A Robust Image Cryptosystem Incorporating Bit-Level Swapping, Dynamic Multi-Map Substitution, And Iterative Block Diffusion

Heba A M ABUGHALI, Prof. Dr. Utku KOSE

Computer Engineering Department, Suleyman Demirel University, Isparta, Turkey

DOI: https://doi.org/10.51584/IJRIAS.2026.11050170

Received: 14 May 2026; Accepted: 19 May 2026; Published: 11 June 2026

ABSTRACT

The rapid expansion of digital communication has necessitated the development of advanced cryptographic frameworks capable of securing visual data against sophisticated cryptanalytic threats. This paper introduces a robust, tripartite image cryptosystem designed to address the inherent redundancies and high spatial correlations found in digital images. Unlike traditional pixel-shuffling methods, the proposed architecture operates at the bit-stream level through three integrated stages: Bit-level Recombination and Permutation, Dynamic Multi-Map Chaotic Substitution, and a Multi-round Iterative Diffusion Layer. The permutation phase utilizes a symmetrical interchanging process to effectively neutralize spatial redundancies. A key innovation in the substitution layer is the implementation of a key-driven dynamic selection mechanism that switches between four distinct chaotic systems—Tent, Lorenz, Logistic, and Henon maps—ensuring session-specific unpredictability and resistance to modeling attacks. Security is further fortified by a block-cipher-based iterative diffusion layer incorporating XNOR-based logical masking and feedback loops to propagate minor input variations throughout the entire ciphertext.

Empirical validation via MATLAB simulations demonstrates that the proposed scheme achieves near-ideal performance benchmarks, including an information entropy of approximately 7.9993 and a perfectly uniform histogram distribution. Furthermore, the system exhibits exceptional resistance to differential attacks, yielding a high Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) scores that outperform several contemporary methods. Additionally, the cryptosystem demonstrates high computational efficiency, with a linear-time complexity of O(M×N), making it an ideal candidate for real-time secure communication and high-definition video encryption. Comparative analyses confirm that the bit-level granularity and iterative diffusion layers successfully eliminate inter-pixel correlations, providing a secure and computationally efficient solution for real-time image protection in modern communication environments.

Keywords: Image Cryptography; Bit-Level Swapping; Block Diffusion; Entropy; Substitution;

INTRODUCTION

In the contemporary digital era, the rapid transmission of multimedia content over insecure networks has become a fundamental aspect of modern communication. This surge in data exchange has intensified the need for robust cryptographic frameworks specifically designed to protect sensitive visual information. However, traditional encryption standards such as the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), while highly effective for textual data, encounter significant challenges when applied to digital images [1-3]. These challenges stem from the intrinsic properties of image data, including extreme data redundancy, massive bulk capacity, and high spatial correlation between adjacent pixels [4-6].

Motivation

The primary motivation behind this research is to address the security gap left by traditional algorithms that fail to account for the high correlation and redundancy found in visual media. While recent academic trends have explored hybrid models combining evolutionary-inspired mechanisms and chaotic systems, many existing schemes remain susceptible to advanced statistical and differential cryptanalysis [7-11]. This study is driven by

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

the necessity to develop a multi-layered architecture that operates at the bit-stream level rather than the pixel level. By integrating Bit-level Recombination and Permutation with a Multi-round Iterative Diffusion Layer, the proposed method aims to achieve a superior degree of ciphertext complexity, ensuring near-ideal randomness and maximum resistance to modern cryptanalytic threats.

Contributions

This paper introduces several significant contributions to the field of image cryptography through the design and validation of a high-complexity hybrid system:

Design of a Tripartite Cryptographic Architecture: The study proposes a novel three-stage framework comprising Bit-level Recombination and Permutation, Chaotic Sequence-based Substitution, and a Multi-round Iterative Diffusion Layer.

Innovation in Dynamic Map Selection: A key contribution is the implementation of a key-driven dynamic switching mechanism that selects between four distinct chaotic maps—Tent, Lorenz, Logistic, and Henon—for each encryption session. This significantly expands the key space and prevents attackers from modeling the system using a single dynamical system.

Innovation in Bit-level Granularity: Unlike conventional pixel-shuffling methods, the proposed Bit-level Recombination treats the image as a one-dimensional bit-stream, employing a symmetrical interchanging process that effectively neutralizes spatial redundancies.

Enhancement of Non-linear Diffusion: The research implements a rigorous block-cipher approach within the Multi-round Iterative Diffusion Layer, utilizing XNOR-based logical masking and feedback mechanisms to achieve superior confusion and diffusion properties.

Empirical Validation and High-Performance Metrics: Through extensive MATLAB simulations, this work demonstrates that the proposed system achieves a near-perfect uniform histogram and an information entropy of approximately 8, confirming its resilience against entropy-based attacks. Robustness against Differential Attacks: The methodology yields exceptional NPCR and UACI values, proving its formidable resistance to plaintext-related and differential attacks compared to state-of-the-art encryption schemes. Security Assessment and Sensitivity Excellence: The study confirms extreme sensitivity to both the secret key and the plaintext, ensuring that even a single-bit alteration in the input renders the original data unrecoverable.

The remainder of this manuscript is organized as follows: Section 2 provides a comprehensive review of the existing literature and related work in the field of image cryptography. Section 3 introduces the architecture of the proposed cryptosystem, detailing the algorithmic procedures of the phases. Section 4 specifies the experimental and computational environment, presenting the visual outcomes of the encryption and decryption processes alongside a rigorous security analysis and robustness evaluation compared against contemporary state-of-the-art methods. Section 5 provides a discussion of the experimental results and their practical implications. Finally, Section 6 concludes the study and outlines prospective trajectories for future research.

LITERATURE REVIEW

The field of digital image encryption has seen substantial advancements through the integration of chaotic systems and multi-layered diffusion strategies. Recent research has focused on enhancing the complexity of chaotic maps and improving the granularity of encryption processes to protect sensitive visual data across various applications.

Chaos-Based Image Encryption and Dynamic Systems

Chaotic maps are highly valued in image encryption due to their non-linear dynamics and sensitive dependence on initial conditions. However, to overcome the limitations of standard maps, such as low adaptability and limited chaotic ranges, researchers have developed more complex architectures:

Dynamic Triple Chaotic Map (D3CM-IES): This scheme utilizes a combination of the Sine-cosine, Sine-Tangent-Sine (STS), and a novel 1D-PCQM map. It employs a dynamic selection procedure to choose sequences for encryption, achieving an NPCR of 99.66% and a UACI of 49.94%, which indicates strong resistance to differential attacks [12].

3D Non-degenerate Hyperchaos (3D-NDHC): Designed for smart home ecosystems and consumer electronics, this globally bounded architecture serves as a robust entropy source. It integrates a chaos-driven 3D S-box with genetic code methods and lightweight wave diffusion to protect visual privacy in IoT networks [13].

Algebraically Enhanced 3D Maps: By utilizing SHA-256 hashing for secure initialization and an algebraically deformed 3D chaotic map, researchers have developed schemes that implement multi-stage diffusion, including Gray code transformations and multi-channel dependencies across color channels [14].

