution Uniform Distribution.
2) Slightly change the initial conditions.

C) Evaluate chaos of the new system. Calculate chaos indices for the modification system (Lyapunov exponent, entropy, autocovariance, etc.).

D) Decision to accept or reject:
1) If the new solution is better, it is adopted.
2) If the solution is worse, it is adopted according to a probability that depends on the degree of cooling.

E) Iteration until reaching the minimum temperature or the maximum number of iterations.

3.3 Methodology

The Simulated Annealing algorithm is based on the annealing principle in materials science, where a material is gradually cooled to reach a more stable structure. In this context, this idea is used to optimize the parameters of a chaotic system by gradually searching for the best values that achieve maximum chaos and randomness.

A) Primary system:
1) An initial chaotic system is created with default parameters and specified initial conditions.
2) The chaotic solution of the system is calculated using its mathematical equations.
3) The level of chaos is evaluated.

B) Improving transactions using Simulated Annealing (SA) Implementing the SA algorithm involves the following steps:
1) Initialize the basic variables of the algorithm:
   - Set the initial temperature T=1.0.
   - Set the minimum temperature $T\_(min\ ) = 0.00001$.
   - Set the cooling rate α = 0.9.
   - Set the maximum number of iterations max iter = 1000.
2) Save the best initial solution based on the randomness of the system.
3) Start the search loop for the best solution:
   - In each iteration, the system is cooled by updating the temperature value according to the equation:
   - $T = T \times \alpha$.
   - Randomly modify parameter values within a specified range:

$$new_{param} = \frac{old_{param}}{times(1 + r)}.$$

Where(r) is a random number in the range [-0.1, 0.1].

   - Randomly change the initial conditions of the chaotic system to maintain diversity in the search.
   - Evaluate the new chaotic system by calculating the chaos indices and checking whether the performance has improved.
   - Accept or reject the new solution based on the Boltzmann criterion:

$$P = \ e\hat{}(\Delta S/T).$$

Where ΔS is the difference between the randomness level of the new solution and the current solution.

   - Update the best solution if the new solution is better than the previous one.
4) Stop the algorithm when the minimum temperature is reached or when the solution does not improve for a certain number of iterations.

3.4 Final Evaluation Results and Parameter Optimization

This section presents a comprehensive evaluation of the chaotic system before and after optimizing its parameters and initial conditions. The optimization process was carried out using the Simulated Annealing (SA) algorithm, aiming to enhance the system's chaotic behavior and randomness. as shown in Table 1.

1) Original System Parameters.Before optimization, the chaotic system was characterized by the following parameter values:
2) $a = 15,\ b = 13,\ c = 0.4,\ d = 0.5,\ e = 14,\ f = 38,\ g = 1.5,\ h = 2,\ I = 6,\ j = 3,\ k = 5,\ l = 15.1,\ m = 30,\ and\ n = 4.$

The initial conditions of the system were set as follows:

$x_1(0) = 5, x_2(0) = 0.7, x_3(0) = 3, x_4(0) = 10, x_5(0) = 0.2, x_6(0) = 0.1, and\ x\_7\ (0) = 0.6.$

3) Optimized System Parameters. Following the optimization process, the parameter values were adjusted to enhance the chaotic properties of the system:

$a = 17.8155,\ b = 13.3657,\ c = 0.4258,\ d = 0.4675,\ e = 13.2520,\ f = 48.7489,\ g = 1.4050,\ h = 1.8502,\ I = 6.3114,\ j = 3.2472,\ k = 5,\ l = 15.1000,\ m = 30,\ and\ n = 3.7520.$

The optimized initial conditions were determined as:

$$x\_1\ (0) = 3.8997,$$
$$x\_2\ (0) = 0.8618, x\_3\ (0) = 2.5929,$$
$$x\_4\ (0) = 8.8134,$$
$$x\_5\ (0) = 0.1243, x\_6\ (0) = 0.0768\ and$$
$$x\_7\ (0) = 0.4294.$$

These modifications led to a more robust chaotic system, Lyapunov exponents, and overall randomness, as evaluated through the designated chaos metrics. The enhancement of these parameters signifies an increased sensitivity to initial conditions, which is a fundamental characteristic of chaotic behavior.

This table provides a comprehensive overview of the changes in the system after applying the Simulated Annealing algorithm to optimize the parameters of the chaotic system, highlighting the significant improvements in the properties of chaos and stability of the system:

- Positive Lyapunov exponent. This is one of the most important indicators for measuring chaos in a system; an increase of 412% indicates an improved ability of the system to generate complex and unpredictable dynamics.
- Larger Lyapunov exponent. Increasing this indicator indicates an increased sensitivity of the system to initial conditions, making the system more dynamically complex.
- Autocovariance. Increasing this measure shows that the system has become more stable in reducing redundancy and predictability in signals, which improves the quality of chaos used in encryption.
- Key coefficients (a, e, f, i). Large changes in these coefficients confirm their importance in determining the behavior of a chaotic system, as their changes have led to improved dynamic performance of the system.

Table 1: Results of applying SA algorithm to chaotic system.

