STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **15**, June 2026, pp 5284–5312.
Published online in International Academic Press (www.IAPress.org)

Fast and Secure Color Image Cryptosystem Based on 2D Henon Chaotic Map and Josephus-ZigZag Permutation

Safae AMINE [1], Fatima KOULOUH [1], Mohammed ES-SABRY [2], Nabil EL AKKAD [1,*]

[1] *Laboratory of Applied Sciences and Emerging Technologies, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco*
[2] *Information Security, Intelligent Systems and Application, Faculty of Sciences, Abdelmalek Essaadi University, Tetouan, Morocco*

Abstract In this study, we propose a novel color image encryption scheme that combines chaotic dynamics and structured permutation strategies to achieve high security and robustness. The proposed algorithm ensures strong confusion through position permutation mechanisms, including zigzag scanning and a Josephus-problem-based scrambling process, effectively disrupting spatial correlations among adjacent pixels. To reinforce diffusion at both pixel and bit levels, a bit-reversal permutation and a two-dimensional (2D) Henon chaotic map are employed to generate key-dependent pseudorandom sequences. These sequences are integrated with the permuted image via XOR operations, enabling rapid propagation of minor changes across the entire cipher image. The security and effectiveness of the proposed algorithm are evaluated using several standard test images. Comprehensive performance analyses, including histogram distribution, correlation coefficient, information entropy, PSNR, and MSE, demonstrate that the encrypted images exhibit uniform statistical properties and negligible residual correlations. Moreover, NPCR and UACI results confirm high sensitivity to slight variations in the plain image and secret keys. Comparative experiments with state-of-the-art image encryption methods indicate that the proposed scheme provides strong security performance while maintaining computational efficiency.

Keywords Color Image Encryption, 2D Chaotic Maps, Josephus Problem, Reversal-Bit Permutation, ZigZag Permutation.

DOI: 10.19139/soic-2310-5070-3210

1. Introduction

In the era of digital transformation and the rapid expansion of the Internet of Things (IoT), multimedia data, particularly digital images, have become the primary vector for global information exchange. Whether dealing with medical imaging diagnostics, confidential military transmissions, biometric surveillance systems, or personal data stored in the cloud, the security of this visual content has emerged as a major concern in contemporary cybersecurity [1]. However, the protection of images presents intrinsic challenges that fundamentally distinguish them from classical text data, namely their massive data size, high information redundancy, and strong correlation between adjacent pixels [2].

These properties render traditional encryption algorithms, such as the Advanced Encryption Standard (AES), inefficient in terms of processing speed and robustness against statistical attacks when applied directly to images [3–8]. Consequently, the scientific community has focused on developing dedicated techniques, primarily based on the confusion-diffusion paradigm and leveraging the complex dynamics of chaotic systems [9–19] like the 2D Hénon Map [20, 21]. While these chaos-based schemes provide essential key sensitivity and

*Correspondence to: Safae AMINE (Email: safae.amine@usmba.ac.ma). Laboratory of Applied Sciences and Emerging Technologies, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

pseudo-randomness, many suffer from critical vulnerabilities: simple permutation methods (e.g., Arnold Cat Map) often exhibit periodicity, and the overall schemes can be broken by sophisticated cryptanalysis, including chosen-plaintext attacks (CPA) and emerging Deep Learning-based attacks [22]. This lack of non-linear, plaintext-dependent permutation combined with insufficient diffusion remains the critical research gap.

To address this gap, this paper proposes a novel, robust, and efficient image encryption scheme. The primary novelty of our scheme lies in the structured and interleaved integration of chaotic key generation, Josephus-based dynamic permutation, and Zigzag-assisted shift diffusion within a unified encryption framework. Unlike conventional approaches where these mechanisms are applied independently, our method coordinates them in a mutually reinforcing architecture, thereby enhancing confusion, diffusion, key sensitivity, and resistance to cryptanalytic attacks.
Our core contribution is based on the synergistic combination of three powerful components:
1. A 2D Hénon Map to generate highly sensitive chaotic sequences for key-stream generation.
2. The Josephus Problem as a dynamic, non-linear permutation mechanism to ensure a superior level of confusion that is highly resistant to CPA.
3. A Shift Permutation-based combined with Zigzag Diffusion technique to rapidly propagate changes across the entire image, ensuring high efficiency and robustness against differential attacks.

The primary objective of this work is to demonstrate that this hybrid approach overcomes the limitations of existing methods by achieving a superior balance between cryptographic security (high entropy, low correlation, strong CPA resistance) and computational efficiency. The remainder of this paper is organized as follows: Section 2 presents the related work and theoretical foundations; Section 3 details the proposed algorithm; Section 4 presents the experimental results and security analysis; finally, Section 5 concludes the study and suggests future perspective.

2. Related work

The development of secure image encryption schemes is fundamentally guided by the confusion-diffusion paradigm, a framework rooted in Shannon's principles [23]. This architecture necessitates a robust source of pseudo-randomness, a role often fulfilled by chaotic systems due to their extreme sensitivity to initial conditions and ergodicity. Among these, the 2D Hénon map has been a subject of extensive research, with early works by Shahna and Mohamed [24] demonstrating its utility in generating permutation sequences. More recently, Lone (2024) [25] explored the combination of the 2D Hénon map with Josephus traversal for secure image transmission, highlighting its robustness against statistical attacks. However, many existing Hénon-based schemes often rely on fixed parameters or simple chaotic sources, which can be vulnerable to phase space reconstruction and modern cryptanalysis.

To enhance the confusion stage and break the high spatial correlation inherent in images, dynamic permutation strategies have become essential. Traditional methods, such as the Arnold Cat Map, suffer from periodicity and are easily broken by chosen-plaintext attacks (CPA). Consequently, the Josephus problem has emerged as a highly effective, non-linear alternative [26]. By treating the image pixels as a circular list and using chaotic sequences to dynamically control the "step size" of the elimination process, Josephus-based permutations achieve a superior level of non-linearity and plaintext-dependency. For example, Hua et al. [27] introduced a Josephus-based scrambling technique coupled with filtering diffusion, proving its effectiveness in breaking spatial redundancy. A critical distinction in recent literature is the transition from fixed-step to variable-step Josephus permutations, as seen in the work of Ghouate et al (2025) [28], who proposed a high-entropy scheme using a Variable Step Josephus Problem (VSJP) to enhance CPA resistance.

For the diffusion stage, which propagates changes across the entire ciphertext, shift permutation (or cyclic shift) is widely used for its balance of computational efficiency and security [29]. Furthermore, the field has seen a critical

shift from purely pixel-level operations to hybrid bit-level and pixel-level encryption [30], where bit-level shifts are essential for thoroughly destroying the correlation within and between the bit-planes. In the context of existing hybrid models, some researchers have attempted to combine these elements, such as the scheme proposed in [31] which integrates a chaotic map, the Josephus problem, and cyclic shift operations.

However, a key limitation in much of the existing literature is the tendency to treat the confusion and diffusion stages, and their underlying chaotic drivers, as independent blocks. Our work addresses this by creating a tight coupling between the 2D Hénon map, the Josephus permutation, and the shift-based diffusion. Specifically, the chaotic sequences from the Hénon map do not just act as static keys but actively drive the dynamic behavior of both the Josephus elimination and the shift-based diffusion, creating a more cohesive and resilient cryptographic structure.

By integrating these advanced techniques and ensuring their synergistic operation, our proposed scheme aims to overcome the periodicity of traditional permutations and the vulnerability of simple chaotic maps to modern cryptanalysis.

3. Mathematical background

The proposed encryption scheme is a hybrid architecture that leverages the chaotic properties of the 2D Hénon Map for key-stream generation, the non-linear dynamics of the Josephus Problem for pixel permutation, and an efficient Shift Permutation mechanism for rapid diffusion.

3.1. Hénon map 2D

The 2D Hénon Map is a classic and widely studied discrete-time dynamical system that exhibits chaotic behavior for certain parameter values. Introduced by Michel Hénon in 1976 as a simplified model of the Poincaré section of the Lorenz system, it is a two-dimensional map that transforms a point x_n, y_n in the plane to a new point x_{n+1}, y_{n+1} [32].
The discrete 2D Hénon Map is defined by the coupled non-linear difference equations (1):

$$F(x,y) = \begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{j+1} = bx_n \end{cases} \tag{1}$$

Where n is the pixel position, and a and b are control parameters.

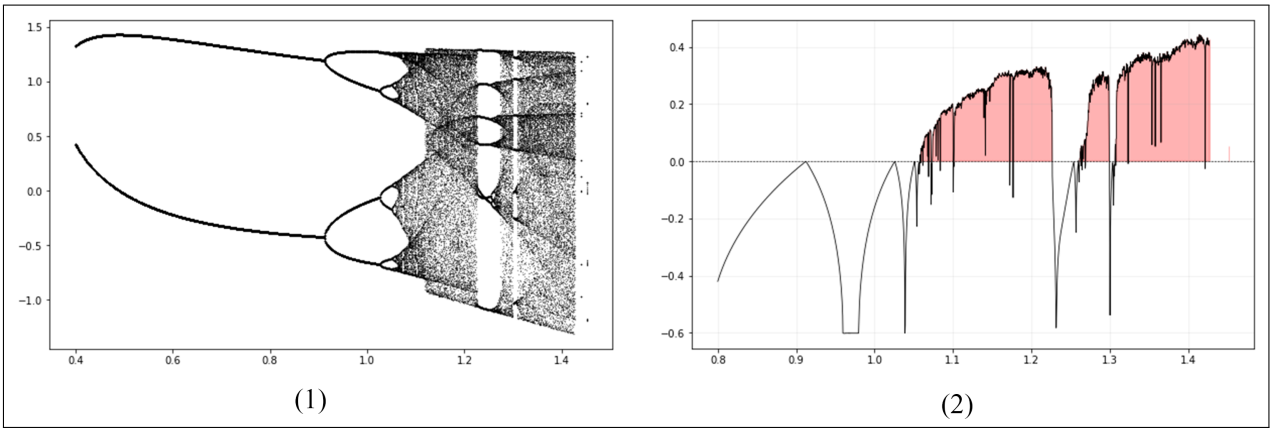


Figure 1. (1) Bifurcation Diagram of 2D Hénon Map. (2) Lyapunov exponent Diagram of 2D Hénon Map.

For the map to exhibit its characteristic chaotic behavior, the parameters are typically set near the original values proposed by Hénon: $a = 1.4$ and $b = 0.3$. Within this parameter range, the system possesses a strange attractor characterized by its fractal geometry and strong sensitivity to initial conditions. The chaotic regime is further validated by the bifurcation diagram and the corresponding Lyapunov exponent spectrum, as illustrated in Figure 1. The bifurcation diagram demonstrates the transition from periodic to chaotic behavior as the control parameter varies, while the positive largest Lyapunov exponent confirms the exponential divergence of nearby trajectories, thereby ensuring the unpredictability required for secure image encryption.

3.2. Josephus problem

The Josephus problem is a classical combinatorial model based on a circular elimination process. Given N elements arranged in a ring, every $K - th$ element is successively removed until a single element remains. The position of the surviving element can be defined recursively as:

$$J(n,k) = \big(J(n-1,k) + k\big) \bmod n \tag{2}$$

With the initial condition $J(1,k) = 0$. This recursive rule induces a deterministic and nonlinear permutation that is highly sensitive to the parameters N and k. Owing to these characteristics, the Josephus problem is commonly employed in computer science for elimination and permutation schemes, and in image encryption it is used to generate pixel permutation patterns that enhance diffusion and resistance against statistical and differential attacks.

3.3. ZigZag operation

The zigzag operation is a deterministic pixel permutation technique widely used to introduce spatial confusion by reordering image elements according to a predefined scanning pattern. Instead of the conventional row-wise or column-wise traversal, the zigzag scan follows alternating diagonal directions, ensuring that adjacent pixels in the original image are relocated to distant positions in the permuted representation. The principle of the zigzag scanning pattern is illustrated in Figure 2, where the diagonal traversal order is clearly depicted. This operation effectively disrupts local spatial correlations, which is a desirable property in image encryption systems.

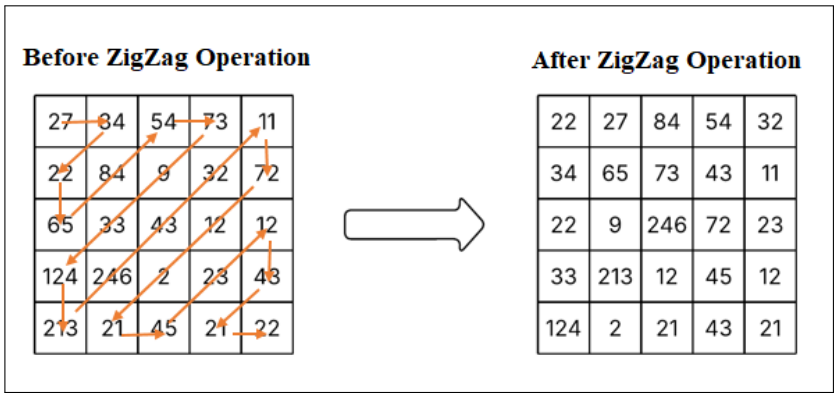


Figure 2. Zigzag Permutation Pattern.

The zigzag operation can be defined as a bijective mapping:

$$P(k) = I(x_k, y_k), \quad k = 0, 1, \ldots, MN - 1 \tag{3}$$

Where $I \in \mathbb{R}^{M \times N}$ is the original image, P its zigzag-permuted version, and x_k, y_k denotes the pixel coordinates generated by the zigzag scanning rule. The inverse zigzag operation reconstructs the original image by applying

the reverse mapping, thus guaranteeing lossless permutation. Due to its simplicity and reversibility, the zigzag operation is well suited for combination with chaotic maps and diffusion processes in secure image encryption frameworks.