In medical imaging, traditional cryptographic methods often fail to protect both diagnostic integrity and data confidentiality. The paper [15] proposes a lightweight, reversible encryption algorithm based on a four-dimensional chaotic system, designed for enhanced security in healthcare communications. It employs SHA-256 for key generation and features a dual-stage permutation-diffusion framework for effective data protection. Experimental results demonstrate strong statistical performance, robustness to attacks, and lossless reversibility, with security levels comparable to or superior to those of recent methods, making it ideal for telemedicine and IoMT applications.

Advanced Permutation and Diffusion Strategies

Modern cryptosystems have shifted toward more granular manipulation of image data to neutralize spatial redundancies and statistical dependencies:

Multi-Image Encryption (MIE): To improve efficiency over single-image methods, the ISL-HMC hyperchaotic map is used to fuse multiple original images into a cube for cubic confusion, followed by bidirectional diffusion and S-box based confusion. This approach achieves a high information entropy of 7.9970 [16].

Bit-Plane Level Shuffling: Some systems exploit bit-plane level content shuffling at both intra- and inter-levels using 3D chaotic systems. This method is effective for both natural grayscale and medical DICOM imaging, achieving ideal entropy values of approximately 7.999 and resisting chosen-plaintext and brute-force attacks [17].

Genetic and Wave Diffusion: The combination of chaos-driven S-boxes with genetic code schemes and wave diffusion processes introduces high levels of confusion, making it significantly more difficult for attackers to decrypt sensitive images from smart devices [18].

Bit-Level Encryption Algorithms

Bit-level encryption algorithms can be categorized into pixel-level and bit-level based on the minimum unit of encryption. Pixel-level operations modify each pixel's position and color value independently, while bit-level encryption processes each bit of a pixel, allowing disturbances to propagate between pixels. By shuffling and diffusing bits, finer-grained encryption effects can be achieved, enhancing resistance to attacks. Wen et al. proposed a novel triple-image bit-level encryption algorithm that converts a colored image into a combined bit-level grayscale matrix and achieves scrambling by randomly swapping binary numbers, with bit-level diffusion implemented through bitwise cyclic shifts and exclusive OR (XOR) operations [19]. Wang et al. generate chaotic sequences using a cross-coupled map lattice (CCML) and employ these sequences to reorder the bits of the image for encryption [20]. Alexan et al. proposed a new image encryption system combining a 5D hyperchaotic system and S-boxes for byte transformation, which offers a large key space and encryption speed suitable for real-time scenarios [21]. Moysis et al. proposed a new Soboleva hyperbolic tangent map combined with efficient bit-level circular shifts, demonstrating good performance on grayscale images, though its application to color images remains to be further tested [22]. Alexan et al. proposed a cryptosystem combining the hyperchaotic 4D Chen system and the Mersenne Twister, utilizing S-boxes , XOR operations to enhance encryption strength [23].

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Compared to pixel-level encryption, bit-level encryption algorithms can alter both the value and position of pixels simultaneously, resulting in a ciphertext pixel distribution that is closer to a uniform distribution. This can provide higher security and stronger resistance to attacks.

The collective results of these studies demonstrate that integrating advanced chaotic foundations with multi-stage, bit-level, or multi-image architectures establishes an optimal balance between high-security benchmarks and computational efficiency.

While the methods surveyed above demonstrate significant advances in chaotic image encryption, a unifying limitation persists: each architecture commits statically to a single underlying dynamical system throughout all encryption sessions, exposing the substitution layer to potential mathematical modeling attacks. Furthermore, although contemporary bit-level algorithms [19-23] have moved beyond traditional pixel-level constraints, they predominantly operate on localized bit-planes or static structures, leaving inter-plane spatial redundancies partially intact.

The proposed cryptosystem simultaneously addresses both gaps. Unlike the schemes in [24]–[27], which employ fixed chaotic maps with varying dimensionality, the proposed framework introduces a key-driven dynamic selection mechanism that rotates among four structurally distinct maps (Tent, Logistic, Henon, and Lorenz) on a per-session basis, rendering the substitution architecture session-specific and non-modelable. Additionally, in contrast to conventional bit-plane methods [17, 19] that process individual planes independently, the proposed Bit-level Recombination phase treats the entire image as a unified one-dimensional bit-stream, achieving a more thorough and global inter-plane decorrelation. These architectural distinctions collectively ensure superior information entropy and enhanced differential resistance, thereby establishing a higher security margin against classical cryptanalytic attacks.

METHODOLOGY

The proposed encryption framework is engineered to achieve high sensitivity to initial conditions and robust resistance against statistical attacks. The architecture is divided into three fundamental stages: Bit-level Permutation, Chaotic Substitution, and Iterative Block Diffusion, as shown in Figure 1 and Algorithm 2.

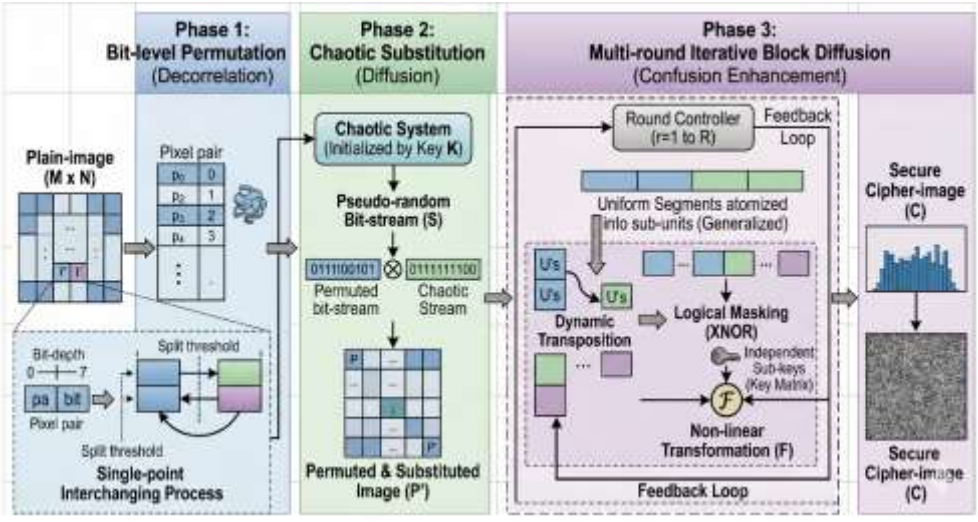


Figure 1. Cryptosystem phases

Key Generation and Chaotic Map Initialization

The secret key K is a composite multi-component structure partitioned into four functionally independent segments, each governing a distinct algorithmic stage, as clarified in Algorithm 1. The first segment defines the single-point split threshold t, mapped to the integer range [1, 7] via $t = (K_1 \bmod 7) + 1$ to ensure valid pixel reconstruction. The second segment supplies the initial conditions for the selected chaotic map as 64-bit double-precision floating-point values, constrained to their respective attractor domains: $x_0 \in (0, 1)$ for the Tent and

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Logistic maps; $(x_0, y_0) \in [-1.5, 1.5] \times [-0.4, 0.4]$ for the Henon map; and (x_0, y_0, z_0) within the bounded chaotic regime of the Lorenz system under standard parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$. The third segment is a discrete 2-bit index that drives the Dynamic Map Selection mechanism, determining the active chaotic system for the current encryption session. The fourth segment comprises $R = 4$ independent 64-bit sub-keys reserved for the XNOR-based Logical Masking rounds in the diffusion phase. To eliminate transient behavior and guarantee stable chaotic regime operation, all selected maps are iterated for 1,000 warm-up steps prior to sequence generation.