Metric	Description	Results before optimization	Results after optimization	Comments
Total score	Aggregated measure of the system’s overall chaotic behavior	2836.1739	14355.0730	An increase of approximately 412% indicates a significant enhancement in dynamic complexity.
Maximum lyapunov exponents	Reflects the system's sensitivity to initial conditions, representing the divergence rate	474.1663	2292.3390	A higher exponent suggests increased sensitivity and more intricate chaotic dynamics.
Sum of positive lyapunov exponents	Sum of all positive exponents, indicating the overall intensity of chaotic behavior	2800.0934	14351.3795	The substantial increase confirms a marked improvement in the system's chaotic intensity.
Autocorrelation decay rate	Measures how quickly correlations decay, signifying the reduction of periodic or repeating patterns	0.0072	0.0105	A faster decay rate suggests fewer repeating patterns, leading to more effective randomness in the system.
Phase space coverage	Evaluates the extent of state-space exploration, reflecting diversity in dynamic behavior	0.0194	0.0043	Lower coverage post-optimization could point to a more concentrated chaotic behavior, optimizing system output.

3.5 Image Encryption Algorithm Using the Optimized 7D-Chaotic System

The proposed algorithm relies on a multidimensional chaotic system to generate non-cyclic encryption keys, which adds a high level of security against conventional attacks, such as brute force and frequency analysis. To achieve higher encryption efficiency, the initial values of the chaotic system are optimized using the Simulated Annealing algorithm, the mechanism of which was explained in the previous section, where its results are used to initialize the chaotic system before starting the encryption process. The encryption process is based on dividing the input image into small blocks of size 16 * 16, so that each block is encrypted independently using different combinations of chaotic values. This approach aims to enhance the algorithm's resistance to various attacks while maintaining performance efficiency and increasing the complexity of reverse analysis of encrypted data. Figure 1 shows the detailed diagram of the proposed image encryption algorithm. The encryption scheme consists of several sequential stages to ensure a high degree of security and complexity in the image encryption process. The scheme relies on the use of chaotic systems to generate random keys and transform the image in a way that makes it difficult to decrypt without knowing the keys and details used.

3.5.1 Encryption Stage

The encryption process goes through several stages to ensure that the image is encrypted effectively. These stages include:

A) Initialization Stage:
   1) The original image is entered, its dimensions are analyzed and then converted into a one-dimensional pixel array.
   2) Inputting the master key.
   3) Initializing the chaotic system with the initial values resulting from the optimization process.

B) Image division stage into blocks: The image is divided into small blocks with dimensions of 16×16 pixels using Algorithm 1, which facilitates the implementation of chaotic operations and achieves a higher degree of security.

Algorithm 1: Divide Image into Blocks.

```
Input        I: Plain image.
             B: Block size (16×16).
Output  Blocks extracted from the image
Begin
Step1   Initialization: Extract image dimensions:
                H ← Image Height
                W ← Image Width

Step2  Convert image to 1-Dimension:

Step 3  Count the Number of Blocks:
  ▪  Compute the total number of blocks
       $NB = ((H*W))/((B*B))$
Step 4  Divide Image into Blocks:
        For each block $i$ = 1: $N$B
  ▪  Extract a segment of $B$ × $B$ pixels from the 1D image array.
  ▪  Store it as an individual block.
     End for
End
```

C) Encryption key generation stage:
   Based on the values of the initial conditions and optimized parameters, seven chaotic sequences are generated using the proposed algorithm (N-7DHCS). The algorithm iterates the process of generating chaotic sequences $(x_{(1,i,)}\ x_{(2,i)}, x_{(3,i)}, x_{(4,i)},$ $x_{(5,i)}, x_{(6,i)}, x_{(7,i)})$. Each chaotic string is the same length as the original image dimensions (h × w), and these strings are converted into seven vectors $((1,i), K_{(2,i)}, K_{(3,i)}, K_{(4,i)}, K_{(5,i)}, K_{(6,i)},$ $K_{(7,i)})$ representing the chaotic sequence. Algorithm 2 shows the pseudocode for generating the chaotic key.

Algorithm 2: Key Generation.

```
Input   Initial condition: $⟦x_1, x⟧_2, x_3, x_4, x_5, x_6, x_7$
parameters:$a, b, c, d, e, f, g, h, i, j, k, l, m$ and $n$
    Iterations = height * width // image size
Output   Keys: $K_{(1,i)}, K_{(2,i)}, K_{(3,i)}, K_{(4,i)}, K_{(5,i)}, K_{(6,i)}, K_{(7,i)}$
Begin
Step1 Initialize the chaotic system: Introduce
       optimized initial values and coefficients to the chaotic system.
Step2   Generating chaotic sequences
       For i = 1: Iterations
Use (3) to generate seven chaotic sequences $x_{(1,i,)}\ x_{(2,i)}, x_{(3,i)}, x_{(4,i)}, x_{(5,i)}, x_{(6,i)}, x_{(7,i)}$
     Takes the floating of $(x_{(1,i,)}\ x_{(2,i)}, x_{(3,i)}, x_{(4,i)}, x_{(5,i)}, x_{(6,i)}, x_{(7,i)})$
     and convert each value to hexadecimal to Produce
     $(K_{(1,i)}, K_{(2,i)}, K_{(3,i)}, K_{(4,i)}, K_{(5,i)}, K_{(6,i)}, K_{(7,i)})$
     $K_i = convert\ to\ hex(x_i * 10^{16})$
       End for
Step 3  return $K_1, K_2, K_3, K_4, K_5, K_6, K_7$
End
```

