An Enhanced Secure and Fast Image Encryption Algorithm Based on Chaos Systems and DNA Coding

Safae Amine
Laboratory of Applied Sciences and Emerging Technologies, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco
safae.amine@usmba.ac.ma

Fatima Koulouh
Laboratory of Applied Sciences and Emerging Technologies, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco
fatima.koulouh@usmba.ac.com

Mohammed Es-Sabry
Department of Information Security, Intelligent Systems and Application, Faculty of Sciences, Abdelmalek Essaadi University, Tetouan, Morocco
m.essabry@uae.ac.ma

Nabil El Akkad
Laboratory of Applied Sciences and Emerging Technologies, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco
nabil.elakkad@usmba.ac.ma

Walid El-Shafai
Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia | Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt
welshafai@psu.edu.sa (corresponding author)

Ahmad Taher Azar
College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia | Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia
aazar@psu.edu.sa

Selma Abdelrahman Hussein
Research and Initiative Center, Prince Sultan University, Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia
sabdulrahman@psu.edu.sa (corresponding author)

Received: 2 December 2025 | Revised: 4 January 2026, 21 January 2026, and 11 February 2026 | Accepted: 13 February 2026

 DOI: https://doi.org/10.48084/etasr.16670

ABSTRACT

This study presents an enhanced color image encryption algorithm that integrates multiple techniques to ensure high levels of security, efficiency, and robustness. The encryption process begins with circular shift and rotation operations to permute the pixel positions and disrupt spatial relationships within the image. This is followed by the application of two one-dimensional chaotic maps, specifically, the Tent Map and the

Hénon Map, which generate pseudo-random sequences that are subsequently combined with the original image through sequential XOR operations, thereby inducing significant confusion in the pixel values. To further strengthen security, a final layer of DNA-based encryption introduces an additional level of complexity and enhances resistance against both statistical and differential attacks. The performance and reliability of the proposed algorithm were rigorously evaluated across multiple test images using a comprehensive set of security metrics, including histogram uniformity, correlation coefficients, entropy, Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE). The proposed algorithm demonstrates high sensitivity to minor changes in either the encryption key or the input image, as evidenced by elevated values in the Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) metrics. Comparative analysis against several state-of-the-art encryption schemes highlights the superiority of the proposed method in terms of both security strength and computational performance. These findings validate the proposed approach as a promising solution for secure image transmission in modern digital communication systems.

Keywords-image encryption; chaotic maps; tent map; Hénon map; DNA cryptography; circular shift and pixel permutation; XOR operation

I. INTRODUCTION

In today's digital landscape, where large volumes of data are transmitted over global networks, cryptography plays a crucial role in ensuring secure information exchange. Its primary objective is to protect the confidentiality, integrity, and authenticity of data from unauthorized access. Cryptographic techniques are widely used in digital image encryption for applications such as medical imaging, computer vision, image segmentation, camera auto-calibration, and 3D reconstruction, where sensitive visual data requires strong protection. Recent studies on secure image data processing report that, despite significant progress, existing image encryption schemes still face challenges related to computational efficiency and practical deployment [1]. These limitations motivate the development of more robust encryption frameworks.

To address these challenges, various cryptographic approaches have been investigated, including chaotic systems, chemical reactions, and optical mechanisms. Among them, chaotic systems have attracted considerable attention due to their deterministic randomness, high sensitivity to initial conditions, and strong dependence on control parameters, which makes them suitable for image encryption [2]. Chaotic systems can be classified into low- and high-dimensional models, each offering different security and computational trade-offs. The Arnold Cat Map is a well-known chaotic transformation that provides both confusion and diffusion. However, its periodic behavior, which can restore the original image after a fixed number of iterations, limits its cryptographic strength. To overcome such weaknesses, modern encryption schemes often combine multiple cryptographic techniques to enhance robustness and resistance to statistical and differential attacks [3].

In image encryption, the encryption key is a critical component of security. Effective keys must be sufficiently complex, large, and sensitive to parameter variations to resist brute-force and plaintext attacks. Chaotic maps with multiple control parameters provide an efficient solution by generating highly sensitive and dynamic keys, significantly improving security [4].

Although numerous chaos-based image encryption schemes have been reported in the literature, several critical limitations remain. Many existing approaches rely on static keys, weak coupling between permutation and diffusion stages, or a limited number of encryption rounds, which reduces their resistance to known-plaintext and chosen-plaintext attacks. Moreover, some hybrid schemes combine chaotic maps in a straightforward manner without fully exploiting dynamic key dependency or non-linear interactions, leading to potential vulnerabilities and reduced robustness. In addition, achieving a balance between high security, computational efficiency, and practical applicability in modern digital communication systems remains a challenging research problem.

Based on these observations, this paper proposes a hybrid image encryption approach, with the following contributions:

1. A hybrid encryption framework combining multiple cryptographic techniques to enhance security and unpredictability.
2. Improved confusion and diffusion mechanisms to strengthen resistance against statistical and differential attacks.
3. Dynamic key generation derived from the plain image, increasing sensitivity to minor content changes.

II. RELATED WORKS

A considerable body of research has focused on the development of image encryption techniques aimed at securing visual data and preventing unauthorized access. These techniques range from classical cryptographic algorithms, such as the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA), to more contemporary approaches, including chaotic systems and hybrid models combining multiple encryption principles. Although traditional algorithms provide a foundational level of security, their deterministic nature and relatively predictable structure often make them less suitable for applications that require high degrees of randomness and nonlinearity, such as image encryption [5-7]. Incorporating advanced operations further enhances resistance to statistical analysis, differential attacks, and brute-force cryptanalysis [8-10].

To overcome these limitations, researchers have increasingly explored hybrid schemes that integrate chaotic systems with DNA-based cryptographic operations. These approaches leverage the inherent unpredictability and

sensitivity to initial conditions of chaotic maps, along with the strong nonlinearity and diverse rules of DNA encoding mechanisms. For instance, in a chaos-DNA-based image encryption scheme [11], chaotic sequences control both pixel permutation and dynamic DNA encoding/decoding rules. Combining multiple chaotic maps with DNA arithmetic operations resulted in strong key sensitivity and excellent resistance to differential attacks, as reflected in high NPCR and UACI values. However, the relatively complex architecture of this scheme may increase computational cost and limit scalability.

In [12], an improved chaos-DNA encryption framework was based on hyperchaotic systems and adaptive DNA operations. Here, chaotic sequences dynamically determine DNA coding rules and arithmetic operations, further enhancing randomness and security. Although the method achieves strong statistical performance, the interaction between the permutation and diffusion stages remains partially decoupled, leaving room to strengthen confusion-diffusion coupling. More recently, a chaos-driven DNA-based image encryption algorithm [13] demonstrated strong resistance to histogram and correlation attacks. This approach effectively leveraged DNA encoding to increase encryption complexity; however, it relied on a limited set of DNA rules and showed relatively weak dependency on plaintext characteristics, which may reduce robustness against advanced chosen-plaintext or chosen-ciphertext attacks.

Despite the effectiveness of chaos-DNA-based schemes, challenges remain, including the use of static or weakly adaptive DNA rules, limited plaintext dependency, and insufficient coupling between chaotic permutation and DNA-based diffusion. These limitations motivate the development of encryption frameworks that further enhance confusion-diffusion interaction, dynamic key dependency, and adaptability to plaintext variations.

Motivated by these observations, this work proposes a novel hybrid image encryption scheme that tightly integrates one-dimensional chaotic maps (Hénon and Tent Maps) with dynamic DNA-based cryptographic operations. Unlike existing approaches, the proposed one strengthens the permutation-diffusion interaction, introduces plaintext-dependent key generation, and employs adaptive DNA rules. This design enhances confusion-diffusion coupling, improves resistance to statistical and differential attacks, and ensures strong robustness against chosen-ciphertext attacks. Comprehensive security analyses, including correlation, histogram uniformity, NPCR, UACI, PSNR, and entropy, confirm the effectiveness and security of the proposed encryption framework.

III. PROPOSED METHOD

This section presents the design and operational details of the proposed image encryption algorithm, which integrates chaotic systems, pixel permutation techniques, and DNA-based cryptographic operations to ensure high security and efficiency. The method is structured into two main phases: the diffusion phase, which disturbs the spatial arrangement of pixels through rotation and circular shift operations, and the confusion phase, which modifies pixel values using chaotic sequences generated from the Tent and Hénon maps. An additional DNA encoding layer is applied to further enhance encryption strength. Each component of the system is carefully selected and configured to maximize entropy, randomness, and sensitivity to initial conditions, thereby ensuring robustness against cryptographic attacks. The following subsections detail the individual building blocks of the proposed approach and their integration into the overall encryption workflow.

A. Circular Shift Operation

Circular shift operation is a fundamental cyclic permutation technique widely utilized in computing applications such as optimization, cryptography, and digital signal processing. Within the context of image encryption, it serves as a crucial mechanism for achieving pixel-level diffusion, thereby obscuring the spatial structure of the original image. The core principle of the circular shift lies in cyclically moving elements, typically bits or pixel values, either to the left or right. Unlike linear shifts that discard bits at the boundaries, the circular shift reinserts the bits that exit from one end back into the opposite end, preserving the overall data volume while altering its arrangement.

Formally, the operation can be described as a permutation δ over E entries, controlled by a shift parameter $n > 0$, which acts as the key for the transformation. The circular shift is defined as follows:

$$\delta\,(p) = (p \pm n)\ mod\ (E);\ \ p = 1, \ldots., E \qquad (1)$$

where p denotes the original position of an element, n represents the number of positions to shift, and the modulus operation ensures that the result wraps around within the bounds of the data array. This operation is particularly effective in the preprocessing stage of image encryption, as it enhances the initial permutation of pixels, thus contributing to the overall confusion and diffusion properties of the encryption algorithm.

B. Tent Map

The Tent Map is a one-dimensional chaotic function frequently employed in dynamical systems and chaos theory due to its simplicity and ability to generate complex, unpredictable sequences. It is particularly well-suited for cryptographic applications, where randomness and sensitivity to initial conditions are critical for ensuring secure data transformation. Mathematically, the Tent Map is defined as a piecewise linear and continuous function that exhibits chaotic behavior under specific parameter constraints. Its iterative form is expressed as follows:

$$x_{j+1} = f(x_j) = \begin{cases} n\,.\,x_j\,, & if\ \ x_j < \frac{1}{2} \\ n\,.\,(1 - x_j), & if\ x_j \geq \frac{1}{2} \end{cases} \qquad (2)$$

In this formulation, $x_j \in [0, 1]$ represents the current state, and n is a control parameter that determines the map's dynamical properties. To ensure the output remains within the unit interval [0, 1] and exhibits chaotic behavior, the value of n must be constrained to the range $0 < n \leq 2$.