Algorithm 1: Key Generation and Chaotic Map Initialization

Input: Composite secret key K, Number of diffusion rounds R = 4

Output: Split threshold t, Map selection index map_id, Initial conditions IC, Diffusion sub-keys {SK_1, SK_2, SK_3, SK_4}.

Procedure:

Step 1 — Key Segmentation:

Extract $K_1 \leftarrow$ bits [0 : 7] of K ▷ 8-bit threshold segment

Extract $K_2 \leftarrow$ bits [8 : 71] of K ▷ 64-bit chaotic IC segment

Extract $K_3 \leftarrow$ bits [72 : 73] of K ▷ 2-bit map selection segment

Extract $K_4 \leftarrow$ bits [74 : 329] of K ▷ 4 × 64-bit diffusion segment

Step 2 — Threshold Derivation:

$t \leftarrow (K_1 \bmod 7) + 1$ ▷ $t \in \{1, 2, ..., 7\}$

Step 3 — Map Selection:

map_id ← integer value of K_3 ▷ map_id ∈ {0, 1, 2, 3}

Step 4 — Initial Condition Derivation:

Each chaotic parameter is derived from an independent 64-bit segment of the secret key K to ensure statistical independence among initial conditions.

Switch (map_id):

Case 0 — Tent Map:

$x_0 \leftarrow K_2 / 2^{64}$ ▷ $x_0 \in (0, 1)$

$IC \leftarrow \{x_0\}$

Case 1 — Logistic Map:

$x_0 \leftarrow K_2 / 2^{64}$ ▷ $x_0 \in (0, 1)$

$IC \leftarrow \{x_0\}$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Case 2 — Henon Map:

$x_0 \leftarrow (K_2 / 2^{64}) \times 3.0 - 1.5$ ▷ $x_0 \in [-1.5, 1.5]$

$y_0 \leftarrow (K_2' / 2^{64}) \times 0.8 - 0.4$ ▷ $y_0 \in [-0.4, 0.4]$

$IC \leftarrow \{x_0, y_0\}$ ▷ K_2' = next 64-bit block

Case 3 — Lorenz System:

$x_0 \leftarrow$ scale(K_2) ▷ within bounded chaotic domain

$y_0 \leftarrow$ scale(K_2') ▷ $\sigma = 10$, $\rho = 28$, $\beta = 8/3$

$z_0 \leftarrow$ scale(K_2'') ▷ K_2'', K_2''' = subsequent 64-bit blocks

$IC \leftarrow \{x_0, y_0, z_0\}$

Step 5 — Diffusion Sub-Key Extraction:

For r = 1 to R:

$SK\_r \leftarrow$ bits $[(r-1)\times 64 : r\times 64-1]$ of K_4 ▷ independent 64-bit sub-key per round

Step 6 — Chaotic Warm-Up:

Initialize the selected chaotic map with IC

Iterate map for 1,000 steps, discarding all outputs ▷ eliminate transient behavior

Return: {t, map_id, IC, {SK_1, SK_2, SK_3, SK_4}}

Bit-level Recombination and Permutation

In this initial stage, the spatial correlation between adjacent pixels is decorrelated through a bit-level swapping mechanism. Unlike conventional pixel-shuffling, this method treats the image as a one-dimensional bit-stream. By selecting symmetrical pixel pairs across the image boundaries and performing a Single-point Interchanging Process, the algorithm effectively scatters the high-frequency components of the image. This process ensures that the position of each bit is significantly altered, fulfilling the primary requirements of a permutation layer in a Feistel-like structure.

Dynamic Chaotic Sequence-based Substitution

To achieve a high degree of diffusion, a substitution layer is integrated using a multi-map non-linear dynamical system. This phase employs a diverse pool of four distinct chaotic maps: The Tent map, Lorenz system, Logistic map, and Henon map. Unlike static encryption schemes, the proposed framework implements a Dynamic Selection Mechanism where the specific chaotic map used for generating the pseudo-random bit-stream is determined by the security key. This ensures that the cryptographic architecture changes for each session, significantly increasing the complexity for attackers attempting to model the system's behavior.

Algorithm 2: Proposed Multi-Layered Hybrid Image Cipher

Input: Plain image P of dimensions M * N, Security Key K, and initial parameters for the Chaotic System.

Output: Secure Cipher image C.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Procedure:

Phase 1: Bit-level Recombination and Permutation (Decorrelation Phase)

1. Vectorization: Flatten the Plain image P into a 1D bit-stream representation.
2. Symmetrical Pairing: For i = 0 to ((M *N) -1) /2
   - Identify the boundary-symmetrical pixel pairs: Pi and P(M *N - 1) - i.
3. Bit-level Interchanging:
   - Define a single-point split threshold within the bit-depth.
   - Apply a Single-point Interchanging Process to swap bit-segments between the symmetrical pairs.
   - Reconstruct the pixels to form the permuted matrix Pperm.

Phase 2: Dynamic Chaotic Sequence-based Substitution (Multi-Map Diffusion Phase)

4. Dynamic Map Selection:

   Use the Security Key K to compute a selection index ID.

   Switch (ID):

   Case 1: Select Tent Map.

   Case 2: Select Lorenz System.

   Case 3: Select Logistic Map.

   Case 4: Select Henon Map.
5. Pseudo-random Synthesis: Generate a chaotic sequence S of length M * N using the non-linear dynamical system initialized by key K.
6. Global Masking: for j = 0 to (M×N - 1)
   - For each pixel Pperm(j) in the permuted matrix:
   - Compute P'j = Pperm(j) bitwise XOR Sj
7. The resulting matrix P' now exhibits flattened statistical properties.

Phase 3: Multi-round Iterative Block Diffusion (Confusion Enhancement)

8. Data Atomization:
   - Segment the bit-stream P' into uniform blocks.
   - Further partition each block into smaller sub-units.
9. Iterative Round Transformation: For each round r = 1 to R:
   - Dynamic Transposition: Reorder the position of sub-units (U) to disrupt structural patterns.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

- Logical Masking: Apply bitwise XNOR between the transposed units and the round-specific independent sub-keys.
- Non-linear Feedback:
    - Process the current sub-blocks through the non-linear transformation function.
    - Execute a feedback loop where the output of the function is integrated as an input for the subsequent computational cycle.