3.4. Bit-Reversal operation

The bit-reversal operation is a deterministic transformation that consists in reversing the order of bits in the binary representation of a value. Let x be an integer represented on m bits as $x = (b_{m-1}b_{m-2}\dots b_0)_2$, where $b_i \in \{0,1\}$. The principle of the bit-reversal transformation is illustrated in Figure 3, where the original bit sequence and its reversed counterpart are presented to clarify the mapping mechanism.

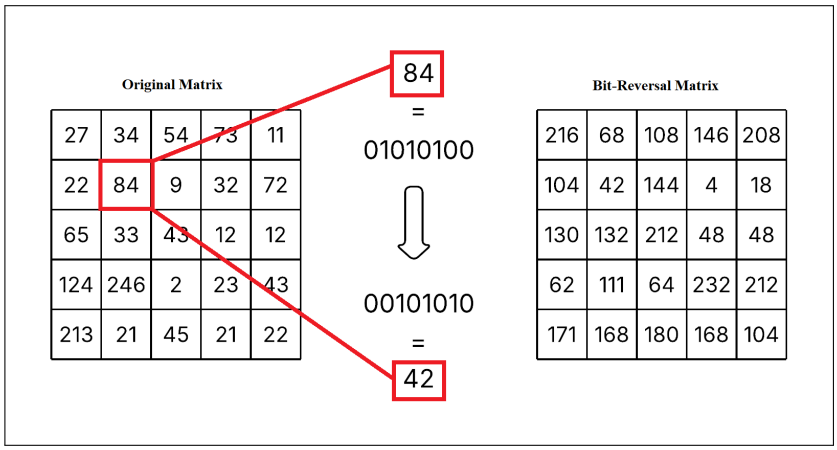


Figure 3. Bit-level Reversal Operation.

The bit-reversed value $R(x)$ is defined as below in the equation:

$$R(x) = \sum_{i=0}^{m-1} b_i \, 2^{m-1-i} \tag{4}$$

Where m is the pixels number and b_i is the bit value.
This operation introduces a nonlinear and bit-level permutation that significantly modifies the numerical structure of the original data. Owing to its simplicity and low computational cost, bit reversal is widely used in signal processing and cryptographic applications. In image encryption schemes, it is commonly applied to pixel values or key streams to enhance confusion, increase sensitivity to bit variations, and reduce statistical correlations.

3.5. The proposed method

The proposed encryption method is based on a hybrid architecture that combines permutation and chaotic diffusion mechanisms to ensure robust security for digital images.
Initially, the original color image is decomposed into its three fundamental chromatic components: Red, Green, and Blue. A content-dependent permutation key is then generated using a global XOR operation applied to the pixels of these three matrices. This key is employed to perform a zigzag permutation on each color component, effectively disrupting the inherent spatial correlations of the original image.
The diffusion stage introduces chaotic dynamics through the two-dimensional Hénon map. Two chaotic matrices are generated, with their initial state determined by parameters y_0, a, b, and x_0 which is computed from the XOR of all pixels in the original image, thereby ensuring high sensitivity to the plaintext. These chaotic matrices are then combined with the zigzag-permuted matrices using a bitwise XOR operation, achieving efficient pixel diffusion.

Subsequently, a second permutation phase based on the Josephus problem is applied, using a key derived from the XOR of the image pixels, which further enhances spatial confusion. Finally, a bit-reversal operation is performed on the resulting data to disturb the binary structure of the encrypted image, increasing complexity and strengthening resistance against statistical and differential attacks.

Begin of our Algorithm1:

Color image input (I) *of size* $M \times N$*:*

1. ***Step 1: Key generation***
   Extract the input image's dimensions: size $(I) = M, N$.
   Compute binary representation P *of* I.
   Calculate $xor\_val = \bigoplus_{i=0}^{L-1} P[i]$, *where* $L = M \times N$.
   Determine Josephus step: $k = (|xor\_val| \bmod (L-1)) + 1$.
   Compute $xor\_global = \bigoplus_{i=0}^{M-1} \bigoplus_{j=0}^{N-1} I(i,j)$ *and* $r = 3.5 + ((xor\_global \bmod 10^6)/10^6) \times 0.5$.
2. ***Step 2: Zigzag chaotic permutation***
   Generate logistic chaotic sequence Z *using* (x_z, r).
   Divide I *into non-overlapping blocks of size* $b \times b$.
   Sort Z *in descending order to obtain block index order.*
   Generate Zigzag scan order inside each block.
   Rearrange pixels of each block according to Zigzag order and move blocks to new positions based on Z.
   Let I_z *be the permuted image.*
3. ***Step 3: Hénon initial condition***
   Compute $xorR = \bigoplus R(i,j)$, $xorG = \bigoplus G(i,j)$, $xorB = \bigoplus B(i,j)$ *for all pixels.*
   Compute $xorRGB = xorR \oplus xorG \oplus xorB$.
   Initialize $x_0 = \epsilon + 0.4 \times (xorRGB/255)$.
4. ***Step 4: Hénon chaotic maps***
   Generate Hénon map H_1 *using* (x_0, y_0, a_1, b_1).
   Generate Hénon map H_2 *using* (x_0, y_1, a_2, b_2).
5. ***Step 5: XOR diffusion***
   For each pixel (i,j), *compute* $D(i,j) = I_z(i,j) \oplus H_1(i,j) \oplus H_2(i,j)$.
6. ***Step 6: Josephus permutation***
   Generate Josephus sequence J *of length* L *using step* k.
   Permute D *using* J: $S(i) = D(J(i))$, *reshape* S *to* I_s *of size* $M \times N$.
7. ***Step 7: Channel-wise XOR key generation***
   Compute $KR = \bigoplus R(I_s(i,j))$, $KG = \bigoplus G(I_s(i,j))$, $KB = \bigoplus B(I_s(i,j))$ *for all pixels.*
8. ***Step 8: Bit-reversal and final diffusion***
   For each pixel (i,j)*:*
   $R \leftarrow reverseBits(R(I_s(i,j))) \oplus KR$,
   $G \leftarrow reverseBits(G(I_s(i,j))) \oplus KG$,
   $B \leftarrow reverseBits(B(I_s(i,j))) \oplus KB$,
   $C(i,j) \leftarrow (R, G, B)$.
9. ***Output:*** *Cipher image* C.

End.

The detailed steps of the proposed encryption algorithm are summarized in Algorithm1, which complements the flowchart presented in Figure 4 by providing a structured pseudo-code description of the RGB decomposition, zigzag permutation, chaotic diffusion, Josephus-based permutation, and bit-reversal operations.

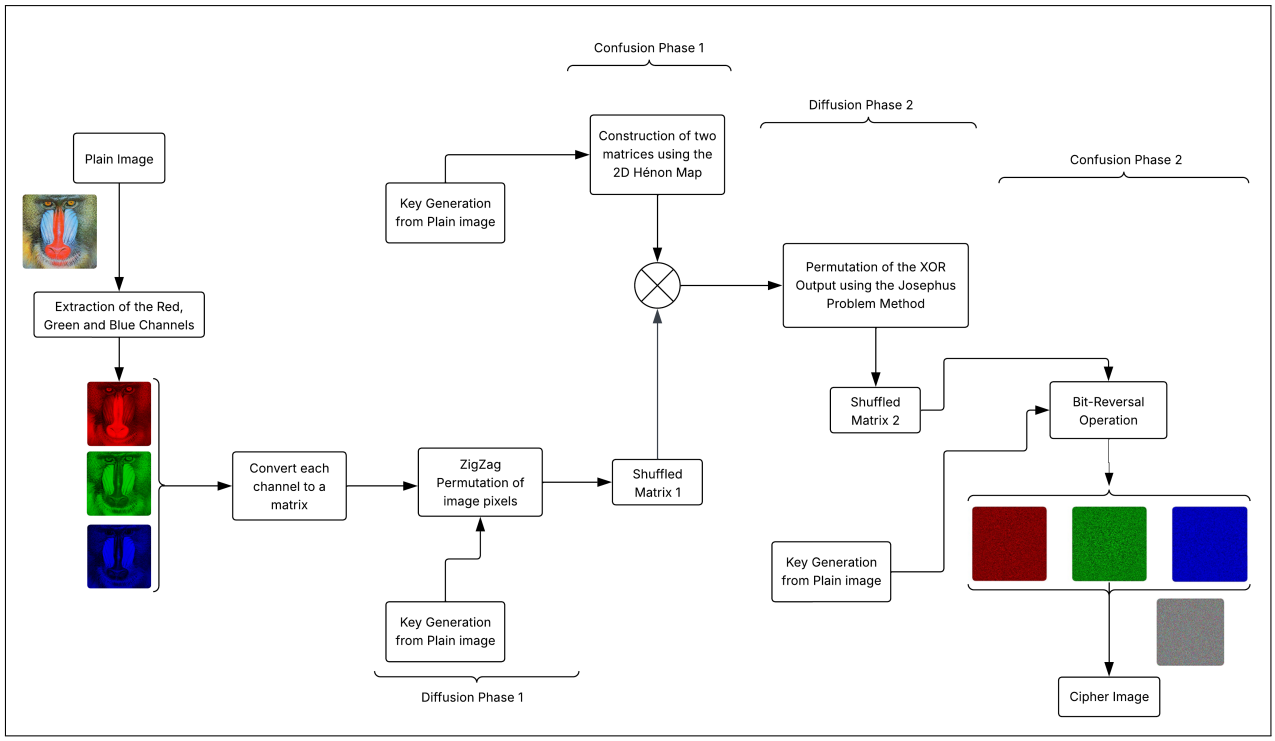


Figure 4. Flow Diagram of the Proposed Method.

4. Experimentation results

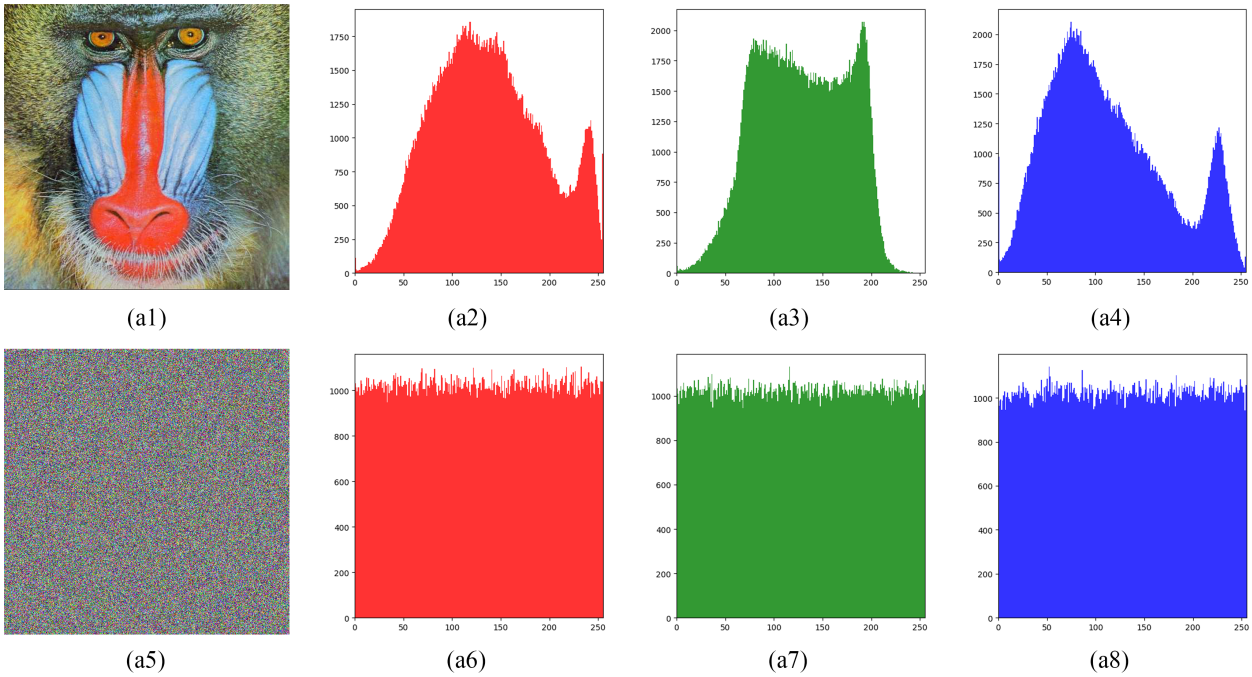
To evaluate the effectiveness and robustness of the proposed encryption scheme, a series of experiments were conducted using standard benchmark images with different sizes, such as Baboon, Peppers, Lena, House and others. The experimental analysis focuses on key performance metrics, including security assessment, statistical characteristics, and sensitivity to key and plaintext variations. Specifically, the results demonstrate the ability of the proposed method to achieve strong confusion and diffusion properties, resist common statistical and differential attacks, and maintain high encryption efficiency. The following subsections provide a detailed discussion of the experimental setup, evaluation criteria, and the outcomes observed for various test scenarios.

4.1. Statistical analysis

4.1.1. Histogram

Histogram analysis is conducted to examine the distribution of pixel intensity values in both the original and encrypted images. We used different sizes of different images to test the uniformity of the histogram.