When properly configured, the Tent Map produces a sequence of values that are highly sensitive to initial conditions and exhibit an apparent randomness, which is essential for

confusion in image encryption algorithms. This pseudo-random behavior enhances the unpredictability of pixel value transformation, significantly increasing the security of the encryption process.

Figure 1 illustrates the bifurcation diagram and the Lyapunov exponent of the Tent Map, both of which provide visual evidence of the map's chaotic nature under varying parameter values.

C. Hénon Map

The Hénon Map is a well-established mathematical model representing a discrete-time, two-dimensional dynamical system that exhibits chaotic behavior. Originally introduced by Michel Hénon in 1976, it serves as a simplified model of the Poincaré section of the Lorenz attractor and has since become a foundational component in the study of nonlinear dynamical systems and chaos theory. The standard form of the Hénon map is defined by the following pair of recursive equations:

$$T(x_{j+1}) = \begin{cases} x_{j+1} = n - x_j^2 + y_j \\ y_{j+1} = m \,.\, x_j \end{cases} \quad (3)$$

In this system, x_j and y_j are the state variables at iteration j, while n and m are real-valued parameters that govern the system's dynamics. For specific values of n and m, the map exhibits a strange attractor, an invariant fractal structure in phase space that is highly sensitive to initial conditions and unpredictable over time, a hallmark of chaotic systems [14].

The proposed encryption method adopts a simplified one-dimensional adaptation of the Hénon Map, which preserves its chaotic characteristics while reducing computational complexity. This modified version is given by:

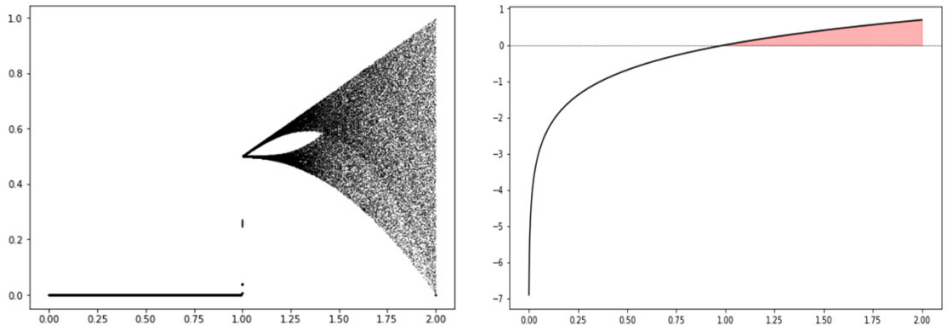
$$x_{j+1} = 1 - n \,.\, x_j^2 + m \,.\, x_j \quad (4)$$

This 1D variant maintains the essential properties of the original Hénon Map and is suitable for generating pseudo-random sequences required in the encryption process. The chaotic sequences generated from this map are used to perturb pixel values, contributing to the confusion phase of the proposed algorithm.

Figure 2 presents the bifurcation diagram and the Lyapunov exponent for the 1D Hénon Map, visually confirming the presence of chaos across various parameter values and validating its effectiveness for cryptographic use.

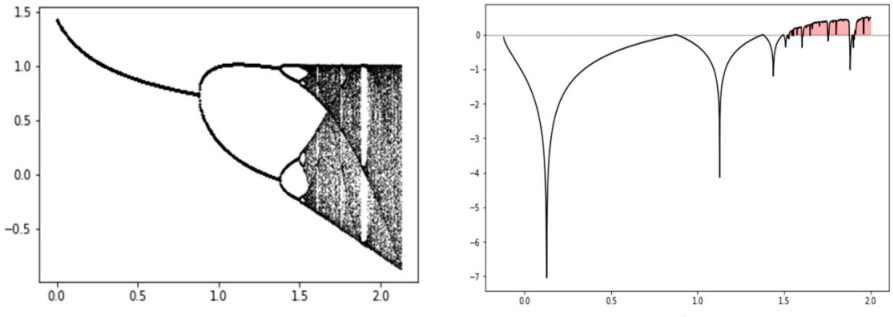
D. DNA-Based Encryption

DNA encryption, also referred to as DNA cryptography, is an innovative approach that leverages principles of molecular biology, particularly DNA coding, to perform secure data encryption. Initially developed to protect genetic data, DNA-based cryptography has gained attention in the field of image encryption due to its inherent advantages, including high information density, ultra-low power consumption, and parallel processing capabilities. These features make DNA a compelling medium for developing highly secure and computationally efficient cryptographic schemes [15].



(a) (b)

Fig. 1. (a) Bifurcation diagram of the Tent Map, and (b) Lyapunov exponent diagram of the Tent map.



(a) (b)

Fig. 2. (a) Bifurcation diagram of the Hénon map, and (b) Lyapunov exponent diagram of the Hénon map.

At its core, DNA encryption relies on the four fundamental nucleotides that constitute DNA strands: Cytosine (C), Thymine (T), Adenine (A), and Guanine (G). These nucleotides can be mapped to binary pairs, enabling digital data to be encoded as DNA sequences. Table I summarizes the typical binary representation used. Each nucleotide has a specific complementary base, which is an essential concept in DNA pairing and encryption. The complementarity relationships illustrated in Table I serve as the basis for encoding, decoding, and performing logical operations (e.g., XOR) on DNA sequences within encryption algorithms.

TABLE I. DNA NUCLEOTIDE COMPLEMENT

DNA nucleotide	Complement
C = 00	G
T = 01	A
A = 10	T
G = 11	C

In image encryption applications, each color channel (red, green, and blue) of a pixel, typically represented by 8-bit values, is segmented into 2-bit groups. These groups are then converted into DNA sequences using the mappings defined above. This process enables the integration of biological encoding principles into digital encryption systems, providing an additional layer of complexity that enhances the algorithm's resistance to brute-force, statistical, and differential attacks.

Each DNA nucleotide is encoded using a unique 2-bit binary representation. In this encryption scheme, which is specifically designed for color images, each pixel comprises 24 bits, 8 bits per color channel (red, green, and blue). To integrate DNA cryptography into this framework, each color channel is processed independently. The 8-bit value of each channel is segmented into four 2-bit pairs, which are then translated into nucleotide sequences based on the established binary-to-nucleotide mapping.

For instance, consider a pixel with the following binary values for its color channels: (R = 01001011, G = 00101100, B = 11010010). The red channel value (01001011) is divided into four 2-bit segments: '01', '00', '10', and '11'. These correspond to the nucleotide sequence 'T', 'C', 'A', and 'G', respectively, forming the DNA representation TCAG. A similar process is applied to the green and blue channels. The same encoding steps are also performed on the encryption key, which is dynamically derived from the original image using modulo operations to ensure sensitivity and uniqueness. After DNA encoding, an addition operation is applied between the key and each encoded channel. This operation is governed by the DNA addition rules defined in Table II, operating similarly to an XOR logic gate but using nucleotide symbols instead of binary digits.

TABLE II. DNA ADDITION TABLE

XOR	C	T	A	G
C	C	T	A	G
T	T	A	G	C
A	A	G	C	T
G	G	C	T	A

To retrieve the original pixel values during decryption, the reverse process is performed using DNA subtraction, which reverts the encoded data to its original form. This operation is outlined in Table III. This DNA-based encoding and arithmetic framework introduces an additional layer of complexity and non-linearity to the encryption algorithm, significantly enhancing its resistance to cryptographic analysis and brute-force decryption attempts.

TABLE III. DNA SUBTRACTION RULES.

XOR	C	T	A	G
C	C	G	A	T
T	T	C	G	A
A	A	T	C	G
G	G	A	T	C

E. The Process of the Proposed Method

The proposed encryption algorithm integrates multiple security layers, combining two one-dimensional chaotic maps, namely the Tent Map and the Hénon Map, with pixel-level permutations and DNA-based cryptographic transformations. These mechanisms are applied through two main phases: a diffusion phase, which modifies pixel positions, and a confusion phase, which alters pixel values. The secret keys used for the rotation operation and the DNA encoding process are derived from the XOR combination of pixel values from each color channel of the input image, making the generated keys highly sensitive to any minor modification in the plaintext image. In addition, the chaotic matrices generated by the Tent and Hénon maps are also considered as part of the secret key material, further enlarging the key space and strengthening resistance against cryptanalytic and brute-force attacks.

Figure 3 illustrates the complete encryption pipeline, highlighting the interaction between the various transformation stages, including key generation, permutation, chaotic mapping, and DNA operations. The algorithm proceeds as follows:

Algorithm 1: Proposed Method

Input: Begin with a color image I of dimensions $M \times N$.

1. Rotation: Compute a rotation angle from the original image using a modulus operation with 90 to avoid data loss and rotate the image accordingly.
2. Circular Shift Operation: Horizontally shift pixel values using a circular permutation, where each pixel x_i is moved to position $x_{i+n} \bmod M$.
3. Channel Separation: Decompose the rotated image into three individual color components: I_R (Red), I_G (Green), and I_B (Blue).
4. Matrix Conversion: Convert each channel into a corresponding matrix: M_R, M_G, and M_B.

5. Tent Map Sequences: Generate two pseudo-random sequences for each channel using the Tent Map: $S1_R$, $S1_G$, $S1_B$ and $S2_R$, $S2_G$, $S2_B$, based on (2).
6. Hénon Map Sequence: Generate one chaotic sequence per channel using the Hénon Map based on (4): $S3_R, S3_G, S3_B$.
7. Matrix Reshaping: Reshape all chaotic sequences into matrices of the same dimension as the respective channels (e.g., $S1_R \rightarrow M1_R$).
8. XOR Operation: For each color channel, perform an XOR operation between the original matrix and the three chaotic matrices, $M_R \oplus S1_R \oplus S2_R \oplus S3_R$, and similarly for the green and blue channels.
9. DNA Encoding: Encode the XOR result for each channel using a DNA coding scheme.
   The key for encoding is generated dynamically from the original image using a modulus operation with 256.
10. Image Reconstruction: The final encrypted image is reconstructed by combining the three DNA-encoded output and restoring the original image shape.

This multi-phase encryption strategy ensures both spatial and statistical obscurity, thereby increasing the algorithm's resilience against various forms of cryptographic attacks. The combined use of dynamic chaotic systems, spatial permutations, and biologically inspired encryption makes the method highly effective for secure image transmission.

