

Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)



A Plaintext Dependent Chaos based Image Encryption Scheme using Bit-Plane Scrambling and XOR based Diffusion

Zahraa Azhar Muhammad*

Collage of Computer Science and Mathematics at the University of Kufa. Najaf, Iraq. .Email:zahraa.alramahi@uokufa.edu.iq

ARTICLE INFO

Article history:

Received: 18 /05/2026

Revised form: 28 /06/2026

Accepted : 05 /07/2026

Available online: 30/09/2026

Keywords:

Image Encryption,

Chaos-based Cryptography,

Logistic Map,

Plaintext-dependent Key,

Bit-plane Decomposition,

Zigzag Permutation,

XOR Diffusion,

Chaotic Sequence,

Image Security

ABSTRACT

Secure image encryption algorithms received considerable development in cyber security applications in the age of digital data. This paper proposes a new hybrid image encryption scheme based on a chaotic system and bit-plane processing. The suggested algorithm uses a key generation mechanism based on plaintext, where the initial condition in a standard Logistic map is influenced by statistical features of the input image in addition to four external secret keys to increase key sensitivity and expand the size of the key space (2186). It is a two-stage encryption process consisting of a permutation and diffusion. The permutation process separated the input image into eight bit-planes and each plane is reordered according to a key-dependent scanning algorithm. During the diffusion phase, a feedback-based XOR operation is performed by using a chaotic key stream obtained from Logistic map such that adjacent pixels are strongly dependent. The experimental results show the proposed scheme presents favorable security performance of both color and gray image. The correlation coefficients of the encrypted images are low (≈ 0.0004 – 0.0044), and their entropy values are high (≈ 7.9970). In addition, the cryptographic algorithm is also very robust against differential attack such as Number of Pixel Change Rate (NPCR) = 99.63% and Unified Average Changing Intensity (UACI) = 33.39%. The results validate that the developed encryption scheme exhibits excellent confusion and diffusion characteristics, significant key sensitivity, and a high level of resistance to statistical and differential attacks, thus making it ideal for secure image transmission applications.

MSC..

<https://doi.org/10.29304/jqcm.2026.18.32908>

1. Introduction

The accelerated rise of digital communication and multimedia technologies in recent years has enhanced the necessity for conveying visual data securely. Medical imaging, military communication, remote sensing and other applications rely primarily on digital images. But according to the public-characteristic of communication networks, these images are prone to unauthorized access, interception and tampering. Thus, at present time preventing unauthorized access and modifying image data has become a major area of research work in the area of Information

*Corresponding author:Zahraa Azhar Muhammad

Email addresses: zahraa.alramahi@uokufa.edu.iq

Communicated by 'sub etitor'

security [1]. Conventional encryption algorithms, including the Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA), are mainly developed for textual data, they might be inefficient for image encrypted because image has some properties from which high redundancy of information, pixels dependence relation and huge quantity of data. Consequently, a wide selection of scholars addressed image encryption methods that could serve these characteristics at very high levels whilst remaining sensible efficiency[2]. chaos, which is the behavior of certain dynamical systems that are highly sensitive to initial conditions. In any simulation system, that a little change in the initial condition can produce impractical outcomes[3]. There is chaos in every field but that should be the way we enter within all human paradigms. As fundamental and applied sciences have progressed, chaos theory became an important center of attention in nonlinear science. Chaos theory is an important support for modern electronics engineering and image processing principles. Chaotic systems are nonlinear, iterative, quasi-random data with high mixing and sensitive dependence on initial conditions. Thus, chaos theory serves as an optimal buildup for good image encryption algorithms. It is also notice that the range of possible encryption keys with a single chaotic system is very small; hence, the algorithm can be attacked as malicious. So, to construct a reliable and competent image encryption algorithm researchers typically combine dynamic systems with other disciplines such as signal processing methods, bit-level processes, and adaptive key generation strategies[4, 5]. Chaotic systems is one of the most perfect techniques in image encryption. Chaotic maps have some important properties such as sensitive to initial conditions, high randomness and ergodicity[6]. but classical chaotic maps are not free from problems Finite precision effects and low chaotic complexity in certain parameter regions can also be inferred as limitations of classical chaotic map. In order to work around these problems, mature and hybrid chaotic strategies have been suggested to advance stochasticity and protection power. Moreover, the incorporation of chaos into bit-level operations like as bit-plane decomposition, permutation-based and diffusion functions has proven legitimate performance enhancement factor for generating more efficient encryption quality[7]. We propose a chaos based image encryption architecture for which a plaintext-dependent initialization process of the chaotic system is established by exploiting statistical characteristics of input image. Our method makes stronger dependence between plaintext and chaotic key generation process. The dependency increases the sensitivity to the key, and enhances nonlinearity of encryption system. We design the proposed scheme in a sequential manner by combining key-dependent permutation, bit-plane decomposition and XOR-based diffusion. In particular, the image is first decomposed into a number of bit-planes and then subjected to key-guided permutation algorithm. In this regard, the diffusion stage is based on a feedback XOR using a chaotic key stream issued from the Logistic map that guarantees a robust propagation of changes throughout the encrypted image. The key to the encryption process is related to the features of the plaintext so that a minor change will cause an operation on input image to generate different result in encrypted output. This enables to make more resistant for differential as well as statistical attacks. Thus, the suggested framework achieves an optimal balance between security efficiency and integrity of the structure without mixing loosely coupled chaos-based encryption systems. The remainder of this paper is organized as follows: Section 2 reviews related work, Section 3 describes the proposed method, Section 4 presents experimental results and security analysis, and Section 5 concludes the paper.