10. Reconstruction: Assemble the processed blocks to generate the final Cipher image C.

The selected map synthesizes a pseudo-random sequence, and each pixel value is subsequently transformed via a bitwise XOR operation with this chaotic stream. This process ensures that the global statistical properties of the image, such as the histogram, are flattened, rendering the cipher-image resilient to frequency analysis. Furthermore, the inherent sensitivity of these chaotic systems to their initial conditions—coupled with the dynamic map selection—guarantees that even a single-bit alteration in the plaintext or the security key results in a completely different ciphertext.

Multi-round Iterative Diffusion Layer

The final security layer adopts a rigorous block-cipher approach to consolidate the diffusion effect, ensuring maximum resistance against cryptanalytic attacks. In this stage, the data is processed in uniform segments, which are subsequently atomized into smaller sub-blocks to facilitate granular manipulation. The methodology involves a multi-layered transformation process where, central to this approach, is the dynamic transposition of sub-units; this reorders data within each iteration to effectively disrupt inherent structural patterns and spatial correlations. This architecture is further strengthened by a logical masking phase, where bitwise XNOR operations are executed against a set of independent sub-keys to inject significant non-linearity into the cipher. Finally, the system employs a round-based transformation mechanism, incorporating a feedback loop that integrates the output of the non-linear function into subsequent computational cycles, thereby ensuring that even minor variations in the input propagate throughout the entire ciphertext.

This multi-layered approach ensures that the confusion and diffusion properties are maximized, providing a high Security Assessment level against modern cryptanalytic threats.

Decryption algorithm

The decryption technique is identical to the encryption procedure; however, it operates in the reverse direction, as shown in Algorithm 3

Algorithm 3: Decryption Procedure for the Proposed Multi-Layered Hybrid Image Cipher

Input: Cipher image C of dimensions M × N

Security Key K

Initial parameters of the Chaotic System

Round sub-keys {SK_1, SK_2, ..., SK_R} (same as encryption)

Output: Recovered Plain image P_dec

Procedure:

Phase 1 — Inverse Multi-Round Iterative Block Diffusion

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

1. Vectorization

- Flatten C into a 1D bit-stream representation C_flat.

2. Inverse Round Transformation

For each round r = R down to 1:

2a. Inverse Non-linear Feedback:

- Remove the feedback contribution of round r by applying the inverse of the non-linear transformation function F^{-1} to the current sub-block state.

- Detach the feedback loop output from the input of the current computational cycle.

2b. Inverse Logical Masking (XNOR is self-inverse):

- For each transposed sub-unit U and its round-specific sub-key SK_r:

U_unmasked = U XNOR SK_r

2c. Inverse Dynamic Transposition:

- Apply the inverse permutation σ^{-1} to restore the original ordering of sub-units within each block.

- Use the same transposition index generated by Key K to reconstruct σ^{-1} deterministically.

3. Block Reassembly

- Reconstruct the full bit-stream P'_flat from the

processed sub-blocks.

- Reshape to matrix P' of dimensions M × N.

Phase 2 — Inverse Dynamic Chaotic Substitution

4. Dynamic Map Re-selection

- Use Security Key K to recompute selection index ID (identical procedure as encryption):

Switch (ID):

Case 1: Select Tent Map.

Case 2: Select Lorenz System.

Case 3: Select Logistic Map.

Case 4: Select Henon Map.

5. Pseudo-random Sequence Regeneration

- Regenerate the identical chaotic sequence S of length M × N using the selected map initialized by Key K.

6. Inverse Global Masking (XOR is self-inverse):

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

- For each pixel P'(j) in matrix P': P_perm(j) = P'(j) XOR S(j), j = 0, 1, ..., MN-1

- The result is the permuted matrix P_perm.

Phase 3 — Inverse Bit-Level Recombination and Permutation

7. Vectorization to Bit-Stream

- Flatten P_perm into a 1D bit-stream of length L = 8·M·N.

8. Inverse Symmetrical Interchanging

- For i = 0 to ((M·N) - 1) / 2:

8a. Identify the same symmetrical pixel pairs: P_perm(i) and P_perm((M·N - 1) - i)

8b. Apply the Inverse Single-point Interchanging Process:

- Using the same split threshold t defined by Key K:

High segment of pixel i ← bits [0 .. t-1] of P_perm(i)

Low segment of pixel i ← bits [t .. 7] of P_perm((M·N-1)-i)

- Reconstruct original pixels by reversing the swap:

P_dec(i) = High(P_perm(i)) ‖ Low(P_perm((M·N-1)-i))

P_dec((M·N-1)-i) = High(P_perm((M·N-1)-i)) ‖ Low(P_perm(i))

9. Reconstruction

- Reshape the recovered bit-stream into the 2D matrix P_dec of dimensions M × N.

Output: Recovered Plain image P_dec ≡ P (original image)

Performance Analysis and Experimental Results

The effectiveness of the proposed cryptographic framework was evaluated through simulations conducted in MATLAB on a system equipped with an Intel Core i7 CPU (2.60 GHz). The experimental study, applied across a diverse dataset of images, confirms that the methodology achieves high security performance. Standard 512 × 512 grayscale images were utilized as input for the benchmarking process. For example, the simulation results displayed in Figure 2(a), and (b), Cipher images are like a noise image, as can be observed.

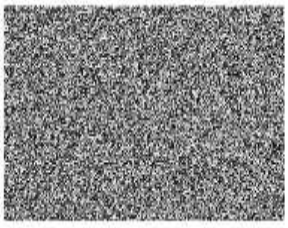
Statistical Security Evaluation

Histogram Uniformity

A critical statistical feature of any image is its histogram, which depicts the distribution of gray-level intensities. While plain images often exhibit regular, non-uniform histograms that attackers can exploit, a secure cipher-image must possess a uniform distribution to prevent information leakage. As illustrated in Figure 3, the encrypted output for the Lena image displays a perfectly flat histogram. This uniformity ensures that no grayscale information can be retrieved, rendering the system resilient against statistical cryptanalysis.

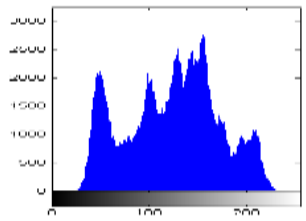
ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

a

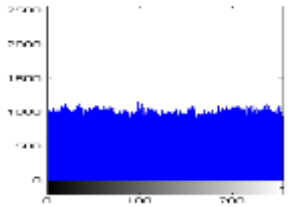


b

Figure 2. Lena image a) original image b) encrypted image



a



b

Figure 3. Histogram of Lena image a) original image b) encrypted image

Information Entropy Analysis

Entropy is a mathematical measure of randomness in data communication. For an 8-bit grayscale image with 256 possible symbols, the ideal entropy value is 8, representing a perfectly random distribution where each symbol has a probability of 1/256.

Table 1 compares the entropy of images encrypted by the proposed system against other contemporary methods. The results indicate that the proposed scheme achieves the highest entropy values, confirming a near-ideal random pixel distribution in the ciphertext.