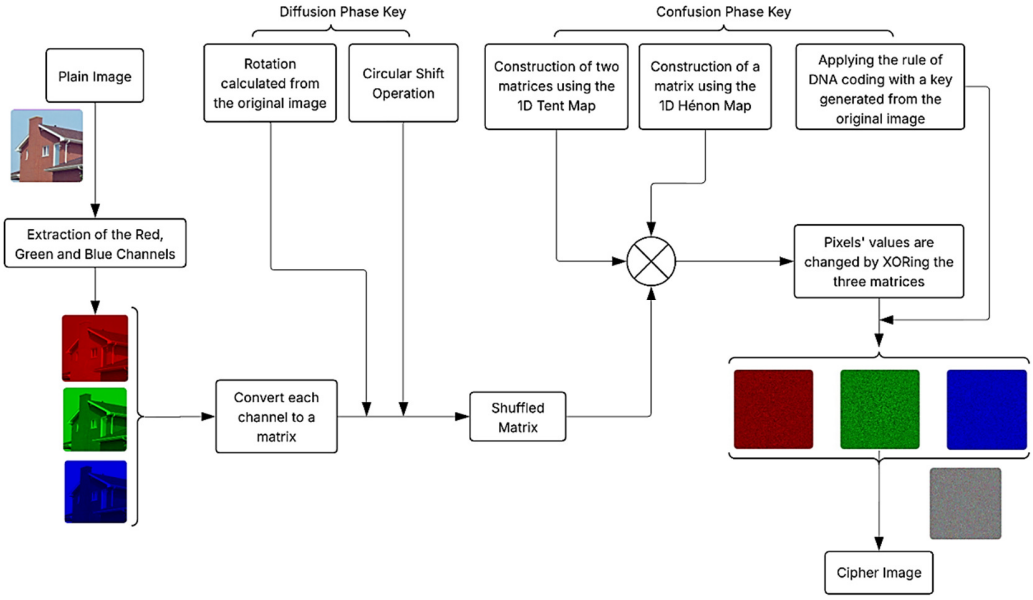


Fig. 3. Flow diagram of the proposed method.

IV. EXPERIMENTAL RESULTS

To validate the effectiveness, security, and robustness of the proposed encryption algorithm, a comprehensive set of experiments was conducted using multiple benchmark images of varying sizes and content types. Evaluation involved several key metrics that are widely recognized in the field of image cryptography, including statistical measures such as histogram uniformity, correlation analysis, entropy, and differential attack resistance (NPCR and UACI), as well as signal quality metrics such as PSNR and MSE. Each experiment was designed to assess a specific aspect of the algorithm's performance, from its ability to eliminate pixel correlation to its sensitivity to key changes and resistance against cryptanalytic techniques. The results were also compared with those of state-of-the-art encryption methods to highlight the advantages of the proposed approach.

A. Statistical Analysis

1) Histograms of Color/Grayscale Figures

Histograms are widely used in image processing and encryption analysis, as they offer a comprehensive statistical representation of the distribution of pixel intensity levels. In the context of image encryption, histogram analysis serves as a critical tool for evaluating the algorithm's ability to obscure the original image's visual characteristics. A strong encryption scheme should produce nearly uniform histograms, thereby eliminating visible patterns and rendering statistical attacks ineffective.

The effectiveness of the proposed encryption method was assessed through a series of experiments on various color images of different dimensions and content types. For each image, histograms were generated for the red, green, and blue

channels, both before and after encryption. The results, as depicted in Figures 4-9, demonstrate a significant transformation in pixel distribution following encryption. Although the original images exhibit clear and structured histograms reflective of their inherent content, the histograms of the encrypted images appear flat and uniformly distributed, indicating the absence of any recognizable pattern or structure.

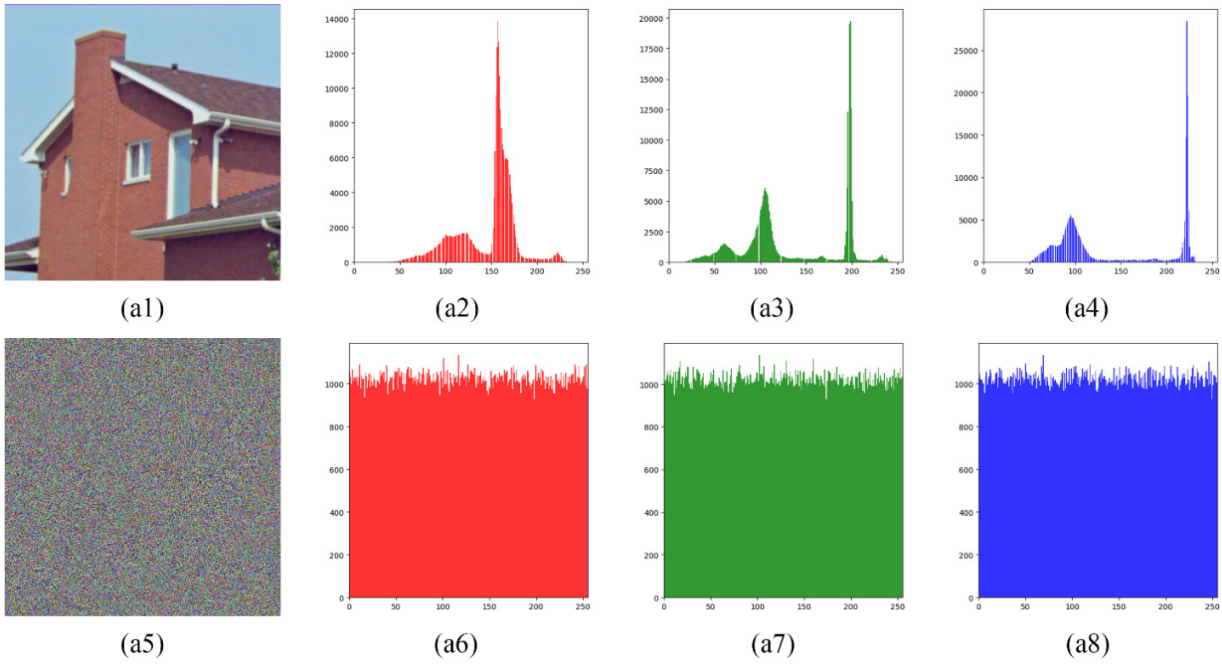


Fig. 4. (a1) House image: (a2) Red channel's histogram, (a3) Green channel's histogram, (a4) Blue channel's histogram; (a5) Encrypted image of House: (a6) Red channel's histogram, (a7) Green channel's histogram, (a8) Blue channel's histogram.

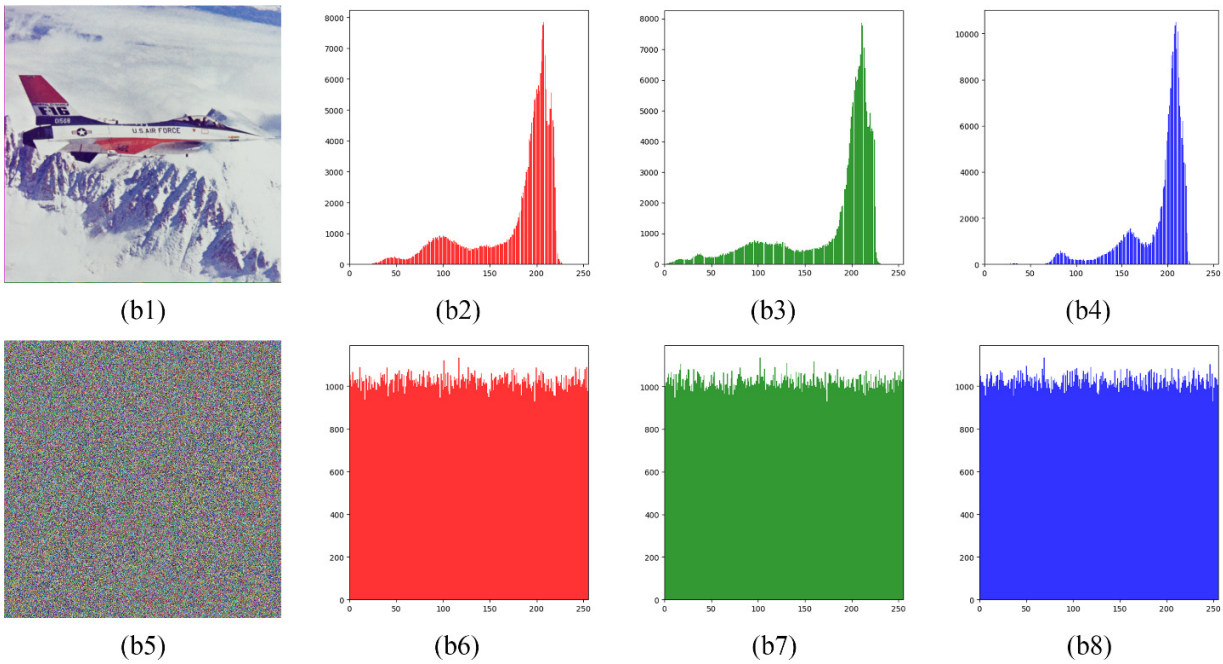


Fig. 5. (b1) Airplane image: (b2) Red channel's histogram, (b3) Green channel's histogram, (b4) Blue channel's histogram; (b5) Encrypted image of Airplane: (b6) Red channel's histogram, (b7) Green channel's histogram, (b8) Blue channel's histogram.