2. Related Work

Over the recent years, image encryption methods based on chaotic systems have received significant research attention. These approaches utilize the natural characteristics of chaos and its sensitivity and pseudo-random characteristic in order to improve the performance of security. However, the current approaches differ in terms of design complexity, key generation mechanisms, and resisting attacks. Hence, this makes it necessary to survey and evaluate recent works available in this area for their merits and demerits.

(J Zheng, T Lv,2022) proposed an image encryption algorithm based on cascaded chaotic map and improved Zigzag transform in this paper. The scrambled image corresponds to use improved Zigzag transform. the new Zigzag transform can fully diffuse all the pixels and increase the randomness of their cipher image. A special diffusion algorithm called wave-shaped is adopted, it has the property of selective alternative direction (alternate between row and column for diffusion). Using SHA256 algorithm and raw image as input, the cipher image with these characters has better noise immunity to select plaintext attack. It obtains three results of Entropy= 7.9971, NPCR=99.6094%, and UACI=33.4635% [8].

(Y Wan, S Wang, B Du ,2023) Based on this system, a novel image encryption algorithm is proposed by integrating hyperchaos with bit-plane decomposition techniques. In this method, two images are first decomposed into bit-planes and then scrambled into a single representation. The image is further divided into high-bit and low-bit

planes, which are stored in separate matrices to improve encryption flexibility and efficiency. An auxiliary matrix generated from a hyperchaotic sequence is then used to perform encryption operations. The algorithm applies a two-stage process consisting of scrambling–diffusion followed by modular diffusion encryption. This layered structure significantly increases the security strength of the encryption scheme. Experimental results demonstrate that the proposed method exhibits high sensitivity to initial conditions and plaintext changes such as correlation ($H=0.90824$ $V=0.94008$ $D=0.95927$) and entropy of the encrypted image is 7.9973[9].

(J Xu, et.al, 2024) proposed an encryption scheme based on a permutation–diffusion structure, in which a new one-dimensional chaotic map (1D-SAM) and plaintext-related and ciphertext feedback mechanism (PRCFM) are involved. Specifically, 1D-SAM introduces additional system randomness and dynamical complexity at multiple levels while PRCFM reinforces dependency on both plaintext and ciphertext to mitigate against chosen-plaintext attacks. Although the scheme utilizes only one round of permutation-diffusion, it is highly efficient, with an execution time of around 0.2854 s for encrypting a 512×512 image. The experimental results show that it has good security performance with NPCR=99.6051% and UACI=33.4452%[10].

(Y Niu, H Zhou,et.al,2024) The proposed scheme used an optimized four-dimensional chaotic system with evolutionary operators for the image encryption security. First, the pseudo-random sequence related to plaintext is generated, this increases sensitivity and enhances resistance against parallel-plaintext attack as well as not take advantage differential attacks. The approach combines chaos scrambling at the bit level by rearranging bits independently plus a permutation based on a selection, for pixel level. Additionally, chaotic sequence controlled crossover and mutation operators are integrated for more randomness before executing diffusion to selected pixel pairs. And lastly ciphertext feedback is being applied for further security. Experimental results show that the methods together greatly increase the robustness of image encryption against noise and cropping attacks, hence even with a very good level of security for transmitted images[11].