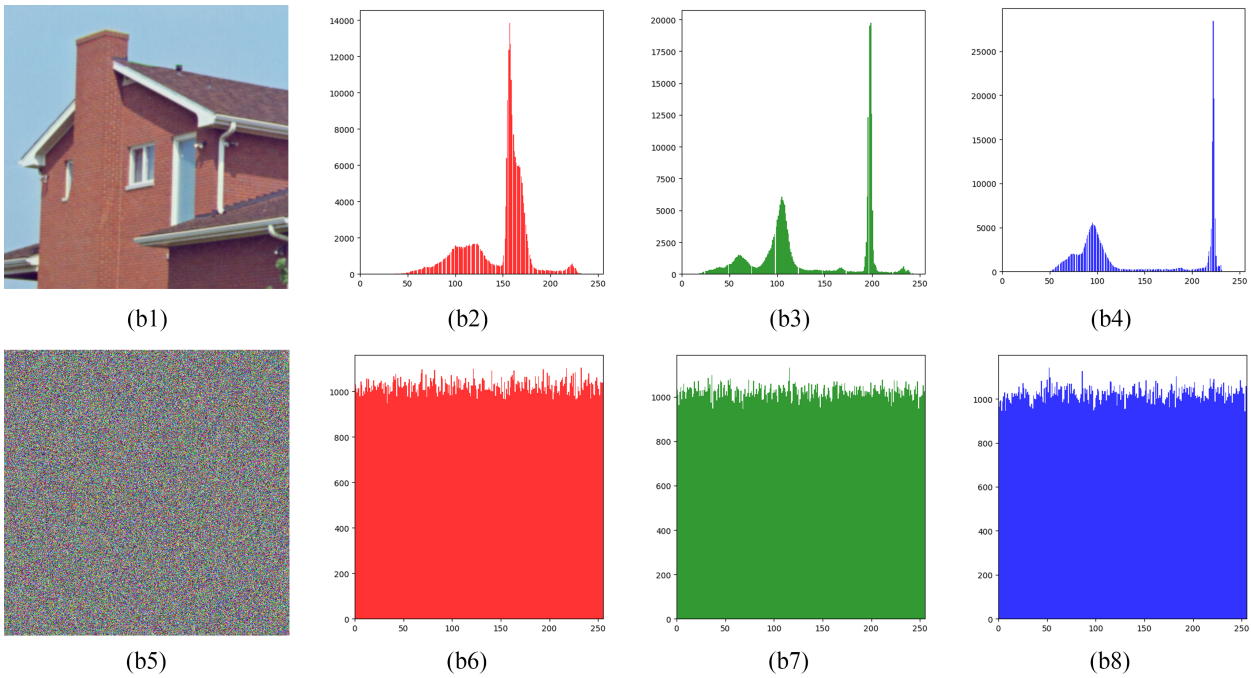
For each image in Figure 5, 6, 7, 8, 9, and 10, the histogram of the original image exhibits the typical peaks and valleys corresponding to spatial redundancy and structural patterns. After applying the proposed encryption scheme, the histograms of the encrypted images are nearly uniform, indicating that the pixel values are well diffused and the visual information is effectively concealed. This demonstrates that the proposed method significantly reduces the correlation and predictability of pixel intensity, enhancing the security against statistical attacks.



(a1) (a2) (a3) (a4)

(a5) (a6) (a7) (a8)

Figure 5. (a1) Baboon image: (a2) Red channel's Histogram; (a3) Green channel's Histogram; (a4) Blue channel's Histogram; (a5) Encrypted Image of Baboon: (a6) Red channel's Histogram; (a7) Green channel's Histogram; (a8) Blue channel's Histogram.



(b1) (b2) (b3) (b4)

(b5) (b6) (b7) (b8)

Figure 6. (b1) House image: (b2) Red channel's Histogram; (b3) Green channel's Histogram; (b4) Blue channel's Histogram; (b5) Encrypted Image of House: (b6) Red channel's Histogram; (b7) Green channel's Histogram; (b8) Blue channel's Histogram.

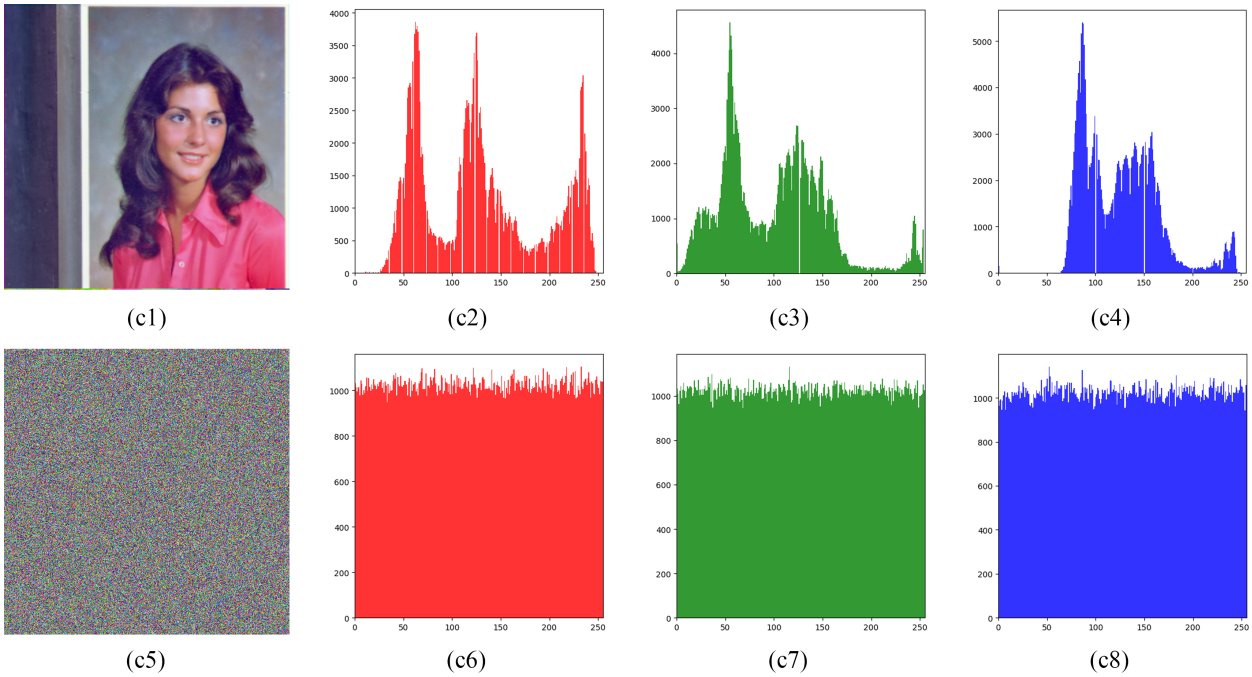


Figure 7. (c1) Female image: (c2) Red channel's Histogram (c3) Green channel's Histogram (c4) Blue channel's Histogram (c5) Encrypted Image of Female: (c6) Red channel's Histogram (c7) Green channel's Histogram (c8) Blue channel's Histogram.

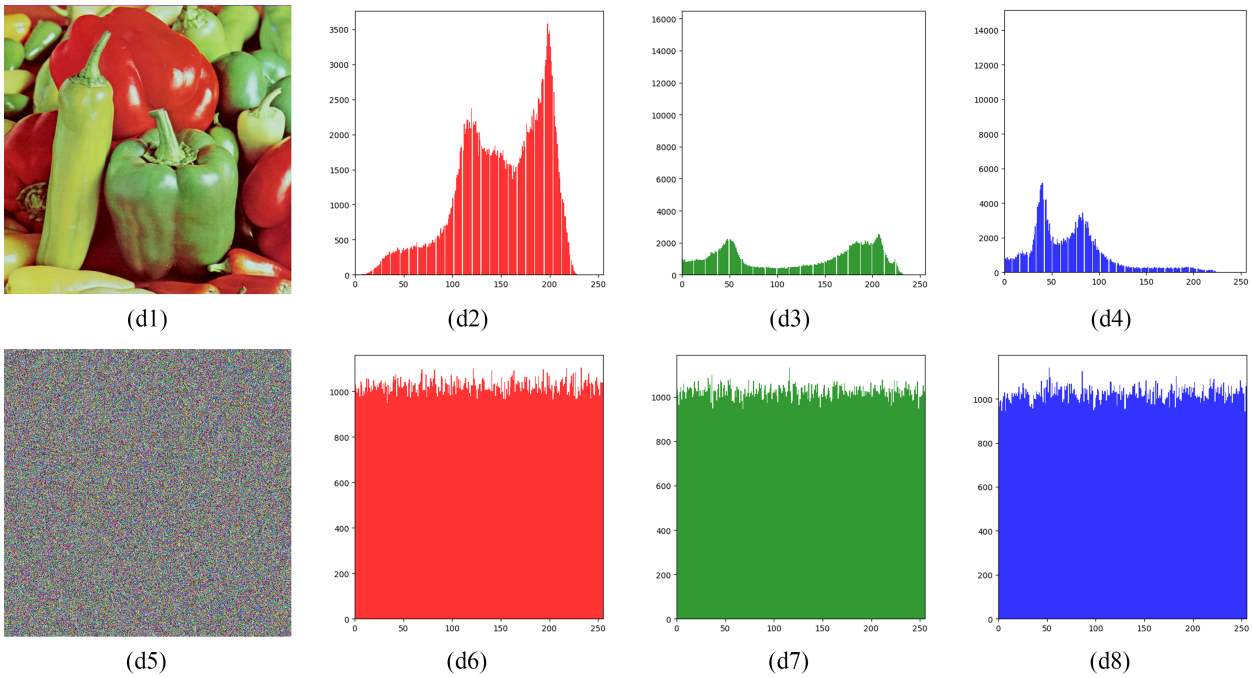


Figure 8. (d1) Peppers image: (d2) Red channel's Histogram (d3) Green channel's Histogram (d4) Blue channel's Histogram (d5) Encrypted Image of Peppers: (d6) Red channel's Histogram (d7) Green channel's Histogram (d8) Blue channel's Histogram.

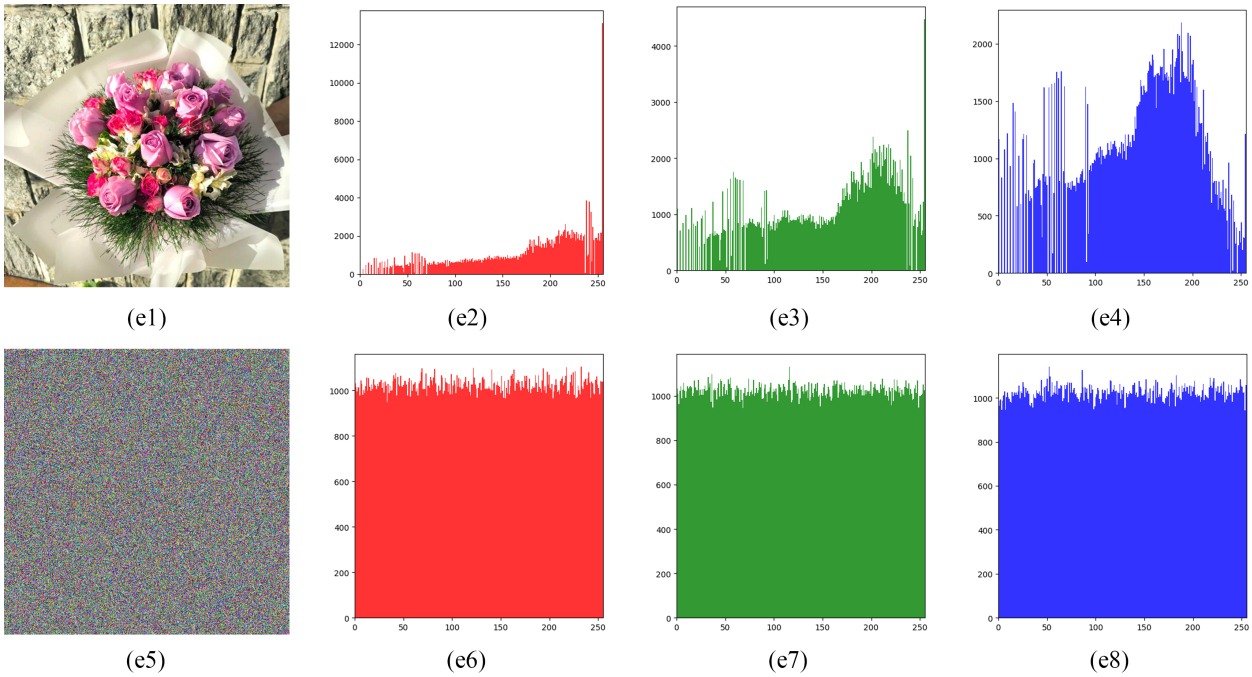


Figure 9. (e1) Flowers image (e2) Red channel's Histogram (e3) Green channel's Histogram (e4) Blue channel's Histogram (e5) Encrypted Image of Flowers: (e6) Red channel's Histogram (e7) Green channel's Histogram (e8) Blue channel's Histogram.