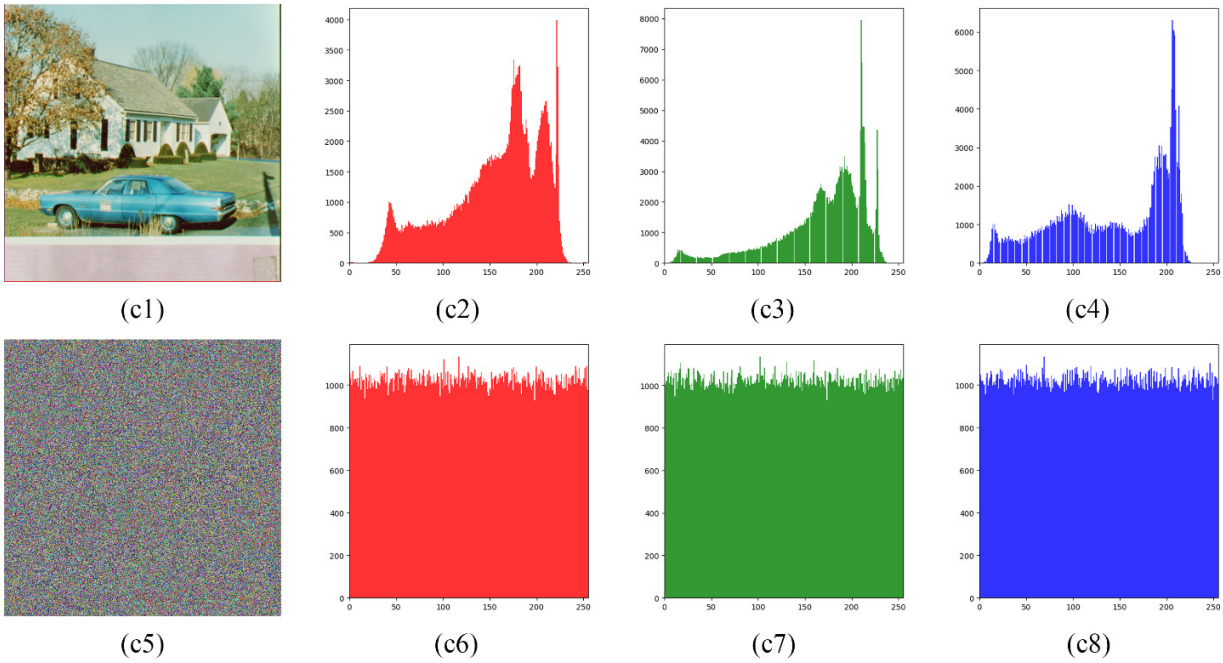


Fig. 6. (c1) Car image: (c2) Red channel's histogram, (c3) Green channel's histogram, (c4) Blue channel's histogram; (c5) Encrypted image of Car: (c6) Red channel's histogram, (c7) Green channel's histogram, (c8) Blue channel's histogram.

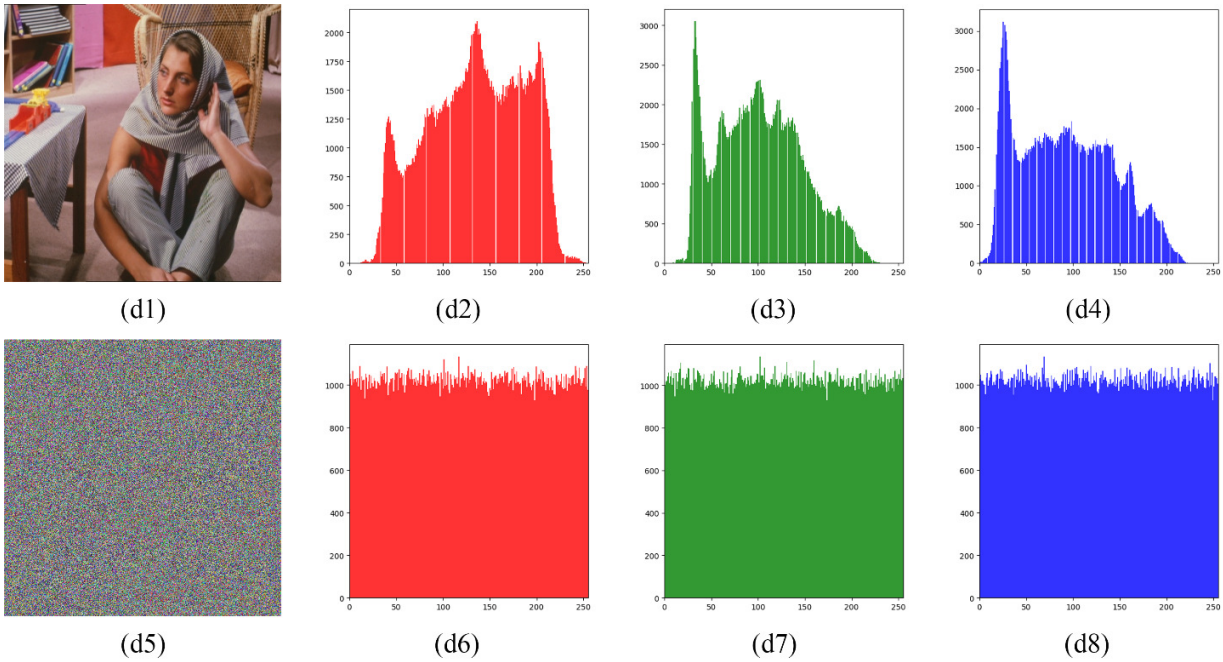


Fig. 7. (d1) Barbara image: (d2) Red channel's histogram, (d3) Green channel's histogram, (d4) Blue channel's histogram; (d5) Encrypted image of Barbara: (d6) Red channel's histogram, (d7) Green channel's histogram, (d8) Blue channel's histogram.

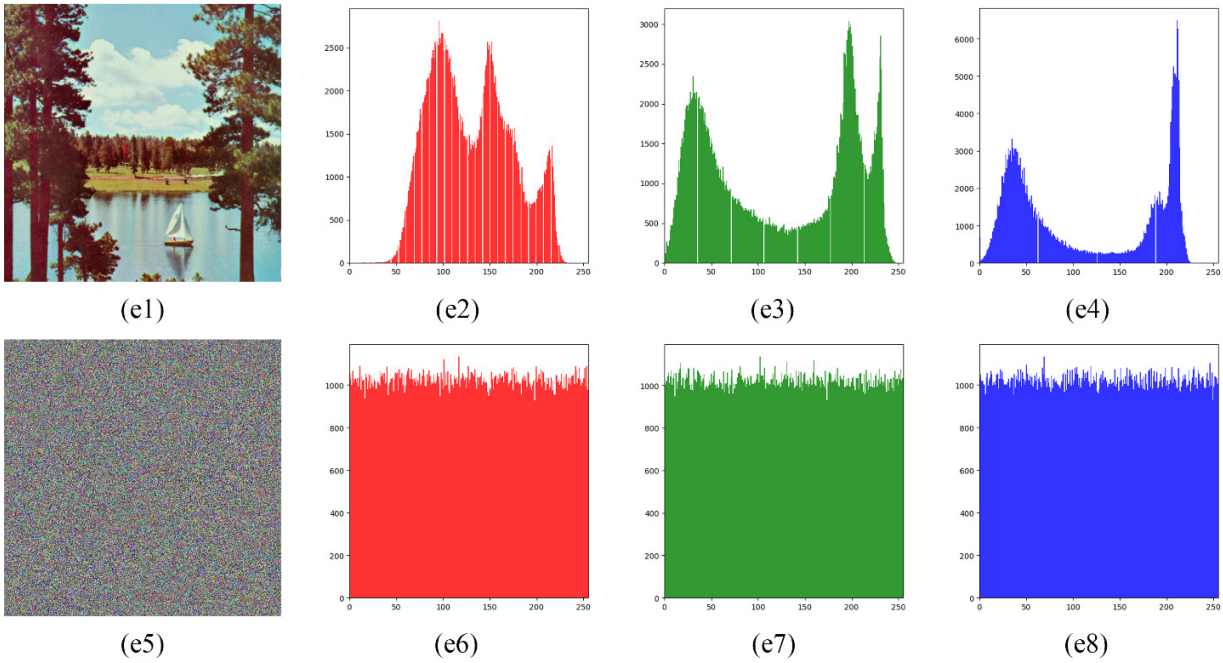


Fig. 8. (e1) Sailboat image (e2): Red channel's histogram, (e3) Green channel's histogram, (e4) Blue channel's histogram; (e5) Encrypted image of Sailboat: (e6) Red channel's histogram, (e7) Green channel's histogram, (e8) Blue channel's histogram.

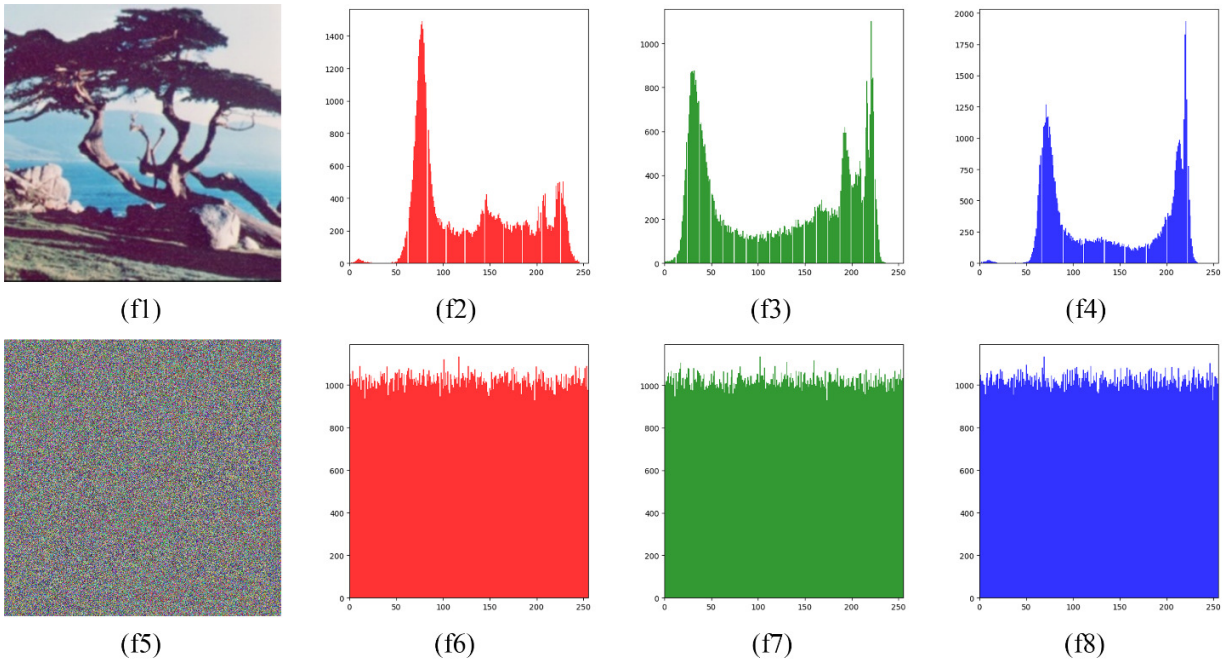


Fig. 9. (f1) Tree image: (f2) Red channel's histogram, (f3) Green channel's histogram, (f4) Blue channel's histogram; (f5) Encrypted image of Tree: (f6) Red channel's histogram, (f7) Green channel's histogram, (f8) Blue channel's histogram.

B. Correlation Analysis

In image encryption, one critical objective is to eliminate the high correlation typically observed between adjacent pixels in natural images. Original images often exhibit strong spatial correlation, especially in smooth regions where neighboring pixel values are similar. This predictable structure poses a significant vulnerability, as it can be exploited in various cryptanalytic attacks. Therefore, an effective encryption scheme must significantly reduce pixel correlation, obscuring the image's statistical characteristics and enhancing its security.