(X Zhang,et.al,2025) this study proposes an innovative encryption framework that synergizes a random Zigzag scrambling scheme with a roulette wheel rotation diffusion method. The system constructs a novel four-dimensional hyperchaotic model by embedding an additional state variable into a classical three-dimensional chaotic structure. The encryption approach effectively disrupts both the pixel positions and intensity values through combined Zigzag path scrambling and rotational diffusion, both of which are deeply coupled with the designed chaotic system. Notably, the chaotic system's initial parameters are computed directly from the grayscale values of the source image, ensuring that encryption is highly sensitive to both the plaintext and the key, thus strengthening security. The method offers an expansive key space on the scale of 2384×1060 , while the entropy of the encrypted image reaches 7.9993 bits per pixel, (NPCR) of 99.6048% and (UACI) of 33.4706% [12].

3. Methodology

In this section, the framework of a high-performance security approach for image encryption and decryption is described that combines bit-level image processing with chaotic systems. The proposed structure consists of a series of successive operations that work together to improve both confusion and diffusion. At first, a plaintext dependent key is generated from statistical features of input image including pixel sum, mean, variance, entropy, and maximum intensity, in addition to four external secret key. These normalized values are used to initialize multiple chaotic logistic map, and therefore ensures that the generated key stream is highly sensitive to input image. Then the pseudo-random key stream generated by iteratively executing the chaotic logistic maps are re-organized into a two dimensional matrix. This vital flow is by then utilized as the scrambling process. Next the image is decomposed into eight binary bit-planes. For every bit-plane, a basic zigzag (row-major transpose-based) is employed to transform. It produces a permutation index through sorting the chaotic key stream and utilizes this index to permute the bit-plane coefficients which adds more spatial confusion. Following performing scrambling, the bit-planes are recombined into an intermediate encrypted image. Then, applying a feedback-based XOR diffusion process where each pixel is encrypted by the composition of the chaotic key stream and previously encrypted pixels value. This can introduce significant inter-pixel dependency and improve diffusion. The color image is decomposed into three channels (R, G, B), and each channel undergoes the same encryption process independently. Finally, the encrypted channels are combined to produce the final cipher image. Finally, the inverse operations are applied in reverse order in the decryption process as they were used for encrypting them which use secret key to obtain an image as close to the original one.

3.1. Proposed image encryption scheme:

Let the original color image be denoted as: $I \in \mathbb{R}^{(M \times N \times 3)}$ Where $M \times N$ is the image size. The overall encryption process includes five main stages: chaotic key generation, bit-plane decomposition, permutation, image reconstruction, and diffusion.

3.1.1. Plaintext-Dependent Chaotic Key Generation:

Initially, initial conditions for the chaotic system are generated as a function of the statistical properties of the input image. Then, multiple features are extracted from the plaintext image, including the pixel sum (S) in equation (1), mean (μ) in equation (2), variance (σ^2) in equation (3)[13], entropy (H) in equation (4)[14], and maximum intensity (I) in equation (5)[15].

$$(1) S = \sum_{x=1}^M \sum_{y=1}^N I(x, y)$$

$$\mu = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N I(x, y) \quad (2)$$

$$\sigma^2 = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N (I(x, y) - \mu)^2 \quad (3)$$

$$H = - \sum_{i=0}^{L-1} p(i) \log_2(p(i)) \quad (4)$$

$$I_{\max} = \max(I(x, y)) \quad (5)$$

These features are combined with four external secret keys to obtain the initial values of the Logistic chaotic map as shown in proposed formulation (6,7,8,9,10).

$$x_0 = \text{mod} \left(\frac{S}{256} + \sin(\pi K_1), 1 \right) \quad (6)$$

$$y_0 = \text{mod} \left(\frac{\mu}{256} + \cos(\pi K_2), 1 \right) \quad (7)$$

$$z_0 = \text{mod} \left(\frac{\sigma^2}{256} + K_3^2, 1 \right) \quad (8)$$

$$w_0 = \text{mod} \left(\frac{H}{256} + \sqrt{|K_4|}, 1 \right) \quad (9)$$

$$u_0 = \text{mod} \left(\frac{I_{\max}}{256} + K_1 K_2, 1 \right) \quad (10)$$

The control parameters of the chaotic maps are defined as:

$$r_1 = 3.99 + 0.001 \sin(K_1) \quad (11)$$

$$r_2 = 3.98 + 0.001 \cos(K_2) \quad (12)$$

$$r_3 = 3.97 + 0.001 \sin(K_3 K_4) \quad (13)$$

Three logistic maps[16] are then iterated according to :

$$x_{i+1} = r_1 x_i (1 - x_i) \quad (14)$$

$$y_{i+1} = r_2 y_i (1 - y_i) \quad (15)$$

$$z_{i+1} = r_3 z_i (1 - z_i) \quad (16)$$

The generated states are combined with nonlinear terms to produce the chaotic sequence as shown in formulation (17):

$$\text{seq}(i) = \text{mod}(x_i + y_i + z_i + w_0 + u_0 + \sin(k_1 i) + \cos(k_2 i) + k_3 k_4) \quad (17)$$