Correlation Coefficient Analysis

In natural images, adjacent pixels (horizontal, vertical, and diagonal) are highly correlated, typically approaching a coefficient of 1. An effective encryption scheme must reduce this correlation to near 0 [30].

To evaluate the general applicability of the proposed Bit-level Recombination and Permutation strategy, the correlation coefficients were calculated for multiple standard test images, as presented in Table 2. The results indicate that for all tested images—including Lena, Peppers, and Baboon—the correlation values in the encrypted ciphertext are negligible, approaching zero. This consistent performance across diverse image textures confirms the algorithm's robustness in eliminating spatial dependencies and its effectiveness as a generalized cryptographic solution.

Table 1. Information Entropy Comparison Between the Proposed Scheme and Existing Methods

Method	**Plain image**	**Ciphered image entropy**	**Plain image**	**Ciphered image entropy**
Proposed method	Baboon	7.9993	Lena	7.9993
Ref. [24]	with entropy	7.9993	with entropy	7.9990
Ref. [25]	7.3738	7.9991	7.4450	7.9993
Ref. [26]		7.9992		7.9993
Ref. [27]		7.9993		7.9993
Ref. [28]		7.9974		7.9967
Ref. [29]		7.9974		-

The statistical relationship between adjacent pixels in both the plain and ciphered versions of the Lena image is summarized in Table 3. While the plain-image exhibits a high degree of correlation (approaching 1) in all

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

directions, the proposed cryptosystem successfully reduces these values to near zero. This significant decorrelation, achieved through the Bit-level Recombination and Permutation phase, confirms the algorithm's effectiveness in neutralizing spatial redundancies and resisting statistical cryptanalysis

Furthermore, the experimental results consolidated in Table 2 and Table 3 demonstrate the consistent performance of the proposed architecture across diverse image textures. The visual distribution of pixel correlations, as depicted in the scatter plots of Figure 4, confirms that the strong linear dependencies found in the plain images are entirely dissipated in their ciphered counterparts. This transition from highly correlated clusters to a uniform, random distribution further validates the algorithm's robustness in mitigating the risk of statistical attacks.

Table 2. Correlation Coefficient Values for Various Encrypted Images

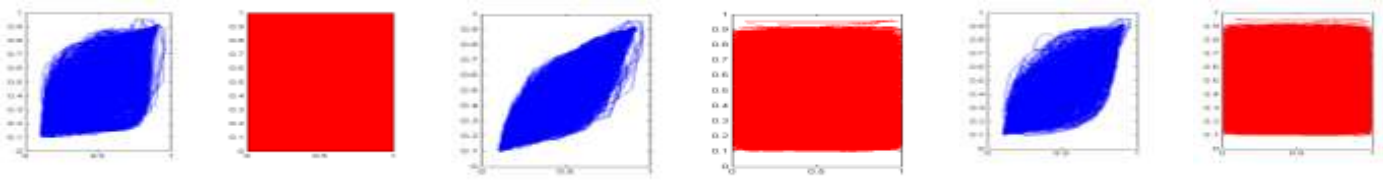
Image	**Correlation coefficient value for the encrypted image**
Lena	-0.0010
Pepper	-0.0013
Baboon	0.0035

Table 3. Correlation Coefficients of Neighboring Pixels for Lena Image

Neighboring pixels direction	**Original image**	**Encrypted image**
Horizontal	0.9719	-0.0009
Vertical	0.9850	0.0001
Diagonal	0.9593	0.0034

Sensitivity and Differential Attack Resistance

A secure cryptosystem must be highly sensitive to even a single-bit change in the plaintext—a property measured by the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) [31].



a b c d e f

Figure 4. Correlation distribution of adjacent pixels in the plain and ciphered, (a, c, e) Horizontal, vertical, and diagonal scatter diagrams of the original image, and (b, d, f) Horizontal, vertical, and diagonal scatter diagrams of cipher image.

NPCR & UACI: Results in Table 4 show that the proposed scheme yields higher NPCR and UACI scores than competing methods, indicating superior robustness against differential attacks.

Plaintext Sensitivity: Analysis of two Lena images differing by only one bit (Table 5) shows a high NPCR and low correlation between their respective ciphertexts. This confirms the system is impervious to plaintext-based attacks.

Table 4. Comparative Analysis of NPCR and UACI with Existing Literature (Lena image)

Method (reference)	**NPCR**	**UACI**
Proposed method	99.6300	33.4527
Ref. [24]	99.6040	33.4694
Ref. [25]	99.6262	33.4223
Ref. [26]	99.6281	33.4608
Ref. [27]	99.6193	33.4834

Key Security Analysis

Key sensitivity is paramount for resisting brute-force attempts. Tests conducted by encrypting the same image with two keys that differ by a single bit show that the resulting cipher images are entirely distinct. As shown in Table 5, the high rate of change confirms that the original data cannot be recovered even if a near-identical key is utilized, ensuring high security against key-space explorations.

Table 5. Sensitivity Analysis Results for Plaintext and Key Variations

	Correlation	**NPCR**	**Note**
Different images	0.0009	99.6223	The same image differed by only one bit with the same key
Different keys	-0.0010	99.4129	The same image with the same key differed by only one bit

Computational Efficiency

The computational efficiency of the proposed cryptosystem is a direct result of its linear time complexity, denoted as $O(M \times N)$. By streamlining the encryption process into three primary stages—bit-level permutation, chaotic substitution, and iterative block diffusion—the algorithm ensures that the total processing time scales proportionally with the number of pixels. The utilization of bitwise logical operations (XOR/XNOR) and symmetrical interchanging mechanisms significantly minimizes the overhead on the Central Processing Unit (CPU), avoiding the heavy transcendental mathematical functions often found in complex non-linear maps. Consequently, this high-throughput architecture provides an optimal balance between rigorous security and speed, making it exceptionally well-suited for real-time applications such as high-definition (UHD) video transmission and secure communication in resource-constrained environments.

Table 6 presents the per-phase computational complexity of the proposed cryptosystem. Since R is a fixed constant (R = 4), the iterative diffusion layer contributes a constant multiplicative factor, preserving the overall linear complexity of $O(M \times N)$. All three phases rely exclusively on bitwise logical operations and index-based memory access, avoiding transcendental functions and matrix inversions. This ensures that the encryption throughput scales linearly with image resolution, making the scheme equally applicable to standard 512×512 images and UHD 4K frames.

Table 6. Chaotic Parameter Contributions to Key Space

Phase	**Operation**	**Time Complexity**	**Space Complexity**
Phase 1: Bit-level Permutation	Symmetrical bit swapping	$O(M \times N)$	$O(M \times N)$
Phase 2: Chaotic Substitution	Sequence generation + XOR	$O(M \times N)$	$O(M \times N)$
Phase 3: Iterative Diffusion	R-round XNOR + feedback	$O(R \times M \times N)$	$O(M \times N)$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Total		$O(M \times N)$	$O(M \times N)$

Key Space Analysis

A fundamental requirement for any cryptographic system is a sufficiently large key space to render exhaustive brute-force attacks computationally infeasible. The theoretical minimum acceptable key space is 2^{128}. The proposed scheme derives its composite key space from four structurally independent components, each arising directly from a distinct algorithmic stage in Algorithm 2.