The correlation coefficient $r(i,j)$ quantifies the degree of linear relationship between two adjacent pixels and ranges from

−1 to +1. A value close to +1 indicates strong positive correlation, while a value near 0 implies little to no correlation, an ideal property for encrypted images. In cryptographic contexts, a correlation coefficient approaching zero is essential for ensuring resistance against statistical attacks and preserving the confidentiality of the image data.

$$r(i,j) = \frac{cov(i,j)}{\sqrt{D(i)} \cdot \sqrt{D(j)}} \quad (5)$$

where $cov(i,j)$ is the covariance between pixel values i and j, and $D(i)$ and $D(j)$ represent the variances of i and j, respectively. The covariance is defined as:

$$Cov(i,j) = \frac{1}{P}\sum_{n=1}^{P}\big(i_n - E(i)\big)\big(j_n - E(j)\big) \quad (6)$$

$$E(i) = \frac{1}{P}\sum_{n=1}^{P} i_n \quad (7)$$

$$E(j) = \frac{1}{P}\sum_{n=1}^{P} j_n \quad (8)$$

To evaluate the proposed algorithm, 30,000 pairs of adjacent pixels were selected using a uniform random sampling strategy over the entire image. Random pixel coordinates were generated such that each valid pixel location had an equal probability of being chosen, while boundary pixels were excluded to ensure the existence of valid adjacent neighbors. For each selected pixel, the corresponding adjacent pixel was taken in the horizontal, vertical, or diagonal direction. The same set of pixel coordinates was applied to both the original and encrypted images to guarantee a fair and consistent comparison. The correlation coefficients were then computed for each spatial direction and for the red, green, and blue channels, as shown in Table IV. The results confirm that the proposed algorithm achieves a significant reduction in correlation across all directions and channels. In most cases, the average correlation values are close to zero or even slightly negative, indicating strong decorrelation.

TABLE IV. CORRELATION COEFFICIENTS

Image	Channel	Directions		
		Horizontal	Vertical	Diagonal
House	Red	0.008983	-0.005521	-0.006882
	Green	-0.001251	-0.003216	0.004407
	Blue	-0.001180	0.007381	-0.002689
	Average	0.002184	-0.000452	-0.001721
Airplane	Red	-0.000881	0.007337	-0.001845
	Green	0.002072	0.004814	0.000466
	Blue	-0.000724	-0.004531	0.000355
	Average	0.000156	0.002540	-0.000342
Female	Red	-0.002346	0.000289	0.002769
	Green	0.003385	-0.001643	0.001439
	Blue	-0.001536	-0.007606	0.001570
	Average	-0.000166	-0.002987	0.001926

To further validate the performance of the proposed algorithm, a comparative study was conducted against several established methods [11, 12, 16, 17]. As shown in Table V, the proposed method achieved the lowest average correlation coefficient, indicating the highest level of pixel decorrelation among all compared methods. The values are significantly closer to zero, particularly in the average and diagonal directions, demonstrating that the encrypted images bear virtually no statistical resemblance to the original images. This confirms the strong obfuscation ability of the proposed method, effectively reinforcing its robustness and resistance to statistical and visual cryptanalysis.

TABLE V. CORRELATION COEFFICIENTS' COMPARISON

Method	Directions			Average
	Horizontal	Vertical	Diagonal	
Proposed	0.002184	-0.000452	-0.001721	0.0000037
[11]	-0.000603487	0.00270027	-0.0036463	-0.0005165
[12]	-0.0030184	0.0052921	0.0032035	0.0018257
[16]	-0.0002699	-0.0103385	0.0104684	-0.0000467
[17]	-0.0092	0.0016	-0.0066	-0.0047

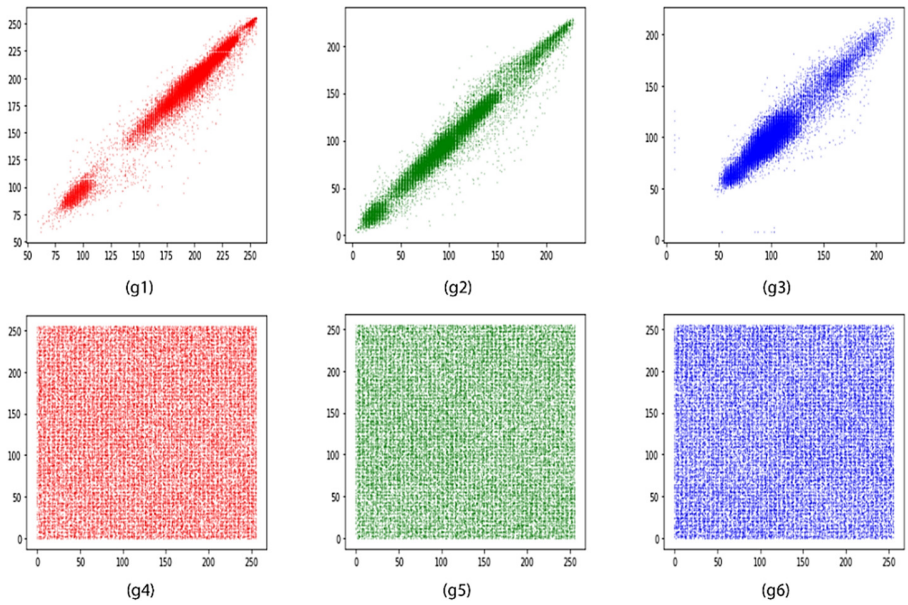


Fig. 10. Horizontal correlation distribution in the House image: (g1) Red data channel, (g2) Green data channel, (g3) Blue data channel, (g4) Red data channel in the cipher image, (g5) Green data channel in the cipher image, (g6) Blue data channel in the cipher image.

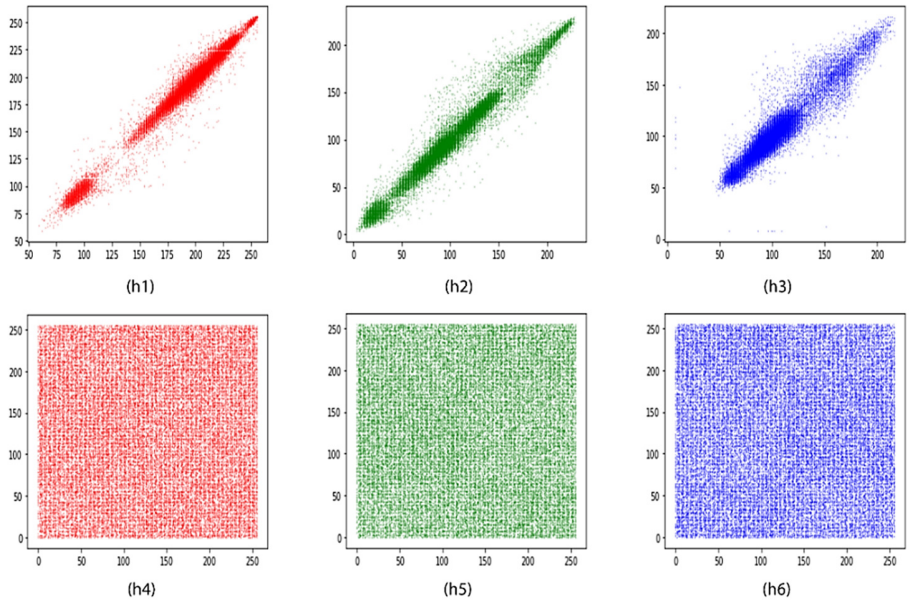


Fig. 11. Vertical correlation distribution in the House image: (h1) Red data channel, (h2) Green data channel, (h3) Blue data channel, (h4) Red data channel in the cipher image, (h5) Green data channel in the cipher image, (h6) Blue data channel in the cipher image.

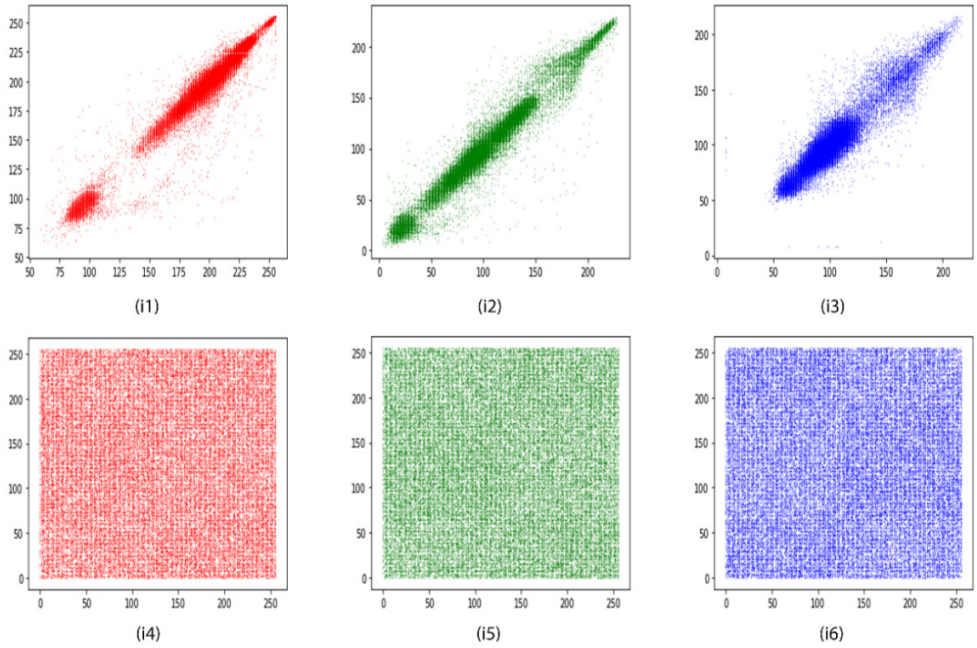


Fig. 12. Diagonal correlation distribution in the House image: (i1) Red data channel, (i2) Green data channel, (i3) Blue data channel, (i4) Red data channel in the cipher image, (i5) Green data channel in the cipher image, (i6) Blue data channel in the cipher image.

Figures 10-12 present a visual interpretation of the correlation analysis results, displaying the pixel distribution trends before and after encryption for the House image across all three color channels. These scatter plots graphically represent the correlation between adjacent pixels in the horizontal, vertical, and diagonal directions. Figure 10 shows the horizontal correlation distribution in the red (g1), green (g2), and blue (g3) channels of the original image, and their corresponding encrypted counterparts (g4, g5, g6). Figure 11 presents the vertical correlation distribution, comparing the original (h1–h3) and encrypted channels (h4–h6). Figure 12 illustrates the diagonal correlation distribution, again highlighting the marked difference between the original (i1–i3) and encrypted (i4–i6) pixel relationships. In all cases, the scatter plots of the encrypted image reveal a highly scattered distribution, indicating a substantial reduction in correlation between neighboring pixels. This confirms the algorithm's effectiveness in disrupting pixel dependencies and thereby enhances its resistance to statistical attacks.