Based on the initialized conditions, a pseudo-random key stream is produced by running $M \times N$ times of iteration of Logistic map (M and N are dimensions in the image). The output sequence is normalized and is converted to a 8-bit integer matrix that are used in the permutation and diffusion stages later. A pseudo-random sequence is generated $X = \{x_1, x_2, \dots, x_{MN}\}$. The key stream is obtained in equation (18) And reshaped into: $K \in Z_{256}^{M \times N}$

$$K(i) = \text{mod}(\lfloor x_i \cdot 10^6 \rfloor, 256) \quad (18) [6]$$

3.1.2. Bit-Plane Decomposition

In the process of bit extraction, each color channel is decomposed into eight binary bit-planes. The decomposition enhances the flexibility of the encryption procedure and allows pixel-level manipulations at various significance levels.

3.1.3. Bit-Pane Permutation (Confusion Stage)

For each color channel, a permutation index is generated using the corresponding chaotic key stream as shown in equation (19):

$$\pi = \text{argsort}(K + \text{mod}(k_2 \times 10^5, 256)) \quad (19) [17]$$

Where π is permutation order which comes from sorting a chaotic key stream K , which is generated using multiple secret parameters derived from plaintext statistical features with four external secret keys. After that Zigzag scanning is used to reshape each bit-plane into a one-dimensional vector as defined in equation(20)

$$V_k = \text{Zigzag}(b_k) \quad (20) [18]$$

then generates the final sequence which is further permuted using sorted chaotic key stream indices as described by equation (21)

$$P_k = V_k(\pi) \quad (21)$$

Such an operation eliminates spatial correlation between neighboring pixels and injects severe confusion into the structure of the image. The bit-planes are rearranged and reconstructed back to matrix form after permutation as shown in equation (22).

$$\hat{B}_k = \text{Zigzag}^{-1}(P_k) \quad (22) [18]$$

3.1.4. Scrambled Image Construction

After processing all bit-planes independently, they are recombined to construct the scrambled image. completing the confusion phase of encryption. A usual grey scale image consists of 8 bit planes, where lower planes correspond to least significant bits and upper ones represent more significant ones. Then the code applies a Zigzag followed by a

permutation using chaotic keys in each bit-plane, reducing spatial correlation between adjacent pixels. The image S , which has been scrambled, is obtained by recombination of the processed bit-planes following their weighting according to the following equation:

$$S(x, y) = \sum_{k=0}^7 \hat{B}_k(x, y) \cdot 2^k \quad (23) [19]$$

where $B_k(i, j)$ is the value of k -th bit-plane scrambles at. This recombination step integrates all modifications introduced during the permutation stage into a single image. This leads to enormous shifts in the pixel positions, and significant distortion of the visual structure. The scrambled image produced with use its input to diffusion stage, which is the second layer of then scheme.

3.1.5. Diffusion Process (Encryption)

In addition, to achieve a secure diffusion mechanism based on cumulative XOR. Every pixel in scrambled image is encrypted with chaotic key stream and also previously encrypted pixels. The initial diffusion state is defined as:

$$C_{prev} = \text{mod}(k_3 \times 10^6, 256) \quad (24)$$

For each pixel, the cipher value is computed as:

$$C(i, j) = S(i, j) \oplus K(i, j) \oplus C_{prev} \quad (25)$$

Where $S(i, j)$ is the scrambled pixel, $K(i, j)$ denotes the chaotic key stream generated from plaintext-dependent features along with four external secret keys, and $C(i, j)$ is the cipher pixel. The feedback state is updated after encrypting each pixel:

$$C_{prev} = C(i, j) \oplus \text{mod}(k_4 \times 10^6, 256) \quad (26)$$

we can ensure that small change in the plaintext propagate to the most of ciphertext.