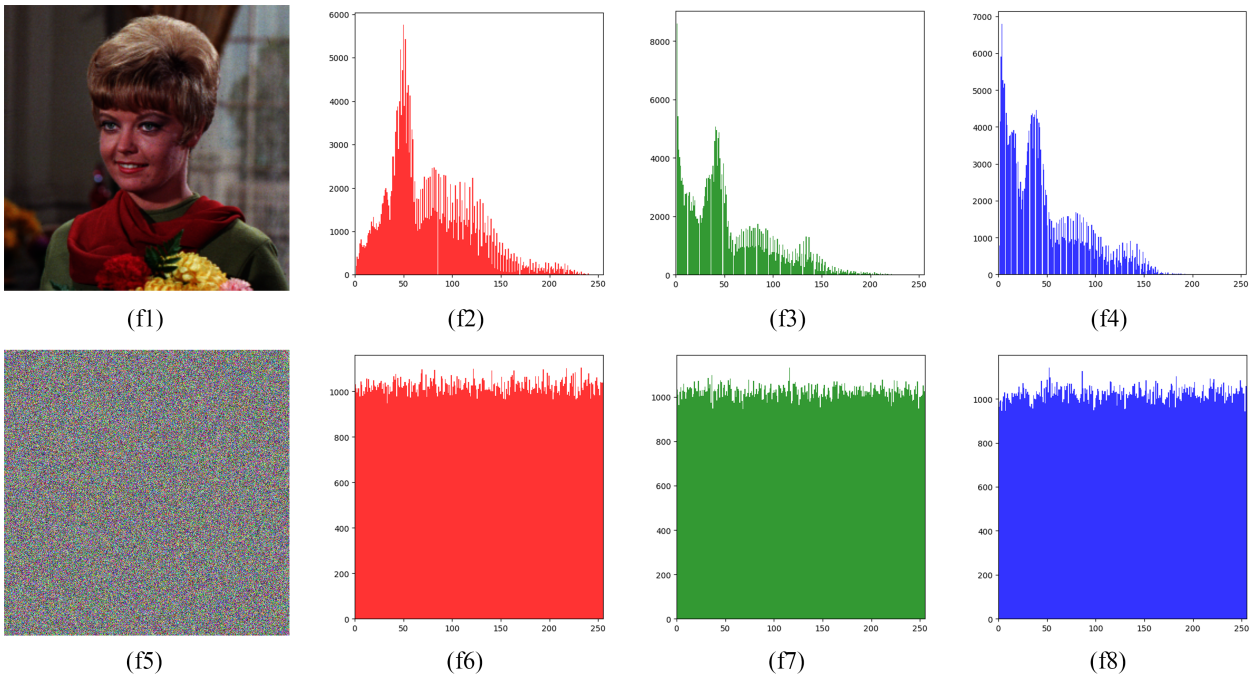


Figure 10. (f1) Female2 image: (f2) Red channel's Histogram (f3) Green channel's Histogram (f4) Blue channel's Histogram (f5) Encrypted Image of Female2: (f6) Red channel's Histogram (f7) Green channel's Histogram (f8) Blue channel's Histogram.

4.1.2. Correlation analysis of adjacent pixels

The correlation between adjacent pixels refers to the degree of statistical dependence between the intensity values of neighboring pixels in an image. It is analyzed to evaluate the capability of the proposed encryption scheme to eliminate the strong spatial redundancy inherent in original images.

Before encryption, adjacent pixels in the horizontal, vertical, and diagonal directions exhibit very high correlation values (close to 1), which is a direct consequence of the smooth variation of intensity levels. This strong correlation is visually illustrated in the corresponding scatter plots, where the pixel distribution forms a narrow diagonal line, indicating a strong linear dependency between neighboring pixels, as shown (g1, g2, g3, h1, h2, h3, i1, i2, i3) in Figure 11, 12, and 13.

After applying the proposed encryption scheme, the scatter plots of the encrypted images show a completely different behavior. The pixel distributions in Figure 11, 12, and 13 (g4, g5, g6, h4, h5, h6, i4, i5, i6) become uniformly scattered over the entire range without forming any specific pattern or diagonal structure, which visually confirms the effective destruction of spatial correlation. These figures clearly demonstrate that the encrypted images do not preserve any statistical relationship between adjacent pixels, highlighting the strong confusion capability of the proposed method.

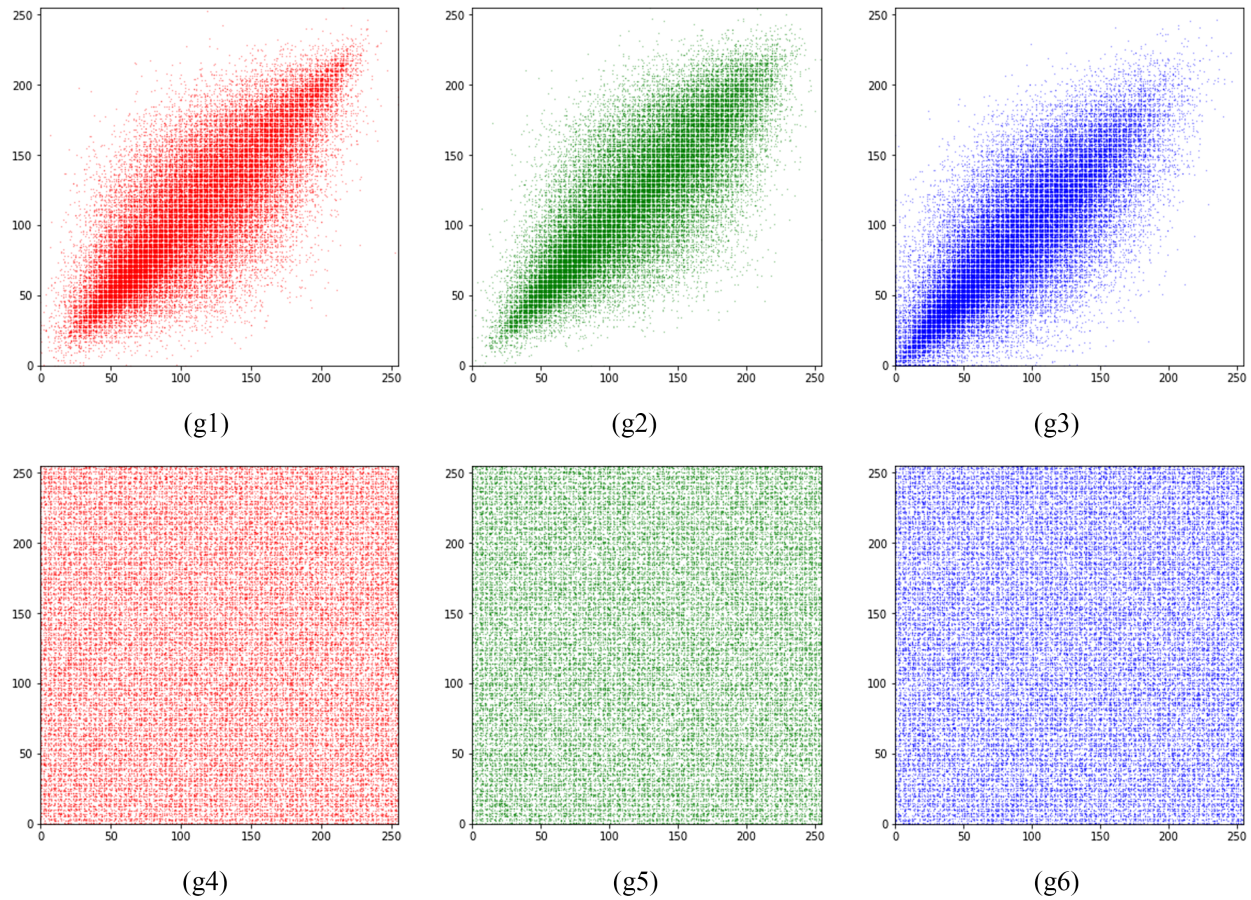


Figure 11. Horizontal Correlation Distribution in Baboon image of: (g1) Red data channel (g2) Green data channel (g3) Blue data channel (g4) Red data channel in Cipher image (g5) Green data channel in Cipher image (g6) Blue data channel in Cipher image.

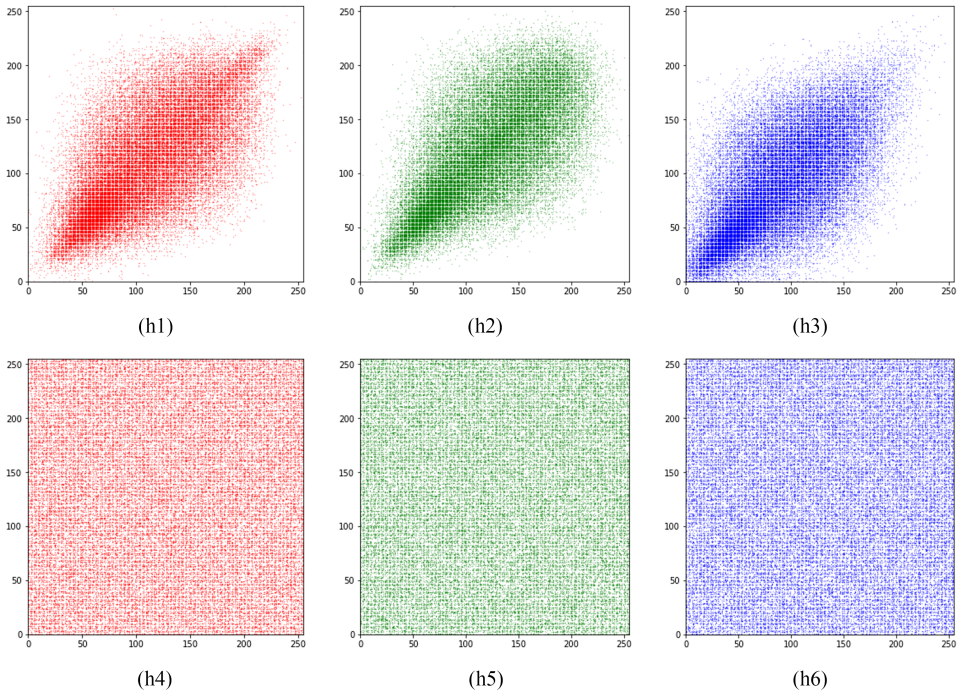


Figure 12. Vertical Correlation Distribution in Baboon image of: (h1) Red data channel (h2) Green data channel (h3) Blue data channel (h4) Red data channel in Cipher image (h5) Green data channel in Cipher image (h6) Blue data channel in Cipher image.

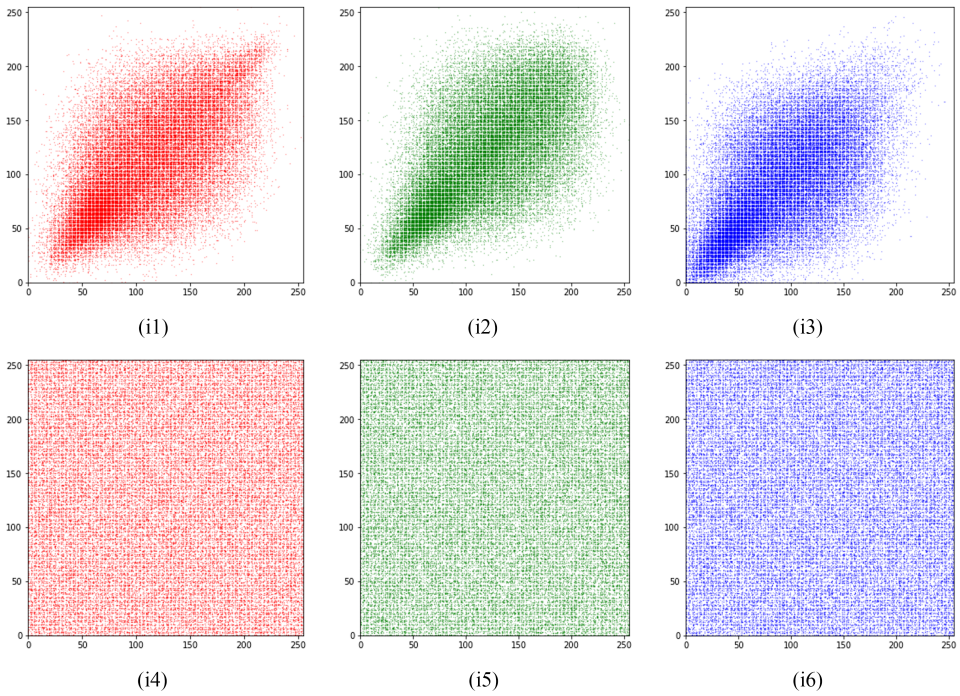


Figure 13. Diagonal Correlation Distribution in Baboon image of: (i1) Red data channel (i2) Green data channel (i3) Blue data channel (i4) Red data channel in Cipher image (i5) Green data channel in Cipher image (i6) Blue data channel in Cipher image.

To further validate this observation, the correlation coefficients between adjacent pixels are computed numerically in the horizontal, vertical, and diagonal directions using equations (5)-(9). The results, summarized in Table 1, show that the correlation coefficients of the encrypted images are significantly reduced and approach zero in all directions. This confirms that the combination of zigzag permutation, chaotic diffusion based on the 2D Hénon map, and Josephus-based permutation effectively breaks pixel dependency and provides strong resistance against statistical attacks.

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

Where:

- $Cov(i,j)$ is the covariance between pixel values i and j,
- $D(i)$ and $D(j)$ represent the variances of i and j, respectively, and it is defined as:

$$D(i) = \frac{1}{P}\sum_{n=1}^{P}(i_n - E(i))^2 \tag{6}$$

- With P is the number of pixels in the image.
- The covariance is defined as:

$$\mathrm{Cov}(i,j) = \frac{1}{P}\sum_{n=1}^{P}(i_n - E(i))(j_n - E(j)) \tag{7}$$

$$E(i) = \frac{1}{P}\sum_{n=1}^{P} i_n \tag{8}$$

$$E(j) = \frac{1}{P}\sum_{n=1}^{P} j_n \tag{9}$$

The Table 2 compares the directional correlation coefficients of standard test images after encryption using the proposed method and several existing approaches. As shown in Table 2, the proposed method generally achieves the lowest or near-lowest correlation values across most images and directions. In the Baboon image, the proposed method attains horizontal, vertical, and diagonal correlation values of 0.002517, 0.001652, and -0.003981, respectively, which are lower than or comparable to those obtained by the referenced techniques [25,33–37]. Similarly, for the Peppers image, the proposed approach yields consistently lower correlation values in all directions, with an average of 0.000658. For other images such as Lena and Plane, the proposed method provides competitive average correlation values (0.000552 and -0.000370, respectively) relative to the existing methods. These results indicate that the proposed encryption scheme effectively disrupts pixel dependencies, enhancing resistance to statistical attacks and improving overall security.