C. Correlation Between the Original Image and Encrypted Image

An essential criterion for a secure image encryption algorithm is its ability to effectively obscure the relationship between the original and the encrypted image. Ideally, a strong encryption scheme should introduce a high level of transformation such that the encrypted image bears no visible or statistical resemblance to the original. One quantitative measure of this effectiveness is the correlation coefficient between the original and encrypted versions of an image. A low or near-zero correlation indicates a high level of opacity, making it exceedingly difficult for adversaries to infer any meaningful information from the cipher image. Low correlation between the original and encrypted images signifies that the encryption algorithm has succeeded in breaking pixel-level dependencies, rendering the output image statistically unrecognizable. This characteristic is especially important in preventing cryptanalysis techniques that rely on residual similarities between the plain and the cipher data. Effective methods typically achieve this through high non-linearity and complex transformation steps, such as pixel substitution, permutation, and multi-layered encryption strategies.

To evaluate the proposed method's effectiveness in this regard, it was applied to multiple standard test images, calculating the correlation coefficients between the original and encrypted images across all color channels (red, green, and blue). The correlation was calculated using:

$$CC = \frac{\sum_{i,j}^{M,N}(C_{i,j}-\bar{C})(C'_{i,j}-\bar{C'})}{\sqrt{\sum_{i,j}^{M,N}(C_{i,j}-\bar{C})^2}\cdot\sqrt{\sum_{i,j}^{M,N}(C'_{i,j}-\bar{C'})^2}} \quad (9)$$

where C and C' represent the original and encrypted images, respectively, and $\bar{C}$ and $\bar{C'}$ are the mean values of the original and encrypted images:

$$\bar{C} = \frac{1}{M\times N}\sum_{i,j}^{M,N} C_{i,j} \quad \text{and} \quad \bar{C'}\ \frac{1}{M\times N}\sum_{i,j}^{M,N} C'_{i,j} \quad (10)$$

where the matrices C and C' have dimensions N and M, respectively. The results are summarized in Table VI, indicating that the correlation coefficients across all channels and images remain close to zero, both positive and negative, further validating the algorithm's ability to produce highly decorrelated encrypted images.

To further highlight the strength of the proposed approach, Table VII compares the correlation coefficients obtained using the proposed method with those produced by two other encryption schemes [13, 16]. The results clearly show that the proposed algorithm yields the lowest average correlation among all compared methods, reinforcing its effectiveness in fully decoupling the encrypted image from its original counterpart. Overall, these results confirm that the proposed algorithm introduces a high degree of non-linearity and decorrelation, making it extremely difficult for unauthorized parties to extract or infer any meaningful content from the encrypted images. This is a critical property for robust image encryption, particularly in sensitive applications such as medical imaging, secure surveillance, and confidential data transmission.

TABLE VI. CORRELATION COEFFICIENTS BETWEEN THE ORIGINAL AND ENCRYPTED IMAGES

Image	Channel	Our Method
House	Red	-0.001793
	Green	-0.001543
	Blue	0.002383
	Average	-0.000318
Airplane	Red	0.000003
	Green	-0.001288
	Blue	-0.001268
	Average	-0.000851
Female	Red	0.003236
	Green	0.000008
	Blue	-0.002404
	Average	0.00028
Sailboat	Red	0.000312
	Green	-0.000458
	Blue	0.000336
	Average	0.000064
Car	Red	0.000113
	Green	0.001963
	Blue	-0.000533
	Average	0.000514

TABLE VII. COMPARISON OF CORRELATION COEFFICIENTS BETWEEN ENCRYPTED AND ORIGINAL IMAGES ACROSS DIFFERENT METHODS

Cipher image	Channel	Proposed Method	[13]	[16]
Baboon	Red	0.000265	-	0.0020906
	Green	0.000035	-	-0.00377277
	Blue	0.000597	-	0.00206403
	Average	0.000299	0.000704	0.00012729
Peppers	Red	-0.001084	-	0.00016207
	Green	-0.000105	-	-0.00312463
	Blue	0.002589	-	0.00651457
	Average	0.000467	0.00241	0.001184

D. Differential Attacks

A critical requirement for any secure image encryption system is its robustness against differential attacks, which are a class of cryptanalytic techniques that attempt to infer the encryption key by analyzing the impact of small, deliberate changes in the input (plaintext) image on the resulting cipher image. An effective encryption algorithm must exhibit extreme sensitivity to minimal changes in the original image, ensuring that even a single pixel modification leads to substantial differences in the encrypted output. This sensitivity is quantitatively assessed using two widely accepted metrics:

- Number of Pixels Change Rate (NPCR), which measures the percentage of differing pixels between two cipher images resulting from slightly different plain images.
- Unified Average Changing Intensity (UACI), which evaluates the average intensity of differences between corresponding pixel values in the two cipher images.

The formulas used to calculate NPCR and UACI are:

$$NPCR = \frac{\Sigma_{i,j}\,\sigma(i,j)}{M\times N}\times 100\% \quad (12)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j}\frac{|I(i,j)-I\prime(i,j)|}{255}\right] \times 100\% \quad (13)$$

$$\sigma(i,j) = \begin{cases} 1, & if\ I(i,j) = I'(i,j) \\ 0, & if\ I(i,j) \neq I'(i,j) \end{cases} \quad (14)$$

where I denotes the cipher image obtained from the original plaintext image, and I' is the cipher image obtained after altering a single pixel in the plaintext. M and N are the image dimensions. According to the ideal expectation values referenced in (15) and (16), a secure encryption system should yield NPCR values greater than 99.6% and UACI values exceeding 33.4% to ensure sufficient diffusion and confusion:

$$N_a^* = \frac{Q - \varphi^{-1}(a)\sqrt{Q/N}}{Q+1} \quad (15)$$

$$U_a^* \begin{cases} U_a^{*-} = S_u - \varphi^{-1}\left(\frac{a}{2}\right)\beta_u \\ U_a^{*+} = S_u + \varphi^{-1}\left(\frac{a}{2}\right)\beta_u \end{cases} \quad (16)$$

To test the resistance of the proposed method against differential attacks, a minimal modification (a one-pixel change) was applied to the House image, evaluating the resulting encrypted image. The NPCR and UACI values were then computed and are presented in Table VIII. To further validate the robustness of the proposed method, a comparative analysis with other prominent encryption schemes was conducted. The results are shown in Table IX, focusing on the House image across all three color channels. The results confirm that the proposed encryption scheme offers superior UACI performance (33.90%), indicating a higher intensity of pixel-level changes in response to minor modifications in the original image. Although NPCR values among competing methods are comparably high, the proposed algorithm maintains a consistent and competitive average of 99.65%, ensuring effective pixel diffusion. These outcomes strongly validate the resilience of the proposed method against differential attacks, making it well-suited for secure and reliable image encryption applications.

TABLE VIII. NPCR AND UACI VALUES OF THE ENCRYPTED IMAGES

Image	Channel	NPCR (%)	UACI (%)
House	Red	99.67	33.88
	Green	99.81	35.04
	Blue	99.91	36.38
	Average	99.80	35.10
Airplane	Red	99.80	34.55
	Green	99.82	34.93
	Blue	99.76	34.57
	Average	99.79	34.68
Female	Red	99.62	33.45
	Green	99.62	33.38
	Blue	99.62	33.48
	Average	99.62	33.44
Sailboat	Red	99.58	33.17
	Green	99.65	33.38
	Blue	99.72	33.74
	Average	99.65	33.43
Tree	Red	99.69	34.47
	Green	99.59	33.40
	Blue	99.80	35.37
	Average	99.69	34.41

E. MSE and PSNR Analysis

The evaluation of image encryption algorithms requires both qualitative and quantitative assessments to ensure their reliability, precision, and resilience against attacks. MSE and PSNR are two widely used metrics in this context, which provide essential insights into the encryption algorithm's ability to obscure image content while preserving data integrity during decryption. MSE measures the average squared difference between the pixel intensities of the original (plain) image and the encrypted (cipher) image. A higher MSE value indicates greater distortion, which is desirable in encryption, as it suggests a reduced correlation with the original image. PSNR, on the other hand, quantifies the ratio between the maximum possible signal value and the power of the noise introduced during encryption. A lower PSNR value for encrypted images implies greater distortion, reinforcing the image's confidentiality. Conversely, a PSNR value of infinity (∞) for decrypted images confirms perfect reconstruction, as no distortion is present.

$$PSNR = 10\,log_{10}\frac{(I_{MAX})^2}{MSE} \quad (17)$$

$$MSE = \frac{\sum_{M,N}[I(i,j)-I\prime(i,j)]^2}{M \times N} \quad (18)$$

where $I(i,j)$ and $I'(i,j)$ denote the pixel values in the original and encrypted images, respectively, $M \times N$ is the image resolution, and I_{MAX} is the maximum possible pixel value (typically 255 for 8-bit images).

The proposed algorithm was applied to multiple test images to assess its performance. The resulting MSE and PSNR values for both encryption and decryption phases are reported in Table X, with the results demonstrating two key findings:

- The MSE values for encryption are relatively high, confirming that the encrypted image significantly differs from the original, thereby enhancing security and ensuring minimal visual similarity.
- The MSE values for decryption are zero, and the PSNR values are infinite, indicating that the original image is perfectly reconstructed after decryption, without any loss of information.

This dual outcome, strong distortion during encryption and flawless restoration upon decryption, validates the accuracy, integrity, and reliability of the encryption algorithm, as it effectively hides the original content from unauthorized access while ensuring high-fidelity data recovery for legitimate users.

F. Entropy Analysis

In the context of image cryptography, entropy is a fundamental metric that quantifies the randomness or unpredictability within an image. It reflects the degree of disorder in pixel intensity values, with higher entropy indicating a more complex and unpredictable data structure. From a security standpoint, an image encryption algorithm should ideally produce a cipher image with maximum entropy, approaching the theoretical limit of 8 bits for 8-bit grayscale or color channels, thereby minimizing any statistical patterns that could be exploited in cryptanalytic attacks.