D) Block-level encryption: This stage is one of the basic stages in the encryption algorithm, where each image block is processed after dividing the image into smaller units. It enhances security by applying several operations, including XOR with chaotic and master keys, shifting rows and columns, and rearranging pixel positions. These operations complicate the data structure, which contributes to hiding the original patterns of the image, thus increasing the difficulty of retrieving it without knowing the correct keys. Algorithm 3 presents the block cipher pseudocode.

Algorithm 3: Block Level Encryption Process.

```
Input    Block of pixels: B of size $16×16$,
             Chaotic key stream: K (generated using a 7D chaotic system),
             Master key: MK
Output  Block Encryption
Bigan
Step 1   Preprocessing Block:
      ▪ Flatten block B into a 1D array P of size 256 for easier manipulation.
      ▪ Normalize the MK-key values to the range [0,256]  to match pixel operations.
      ▪ key = XOR_ALL(MK)
Step 2   Chaotic Permutation:
      ▪ Use the chaotic sequence $K4$  (four part of K) to permute the pixels in P.
      ▪ Sort $K4$  to determine the new order of indices.
      ▪ Reorder P based on the sorted indices.
          Bitwise XOR Encryption:
         Perform a bitwise XOR operation between each pixel and its corresponding chaotic mask:
         P = P ⊕ MK
         Shift = MK[i] ⊕ $K_1$[i] mod 3
         P[i] = $Shift_{color}$(P[i], Shift)
         R, G, B = get color(P[i])
         R = R ⊕ $K_1$[i] ⊕ $K_3$[i] ⊕ $K_5$[i]
         R = R ⊕ Circle shift left ($K_4$[i],2) ⊕ Circle shift right ($K_2$[i],4) ⊕ Circle shift left ($K_6$ [i],5)
         R = (R + (Circle shift left ($K_7$ [i],2) AND 0xFF)) AND 0xFF
         R = R ⊕ (~$K_2$[i]) & 0xFF
         G = G ⊕ $K_2$[i] ⊕ $K_4$[i] ⊕ $K_7$[i]
         G = G ⊕ Circle shift left ($K_1$[i],3) ⊕ Circle shift right($K_5$[i],2) ⊕ Circle shift left ($K_3$[i],4)
         G = (G + (Circle shift right ($K_6$ [i],1) OR 0xAA)) AND 0xFF
         G = G ⊕ (~$K_4$[i]) & 0xFF
         B = B ⊕ $K_1$[i] ⊕ $K_3$[i] ⊕ $K_5$[i]
         B = B ⊕ Circle shift right ($K_1$ [i],3) ⊕ Circle shift left($K_7$[i],2) ⊕ Circle shift right ($K_3$[i],4)
         B = (B + (Circle shift left ($K_4$[i] AND $K_4$[i],1) ) AND 0xFF
         B = B ⊕ (~$K_5$[i]) & 0xFF
         P′[i] = [R, G, B]
Step 3   Diffusion Layer: Apply a diffusion operation to ensure that small changes in P affect all pixels in $P^\wedge{}'$.
                 $P''[i] = P'[i] \oplus P'[i-1] \oplus K_6[i]$
Step 4    Rebuild the Block: Reshape P′′ back to its original $16×16$ structure.
Step 5     Final Chaotic Mixing: Apply a final mixing step using $K_7$  (row and column shifts based on chaotic values).
              $P^\wedge{}'' = Shift\_(rows - Pixel)\ (P^\wedge{}'', K\_7)$
           $P^\wedge{}''' = Shift\_(Columns - Pixel)\ (P^\wedge{}'', K\_7)$
Step 6      Update MK and Encrypted Block:
                      $MK = MK \oplus B_{encrypted}$
                      $B\_encrypted = P^\wedge{}''' \oplus key$
End          Return Encrypted block $B_{encrypted}$
```

Algorithm 4 provides a detailed description of the proposed main algorithm for image encryption, which is based on a seven-dimensional chaotic system. This algorithm aims to achieve a high level of security by employing chaotic dynamics to complicate the encryption process, making it difficult to recover the original image without exact knowledge of the keys used.