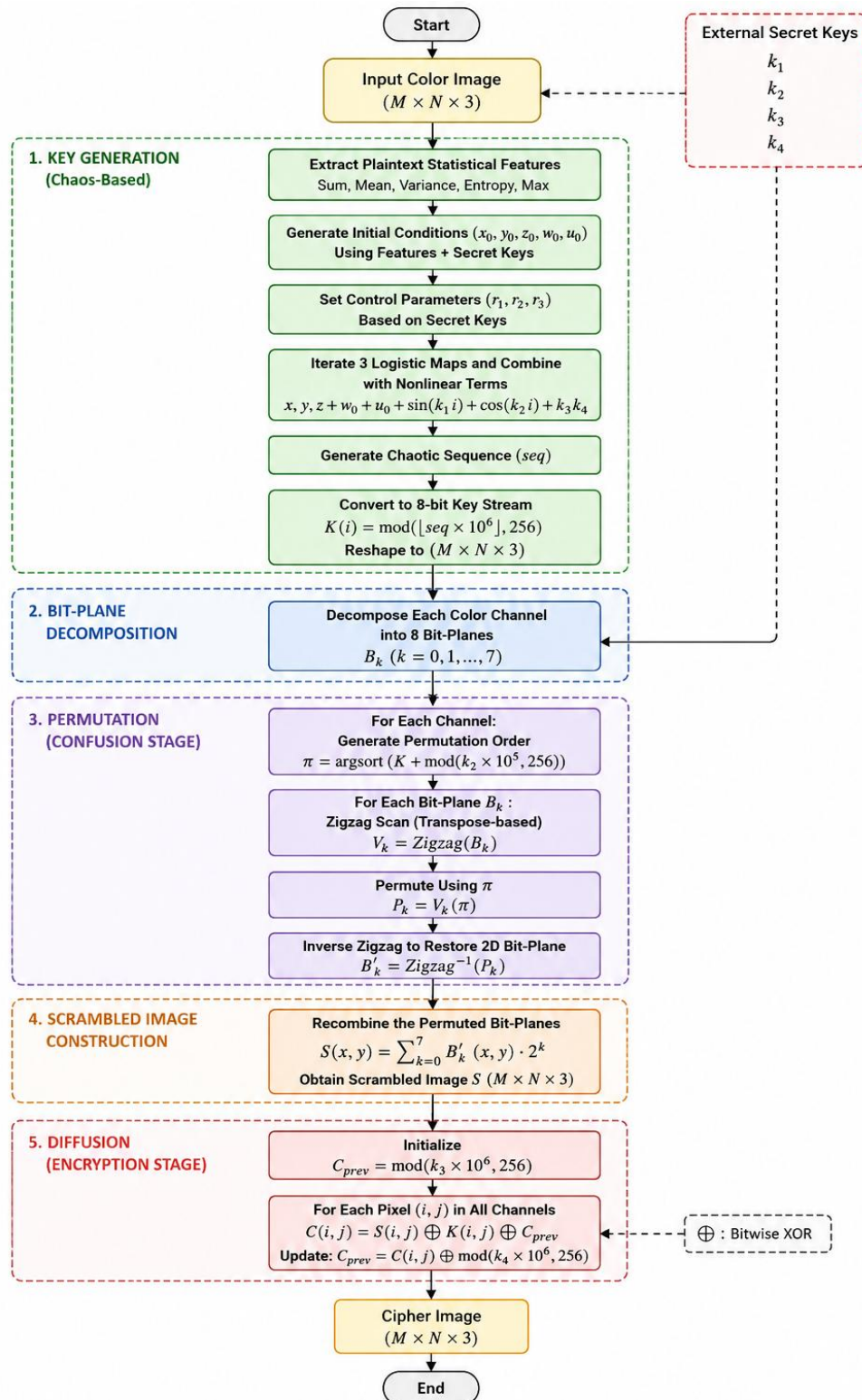


Fig. 1 – Flowchart of Proposed Image Encryption method.

3.2. Proposed Image Decryption Scheme:

The decryption process performs the inverse operations in reverse order of the encryption stages. First, inverse diffusion is performed using the same secret keys and chaotic key stream. The original scrambled image is then recovered. Subsequently, inverse permutation is applied to each bit-plane using the stored permutation indices. Finally, all recovered bit-planes are recombined to reconstruct the original image without loss of information