4.1.3. Correlation between the Plain and Cipher images

The correlation between the original image and its corresponding encrypted image is also investigated to assess the resistance of the proposed scheme against statistical and known-plaintext attacks.

While the correlation between adjacent pixels measures local spatial dependencies within an image, the correlation between the original image (plaintext) and the encrypted image (ciphertext) assesses global similarity. In original image, pixel values are highly dependent on their neighbors and on the image itself. A secure encryption algorithm should eliminate this global dependency, ensuring that the encrypted image is statistically independent from the original. This correlation coefficient is calculated by the equations below (10)-(12):

Table 1. Adjacent Pixels Correlation of the Plain and Encrypted test images in different directions.

Image		Plain Image			Encrypted Image		
		Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Baboon	Red	0.785068	0.658650	0.601674	0.000390	0.005501	-0.006982
	Green	0.787717	0.663559	0.606181	0.001332	-0.003005	-0.005227
	Blue	0.781747	0.652056	0.592392	0.005829	0.002458	0.000265
	Average	0.784844	0.658088	0.600083	0.002517	0.001652	-0.003981
House	Red	0.938505	0.864823	0.814862	-0.001528	-0.001996	-0.003622
	Green	0.997719	0.906908	0.904001	-0.006580	-0.002334	0.005284
	Blue	0.996901	0.997059	0.993708	0.001292	-0.002072	0.002689
	Average	0.977708	0.922930	0.904191	-0.002272	-0.002134	0.001450
Lena	Red	0.988310	0.990987	0.979865	0.003206	0.003014	0.000459
	Green	0.982399	0.983273	0.974785	-0.003320	0.004426	-0.000905
	Blue	0.943171	0.948118	0.933019	-0.002571	0.004282	-0.003622
	Average	0.971293	0.974126	0.962556	-0.000895	0.003907	-0.001356
Female	Red	0.991123	0.991226	0.981893	-0.006191	-0.000140	0.002222
	Green	0.991430	0.992426	0.983221	0.000134	-0.005046	0.005930
	Blue	0.989271	0.988083	0.976715	0.003564	-0.001150	0.002314
	Average	0.990608	0.990578	0.980609	-0.000831	-0.002126	0.003489
Peppers	Red	0.960306	0.955216	0.942106	-0.001520	0.002198	0.001411
	Green	0.981678	0.960945	0.946441	-0.004075	-0.000233	0.007425
	Blue	0.967624	0.935726	0.912629	-0.001663	0.004768	-0.002387
	Average	0.969869	0.950629	0.933725	-0.002420	0.002244	0.002150
Flower	Red	0.910212	0.956823	0.874616	0.009940	-0.003747	-0.002797
	Green	0.907189	0.954937	0.870263	-0.001773	0.007221	-0.007882
	Blue	0.899825	0.949021	0.859553	0.008569	-0.000977	0.002081
	Average	0.905742	0.953594	0.868144	0.005579	0.000832	-0.002866
Female2	Red	0.995619	0.992839	0.989178	0.003666	0.001490	-0.000087
	Green	0.994486	0.990463	0.986482	0.001085	0.000576	0.013545
	Blue	0.991651	0.987542	0.981949	0.002148	-0.001150	-0.006849
	Average	0.993918	0.990281	0.985870	0.002300	0.000306	0.002203
Sailboat	Red	0.942647	0.921808	0.913190	0.001217	0.004579	0.004530
	Green	0.967011	0.938896	0.923956	0.002765	0.000002	0.004208
	Blue	0.962718	0.955430	0.936293	-0.003452	-0.000081	0.000858
	Average	0.957459	0.938712	0.924479	0.000177	0.001500	0.003198
Plane	Red	0.987111	0.949455	0.944775	0.003936	-0.001116	-0.005383
	Green	0.933774	0.977750	0.920210	-0.003258	-0.000782	-0.001766
	Blue	0.867046	0.910838	0.846014	0.007999	-0.001747	-0.001220
	Average	0.929310	0.946014	0.903666	0.002893	-0.001215	-0.002789

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{i,j}-\bar{C})(C'_{i,j}-\bar{C}')}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{i,j}-\bar{C})^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(C'_{i,j}-\bar{C}')^2}} \tag{10}$$

Table 2. Comparison of Coefficient Correlation of adjacent pixels Between Our Proposed Algorithm and Others.

Image	Methods	Directions			Average
		Horizontal	Vertical	Diagonal	
Baboon	Ours	0.002517	0.001652	-0.003981	0.000063
	[33]	0.00152662	0.00793051	-0.00774664	0.00057016
	[34]	0.0003	0.0011	-0.0005	0.0003
	[35]	-0.0023	-0.0010	0.0012	-0.0007
	[36]	0.00113408	-0.0019799	-0.004713	-0.005559
	[25]	0.0037	0.0002	0.0045	0.0028
	[37]	0.004002	0.014838	0.006866	0.008569
House	Ours	-0.002272	-0.002134	0.001450	-0.000985
	[33]	-0.00293837	0.00292358	-0.0021016	-0.00070546
	[34]	-	-	-	-
	[35]	0.0030	-0.0011	-0.0072	-0.0018
	[36]	-0.0030184	0.0032035	0.0052921	0.0018257
	[25]	-	-	-	-
	[37]	-	-	-	-
Peppers	Ours	-0.002420	0.002244	0.002150	0.000658
	[33]	0.00514879	-0.00370758	0.0053627	0.00226797
	[34]	-0.0008	-0.0002	-0.0001	0.0004
	[35]	0.0009	-0.0023	0.0018	0.0001
	[36]	-0.0020878	-0.0015191	0.00065688	-0.00098334
	[25]	-0.0022	0.0037	-0.0002	0.0004
	[37]	-0.002872	0.019810	0.010563	0.009167
Lena	Ours	-0.000895	0.003907	-0.001356	0.000552
	[33]	0.00787146	-0.00364176	-0.00154567	0.00089468
	[34]	-0.0007	0.0005	-0.001	-0.0004
	[35]	-	-	-	-
	[36]	0.0079784	0.0011584	-0.00012531	0.00300383
	[25]	-0.0054	-0.0033	0.0004	-0.0028
	[37]	0.000802	-0.001842	-0.000460	-0.0005
Plane	Ours	0.002893	-0.001215	-0.002789	-0.000370
	[33]	0.00175092	0.0024688	0.00214374	0.00212115
	[34]	-0.0014	0.0024	-0.0006	0.0001
	[35]	-0.0017	0.0007	-0.0040	-0.0017
	[36]	-0.0022452	0.0017223	0.0013559	0.00027767
	[25]	-0.0064	-0.0004	-0.0005	0.0024
	[37]	-	-	-	-

Where:

$$\bar{C} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} C_{i,j} \tag{11}$$

$$\bar{C}' = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} C'_{i,j} \tag{12}$$

Where Cr and Cr' are respectively the pixel on original image and the same pixel on cipher image.
The results on table 3 show that the correlation coefficients between the plain images and their encrypted counterparts are extremely low, indicating negligible similarity between them. This confirms that the encrypted images do not preserve any meaningful information from the original images and that the proposed encryption scheme ensures strong plaintext sensitivity and effective information concealment.

Table 3. Coefficient correlation between the plain and the cipher images.

Image		**Baboon**	**House**	**Female**	**Peppers**	**Plane**	**Lena**
After Encryption	Red	-0.005540	0.003156	-0.002214	0.001780	-0.001852	0.001422
	Green	0.001803	-0.003674	0.001350	-0.003125	0.000482	-0.002565
	Blue	-0.001001	0.001456	-0.001179	0.000151	0.000869	0.002231
	Average	-0.001579	0.000313	-0.000681	-0.000398	-0.000167	0.000363

4.1.4. Shanon Global Entropy
Information entropy is widely used to evaluate the degree of randomness and uncertainty in encrypted images. For an 8-bit image, the ideal entropy value is 8, corresponding to a uniform distribution of pixel intensities. Due to inherent spatial redundancy, the entropy of the original image is significantly lower than the ideal value. After applying the proposed encryption scheme, the entropy values of the ciphertext images increase markedly and approach the theoretical maximum. This indicates that the encrypted images exhibit high randomness and do not leak statistical information. The entropy values obtained, by equation (13), for different test images are reported in Table 4, demonstrating the effectiveness of the proposed scheme against entropy-based statistical attacks.

$$E_{\text{Global}} = -\sum_{i=1}^{2^m-1} P(i)\ \log_2\big[P(i)\big] \tag{13}$$

Where:

- i denotes the pixel intensity level.
- $P(i)$ represents the probability of occurrence of intensity level i, defined as $P(i) = \frac{n_i}{N}$, where n_i is the number of pixels having intensity value i and N is the total number of pixels in the image.

Specifically, if the random information source is considered ideal, it has exactly 2^m states, ad its entropy is equal to m. Generally, an entropy of perfect equality would be m. In our approach, the both entropy, local and global, are calculated for the three channels (red, green, blue) and the results illustrated in Table 4 confirm that our proposed algorithm exhibits a favorable advantage in entropy values.

As shown in the Table 5, our algorithm consistently achieves entropy values ranging from 7.999236 to 7.999342, approaching the theoretical maximum of 8 for 8-bit images, which indicates near-ideal randomness. Competing methods [33, 35, 36, 38] exhibit slightly lower entropy values (7.99698–7.99992), while [25] and [37] show incomplete or reduced entropy measurements. Notably, high-frequency images, such as Baboon and Peppers, retain slightly higher entropy with our method, highlighting its robustness against complex and highly textured content. Conversely, smoother images, including House and Sailboat, also achieve near-maximum entropy, demonstrating the algorithm's versatility across diverse image types. Overall, these results confirm that the proposed algorithm not only matches but often surpasses existing approaches, providing strong diffusion,

Table 4. Entropy values of the plain and encrypted images of different sizes.

Image	Image Size	Plain Image			Encrypted Image			Average
		E_R	E_G	E_B	E_R	E_G	E_B	
Tree	251×251	7.237258	7.463102	6.984606	7.997210	7.997126	7.997594	7.997310
Baboon	256×256	7.662099	7.360801	7.682857	7.997002	7.996888	7.996776	7.996889
Lena	256×256	7.268828	7.597630	6.971601	7.997234	7.997002	7.996932	7.997056
Peppers	256×256	7.301116	7.559621	7.094718	7.996939	7.997520	7.997086	7.997182
Baboon	512×512	7.752819	7.465409	7.766575	7.999365	7.999426	7.999236	7.999342
House	512×512	6.376789	6.479787	6.188162	7.999159	7.999241	7.999309	7.999236
Peppers	512×512	7.338827	7.496253	7.058306	7.999329	7.999270	7.999232	7.999277
Plane	512×512	6.717765	6.798979	6.213774	7.999338	7.999242	7.999305	7.999295
Sailboat	512×512	7.312387	7.646107	7.213727	7.999222	7.999334	7.999255	7.999270
Female	512×512	7.416301	7.444649	6.943694	7.999209	7.999296	7.999282	7.999262
Female2	512×512	7.222050	6.980135	6.828047	7.999295	7.999391	7.999368	7.999351
Flower	512×512	7.509801	7.702626	7.706052	7.999368	7.999339	7.999435	7.999381
Baboon	1024×1024	7.713989	7.419466	7.730783	7.999808	7.999819	7.999850	7.999826
Tiffany	1024×1024	4.394355	6.716218	6.408853	7.999807	7.999818	7.999835	7.999820

Table 5. Comparison of entropy values between our algorithm and others.

Image	Ours	[33]	[34]	[35]	[36]	[25]	[37]
Baboon (512×512)	7.999342	7.99902	7.9992	7.9975	7.99721	7.9974	7.99861300
House (512×512)	7.999236	7.99927	-	7.9972	7.99698	-	-
Lena (512×512)	7.999310	7.99901	7.9993	-	7.99721	7.9974	7.99940323
Peppers (512×512)	7.999277	7.99896	7.9993	7.9974	7.99716	7.9972	7.99838484
Plane (512×512)	7.999295	7.99903	7.9993	7.9976	7.99698	7.9969	-
Sailboat (512×512)	7.999270	7.99912	-	7.9972	7.99725	-	-

excellent unpredictability, and reliable security performance, making it highly suitable for robust image encryption.

4.1.5. Shanon Local Entropy

Although global entropy provides an overall measure of randomness, it may not fully capture local irregularities within encrypted images. To address this limitation, a local entropy analysis is performed by dividing the encrypted image into multiple non-overlapping blocks of size 44×44 pixels and computing the entropy of each block independently. A secure encryption scheme should yield local entropy values close to the ideal value of 8 across all blocks. The results of the local entropy analysis are summarized in Table 6, where the reported values consistently approach the theoretical maximum. This confirms that the proposed encryption algorithm ensures uniform randomness at both global and local levels, thereby enhancing resistance to localized statistical and differential attacks. Entropy values are calculated using Equation (14):

$$E_{\text{Local}}(x, y) = -\sum_{i=1}^{2^m-1} P_{x,y}(i)\, \log_2\left[P_{x,y}(i)\right] \tag{14}$$

Where:

- (x, y) denotes the position of the current pixel in the image.