Algorithm 4: Encrypted Image.

```
Input      Original Image ($RGB$),
                Chaotic System Parameters,
                Master key: MK

Output    Encrypted Image

Bigan
Step 1     Initialize Master key and Chaotic System with Optimal Parameters
    ▪ Generate chaotic values ($K_1$, $K_2$, ..., $K_7$) Using Algorithm (2)
    ▪ Generate Master key with size 256 byte
          MK =   SHA256(MK, $K_1$[1], $K_3$[1], $K_5$[1], $K_7$[1])
          For i=1:7
```

```
                    MK =   MK + SHA256(MK)
Step 2    Divide image into Blocks(B) (size 16x16) Using
                Algorithm (1)
Step 3     Encrypt Each Block:
             For x = 1: count Blocks
             If Block size = 16x16
          $B_{encry}$ [x]= encrypt Block[x] Using
    Algorithm (3)
            Else
           For i = 0: count pixel(B)
                $B_{encryp}$[x] = B[x][i] $\oplus$ K$_1$[i] $\oplus$ K$_3$[i] $\oplus$ K$_5$[i]
Step 4    Merge Blocks to Create Encrypted Image
End       Return Encrypted Image
```

4 RESULTS AND ANALYSIS

Table 2 shows the experimental results, which include the original image, the encrypted image, and the image after decryption. The data shows that the encrypted image has a high degree of randomness, which makes it impossible for attackers to extract any useful information from it, and thus the algorithm enhances the security level by completely hiding the visual patterns of the original image.

4.1 Histogram Analysis

To ensure encryption security, any statistical correlation between the plain and encrypted images must be eliminated. A uniform histogram distribution in the encrypted image indicates effective encryption [3]. As shown in Figures.3-5, the distinct histogram differences confirm the algorithm's ability to obscure statistical features and enhance security.

4.2 PSNR Analysis

The peak signal to noise ratio (PSNR) reflects the encryption quality. The lower value of PSNR is the better encryption quality. The PSNR formula are as shown in (2) [22]:

$$PSNR = 20\left(\frac{255}{\sqrt{MSE}}\right). \qquad (2)$$

4.3 Entropy Analysis

Entropy is the significant characteristic that reflects information's randomness and unpredictability [22]. The entropy of the cipher image should be close to 8. The entropy of H (s) can be calculated as shown in (3):

$$H(s) = -\sum_{i=0}^{N-1} p(s_i)(s_i). \qquad (3)$$

Where N denotes the number needed to represent the symbol s_i, s denotes the source, and P (si) is the symbol's probability[23].

4.4 Correlation Coefficient Analysis

The correlation coefficient of a visible image is one, but it is much lower for a ciphered image (almost equal to zero. Equation (4) calculates the correlation between original and ciphered pixel values.

$$Corr\ (x,y) = \frac{E[(x-\mu x)(y-\mu y)]}{\sigma x\ \sigma y}. \qquad (4)$$

where μx and μy represent mean values of x and y, σx and σy are the standard deviations of x and y, and E [·] is the expectation function [22].

Table 3 presents the encryption analysis results for three images using PSNR, entropy, and correlation coefficient metrics. The findings show that the encryption process significantly alters the images, with high entropy values ensuring randomness and correlation coefficients near zero indicating strong security against analytical attacks.

4.5 NPCR and UACI Analysis

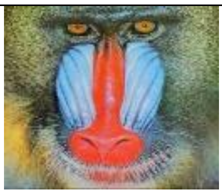
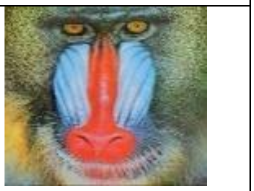
Two differential assault metrics are used to evaluate how vulnerable the original data is to slight alterations: (NPCR) Number of Pixels Change Rate as well as (UACI) Unified Average Changing Intensity. Suppose the enciphered image is (C and C') before and after changing one pixel in the original image [22]. The results of applying the proposed method on tested images are represented in Table 4. Equations (5) and (6) [24], express the NPCR and UACI formulas, respectively.

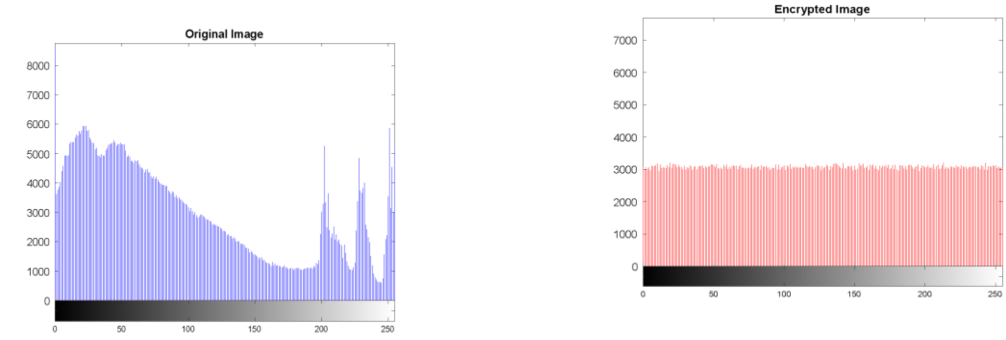
$$NPCR = \left(\sum_{i,j} D(i,j)\right)/(W \times H) \times 100\% \qquad (5)$$

$$UACI = 1/(W \times H)\left[\left(\sum_{i,j} |c(i,j) - c'(i,j)|\right)/255\right] \times 100\%. \qquad (6)$$

The results confirm a complete image transformation during encryption, with NPCR at 100%, indicating all pixels are altered. UACI values range from 33.48% to 33.50%, reflecting significant intensity changes, enhancing security.