3.2.1. Reverse Diffusion

This stage is reversed by applying XOR operation with the same key stream and the previous feedback value as shown in equation(27)

$$S(i, j) = C(i, j) \oplus K(i, j) \oplus C_{\text{prev}} \quad (27)$$

where C_{prev} represents the previously processed cipher pixel

3.2.2. Bit-Plane Decomposition:

The recovered intermediate image S is decomposed into bit-planes

$$S \rightarrow \{\hat{B}_k\} \quad (28)$$

3.2.3. Inverse Permutation:

Each bit plane transformed to one dimensional vector using same zigzag scanning method:

$$P_k = \text{Zigzag}(\hat{B}_k) \quad (29)$$

The original permutation order generated during encryption is then inverted using π . Original vector is reconstructed as:

$$V_k = P_k(\pi^{-1}) \quad (30)$$

At last, the inverse Zigzag operation converts the recovered vector back into its two-dimensional bit-plane:

$$B_k = \text{Zigzag}^{-1}(V_k) \quad (31)$$

3.2.4. Image Reconstruction

After recovering all eight bit-planes, they are recombined to reconstruct each color channel according to:

$$I(x, y) = \sum_{k=0}^7 B_k(x, y) \cdot 2^k \quad (32)$$

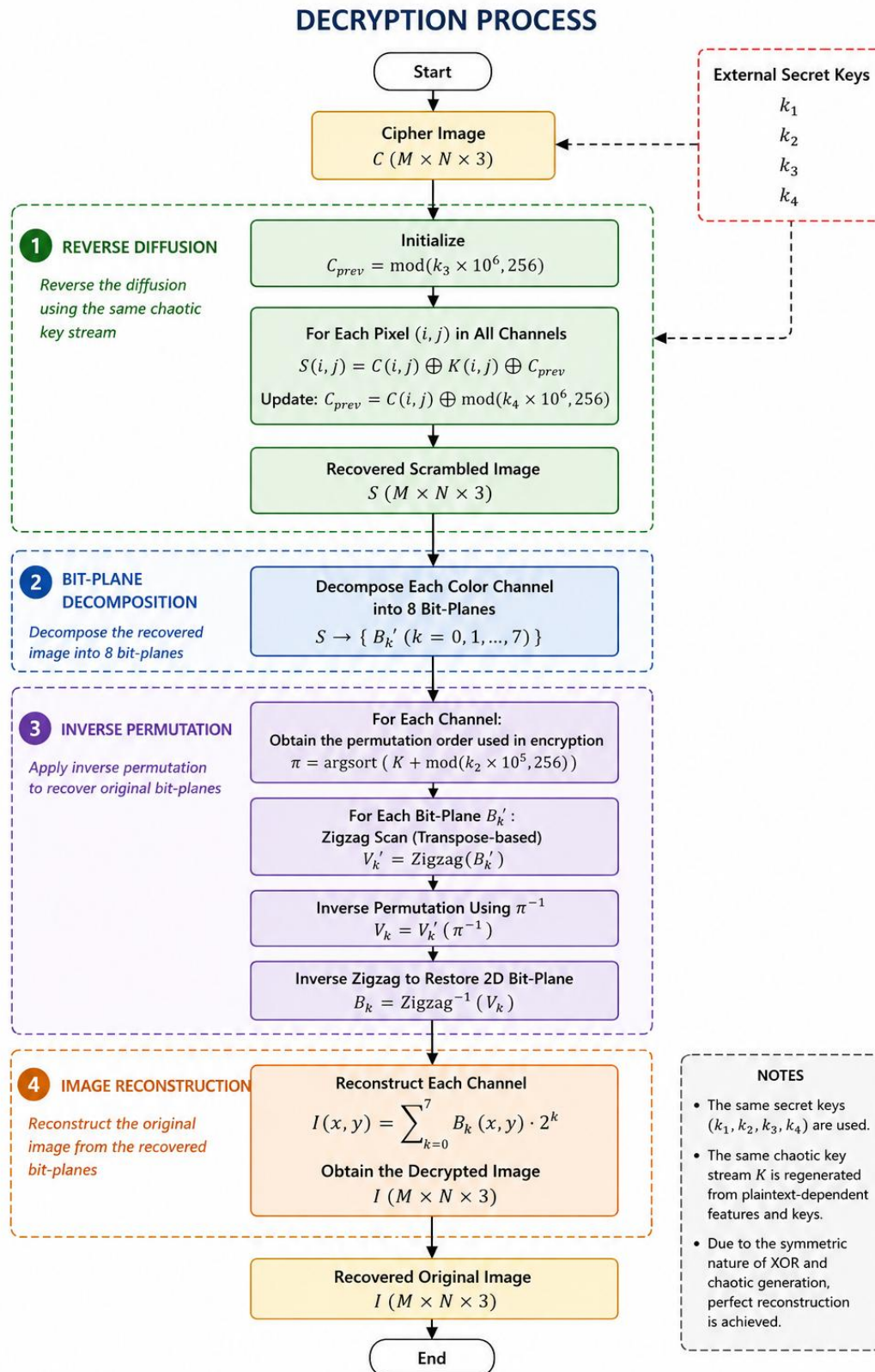


Fig. 2 – Flowchart of Proposed Image Decryption method.