TABLE IX. COMPARISON OF NPCR AND UACI OF THE ENCRYPTED IMAGE BETWEEN THE PROPOSED AND OTHER ALGORITHMS

Image	Channels	Proposed method		[11]		[13]		[16]		[17]	
		NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
House	Red	99.67	33.88	-	-	-	-	99.719702	33.795178	-	-
	Green	99.81	35.04	-	-	-	-	99.760900	33.561892	-	-
	Blue	99.91	36.38	-	-	-	-	99.713598	33.504208	-	-
	Average	99.80	35.10	99.6145	29.4337	99.6063	29.3973	99.731400	33.620426	99.6445	33.6547

TABLE X. COMPARISON OF PSNR AND MSE VALUES BETWEEN ENCRYPTED AND DECRYPTED IMAGES

Image	Channel	Encryption		Decryption	
		MSE	PSNR (dB)	MSE	PSNR (dB)
House	Red	6798.4838	9.806683	0	Inf
	Green	8588.1559	8.791804	0	Inf
	Blue	9579.9461	8.317173	0	Inf
	Average	8322.1953	8.971887	0	inf
Airplane	Red	9940.3179	8.156800	0	Inf
	Green	10675.6245	7.846870	0	Inf
	Blue	10410.8578	7.955938	0	Inf
	Average	10342.2667	7.986536	0	Inf
Female	Red	9364.5112	8.415952	0	Inf
	Green	9058.7032	8.560143	0	Inf
	Blue	6981.7644	9.691152	0	Inf
	Average	8468.3263	8.889083	0	Inf
Sailboat	Red	7311.2566	9.790204	0	Inf
	Green	11501.6728	8.803713	0	Inf
	Blue	11524.9949	8.339302	0	Inf
	Average	10112.6414	8.977739	0	Inf
Tree	Red	8675.4219	8.747897	0	Inf
	Green	11198.2815	7.639289	0	Inf
	Blue	9612.5399	8.302422	0	Inf
	Average	9828.7477	8.229869	0	inf

TABLE XI. COMPARISON OF ENTROPY VALUES OF ENCRYPTED IMAGES BETWEEN THE PROPOSED AND OTHER METHODS

Image		Our method		[11]	[12]	[13]	[16]	[17]
		Original image	Encrypted image					
House	Red	6.376789	7.999326	-	7.99688	-	7.9990407	-
	Green	6.479787	7.999281	-	7.99678	-	7.9986954	-
	Blue	6.188162	7.999406	-	7.99729	-	7.9989805	-
	Average	6.348146	7.999338	7.99897	7.99698	7. 9577	7.9989055	7.9970
Airplane	Red	6.717765	7.999252	-	-	-	-	-
	Green	6.798978	7.999251	-	-	-	-	-
	Blue	6.213774	7.999363	-	-	-	-	-
	Average	6.576839	7.999288	-	-	-	-	-
Baboon	Red	7.752819	7.999235	-	7.99772	-	7.9998850	-
	Green	7.465408	7.999316	-	7.99717	-	7.9985228	-
	Blue	7.766575	7.999223	-	7.99741	-	7.9991068	-
	Average	7.661600	7.999258	7.99916	7.99743	7.9905	7.9991716	7.9973
Female	Red	7.416301	7.999471	-	-	-	7.99906030	-
	Green	7.444649	7.999366	-	-	-	7.99885938	-
	Blue	6.943694	7.999364	-	-	-	7.99910950	-
	Average	7.268215	7.999400	-	-	-	7.99900973	-
Sailboat	Red	7.312386	7.999317	-	7.99732	-	-	-
	Green	7.646106	7.999276	-	7.99703	-	-	-
	Blue	7.213727	7.999364	-	7.99741	-	-	-
	Average	7.390739	7.999319	7.99901	7.99725	-	-	-
Tree	Red	7.166794	7.999275	-	7.99711	-	-	-
	Green	7.417910	7.999324	-	7.99753	-	-	-
	Blue	6.898167	7.999332	-	7.99701	-	-	-
	Average	7.160957	7.999310	7.99907	7.99722	-	-	-

Entropy is particularly influenced by the combined effects of the confusion and diffusion phases of an encryption algorithm. Confusion aims to obscure the relationship between the key and ciphertext, while diffusion spreads the influence of each bit of the plaintext across the ciphertext. Together, these mechanisms enhance entropy, thereby increasing resistance against both statistical and brute-force attacks. The entropy (a) of an image channel is calculated using:

$$E(a) = -\sum_{i=1}^{2^m-1} P(a_i)\, log_2[P(a_i)] \quad (18)$$

where $P(a_i)$ is the probability of the occurrence of the symbol a_i, and 2^m is the total number of possible intensity levels (256 for 8-bit images). The ideal entropy value for a perfectly random 8-bit image is 8.

The entropy values for each RGB channel of various encrypted images were calculated, and the results were compared with those of several existing methods. The results in Table XI clearly demonstrate that the proposed encryption algorithm consistently produces entropy values extremely close to the ideal value of 8 for all channels and across different images. The entropy values of the encrypted images are consistently greater than 7.999, approaching the ideal value of 8. This high degree of randomness implies that the encrypted images carry no discernible patterns, making them extremely difficult to compress or predict. Such results underscore the high security level and statistical strength of the proposed encryption algorithm.

G. Impact of Image Compression on Decryption Accuracy

Since the proposed encryption algorithm operates at the pixel level and introduces strong nonlinear transformations, applying lossy compression techniques such as JPEG after encryption may alter the encrypted data and lead to imperfect decryption. This behavior is inherent to most chaos-based and pixel-wise encryption schemes. Experimental observations confirm that when lossless compression formats (e.g., PNG) are applied to the encrypted image, the original plain image is perfectly recovered after decryption. Conversely, lossy compression introduces quantization errors that prevent exact reconstruction. Therefore, the proposed method is best suited for secure transmission scenarios adopting either lossless compression or a compress-then-encrypt strategy, which is widely recommended in modern secure communication systems.

H. Execution Time Analysis

An important aspect of evaluating the proposed image encryption algorithm is its computational efficiency. To assess this, execution time was measured on a standard PC equipped with an Intel i5 processor and 8 GB of RAM. The results presented in Table XII show that the algorithm can encrypt a 512×512 image in only 0.31 s. This short execution time demonstrates that the proposed scheme is not only secure but also highly efficient, making it suitable for real-time or large-scale applications in modern digital communication systems where both security and speed are critical.

TABLE XII. EXECUTION TIME ANALYSIS RESULTS

Size	256×256	512×512	CPU and RAM of the machine used
Proposed	0.22 s	0.31 s	Core i5-5300 2.30 GHz CPU, 8 GB
[3]	0.242 s	-	-
[12]	0.32 s	1.33 s	-
[13]	1.42545 s		2.9 GHz Intel Core i9, 32 GB
[17]	0.8253 s	-	-
[18]	0.6007 s	-	Core i7-9700 3.00GHz CPU and 16 GB

I. Key Sensitivity Analysis

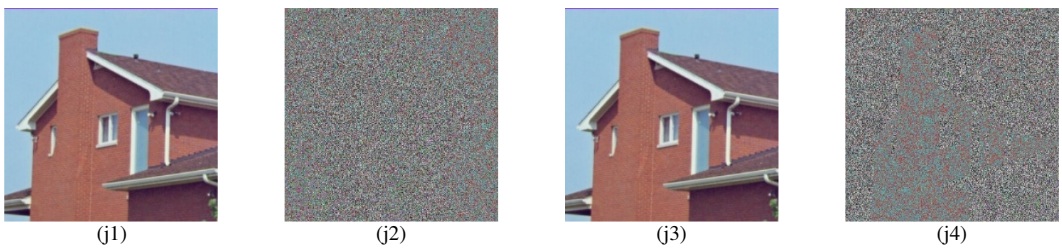
In image cryptography, sensitivity to encryption keys is a vital requirement for ensuring the security and confidentiality of visual data. A secure encryption algorithm must exhibit a high degree of responsiveness to even the slightest changes in its cryptographic keys. In practice, this means that a minor modification to any key parameter should produce a vastly different encrypted or decrypted image. Such sensitivity is essential to defending against brute-force attacks and differential cryptanalysis, as it prevents attackers from gradually refining incorrect keys toward the correct one.

The robustness of the proposed algorithm in this regard stems from its complex and nonlinear key-to-image relationship, especially through the use of chaotic maps such as the Tent Map and the Hénon Map. To assess this property, a key sensitivity analysis was conducted by introducing small changes, at the scale of 10^{-14}, to individual parameters used in the chaotic sequences. Specifically, the value of the parameter n in the first Tent Map matrix during the decryption phase was altered while keeping all other keys unchanged. Table XIII presents both the correct and perturbed key sets used in this evaluation.

TABLE XIII. CORRECT VS. WRONG KEYS USED IN THE PROPOSED ALGORITHM.

Chaotic source	The correct key	The wrong key
1st Tent Map Matrix	X_0= 0.18748384384734 n = 1.99362482460643	X_0= 0.187483843847341 n = 1.99362482460643
2nd Tent Map Matrix	X_0= 0.42745232952648 n = 1.96794355822952	X_0= 0.42745232952648 n = 1.96794355822952
Hénon Map Matrix	X_0= 0.13437656456235 n = 2.11632574671353 m = 0.34354564753268	X_0= 0.13437656456235 n = 2.11632574671353 m = 0.34354564753268

The results of the decryption process using the correct and incorrect keys are visually represented in Figures 13 and 14:



(j1) (j2) (j3) (j4)

Fig. 13. Key sensitivity analysis: (j1) Original image House, (j2) Encrypted image, (j3) Decrypted image with the correct key, (j4) Decrypted image with the wrong key.

(k1) (k2) (k3) (k4)

Fig. 14. Key sensitivity analysis: (k1) Original image female, (k2) Encrypted image, (k3) Decrypted image with the correct key, (k4) Decrypted image with the wrong key.

These results provide strong visual confirmation of the algorithm's extreme sensitivity to key alterations. Even a minute variation in a single parameter completely disrupts the decryption process, making unauthorized recovery of the image computationally infeasible. To quantify the effect of these small changes, each parameter was sequentially modified in isolation, and the percentage of differing pixels between the decrypted image with the correct key and the one obtained using the altered key was computed. These results are summarized in Table XIV.

TABLE XIV. RATE OF CHANGE IN DECRYPTED IMAGES DUE TO SLIGHT KEY VARIATIONS

Parameter modified	Change rate (%)
X_0 of 1st matrix of Tent Map	99.5983
n of 1st matrix of Tent Map	99.6025
X_0 of 2nd matrix of Tent Map	99.5979
n of 2nd matrix of Tent Map	99.5998
X_0 of Hénon Map	99.6643
n of Hénon Map	99.6646
m of Hénon Map	99.6574

These extremely high change rates (≈99.6%) reinforce the conclusion that the proposed algorithm is highly sensitive to key values. Such sensitivity is a hallmark of secure chaotic cryptosystems and confirms the algorithm's strength against key-related attacks. Even minor perturbations to the encryption key yield a completely different output, thereby maximizing cryptographic robustness and ensuring data integrity.