Table 2: Experimental results (encrypted and decrypted).

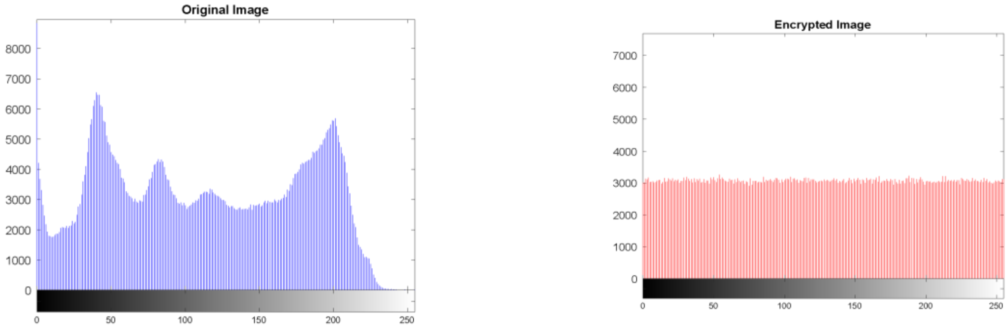
Image	Size	Original image	Encrypted image	Decrypted image
Panda	512 * 512			
Peppers	512 * 512			
Baboon	512 * 512			



(a) Original

(b) Encrypted

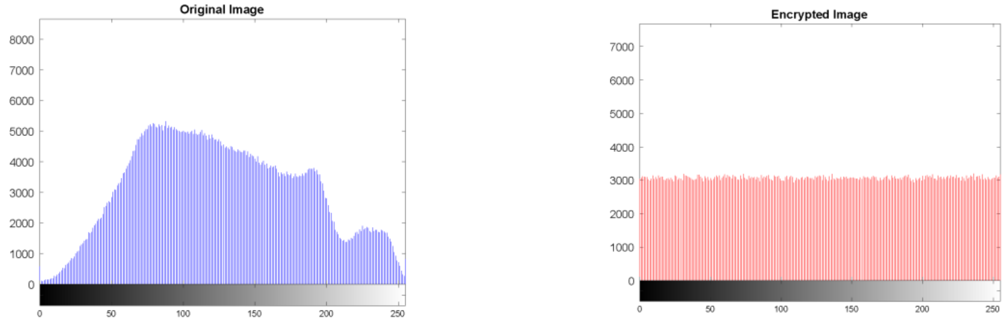
Figure 3: Histogram of the Panda image.



(a) Original

(b) Encrypted

Figure 4: Histogram of the Peppers image.



(a) Original

(b) Encrypted

Figure 5: Histogram of the Baboon image.

Table 3: Encryption analysis results.

Image	PSNR	Entropy Original	Entropy Encryption	Correlation
Panda	7.37	7.5655	7.9993	-0.0003
Peppers	7.10	7.3558	7.9998	0.0009
Baboon	8.80	7.6557	7.9994	-0.0025

Table 4: NPCR and UACI results.

Image	NPCR %	UACI %
Panda	100	33.48
Peppers	100	33.50
Baboon	100	33.48

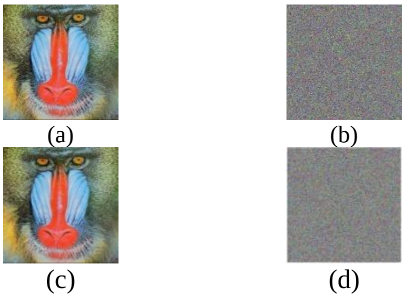


Figure 6: Key sensitivity results for slight variation in $x_1(0)$.

4.6 Key Space and Key Sensitivity Analysis

A secure encryption algorithm requires a sufficiently large key space to resist brute-force attacks, ideally exceeding 2^{128} [25]. The proposed algorithm utilizes a key space of $(10^{16})^{21}$ + 2^{11}≃ 2^1127 , incorporating initial conditions values (x1(0) …, x7(0)) at a precision of 10^{-16} In addition to the master key, which is (2^{11}) 256 bytes in size, ensuring robustness against brute-force attacks. Key sensitivity analysis demonstrated that altering x1(0) from 3 to 3.00000000000000001 (≈10^{-16}) led to complete image recovery failure. This high sensitivity reinforces the system's security, preventing decryption with even minimal key variations. Figure 6 illustrate this sensitivity a) original image, b) encrypted image, c) decrypted using $x_1(0) = 3$, and d) decrypted using $x_1(0) = 30000000000000001$.

4.7 Waveform Analysis of the Novel Chaotic System

A fundamental characteristic of chaotic systems is their aperiodic waveforms. To verify the chaotic nature of the proposed system, Figure. 7 present time-domain plots of the state variables x_1 (t), x_2 (t), x_3 (t), x_4 (t), x_5 (t), x_6 (t), x_7 (t), obtained from MATHEMATICA simulations. The results confirm the aperiodicity of these waveforms, distinguishing the system from complex periodic motions and reinforcing its chaotic behavior.