Component 1 — Bit-Level Split Threshold (Stage 1, Step 1)

In the Bit-level Recombination and Permutation phase, a single-point split threshold t is defined within the 8-bit pixel depth to govern the Single-point Interchanging Process. Since t can take any integer value within the 8-bit depth: $KS_1=2^8=256$

Component 2 — Chaotic Map Initial Conditions (Stage 2, Step 4–5)

The Security Key K initializes the selected chaotic system with d initial condition parameters, each represented as a 64-bit double-precision floating-point value. The effective precision of each parameter is bounded by the machine epsilon ($\approx 10^{-15}$), yielding approximately $10^{15} \approx 2^{50}$ distinguishable values per parameter, shown in Table 7. Thus: $KS_2=(10^{15})^d \approx 2^{50d}$

Component 3 — Dynamic Map Selection Index (Stage 2, Step 4)

The key-driven Switch (ID) mechanism selects among four distinct chaotic maps, introducing a discrete selection dimension: $KS_3=4=2^2$

Although modest in isolation, this component ensures session-specific architectural unpredictability, preventing an adversary from assuming a fixed underlying dynamical system.

Component 4 — Independent Round Sub-Keys (Stage 3, Step 9)

The Multi-round Iterative Diffusion Layer executes R rounds, each employing an independent 64-bit sub-key matrix for the XNOR-based Logical Masking operation. These sub-keys are structurally independent across rounds, yielding: $KS_4=(2^{64})^R=2^{64R}$ For R = 4 rounds: $KS_4 = 2^{256}$.

Since all four components are mutually independent—each arising from a distinct algorithmic stage—the total key space is their product: $KS_{total}=KS_1 \times KS_2 \times KS_3 \times KS_4$

Taking the most conservative case (Tent map, R = 4): $KS_{total}=2^{50} \times 2^2 \times 2^8 \times 2^{256}=2^{316}$

This vastly exceeds the 2^{128} threshold recommended by NIST, confirming that the proposed cryptosystem is computationally immune to brute-force enumeration.

Table 7. Chaotic Parameter Contributions to Key Space

Map	**Parameters (d)**	**Contribution**
Tent Map	1	2^{50}
Logistic Map	1	2^{50}
Henon Map	2	2^{100}
Lorenz System	3	2^{150}

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Formal Cryptanalysis and Mathematical Security Proof

To address the theoretical foundations of the proposed cryptosystem, a rigorous formal cryptanalysis and mathematical security evaluation were conducted to verify its resistance against known classical and adaptive attacks, specifically chosen-plaintext (CPA), chosen-ciphertext (CCA), and brute-force attacks.

Mathematical Proof of Resistance Against CPA and CCA

The security against chosen-ciphertext attacks (CCA) is guaranteed by the non-invertible and tight coupling between the ciphertext feedback and the chaotic parameter updating mechanism. Let $\mathrm{C_i}$ be the i-th ciphertext block and K_i be the dynamically updated chaotic state. The encryption function can be modeled as a non-linear composition:

$$\mathrm{C_i} = \mathrm{F}(P_\mathrm{i}, K_\mathrm{i}) \text{ where } K_\mathrm{i} = \mathrm{G}(k_{\mathrm{i}-1}, C_{\mathrm{i}-1}) \quad (1)$$

Because the dynamic map selection and the parameter state $K_\mathrm{i}$depend strictly on the previous ciphertext $C_{\mathrm{i}-1}$, any adaptive alteration of a ciphertext block during a CCA scenario completely disrupts the state evolution equation G for all subsequent steps. This mathematical avalanche effect ensures that an attacker cannot deduce any meaningful differential relation between the chosen ciphertexts and their corresponding plaintexts.

Regarding resistance against classical cryptanalytic attacks, the proposed cryptosystem demonstrates strong robustness against chosen-plaintext (CPA) and chosen-ciphertext (CCA) attacks due to the combined effect of dynamic chaotic map selection and feedback-driven diffusion. A minute modification in the plaintext, even at the single-bit level, propagates nonlinearly through the encryption pipeline and significantly alters the generated chaotic sequences, substitution behavior, and diffusion outputs. Experimental analysis confirms this high sensitivity, where a one-bit modification in the plaintext yields an NPCR value of 99.6223% and produces ciphertexts with negligible correlation (0.0009), indicating that statistically related plaintexts generate completely decorrelated ciphertexts.

Furthermore, the key-dependent dynamic map selection mechanism prevents an attacker from predicting or reconstructing the substitution architecture, since different sessions may employ entirely different chaotic systems and initial conditions. Even a one-bit modification in the encryption key produces substantially different ciphertext outputs, achieving an NPCR of 99.4129% with near-zero correlation (−0.001). This high key sensitivity ensures that neither the selected chaotic map nor the generated substitution sequence can be reliably inferred through adaptive plaintext–ciphertext observations.

The effectiveness of the diffusion stage is further supported by the extremely low adjacent-pixel correlation coefficients observed in encrypted images, approaching zero across horizontal (−0.0009), vertical (0.0001), and diagonal (0.0034) directions, compared to the strong correlations present in the original image. In addition, the encrypted images achieve an information entropy of 7.993, which is very close to the ideal value of 8 for a perfectly random 8-bit image. Collectively, these properties indicate that the proposed cryptosystem effectively suppresses statistical leakage and exhibits strong resistance against statistical, chosen-plaintext, and related adaptive cryptanalytic attacks.

Brute-Force Complexity Evaluation

A fundamental requirement for the proposed cryptosystem is establishing a computationally unfeasible barrier against exhaustive search attacks. As comprehensively detailed and mathematically calculated in Section 4.5 (Key Space Analysis), the total key space K_{Stotal} is derived from four mutually independent algorithmic stages. Under the most conservative operational scenario (employing the 1-dimensional Tent map and executing a minimal R = 4 diffusion rounds), the lower bound of the total key space is established at 2^{316}. Consequently, the brute-force attack complexity for the proposed scheme is strictly bounded by $O(2^{316})$. Since this security margin vastly transcends the standard NIST threshold of 2^{128}, an exhaustive key enumeration attack remains computationally impossible and completely out of reach for modern and foreseeable high-performance computing infrastructures

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

DISCUSSION AND LIMITATIONS

The experimental results demonstrate that the proposed image cryptosystem effectively addresses the primary vulnerabilities associated with digital image transmission. The integration of dynamic bit-level swapping, multi-map substitution, and multi-round iterative diffusion provides a comprehensive multi-layered defense that significantly outperforms standard cryptographic methods.

Discussion

The following subsections present a structured analysis of the experimental outcomes, examining the synergistic interactions between the proposed architectural components, their collective resistance to modern cryptanalytic threats, and their practical implications relative to contemporary encryption methods.