- 2^m represents the information source's total number of states.
- i represents the pixel intensity level, where, $i \in \{0, 1, 2, \ldots, 255\}$.
- $P_{x,y}(i)$ denotes the local probability of occurrence of intensity level i within the window centered at (x, y). It is defined as $P_{x,y}(i) = \frac{n_{i,(x,y)}}{k^2}$, where $n_{i,(x,y)}$ is the number of pixels having intensity value i and N inside the local window, and k^2 represents the total number of pixels within the window.

Table 6. Local Entropy values of different test images.

Images		**Baboon**	**House**	**Lena**	**Peppers**	**Plane**	**Female**	**Tiffany**
E_{Local}	Red	7.901715	7.903385	7.901607	7.902449	7.902692	7.901092	7.902300
	Green	7.902976	7.901731	7.899176	7.900127	7.903764	7.901825	7.902049
	Blue	7.903149	7.903117	7.901551	7.901037	7.902945	7.903658	7.902185
	Average	7.902614	7.902744	7.900778	7.901204	7.903134	7.902192	7.902178

4.2. Differential attacks

Differential analysis evaluates the effect of small changes in the plaintext on the ciphertext using Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) metrics. High NPCR and UACI values indicate that a single-pixel modification in the original image produces substantial changes in the encrypted image, confirming the scheme's strong diffusion properties.

To evaluate the resistance of the proposed encryption scheme against differential attacks, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are employed. These metrics measure the sensitivity of the encryption algorithm to slight changes in the plaintext image. Specifically, two ciphertext images are generated by encrypting two original images that differ by only one pixel, and NPCR quantifies the percentage of pixels that change between the two encrypted images, while UACI measures the average intensity difference. A secure image encryption scheme should produce high NPCR values close to 100% and UACI values close to the theoretical ideal of 33.33% for 8-bit images, indicating strong diffusion and high sensitivity to plaintext variations. These two metrics are mathematically defined as follows:

$$NPCR = \frac{\sum_{i,j} \sigma(i,j)}{M \times N} \times 100\% \tag{15}$$

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|I(i,j) - I'(i,j)|}{255} \right] \times 100\% \tag{16}$$

$$\sigma(i,j) = \begin{cases} 1, & \text{if } I(i,j) = I'(i,j) \\ 0, & \text{if } I(i,j) \neq I'(i,j) \end{cases} \tag{17}$$

Where I and I' denote the two encrypted images corresponding to the original images differing by one pixel, and $M \times N$ represents the image size.

According to the equation (16 and 17) of the ideal expectation values of NPCR N_a^* and UACI interval U_a^* (U_a^{*+} and U_a^{*-}), the values of UACI and NPCR must, respectively, surpass 33.4% and 99.6%.

$$N_a^* = \frac{Q - \phi^{-1}(a)\sqrt{Q/N}}{Q+1} \tag{18}$$

$$U_a^* = \begin{cases} U_a^{*-} = S_u - \phi^{-1}(a/2)\,\beta_u \\ U_a^{*+} = S_u + \phi^{-1}(a/2)\,\beta_u \end{cases} \tag{19}$$

The NPCR and UACI results in Table 7 demonstrate the strong sensitivity of the proposed algorithm to small changes in the plain image. The NPCR values for all color channels (Red, Green, Blue) consistently range from 99.59% to 99.63%, with an average of approximately 99.61%, indicating that nearly all pixels are effectively altered during encryption. This confirms excellent diffusion properties.

Similarly, the UACI values remain consistently around 33.41% to 33.51% across all images and color channels, close to the ideal value of 33.4% for 8-bit images. These results indicate that the proposed encryption scheme provides strong diffusion and high unpredictability across all tested images.

Table 7. NPCR and UACI values of the several encrypted test images.

Image		**Baboon**	**House**	**Female**	**Peppers**	**Flowers**	**Female2**	**Sailboat**	**Lena**
NPCR (%)	Red	99.63	99.62	99.60	99.62	99.61	99.61	99.61	99.61
	Green	99.59	99.63	99.60	99.61	99.61	99.62	99.61	99.60
	Blue	99.61	99.63	99.63	99.62	99.60	99.62	99.59	99.60
	Average	99.61	99.63	99.61	99.62	99.61	99.62	99.60	99.60
UACI (%)	Red	33.46	33.48	33.48	33.44	33.49	33.37	33.46	33.40
	Green	33.49	33.49	33.49	33.44	33.53	33.50	33.44	33.49
	Blue	33.44	33.36	33.52	33.49	33.52	33.48	33.48	33.34
	Average	33.46	33.44	33.50	33.46	33.51	33.45	33.46	33.41

Table 8 compares the proposed algorithm with existing methods [25, 33, 35–38]. The proposed algorithm achieves NPCR values of 99.59%–99.62% and UACI values of 33.41%–33.51% across all tested images, indicating strong pixel-level diffusion and uniform intensity variation. Such performance ensures high sensitivity to plaintext changes, making the scheme resistant to both known-plaintext and chosen-plaintext attacks. Some existing approaches report lower values, reflecting weaker resistance to these attacks. Furthermore, the proposed algorithm maintains consistent performance across different image types, demonstrating robust security against various plaintext-based attack scenarios.

Table 8. Comparison of NPCR and UACI values of the encrypted image between our method and other algorithms.

Image	**Ours**		**[33]**		**[34]**		**[35]**		**[36]**		**[25]**		**[37]**	
	NPCR	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**
Baboon	99.61	33.47	99.6089	29.4430	-	-	99.6102	33.4630	-	-	99.6002	33.6070	99.659604	33.442805
House	99.63	33.44	99.6129	29.5530	-	-	99.6185	33.4701	-	-	-	-	-	-
Plane	99.59	33.45	99.6043	32.5245	99.6083	33.4469	99.6119	33.4811	-	-	99.6262	33.3475	-	-
Peppers	99.62	33.46	99.6134	32.0665	99.6103	33.4248	99.6048	33.4706	-	-	99.5804	33.4553	99.659734	33.482305
Lena	99.60	33.41	99.6124	30.3951	99.6097	33.4680	-	-	99.6217	31.507	99.6368	33.5372	99.652013	33.524416
Sailboat	99.60	33.46	99.6134	32.1299	99.6094	33.5176	99.5781	33.5047	-	-	-	-	-	-

4.3. Quality and Performance Metrics

4.3.1. PSNR & MSE

The Peak Signal-to-Noise Ratio (PSNR) is employed to quantify the similarity between the original image and the encrypted image. Unlike image compression, where a high PSNR is preferred, a secure image encryption scheme

should yield low PSNR values, indicating minimal resemblance between the plaintext and ciphertext images. The obtained PSNR results for the tested images are notably low, which confirms that the encrypted images do not retain perceptual features of the original images. This further validates the robustness of the proposed encryption algorithm against visual and statistical analysis.

The Mean Square Error (MSE) is used to measure the average squared difference between the original image and the corresponding encrypted image. In the context of image encryption, a high MSE value is desirable, as it indicates a significant distortion between the plaintext and ciphertext images.

These two values are calculated between the cipher image and the original image using the given equations (20) and (21):

$$PSNR = 10 \log_{10} \left(\frac{I_{\text{MAX}}^2}{MSE} \right) \tag{20}$$

$$MSE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I'(i,j)]^2}{M \times N} \tag{21}$$

Where I_{MAX} is the highest value that one pixel can have, I is the plain image and I' is the cipher image.
The Table 9 shows that the proposed encryption scheme produces high MSE values for all tested images, confirming that the encrypted images are substantially different from their original counterparts. This behavior demonstrates the strong diffusion capability of the proposed method and its effectiveness in concealing visual information.

4.3.2. SSIM

The Structural Similarity Index Measure (SSIM) evaluates the perceptual similarity between two images by considering luminance, contrast, and structural information. For image encryption applications, low SSIM values close to zero are expected, as they indicate a lack of structural similarity between the original and encrypted images. As shown on table 9, the values calculated by equation (22) demonstrate that the SSIM obtained using the proposed scheme are extremely low for all benchmark images, confirming that the encrypted images don't preserve any structural information from the original images. This highlights the strong resistance of the proposed method against perceptual attacks.

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)(\text{cov}_{xy} + c_3)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)(\sigma_x\sigma_y + c_3)} \tag{22}$$

Where :

- x and y denote the original and encrypted images, respectively,
- μ_x and μ_y are the mean intensity values of x and y,
- σ_x and σ_y represent the standard deviations of x and y,
- $\text{cov}_{x,y}$ is the covariance between x and y,
- c_1, c_2 and c_3 are small positive constants introduced to avoid instability.

In addition, the results of Table 9 confirm that the decryption algorithm successfully reconstructs the original input image (SSIM $\approx$ 1, MSE = 0 and PSNR = inf). Furthermore, the SSIM, PSNR and MSE values of the algorithm for encrypting demonstrate that the cipher image doesn't contain any similar information to the original image.

4.3.3. Encryption time
The proposed encryption algorithm exhibits a computational complexity that primarily arises from its permutation and diffusion operations. For a plain RGB image of size $m \times n$, the image first undergoes a zigzag permutation,

Table 9. Comparison of PSNR, MSE and SSIM values between the encrypted and decrypted image.

Image	Channel	Encryption			Decryption		
		MSE	PSNR (dB)	SSIM	MSE	PSNR (dB)	SSIM
Baboon	Red	8682.0259	8.744592	-	0	Inf	-
	Green	7590.0816	9.328339	-	0	Inf	-
	Blue	9356.5902	8.419627	-	0	Inf	-
	Average	8542.8992	8.830853	0.005348	0	Inf	0.984566
House	Red	8662.2091	8.754516	-	0	Inf	-
	Green	7605.2979	9.319641	-	0	Inf	-
	Blue	9318.4724	8.437356	-	0	Inf	-
	Average	8528.6598	8.837171	0.007493	0	Inf	0.965653
Female	Red	9376.9021	8.410209	-	0	Inf	-
	Green	9073.5546	8.553029	-	0	Inf	-
	Blue	7012.4124	9.672129	-	0	Inf	-
	Average	8487.6230	8.878455	0.006518	0	Inf	0.936689
Lena	Red	10645.5752	7.859112	-	0	Inf	-
	Green	9103.6816	8.538633	-	0	Inf	-
	Blue	7099.5057	9.618522	-	0	Inf	-
	Average	8949.5875	8.672089	0.007674	0	Inf	0.964122
Peppers	Red	7994.2021	9.103052	-	0	Inf	-
	Green	11294.7047	7.602054	-	0	Inf	-
	Blue	11144.3250	7.660265	-	0	Inf	-
	Average	10144.4106	8.121791	0.005859	0	Inf	0.971637
Flowers	Red	11963.9347	7.352063	-	0	Inf	-
	Green	10774.1428	7.806976	-	0	Inf	-
	Blue	9401.9174	8.398639	-	0	Inf	-
	Average	10713.3316	7.852559	0.005695	0	Inf	0.979069
Female2	Red	9934.0841	8.159525	-	0	Inf	-
	Green	12781.8045	7.064881	-	0	Inf	-
	Blue	13468.1646	6.837719	-	0	Inf	-
	Average	12061.3511	7.354042	0.007111	0	Inf	0.980953
Sailboat	Red	7300.5023	9.497276	-	0	Inf	-
	Green	11496.5345	7.525134	-	0	Inf	-
	Blue	11508.4185	7.520647	-	0	Inf	-
	Average	10101.8185	8.181019	0.005624	0	Inf	0.982171

requiring $O(m \times n)$ operations. Two independent Hénon chaotic sequences are then generated for all pixels, contributing $O(2 \times m \times n)$ operations. The permuted image is combined with these sequences through XOR applied separately to each color channel, adding $O(3 \times 2 \times m \times n)$ operations. This is followed by a Josephus-based pixel permutation with $O(m \times n)$ complexity, and finally, a bit-reversal operation applied individually to all three color channels, which contributes $O(3 \times m \times n)$. Summing these contributions, the overall theoretical computational complexity of the algorithm can be expressed as $O(13 \times m \times n)$, indicating linear scaling with the number of pixels.

To validate the practical efficiency, simulation times were measured under identical hardware and software conditions. Despite the multiple stages involved, execution times remain low, demonstrating an effective trade-off between high security and computational efficiency.

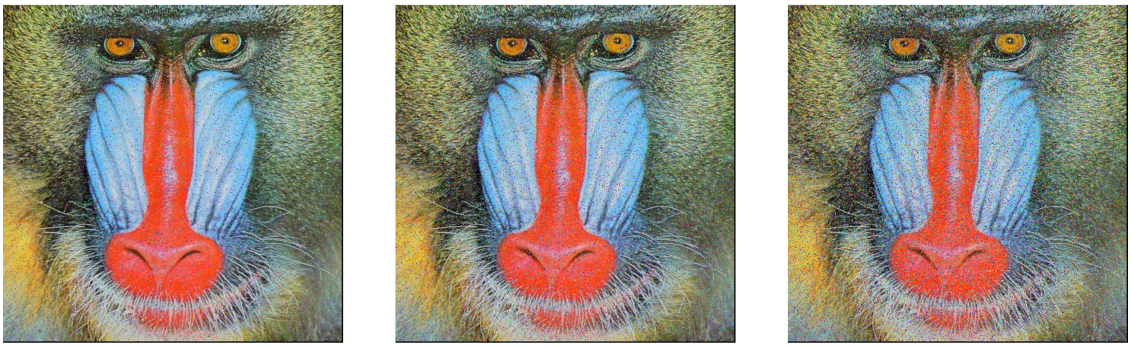
Table 10 summarizes the average encryption times for different image sizes, showing 0.069 s, 0.168 s, and 0.787 s for $256 \times 256, 512 \times 512$, and 1024×1024 images, respectively, on modest hardware. Compared with existing methods, the proposed scheme consistently outperforms previous schemes in terms of computational efficiency, confirming its suitability for real-time image encryption applications.