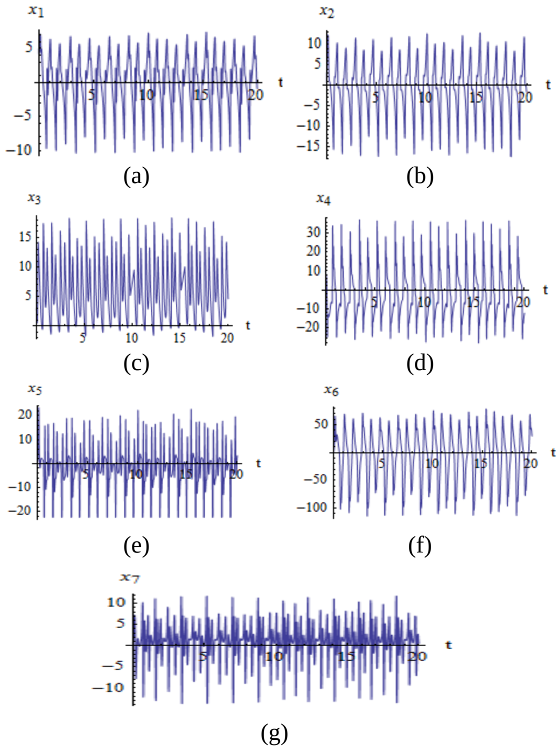


Figure 7: Temporal Analysis of the Chaotic System Variables (X_1 to X_7) Corresponding to Symbols a)–g).

4.8 Phase Portraits

Numerical simulations of the nonlinear system were performed using the MATHEMATICA program. The system exhibits complex and diverse chaotic behaviors. Three-dimensional strange attractors are presented in Figures 8a-8d, while two-dimensional attractors are shown in Figures 8e-8h. Notably, as observed in Figure 8a, the attractor's topology resembles the shape of a butterfly with flapping wings, leading to the concept of the "Butterfly Effect."

4.9 Bifurcation Diagram

The new chaotic system (1) [26] is numerically analyzed using Mathematica, where the bifurcation behavior of $\mathbf{X_1}$ is examined as parameter **a** varies. Notably, in the range a=14.2 to a=14.4, $\mathbf{X_1}$ exhibits bifurcation, indicating a transition in the system's dynamics. This property, a hallmark of chaotic systems, is confirmed in the proposed model, as illustrated in Figure 9.

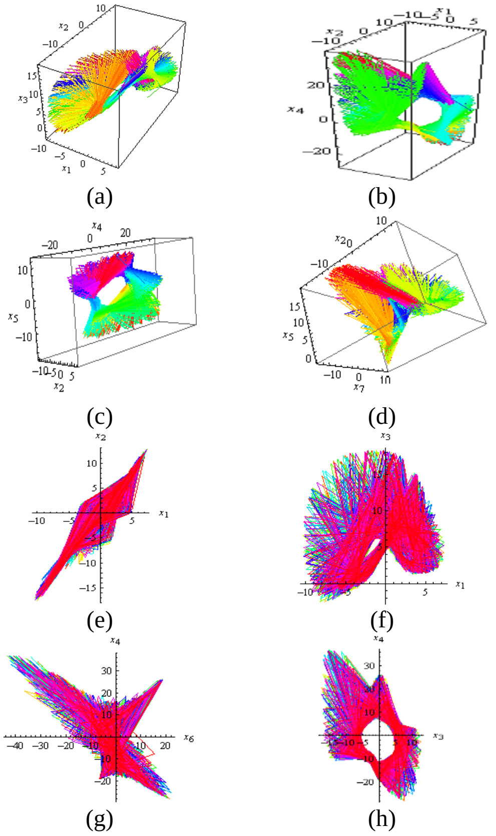


Figure 8: Chaotic attractors: 3D views (a) (x_1-x_2-x_3), (b) (x_1-x_2-x_4), (c) (x_4-x_5-x_2), (d) (x_2-x_5-x_7);and phase planes: (e) (x2-x1), (f) (x3-x1), (g) (x4-x6), and (h) (x4-x3).

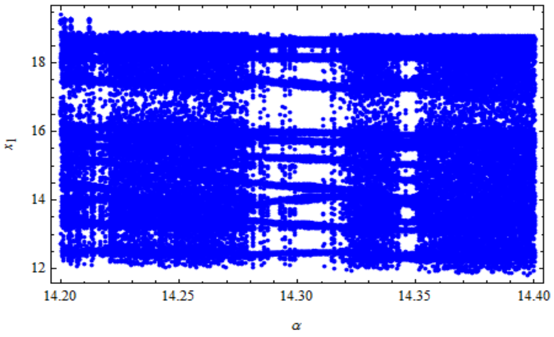


Figure 9: Bifurcation diagram of X_1 vs. a**.**

4.10 Comparison

Table 5 shows the performance evaluation metrics attained by our proposed method with those given in previous studies. Also, shows the proposed method given better results than methods in the previous studies. Thus, improved the efficiency of the proposed system.