Synergistic Effect of Permutation and Dynamic Diffusion

The high entropy and uniform histograms observed are direct results of the hybrid architecture. By treating the image as a one-dimensional bit-stream and employing symmetrical bit-level swapping, the system breaks spatial correlations more effectively than traditional pixel-shuffling. Furthermore, the introduction of a key-driven dynamic switching mechanism—which rotates between Tent, Lorenz, Logistic, and Henon maps—ensures that the substitution process is session-specific and highly unpredictable. This is evidenced by the correlation coefficients, which drop from near-unity to near-zero, successfully masking the structural features of the original image.

Robustness Against Modern Cryptanalysis

The system's performance in NPCR and UACI tests highlights its formidable strength against differential attacks. The sensitivity of the dynamic chaotic selection, combined with the feedback-driven iterative diffusion layer, ensures that small changes in either the plaintext or the key propagate exponentially throughout the ciphertext. This multi-map approach specifically mitigates the risk of modeling attacks, as the underlying dynamical system changes based on the security key.

Comparison and Practical Implications

When compared to existing systems, the proposed approach consistently yields superior metrics in entropy and differential resistance. The use of XNOR-based logical masking and independent sub-keys ensures that the system remains computationally efficient with a linear time complexity of $O(M \times N)$ while providing high-level security. These findings suggest that the methodology is well-suited for secure real-time image communication and high-definition video encryption in environments where statistical and differential attacks are prevalent.

Limitations

One of the primary constraints of our framework lies in its sensitivity to synchronous chaotic parameters. Since the effectiveness of the Chaotic Sequence-based Substitution phase relies heavily on the precise initialization of the non-linear dynamical system, any negligible discrepancy in floating-point precision across diverse hardware architectures can pose challenges for decryption consistency. This necessitates a high degree of synchronization between the encryption and decryption environments to ensure the integrity of the recovered data.

Furthermore, the architecture is currently constrained by fixed block-size requirements within the Multi-round Iterative Diffusion Layer. While the segmentation process is highly optimized for uniform data blocks, it may encounter limitations when processing images with non-standard resolutions that do not align perfectly with the predefined block dimensions. In such instances, the system requires additional padding mechanisms or pre-processing steps, which could slightly increase the overall data overhead during the transmission of non-conventional visual data.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

CONCLUSION AND FUTURE WORK

This paper presented a tripartite image cryptosystem that addresses the fundamental vulnerabilities inherent to digital image transmission by operating directly at the bit-stream level rather than the conventional pixel level. The proposed architecture integrates three structurally complementary stages: Bit-level Recombination and Permutation, Dynamic Multi-Map Chaotic Substitution, and a Multi-round Iterative Block Diffusion Layer, each engineered to target a distinct class of cryptanalytic threat.

The first stage disrupts spatial redundancies through a symmetrical Single-point Interchanging Process applied uniformly across the image bit-stream, achieving near-zero inter-pixel correlation across horizontal, vertical, and diagonal directions—with empirical values collapsing from approximately 0.97 in the plain image to below 0.004 in the ciphertext. The second stage introduces session-specific unpredictability through a key-driven dynamic selection mechanism that rotates among four structurally distinct non-linear dynamical systems: the Tent, Logistic, Henon, and Lorenz maps. This architectural variability prevents adversaries from constructing a fixed model of the substitution layer and significantly expands the effective key space. The third stage consolidates the diffusion effect through an iterative block-cipher structure employing XNOR-based logical masking against independent round sub-keys and a non-linear feedback loop, ensuring that local plaintext perturbations propagate globally throughout the ciphertext.

Quantitative evaluation across standard 512×512 benchmark images confirmed the following empirical outcomes. The system achieves a ciphertext information entropy of 7.9993—approaching the theoretical maximum of 8.0 for an 8-bit grayscale image—alongside a near-uniform histogram distribution, collectively confirming resistance to statistical and frequency-based cryptanalysis. Differential attack resistance was validated through NPCR and UACI metrics of 99.6300% and 33.4527%, respectively, which are competitive with contemporary state-of-the-art schemes. Plaintext sensitivity analysis further demonstrated that a single-bit modification in the input image produces ciphertexts with a correlation of 0.0009 and an NPCR of 99.6223%, while a one-bit perturbation in the secret key yields a correlation of −0.001 and an NPCR of 99.4129%, confirming that neither the plaintext nor the key can be approximated without complete knowledge of both. The composite key space, derived from four structurally independent algorithmic components, satisfies a lower bound of 2^{316}, vastly exceeding the NIST-recommended threshold of 2^{128}. Finally, the linear time complexity of $O(M \times N)$, achieved through exclusive reliance on bitwise logical operations, ensures that the security gains are not purchased at the cost of computational feasibility, making the scheme viable for real-time and resource-constrained deployment scenarios.

Taken collectively, these results establish that the proposed cryptosystem achieves a principled balance between cryptographic depth and computational efficiency. The bit-level granularity of the permutation stage, the architectural session-specificity of the substitution layer, and the feedback-driven non-linearity of the diffusion stage form a mutually reinforcing defense that demonstrates strong resistance against statistical and differential attacks while maintaining a sufficiently large key space against brute-force exploration.

Future Work

Building upon the findings of this study, several avenues for future research are identified to further advance the field of secure image communication. A primary focus will be directed toward hardware acceleration and optimization. Future research will focus on the hardware implementation of the proposed architecture using FPGA or GPU acceleration to mitigate computational latency and facilitate high-speed real-time encryption for ultra-high-definition (UHD) video streams.

Furthermore, future investigations will explore the integration of adaptive chaotic systems, specifically utilizing the use of hyper-chaotic systems with higher-dimensional maps to further expand the key space and enhance the complexity of the Chaotic Sequence-based Substitution layer.

Finally, future iterations of this work will aim to extend the cryptosystem's capabilities to accommodate volumetric and multi-dimensional data formats, i.e., 3D medical imaging (DICOM), ensuring robust protection for diverse data formats.