Table 10. Encryption Time Comparison.

Method	**Encryption time (s)**			**Decryption time (s)**			**Machine performance (CPU and RAM)**
	256×256	512×512	1024×1024	256×256	512×512	1024×1024	
Ours	0.069	0.168	0.787	0.0896	0.208	0.833	i5-5300U CPU 2.30 GHz, 8 GB
[34]	0.9782	3.7066	-	0.8775	3.8762	-	Intel Core i5-12600 CPU 3.30 GHz, 16 GB
[35]	-	1.33	-	-	-	-	8 GB
[36]	0.32	1.33	5.76	0.31	1.33	5.78	3.3 GHz AMD Ryzen 9 5900HX, 32 GB
[38]	-	1.56623	-	-	0.587445	-	2.50 GHz, 4 GB

4.4. Noise attacks

To evaluate the robustness of our scheme, the encrypted images were subjected to three types of attacks: salt-and-pepper noise, cropping, and occlusion. The salt-and-pepper noise randomly inserts black or white pixels, simulating impulsive corruption, while the cropping attack removes a portion of the image, testing the decryption resilience against partial information loss. The occlusion attack consists of covering or replacing a specific region of the encrypted image with black, white, or random noise patterns instead of completely removing it, thereby evaluating the algorithm's resistance to localized obstruction and data alteration. The decrypted images under these attacks are presented in Figure 14, 15, and 16, illustrating the visual impact of each perturbation.



(SPN1) (SPN2) (SPN3)

Figure 14. Decrypted Baboon image after applying Salt-and-Pepper Noise with : (SPN1) Variance = 0.05 ; (SPN2) Variance = 0.1; (SPN3) Variance = 0.2.

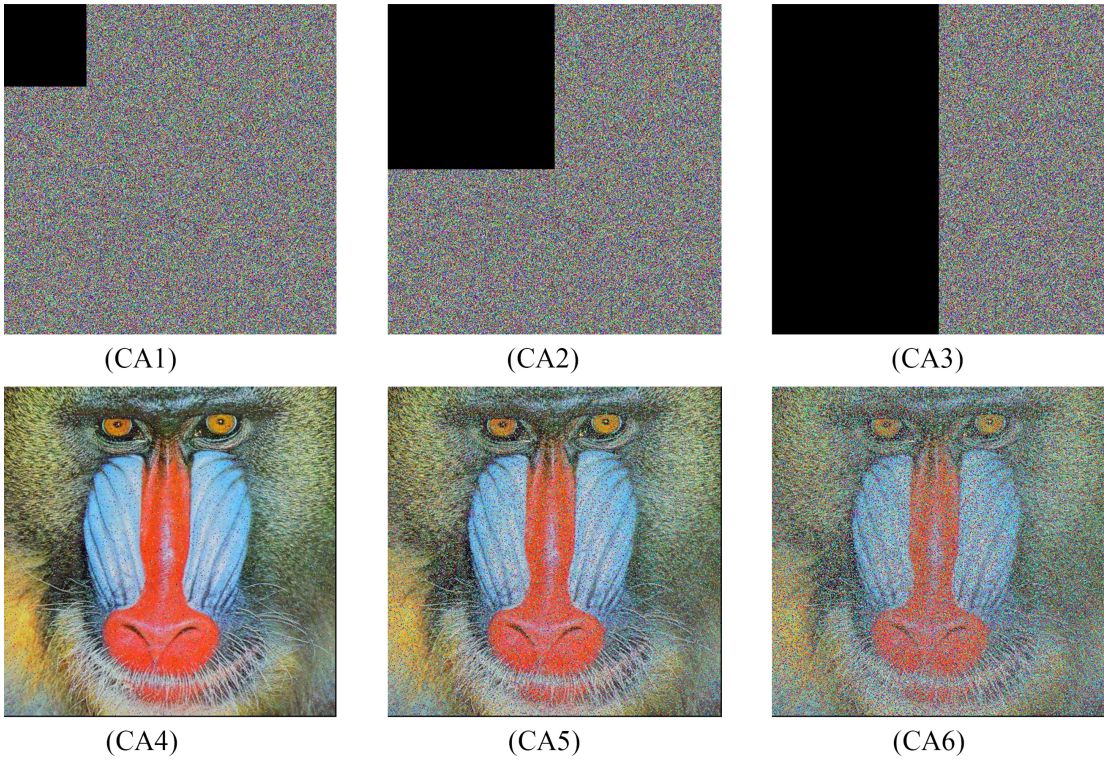


Figure 15. Visual robustness evaluation against cropping attack. (CA1–CA3) Encrypted images with cropping ratios of 1/16, 1/4, and 1/2, respectively. (CA4–CA6) Corresponding decrypted results.

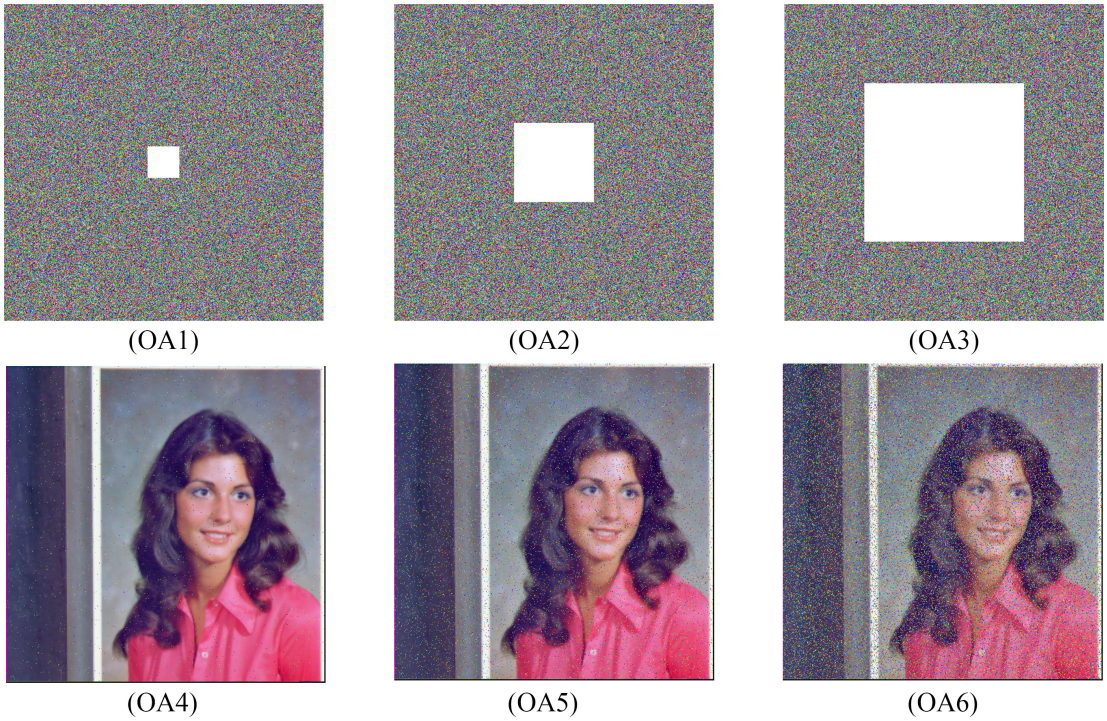


Figure 16. Visual robustness evaluation against white occlusion noise. (OA1–OA3) Encrypted images with occlusion noise of 10%, 25%, and 50% of image, respectively. (OA4–OA6) Corresponding decrypted results.

Furthermore, the performance is quantitatively assessed using metrics such as PSNR, SSIM, and decryption change rate, with the results summarized in Table 11. These metrics provide a clear comparison of the visual quality and robustness of the decrypted images under different types of perturbations. Salt-and-Pepper attacks were applied at three different level densities (0.05, 0.1, and 0.2), while Cropping attacks were performed by removing 1/16, 1/4, and 1/2 of the encrypted image, and Occlusion attacks were applied by replacing 10%, 25% and 50% pixels of encrypted image with white pixels.

The results indicate that the proposed method consistently maintains good visual quality and low decryption change rates across all attack intensities. As the attack severity increases, a gradual reduction in image quality is observed, but the decrypted images remain recognizable, demonstrating the robustness of the proposed scheme against different levels of noise, occlusion attacks and cropping attacks.

Table 11. PSNR, SSIM, MSE and Rate of Change of image after applying occlusion, cropping, and noise attacks.

Metrics	**Salt-and-Pepper attacks**			**Cropping attacks**			**Occlusion attacks**		
	0.05	0.1	0.2	1/16	1/4	1/2	10%	25%	50%
MSE	501.3848	890.8892	1617.1256	630.3694	2247.5920	4409.9168	395.2123	842.2052	2425.9297
PSNR	21.132806	18.640205	16.054413	20.144637	14.630938	11.704676	22.171806	18.901820	14.318221
SSIM	0.916611	0.855601	0.748716	0.896617	0.664639	0.407516	0.920998	0.841354	0.601583
Rate of Change (%)	5.600357	10.218811	18.681335	6.980133	25.579071	50.387192	1.765823	6.983566	25.596237

4.5. NIST analysis

To further evaluate the randomness quality of the encrypted images, the NIST statistical test suite was employed. Bit sequences extracted from the encrypted images were subjected to several standard NIST tests, including frequency, block frequency, runs, and approximate entropy tests. The results of these tests are summarized in Table 12, which reports the corresponding p-values for each test. As shown in the table, the proposed encryption scheme passes all selected NIST tests with satisfactory p-values, demonstrating that the encrypted data exhibit strong randomness characteristics comparable to those of true random sequences. These results confirm the effectiveness of the chaotic diffusion and bit-level operations in generating highly random ciphertext images, highlighting the robustness of the proposed method against randomness-based cryptanalytic attacks.

4.6. Key-based attacks

4.6.1. key sensitivity

The encryption algorithm's sensitivity to modifications in keys in image cryptography is of essential necessity to guarantee the security of visual data. When an encryption key is altered, the transformation applied to an image must be responsive to this change to preserve communication security. This implies that small variations in the key should have a big impact on the resulting image. Sensitivity to key changes enhances the resilience of image cryptography against brute-force attacks and cryptanalysis attempts. By ensuring a complex and nonlinear relation between the key and the cipher image, we alter the key during the decryption phase by adding 10^{-15} to the parameter x_0 of the ZigZag Operation as mentioned in the Table 13. Figure 17 illustrates the outcome of our decryption algorithm with the correct key and the modified key.

Table 12. Results of NIST Statistical Tests for Encrypted Images.

Test	**P-Values**	**Decision**
Frequency Test	0.795700	Pass
Block Frequency Test	0.633979	Pass
Run Test	0.835605	Pass
Longest run of ones in a block	0.916975	Pass
Binary matrix rank test	0.811544	Pass
DFT Test	0.154345	Pass
Non-overlapping template matching test	1	Pass
Overlapping template matching test	1	Pass
Universal statistical test	0.725693	Pass
Linear complexity test	1	Pass
Serial test	0.8706095	Pass
Approximate entropy test	0.112612	Pass
Forward cumulative sums test	0.408319	Pass
Reverse cumulative sums test	0.408319	Pass
Random excursions test	0.144507	Pass
Random excursions variant test	0.999998	Pass

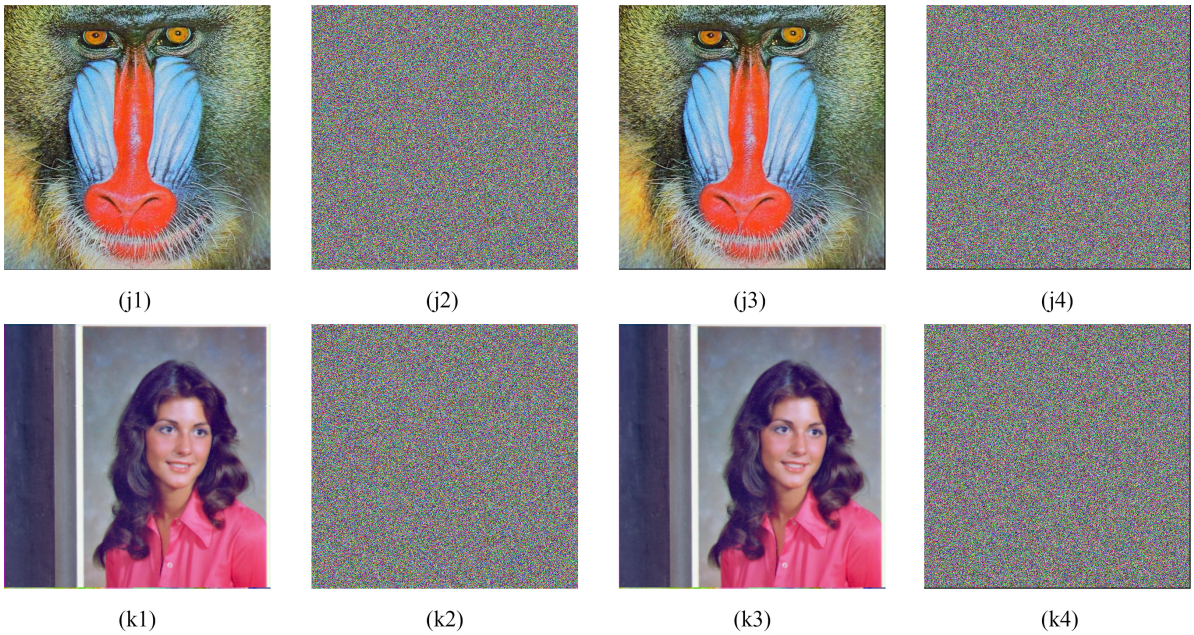


Figure 17. Key sensitivity analysis: (j1) Original Image Baboon, (j2) Encrypted Image, (j3) Decrypted Image with the correct key, (j4) Decrypted image with the wrong key, (k1) Original Image Female, (k2) Encrypted Image, (k3) Decrypted Image with the correct key, (k4) Decrypted image with the wrong key.