Table 5: Comparison between the proposed encryption method and previous studies.

Measurement	Proposed	[19]	[27]	[28]
PSNR	7.10	7.3737	-	28.0397
Entropy	7.9998	7.9997	7.9974	7.2682
NPCR	100	99.600	99.604	99.6096
UACI	33.50	34.362	33.402	33.4599
Correlation	0. 0009	0.0409	0.0033	-0.0028

5 CONCLUSIONS

This research presented a novel image encryption system based on a seven-dimensional chaotic map integrated with an optimal parameter selection mechanism, notably using the Simulated Annealing (SA) algorithm. The proposed system demonstrated a high level of security, robustness, and computational efficiency through comprehensive theoretical and experimental evaluation. The system achieved near-ideal entropy values (up to 7.9998), indicating excellent randomness in the encrypted images. Correlation between adjacent pixels approached zero (e.g., 0.0009 for Peppers), suggesting significant decorrelation. The encryption scheme exhibited complete resistance to differential attacks, with NPCR reaching 100% and UACI around 33.50% across tested standard images (Panda, Peppers, Baboon). The SA optimization enhanced the Lyapunov exponent by 412%, confirming the increase in system chaoticity and encryption performance. The key space was approximately 2^{1127}, greatly exceeding the requirement to resist brute-force attacks. Key sensitivity analysis showed that minute changes (on the order of 10^{-16}) in initial conditions led to complete decryption failure, highlighting the system's high sensitivity and security strength.

This study makes a substantial contribution to secure image transmission by integrating a high-dimensional chaotic system with evolutionary optimization, resulting in a robust encryption scheme that can withstand a variety of attacks.

The proposed encryption approach can be applied in numerous sectors, including securing real-time transmission of sensitive images, protecting surveillance data, integrating into smart surveillance systems, and other applications.

ACKNOWLEDGMENTS

The Authors would like to thank Mustansiriyah University)www.uomustansiriyah.edu.iq) Bagdad-Iraq for its support in the present work.

REFERENCES

[1] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," International Journal of Bifurcation and Chaos, vol. 08, no. 06, pp. 1259-1284, Jun. 1998, [Online]. Available: https://doi.org/10.1142/S021812749800098X.

[2] A. S. Edu, D. Agozie, and M. Agoyi, "Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis," PeerJ Comput Sci, vol. 7, pp. 1-26, 2021, [Online]. Available: https://doi.org/10.7717/PEERJ-CS.658.

[3] A. A. Rashid and K. A. Hussein, "A Lightweight Image Encryption Algorithm Based on Elliptic Curves and a 5D Logistic Map," Iraqi Journal of Science, vol. 64, no. 11, pp. 5985-6000, 2023, [Online]. Available: https://doi.org/10.24996/ijs.2023.64.11.41.

[4] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006, [Online]. Available: https://doi.org/10.1142/S0218127406015970.

[5] G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption based on 3D chaotic cat maps," Chaos Solitons Fractals, vol. 21, pp. 749-761, Jul. 2004, [Online]. Available: https://doi.org/10.1016/j.chaos.2003.12.022.

[6] S. Kulkarni-Pai, "Attribute Based Cryptography: Overview & Applications," [Online]. Available: http://www.ripublication.com.

[7] Md. M. Ahamad and Md. I. Abdullah, "Comparison of Encryption Algorithms for Multimedia," Rajshahi University Journal of Science and Engineering, vol. 44, pp. 131-139, Nov. 2016, [Online]. Available: https://doi.org/10.3329/rujse.v44i0.30398.

[8] A. Fultz, K. Hmieleski, and T. Baker, "The Effect of Resource Constraints and Bricolage on Dynamic Capabilities and New Venture Performance," Academy of Management Proceedings, vol. 2023, Aug. 2023, [Online]. Available: https://doi.org/10.5465/AMPROC.2023.18365abstract.

[9] J.-Y. Oh and H.-J. Kouh, "A Study on AES Extension for Large-Scale Data," The Journal of the Institute of Webcasting, Internet and Telecommunication, vol. 9, Jan. 2009.

[10] S. C. Koduru and V. Chandrasekaran, "Integrated confusion-diffusion mechanisms for chaos based image encryption," in Proceedings - 8th IEEE International Conference on Computer and Information Technology Workshops, CIT Workshops 2008, 2008, pp. 260-263, [Online]. Available: https://doi.org/10.1109/CIT.2008.Workshops.33.

[11] Z. E. Musielak and D. E. Musielak, "High-dimensional chaos in dissipative and driven dynamical systems," 2009, World Scientific Publishing Co. Pte Ltd., [Online]. Available: https://doi.org/10.1142/S0218127409024517.

[12] B. J. Alkhafaji, M. A. Salih, S. A. Shnain, O. A. Rashid, A. A. Rashid, and M. T. Hussein, "Applying the Artificial Neural Networks with Multiwavelet Transform on Phoneme recognition," in Journal of Physics: Conference Series, IOP Publishing Ltd, Mar. 2021, [Online]. Available: https://doi.org/10.1088/1742-6596/1804/1/012040.