REFERENCES

1. Su, Y., Teng, L., Yan, X., Sun, C., & Xian, Y. (2026). Spatiotemporal chaos in a recursively permuted lattice with dual maps on odd and even sites and its application in image encryption. Physica Scripta, 101, Article 075203. https://doi.org/10.1088/1402-4896/ae3fde
2. Jackson, J., & Perumal, R. (2026). A robust medical image encryption technique using inverse cosine chaotic map. Expert Systems with Applications, 298, Article 129574. https://doi.org/10.1016/j.eswa.2025.129574
3. Devi, C. S., & Amirtharajan, R. (2025). A novel 2D MTMHM based key generation for enhanced security in medical image communication. Scientific Reports, 15, Article 25411. https://doi.org/10.1038/s41598-025-10485-1
4. Wang, X., Liu, X., & Peng, J. (2025). A novel image encryption scheme based on a 3D enhanced chaotic map and DNA computing model. Journal of the Franklin Institute, 362, Article 107790. https://doi.org/10.1016/j.jfranklin.2025.107790
5. Özpolat, E., Çelik, V., & Gülten, A. (2025). Hyperchaotic system-based PRNG and S-box design for a novel secure image encryption. Entropy, 27, Article 299. https://doi.org/10.3390/e27030299
6. Qiu, D., Zhang, T., Liu, J., Liu, S., & He, P. (2025). An innovative image encryption algorithm based on the DNAS_box and hyperchaos. Entropy, 27, Article 239. https://doi.org/10.3390/e27030239
7. Ding, S., Shi, F., Erkan, U., Toktas, A., Li, Q., Wang, C., Gao, S., & Mou, J. (2026). Design of a three-dimensional Logistic map and its application to seafood image encryption. The Journal of Supercomputing, 82, Article 225. https://doi.org/10.1007/s11227-025-08196-5
8. Obaid, M. J., Neamah, A. A., Shukur, A. A., Pham, V. T., & Grassi, G. (2025). A reliable color image encryption scheme based on a novel dual-wing hyperchaotic map. Expert Systems with Applications, 289, Article 128237. https://doi.org/10.1016/j.eswa.2025.128237
9. Lin, Y., Wei, Y., Chen, D., Li, Y., Erkan, U., Toktas, A., Gao, S., & Zhang, Y. (2026). Cryptanalysis and improvement of a video cryptosystem via chaos and S-box. ACM Transactions on Multimedia Computing, Communications, and Applications. Advance online publication. https://doi.org/10.1145/3808699
10. Sun, S., Yang, W., Yin, Y., Tian, X., Li, G., & Deng, X. (2025). A color image encryption scheme utilizing a logistic-sine chaotic map and cellular automata. Scientific Reports, 15, Article 21603. https://doi.org/10.1038/s41598-025-04968-4
11. Gao, J., & Teng, L. (2025). A chaotic multi-image encryption scheme based on block space jump scrambling and dynamic sliding queue diffusion. Nonlinear Dynamics, 113, 31691–31723. https://doi.org/10.1007/s11071-025-11690-3
12. Sarra, B., Sun, H., Dua, M., Dua, S., & Dhingra, D. (2026). A novel 1D powered Chebyshev quadratic map-based image encryption using dynamic permutation-diffusion. Scientific Reports, 16, Article 9469. https://doi.org/10.1038/s41598-026-38483-x
13. Lin, Y., Liao, Y., Zeng, W., Wei, Y., Chen, D., Yuan, X., Li, Y., Erkan, U., Toktas, A., & Zhang, C. (2026). 3D non-degenerate hyperchaos: Design, analysis, and application in image encryption. IEEE Transactions on Consumer Electronics. Advance online publication. https://doi.org/10.1109/TCE.2026.3672135
14. Kareem, S., & Pirdawood, M. (2026). Algebraically enhanced 3D chaotic map with hash-based initialization for secure image encryption. Theory of Computing Systems, 70, Article 30. https://doi.org/10.1007/s00224-026-10274-x
15. Yan, S., Liu, Y., Zhang, J., & Jiang, D. (2026). Medical image encryption algorithm based on a novel 4D chaotic system and dynamic zigzag transformation. Physica Scripta, 101(8), Article 085202. https://doi.org/10.1088/1402-4896/ae45d5
16. Duan, Y., Xu, X., Banerjee, S., Cao, Y., & Mou, J. (2026). A multi-image encryption scheme for gray-color images based on 2D chaotic map and dual S-boxes. Nonlinear Dynamics, 114, Article 249. https://doi.org/10.1007/s11071-025-12116-w
17. Deepankumar, S., Rengaraj, R., Pranesh, R., Mishra, P., & Pal, A. K. (2026). A 3D chaotic map-based novel intra and inter-level bit plane image content encryption. Journal of Information Security and Applications, 98, Article 104389. https://doi.org/10.1016/j.jisa.2026.104389

18. Wu, L., Tian, Z., & Chen, W. (2026). Color image encryption scheme based on 5D fractional-order complex chaotic system and eight-base DNA cubes. Expert Systems with Applications, 299, Article 129950. https://doi.org/10.1016/j.eswa.2025.129950
19. Wen, J., Xu, X., Sun, K., Jiang, Z., & Wang, X. (2023). Triple-image bit-level encryption algorithm based on double cross 2D hyperchaotic map. Nonlinear Dynamics, 111(7), 6813–6838. https://doi.org/10.1007/s11071-022-08158-z
20. Wang, M., Wang, X., Zhao, T., Zhang, C., Xia, Z., & Yao, N. (2021). Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme. Information Sciences, 544, 1–24. https://doi.org/10.1016/j.ins.2020.07.051
21. Alexan, W., Shabasy, N. H. E., Ehab, N., & Maher, E. A. (2025). A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations. Scientific Reports, 15(1), Article 31246. https://doi.org/10.1038/s41598-025-15794-z
22. Moysis, L., Lawnik, M., Alexan, W., Goudos, S. K., Baptista, M. S., & Fragulis, G. F. (2025). Exploiting circular shifts for efficient chaotic image encryption. IEEE Access, 13, 92997. https://doi.org/10.1109/ACCESS.2025.3572589
23. Alexan, W., Youssef, M., Hussein, H. H., et al. (2025). A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5. Scientific Reports, 15, Article 9775. https://doi.org/10.1038/s41598-025-92065-x
24. Lin, Z., & Liu, H. (2024). Constructing a non-degeneracy 3D hyperchaotic map and application in image encryption. Multimedia Tools and Applications, 83, 82049–82068. https://doi.org/10.1007/s11042-024-18741-8
25. Wang, M., Teng, L., Zhou, W., Yan, X., Xia, Z., & Zhou, S. (2025). A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption. Expert Systems with Applications, 261, Article 125328. https://doi.org/10.1016/j.eswa.2024.125328
26. Zhang, J., Zhou, W., Wang, M., & Lin, Y. (2026). 3D-TCM-driven bit-level image encryption via S-box feedback algorithm. Entropy, 28(5), Article 535. https://doi.org/10.3390/e28050535
27. Zhang, X., & Hu, H. (2026). Image encryption algorithm based on a new two-dimensional chaotic system and rotating dial model. Entropy, 28(5), Article 530. https://doi.org/10.3390/e28050530
28. Wu, W., & Kong, L. (2024). Image encryption algorithm based on a new 2D polynomial chaotic map and dynamic S-box. Signal, Image and Video Processing, 18, 3213–3228. https://doi.org/10.1007/s11760-023-02984-3
29. Wang, Q., Zhang, X., & Zhao, X. (2023). Image encryption algorithm based on 2D hyper-chaotic system and central dogma of molecular biology. Physica Scripta, 98, Article 085244. https://doi.org/10.1088/1402-4896/ace5ee
30. Liu, X., Zheng, S., & Yang, J. (2026). Color image encryption scheme based on a novel 2D-CLCM chaotic system and RNA encoding. Mathematics and Computers in Simulation, 239, 340–360. https://doi.org/10.1016/j.matcom.2025.06.009
31. Aibai, A., Nuermaimaiti, M., Tuersun, Y., & Ghopur, D. (2026). A novel 2D hyperchaotic map for secure financial data encryption. Entropy, 28, Article 262. https://doi.org/10.3390/e28030262