To ascertain the extent of the impact of minor alterations in one of our algorithm parameters, we sequentially adjust each parameter, akin to the procedure employed for the ZigZag Operation. Subsequently, we compute the rate of change in the decrypted image. The change rates delineated in Table 14 evince the heightened sensitivity of our algorithm, even to slight modifications in a single key, thereby attesting to the formidable challenge faced by potential assailants seeking to compromise its integrity.

Table 13. The correct and the wrong keys used in the decryption phase.

	ZigZag Operation	1^{st} **matrix of Hénon Map**	2^{nd} **matrix of Hénon Map**
Correct keys	x_0 = 0.54321832490123 block size = 3	y_0 = 0.21325473181134 a = 1.37122453111523 b = 0.31211364122318	y_0 = 0.12134221232157 a = 1.42317312132391 b = 0.31129331227119
Incorrect keys	x_0 **= 0.54321832490124** block size = 3	y_0 = 0.21325473181134 a = 1.37122453111523 b = 0.31211364122318	y_0 = 0.12134221232157 a = 1.42317312132391 b = 0.31129331227119

Table 14. Rate of change on the decrypted image in %.

Parameters	**Change Rate (%)**
x_0 of zigzag	99.2199
r of zigzag	99.2203
x_0 of 1st matrix of henon map	99.2228
y_0 of 1st matrix of henon map	99.1287
a of 1st matrix of henon map	99.2203
b of 1st matrix of henon map	99.2203
x_0 of 2nd matrix of henon map	99.2228
y_0 of 2nd matrix of henon map	99.1287
$a$of 2nd matrix of henon map	99.2203
b of 2nd matrix of henon map	99.2203
k of Josephus Problem	99.2153

4.6.2. key space

Key space analysis is conducted to assess the resistance of the proposed encryption scheme against brute-force attacks. A secure encryption algorithm must provide a sufficiently large key space to make exhaustive key search computationally infeasible.

In the proposed encryption scheme, the secret keys are dynamically generated is ensured by a multiple independent encryption stages. Specifically, the 2D Hénon chaotic map contributes 4 secret parameters, including its initial conditions and control parameters. Our proposed method utilizes two matrices of this chaotic system, introducing $4 \times 2 = 8$ variables. The Zigzag permutation process introduces 3 additional secret parameters related to its traversal configuration. Furthermore, the Josephus permutation mechanism is controlled by 2 secret parameters, while the bit-reversal operation adds 4 independent parameters governing the inversion of significant and insignificant bits. Finally, the XOR diffusion stage is driven by 3 secret parameters.

Assuming a computational precision of 10^{-16} for each real-valued parameter, each parameter contributes approximately 10^{16} possible values. As a result, the total number of secret parameters equals 20, leading to a key space of approximately $(10^{16})^{20} = 10^{320} \approx 2^{1063}$. This extremely large key space effectively protects the proposed encryption scheme against brute-force attacks.

Table 15 presents a quantitative comparison of the key space between the proposed scheme and related methods. As observed, the proposed algorithm provides a substantially larger key space than those reported in [34] (2^{732}), [35] (2^{584}), [36] (2^{744}), and [25] (2^{199}). This improvement is mainly due to the use of multiple independent secret parameters distributed across chaotic generation, permutation, bit-level transformation, and diffusion stages. The

significantly enlarged key space increases the computational complexity of brute-force attacks and provides a higher theoretical security margin.

Table 15. Key space comparison of our proposed method and others.

Methods	**Ours**	**[34]**	**[35]**	**[36]**	**[25]**
Key Space	2^{1063}	2^{732}	2^{584}	2^{744}	2^{199}

5. Conclusion

In this paper, a novel image encryption scheme has been proposed, combining the 2D Hénon chaotic map, Zigzag permutation, Josephus problem, and bit-reversal operation. The primary novelty of the proposed scheme lies in the coordinated integration and interleaving of these components within a unified encryption framework, where chaotic sequences dynamically guide permutation and diffusion operations. This design ensures that even minor changes in the plaintext result in significant variations in the ciphered image, enhancing both confusion and diffusion.

Extensive experimental evaluations have been conducted across images of different sizes, including statistical analyses (histogram, correlation of adjacent pixels), security metrics (NPCR, UACI, key sensitivity, key space), and quality measures (PSNR, SSIM, MSE). Furthermore, robustness tests against salt-and-pepper noise and cropping attacks were performed. The results demonstrate that the proposed scheme achieves high encryption effectiveness, strong resistance to differential and statistical attacks, and maintains accurate and stable decryption performance.

Comparative analysis with several recently reported methods confirms that the proposed algorithm provides a larger key space, higher security margin, and competitive computational efficiency. The combination of multiple independent secret parameters across chaotic generation, permutations, bit-level transformations, and diffusion stages significantly increases the algorithm's structural complexity and unpredictability, making exhaustive search and common cryptanalytic attacks computationally infeasible.

Despite its effectiveness, the proposed scheme has some limitations, including relatively higher computational cost for large images and the lack of formal cryptanalysis under adaptive attack models. Future work will address these limitations by exploring real-time implementations, conducting formal cryptanalysis under chosen-plaintext and chosen-ciphertext attacks, and developing hardware-oriented optimizations to enable deployment in resource-constrained environments.

Acknowledgement

This work was supported by the Sidi Mohamed Ben Abdellah University (USMBA), Fez, Morocco.

REFERENCES

1. S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, *Breaking a Chaotic Image Encryption Algorithm*, Multimedia Tools and Applications, vol. 79, no. 35–36, pp. 25635–25655, 2020.
2. G. Chen, Y. Mao, and C. K. Chui, *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749–761, Jul. 2004.
3. S. Lian, *Multimedia Content Encryption: Techniques and Applications*, Auerbach Publications, 2008.

4. H. Touil, N. El Akkad, and K. Satori, *Homomorphic Method Additive Using Pailler and Multiplicative Based on RSA in Integers Numbers*, in 5th Int. Conf. on Big Data and Internet of Things, 2022.
5. M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, *A Novel Text Encryption Algorithm Based on the Two-Square Cipher and Caesar Cipher*, in Big Data, Cloud and Applications, 2018.
6. H. Touil, N. El Akkad, and K. Satori, *Text Encryption: Hybrid Cryptographic Method Using Vigenere and Hill Ciphers*, in Int. Conf. on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 2020.
7. 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, pp. 34901–34925, 2019.
8. F. Kolouh, S. Amine, M. Es-sabry, and N. El Akkad, *Enhancing Data Security Through Hybrid Cryptographic Techniques: XOR and RSA Integration for RGB Image Encryption*, Digital Technologies and Applications, Springer Nature Switzerland, vol. 1099, pp. 129–138, 2024.
9. H. Gao, Y. Zhang, S. Liang, and D. Li, *A new chaotic algorithm for image encryption*, Chaos, Solitons & Fractals, vol. 29, no. 2, pp. 393–399, Jul. 2006.
10. M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, *A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method*, Scientific African, vol. 16, p. e01217, Jul. 2022.
11. Y. Luo, J. Yu, W. Lai, and L. Liu, *A novel chaotic image encryption algorithm based on improved baker map and logistic map*, Multimed Tools and Applications, vol. 78, no. 15, pp. 22023–22043, 2019.
12. M. Hanif *et al.*, *A Novel Grayscale Image Encryption Scheme Based on the Block-Level Swapping of Pixels and the Chaotic System*, Sensors, vol. 22, no. 16, p. 6243, 2022.
13. M. Es-Sabry, N. El Akkad, M. Merras, K. Satori, W. El-Shafai, T. Altameem, M. Fouda, *Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques*, IEEE Access, vol. 11, pp. 100856–100878, 2023.
14. S. Amine, F. Koulouh, M. Es-Sabry, R. Taouil, F. Hdioud, and N. E. Akkad, *Advanced 3D Color Image Encryption Using Lorenz and Rössler Chaotic Systems:A Multi-Layered Approach*, 3rd International Conference on Embedded Systems and Artificial Intelligence (ESAI), IEEE, pp. 1–7, 2024.
15. F. Elazzaby, N. El Akkad, and S. Kabbaj, *Advanced Encryption of Image Based on S-box and Chaos 2D (LSMCL)*, in 1st Int. Conf. on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 2020.
16. M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, *A New Hybrid Digital Chaotic System With Applications in Image Encryption*, Signal Processing, vol. 160, pp. 45–58, 2019.
17. K. H. Sabour, S. Kabbaj, F. Elazzaby, and N. El Akkad, *A New Contribution of Image Encryption Based on Chaotic Maps and the Z/nZ Group*, Journal of Theoretical and Applied Information Technology, vol. 101, no. 11, pp. 37–47, 2023.
18. S. Amine, F. Koulouh, M. Es-sabry, and N. El Akkad, *Securing Visual Data: A Fresh Approach with Arnold Cat Map and Chebyshev Map Encryption*, Digital Technologies and Applications, vol. 1099, Springer Nature Switzerland, pp. 278–287, 2024.
19. R. Abou-Bakr and E. A. Elmanfaloty, *An Image Encryption Scheme Using a 1D Chaotic Double Section Skew Tent Map*, Complexity, vol. 2020, pp. 1–18, 2020.
20. S. Kanwal, S. Inam, M.T. Othman, M. Ibrahim, F. Nawaz, A. Nawaz, and H. Hamam, *An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices*, Sensors, vol. 22, no. 12, p. 4359, 2022.
21. A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, W.J. Buchanan, *Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution*, IEEE Access, vol. 8, pp. 140876–140895, 2020.
22. S. Amiri and M. Zaied, *Cryptanalysis of chaos-based image encryption using DL attack*, Procedia Computer Science, vol. 270, pp. 106–115, 2025.
23. J. Fridrich, *Symmetric Ciphers Based on Two-Dimensional Chaotic Maps*, Int. J. Bifurcation Chaos, vol. 08, no. 06, pp. 1259–1284, Jun. 1998.
24. K. U. Shahna and A. Mohamed, *An Image Encryption Method Using Henon Map and Josephus Traversal*, Innovations in Bio-Inspired Computing and Applications, Springer International Publishing, vol. 939, pp. 375–385, 2019.
25. M. Lone, *Encryption Scheme for the Security of Digital Images Based on Josephus Traversal and Chaos Theory*, Steganography -The Art of Hiding Information, J. Mayer, Ed., IntechOpen, 2024.
26. R. Wang, G.-Q. Deng, and X.-F. Duan, *An image encryption scheme based on double chaotic cyclic shift and Josephus problem*, Journal of Information Security and Applications, vol. 58, p. 102699, May 2021.
27. Z. Hua, B. Xu, F. Jin, and H. Huang, *Image Encryption Using Josephus Problem and Filtering Diffusion*, IEEE Access, vol. 7, pp. 8660–8674, 2019.
28. N.E. Ghouate, M.A. Tahiri, A. Bencherqui, H. Mansouri, A.E. Maloufy, H. Karmouni, M. Sayyouri, S. Askar, and M. Abouhawwash, *A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy*, Scientific Reports, vol. 15, no. 1, p. 29439, Aug. 2025.
29. M. Jiang and H. Yang, *Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation*, Entropy, vol. 25, no. 11, p. 1516, Nov. 2023.
30. S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, *A novel color image encryption algorithm based on spatial permutation and quantum chaotic map*, Nonlinear Dynamics, vol. 81, no. 1–2, pp. 511–529, Jul. 2015.
31. A. J. Vithayathil and A. Sreekumar, *Image Encryption Through Aperiodic Josephus Permutation And Novel Cyclic Shift Operation*, 3rd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), IEEE, pp. 81–88, May 2023.
32. 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.
33. W. Alexan, K. Hosny, and M. Gabr, *A new fast multiple color image encryption algorithm*, Cluster Computing, vol. 28, no. 5, p. 325, Aug. 2025.
34. H. Zhang, X. Liu, K. Chen, R. Te, and F. Yan, *Robust Image Encryption with 2D Hyperchaotic Map and Dynamic DNA-Zigzag Encoding*, Entropy, vol. 27, no. 6, p. 606, Jun. 2025.

35. X. Zhang, Y. Liu, M. Liu, and Y. Niu, *Image encryption algorithm based on Zigzag transformation and roulette wheel rotation mechanism*, Journal of King Saud University Computer and Information Sciences, vol. 37, no. 8, p. 239, Oct. 2025.
36. 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, p. 54928 - 54956, 2023.
37. M. Es-Sabry, N. El Akkad, L. Khrissi, K. Satori, W. El-Shafai, T. Altameem, and R. S. Rathore, *An Efficient 32-bit Color Image Encryption Technique Using Multiple Chaotic Maps and Advanced Ciphers*, Egyptian Informatics Journal, vol. 25, no. 2, p. 100449, 2024.
38. F. El Azzaby, K. H. Sabour, N. El Akkad, W. El-Shafai, A. Torki, and S. R. Rajkumar, *Color Image Encryption Using a Zigzag Transformation and Sine–Cosine Maps*, Scientific African, vol. 22, p. e01955, 2023.