From a system-level perspective, the issue of key management and secure key exchange is addressed at the integration stage rather than within the core encryption process itself. In general, the secret key can be shared directly with the receiver, through a private channel, or through an asymmetric (public-key) cryptosystem. Asymmetric systems allow secure key exchange without requiring a prior shared secret, which reduces the risk of interception during transmission. In the proposed method, the RSA asymmetric encryption system was adopted to securely distribute the secret keys and chaotic parameters between communicating parties. Additionally, a distinctive feature of the proposed scheme lies in the dynamic derivation of a subset of encryption parameters from the plain image. This property significantly mitigates the risks associated with key reuse and partial key exposure, as the effective encryption behavior varies with each input image, even when the same master key is used. Consequently, the proposed approach enhances overall system-level security and makes the scheme well-suited for deployment in modern digital communication environments.

J. Key Space Analysis

The key space of the proposed image encryption algorithm is defined by all secret and independent keys involved in the encryption process. These keys include a 32-bit DNA encoding key, a discrete rotation angle with four possible values (0°, 90°, 180°, 270°), two Tent Map keys, each composed of an initial condition X_0 and a control parameter n, and one Hénon map key, composed of an initial condition X_0 and two control parameters n and m. For the chaotic systems, a computational precision of 10^{-14} is assumed, which is commonly adopted in chaos-based cryptographic schemes. $K_{total} = K_{DNA} \times K_{angle} \times K_{Tent1} \times K_{Tent2} \times K_{Henon} = 2^{32} \times 2^2 \times 10^{28} \times 10^{28} \times 10^{42}$, therefore $K_{total} = 2^{34} \times 10^{98}$.

The total key space is obtained by multiplying the key spaces of all individual components and is estimated to exceed 2^{359}. This value is significantly larger than the standard security threshold of 2^{128}, ensuring strong resistance against brute-force attacks.

TABLE XV. KEY SPACE COMPARISON WITH OTHER METHODS

Methods	Key space
Ours	2^{359}
[3]	2^{136}
[13]	2^{372}
[17]	$10^{90} \sim 2^{299}$
[18]	2^{249}

As summarized in Table XV, the key space of the proposed scheme compares favorably with several existing image encryption methods. With a key space of 2^{359}, the proposed algorithm offers a substantially larger key space than those reported in [3, 17, 18], thereby providing enhanced resistance to brute-force attacks. Although the method presented in [13] achieves a slightly higher key space, the key space of the proposed approach remains sufficiently large to meet practical security requirements and ensures a high level of cryptographic robustness.

V. CONCLUSION

This paper presented a comprehensive and secure image encryption framework that combines the strengths of chaotic systems and bio-inspired cryptographic techniques. The proposed algorithm integrates two well-established one-dimensional chaotic maps, the Tent Map and the Hénon Map, with a DNA-based encryption layer to construct a multi-level cryptosystem capable of achieving high degrees of confusion, diffusion, and statistical randomness. The chaotic maps

introduce unpredictability and sensitivity to initial conditions, while the DNA cryptography offers an additional nonlinear transformation that enhances resistance to both differential and statistical attacks. Furthermore, pixel-level permutation is implemented through circular shift and rotation operations, both of which are dynamically driven by key values derived from the input image. This ensures that even the slightest alteration in the plain image leads to significant deviations in the encrypted output, as quantitatively demonstrated through high NPCR and UACI scores.

A series of rigorous experiments validated the algorithm's performance using a wide range of security metrics. Histogram analysis of encrypted images confirmed the elimination of predictable intensity patterns. Correlation coefficient values approached zero across horizontal, vertical, and diagonal orientations, indicating the successful destruction of spatial dependencies among adjacent pixels. The entropy values for all encrypted images consistently approached the theoretical maximum of 8, reflecting a high level of randomness. Furthermore, PSNR and MSE analyses verified that the encryption process introduces substantial distortion to protect image content while ensuring perfect reconstruction during decryption. Key sensitivity tests highlighted the algorithm's robustness, demonstrating that even minimal changes to key parameters result in decryption failure, thereby defending against brute-force and key-guessing attacks. When benchmarked against existing state-of-the-art algorithms, the proposed method consistently outperformed them across all tested dimensions, establishing it as a strong candidate for secure image transmission and storage in real-world applications.

Due to its high security level, low computational complexity, and strong resistance to cryptographic attacks, as confirmed by metrics such as NPCR, UACI, entropy, correlation, PSNR, and MSE, the proposed encryption scheme is particularly suitable for security-critical applications such as medical image transmission, military surveillance systems, secure cloud storage, and IoT-based multimedia communications. Additionally, the very short execution time (0.33 s on a standard PC with 8 GB RAM and Intel i5) ensures practical deployment in real-time scenarios. These results collectively demonstrate that the proposed algorithm is highly effective and well-suited for these fields.

Despite its advantages, the proposed algorithm has certain limitations. In particular, if an encrypted image is compressed (e.g., JPEG), perfect reconstruction of the original image may not be guaranteed, as lossy compression alters pixel values and affects the encryption process. Future work could address this limitation by developing compression-robust encryption techniques. Additionally, the framework can be extended by incorporating higher-dimensional chaotic systems, adaptive DNA encoding, and machine learning-based key optimization, as well as applying it to video, medical images, or biometric data. These directions aim to further enhance the robustness, scalability, and practical applicability of the proposed image encryption scheme.

DECLARATIONS OF COMPETING INTERESTS

The authors declare no conflict of interest.

DATA AVAILABILITY

All data are available upon request from the corresponding author.

ACKNOWLEDGEMENT

This paper was derived from a research grant funded by the Research, Development, and Innovation Authority (RDIA), Kingdom of Saudi Arabia, with grant number 13382-psu-2023-PSNU-R-3-1-EI-. The authors would like to acknowledge the support of Prince Sultan University, Riyadh, Saudi Arabia, in paying the article processing charges of this publication. This research is supported by the Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia.

REFERENCES

[1] Q. Chen, H. Li, S. B. Ariffin, and N. A. B. Mustapa, "A Comprehensive Study on the Homomorphic Encryption for Secure Image Data Processing," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21783–21790, Apr. 2025, https://doi.org/10.48084/etasr.10007.

[2] W. Ali, C. Zhu, R. Latif, M. Asim, and M. U. Tariq, "Image Encryption Scheme Based on Orbital Shift Pixels Shuffling with ILM Chaotic System," *Entropy*, vol. 25, no. 5, May 2023, https://doi.org/10.3390/e25050787.

[3] A. K. Panigrahy *et al.*, "A Faster and Robust Artificial Neural Network Based Image Encryption Technique With Improved SSIM," *IEEE Access*, vol. 12, pp. 10818–10833, 2024, https://doi.org/10.1109/ACCESS.2024.3353294.

[4] F. ElAzzaby, K. H. Sabour, N. ELakkad, W. El-Shafai, A. Torki, and S. R. Rajkumar, "Color image encryption using a Zigzag Transformation and sine–cosine maps," *Scientific African*, vol. 22, Nov. 2023, Art. no. e01955, https://doi.org/10.1016/j.sciaf.2023.e01955.

[5] M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators," *Soft Computing*, vol. 24, no. 5, pp. 3829–3848, Mar. 2020, https://doi.org/10.1007/s00500-019-04151-8.

[6] S. Deb, B. Biswas, and B. Bhuyan, "Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 34901–34925, Dec. 2019, https://doi.org/10.1007/s11042-019-08086-y.

[7] W. El-Shafai and E. E. D. Hemdan, "Robust and efficient multi-level security framework for color medical images in telehealthcare services," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 4, pp. 3675–3690, Apr. 2023, https://doi.org/10.1007/s12652-021-03494-1.

[8] C. Zhang, J. Chen, and D. Chen, "Cryptanalysis of an Image Encryption Algorithm Based on a 2D Hyperchaotic Map," *Entropy*, vol. 24, no. 11, Oct. 2022, https://doi.org/10.3390/e24111551.

[9] A. Mokhnache and L. Ziet, "Cryptanalysis of a Pixel Permutation Based Image Encryption Technique Using Chaotic Map," *Traitement du Signal*, vol. 37, no. 1, pp. 95–100, Feb. 2020, https://doi.org/10.18280/ts.370112.

[10] A. Arora and R. K. Sharma, "Cryptanalysis and enhancement of image encryption scheme based on word-oriented feed back shift register," *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 16679–16705, May 2022, https://doi.org/10.1007/s11042-022-11973-6.

[11] W. Alexan, D. El-Damak, and M. Gabr, "Image Encryption Based on Fourier-DNA Coding for Hyperchaotic Chen System, Chen-Based Binary Quantization S-Box, and Variable-Base Modulo Operation," *IEEE Access*, vol. 12, pp. 21092–21113, 2024, https://doi.org/10.1109/ACCESS.2024.3363018.

[12] W. Alexan, M. Gabr, E. Mamdouh, R. Elias, and A. Aboshousha, "Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map of Fractional-Order and Hybrid DNA Coding," *IEEE Access*, vol. 11, pp. 54928–54956, 2023, https://doi.org/10.1109/ACCESS.2023.3282160.

[13] M. Gabr *et al.*, "Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem," *Symmetry*, vol. 14, no. 12, Dec. 2022, https://doi.org/10.3390/sym14122559.

[14] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018, https://doi.org/10.1016/j.sigpro.2018.06.008.

[15] M. Es-Sabry *et al.*, "Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques," *IEEE Access*, vol. 11, pp. 100856–100878, 2023, https://doi.org/10.1109/ACCESS.2023.3315658.

[16] F. Elazzaby, N. Elakkad, and K. Sabour, "The Coupling of a Multiplicative Group and the Theory of Chaos in the Encryptions of Images," *The International Arab Journal of Information Technology*, vol. 21, no. 1, Jan. 2024, https://doi.org/10.34028/iajit/21/1/1.

[17] L. Wang, W. Song, J. Di, X. Zhang, and C. Zou, "Image Encryption Method Based on Three-Dimensional Chaotic Systems and V-Shaped Scrambling," *Entropy*, vol. 27, no. 1, Jan. 2025, https://doi.org/10.3390/e27010084.

[18] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding," *Mathematics*, vol. 11, no. 1, Jan. 2023, https://doi.org/10.3390/math11010231.