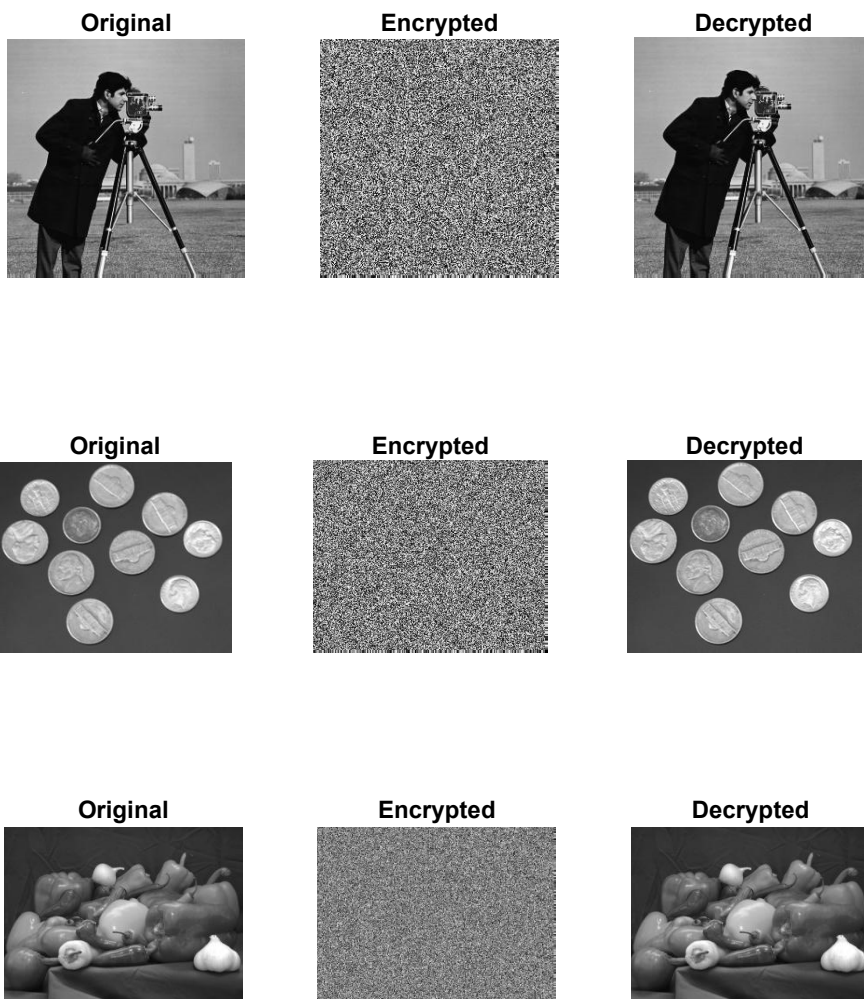
4. Result and Discussion

4.1. Experimental Setup

The Proposed image encryption algorithm was developed using MATLAB R2023a. We evaluated the method with grayscale and color images. Several evaluation metrics like histogram analysis, correlation coefficient, entropy NPCR and UACI were used to assess the performance of the system.

4.2. Visual result

The effectiveness of the proposed encryption algorithm are first evaluated by visually inspecting original, encrypted and decrypted images. The original image contains structural and spatial information whereas the encrypted image appears noise-like with no discernible patterns or visual information this indicates that the proposed method effectively conceals the visual content of the original image. The decrypted image is the same as the original image which validates that proposed method works with lossless and perfect reconstruction.