[13] M. Marwan, A. Xiong, M. Han, and R. Khan, "Chaotic Behavior of Lorenz−Based Chemical System under the Influence of Fractals," Match, vol. 91, no. 2, pp. 307-336, 2024, [Online]. Available: https://doi.org/10.46793/match.91-2.307M.

[14] M. Rizki, E. Iman, H. Ujianto, and R. Rianto, "Digital Image Encryption Using Logistic Map," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 7, no. 6, pp. 1292-1299, Nov. 2023, [Online]. Available: https://doi.org/10.29207/resti.v7i6.5389.

[15] M. I. Kopp and I. Samuilik, "Chaotic dynamics of a new 7D memristor-based generator: computer modeling and circuit design," Mathematical Modeling and Computing, vol. 12, no. 1, pp. 116-131, 2025, [Online]. Available: https://doi.org/10.23939/mmc2025.01.116.

[16] A. Hedayatipour, R. Monani, A. Rezaei, M. Aliasgari, and H. Sayadi, "A Comprehensive Analysis of Chaos-Based Secure Systems," 2022, pp. 90-105, [Online]. Available: https://doi.org/10.1007/978-3-030-96057-5_7.

[17] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Analysis of novel seven-dimension hyper chaotic by using SDIC and waveform," in 2020 3rd International Conference on Engineering Technology and its Applications, IICETA 2020, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 95-99, [Online]. Available: https://doi.org/10.1109/IICETA50496.2020.9318940.

[18] R. Lan, J. He, S. Wang, Y. Liu, and X. Luo, "A Parameter-Selection-Based Chaotic System," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. PP, p. 1, Aug. 2018, [Online]. Available: https://doi.org/10.1109/TCSII.2018.2865255.

[19] N. N. Jasem and S. A. Mehdi, "Multiple Random Keys for Image Encryption Based on Sensitivity of a New 6D Chaotic System," International Journal of Intelligent Engineering and Systems, vol. 16, no. 5, pp. 576-585, 2023, [Online]. Available: https://doi.org/10.22266/ijies2023.1031.49.

[20] F. Budiman, P. N. Andono, and D. R. I. M. Setiadi, "Image Encryption using Double Layer Chaos with Dynamic Iteration and Rotation Pattern," International Journal of Intelligent Engineering and Systems, vol. 15, no. 2, pp. 57-67, Apr. 2022, [Online]. Available: https://doi.org/10.22266/ijies2022.0430.06.

[21] R. Li, Q. Liu, and L. Liu, "Novel image encryption algorithm based on improved logistic map," IET Image Process, vol. 13, no. 1, pp. 125-134, Jan. 2019, [Online]. Available: https://doi.org/10.1049/iet-ipr.2018.5900.

[22] A. A. Rashed and K. A. Hussein, "A Lightweight Image Encryption Algorithm Based on Elliptic Curves and Chaotic In Parallel," in 3rd Information Technology to Enhance e-Learning and Other Application, IT-ELA 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 24-30, [Online]. Available: https://doi.org/10.1109/IT-ELA57378.2022.10107924.

[23] O. A. Jasim, S. R. Amer, S. F. Hussein, and S. A. Mehdi, "Enhanced Image Encryption Using a Novel Chaotic System and Scramble Dithering Technique," International Journal of Safety and Security Engineering, vol. 14, no. 5, pp. 1465-1476, Oct. 2024, [Online]. Available: https://doi.org/10.18280/ijsse.140514.

[24] H. R. Shakir, S. A. Mehdi, and A. A. Hattab, "A New Method for Color Image Encryption Using Chaotic System and DNA Encoding," Mustansiriyah Journal of Pure and Applied Sciences, vol. 1, no. 1, pp. 68–79, Nov. 2022, [Online]. Available: https://doi.org/10.47831/mjpas.v1i1.9.

[25] H. J. S. Sadiq A. Mehdi, "Enhancing Data Security with a New Color Image Encryption Algorithm Based on 5D Chaotic System and Delta Feature for Dynamic Initialization," pp. 90-105, 2024.

[26] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Design and Analytic of A Novel Seven-Dimension Hyper Chaotic Systems," in Proceedings of 2020 1st Information Technology to Enhance E-Learning and other Application Conference, IT-ELA 2020, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 77-81, [Online]. Available: https://doi.org/10.1109/IT-ELA50150.2020.9253077.

[27] D. F. Chalob, R. H. Hasan, and R. F. Yaser, "Image Cryptography Based on Confusion and Diffusion Using 6D Hyper Chaotic System and Fibonacci Q-matrix," International Journal of Intelligent Engineering and Systems, vol. 17, no. 4, pp. 944-956, 2024, [Online]. Available: https://doi.org/10.22266/IJIES2024.0831.71.

[28] Z. Qiu-yu and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," Multimed Tools Appl, vol. 80, Apr. 2021, [Online]. Available: https://doi.org/10.1007/s11042-020-10437-z.