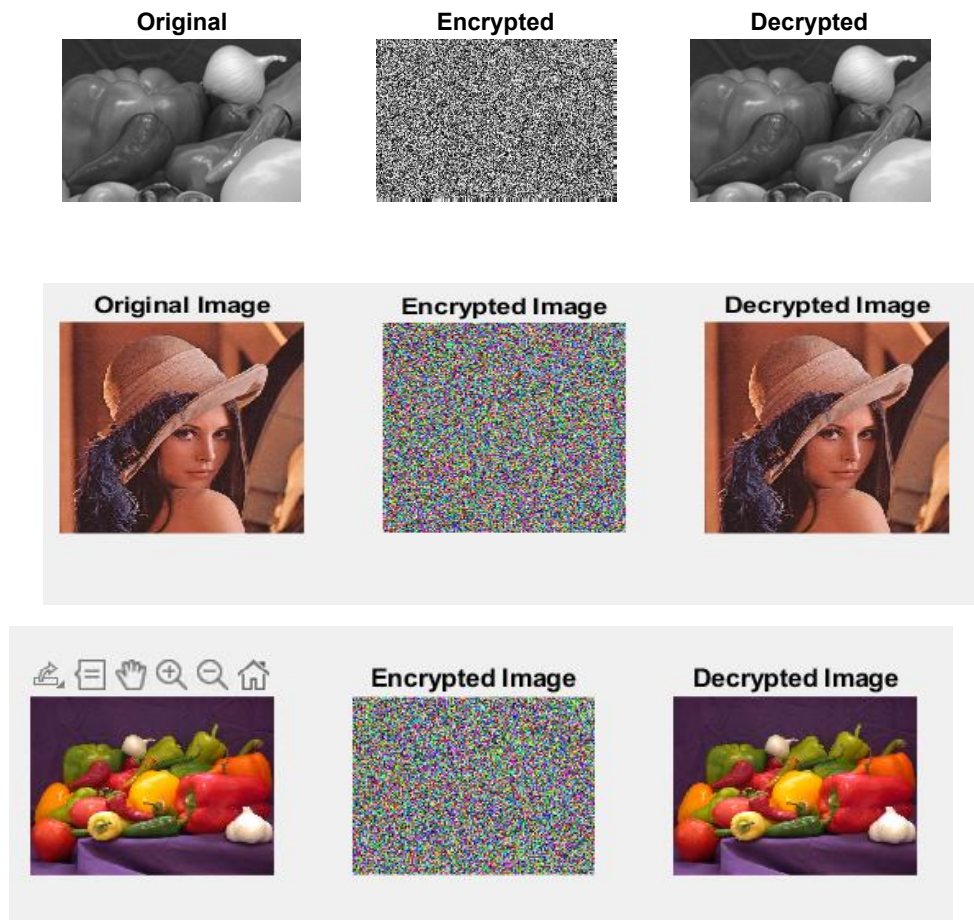


Fig. 3 – Original, Encrypted and decrypted images.

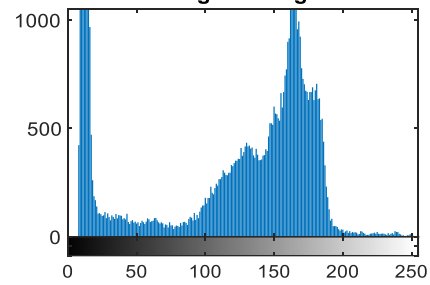
4.3. Histogram Analysis

Histogram analysis is done to analyze the pixel intensities before and after encryption. The histogram of the original image is typically non-uniform, reflecting the inherent structural and statistical properties of natural images. Conversely, the histogram of the ciphered image appears nearly uniform, indicating that the pixel values are evenly distributed across the intensity range. This uniformity minimizes the risk of statistical attacks and improves the robustness for this type of encryption design. Therefore, the proposed encryption scheme demonstrates strong resistance against histogram-based attacks and enhances overall security.

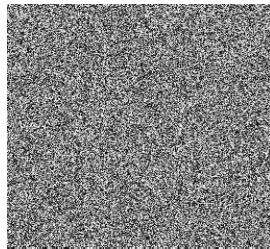
Original



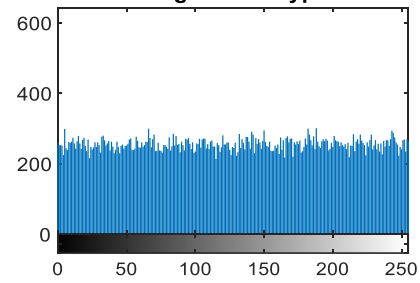
Histogram Original



Encrypted



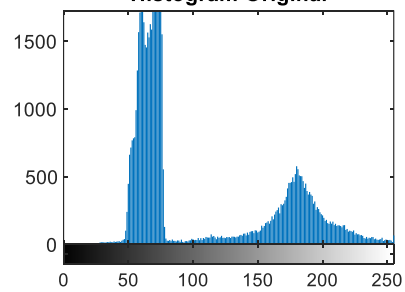
Histogram Encrypted



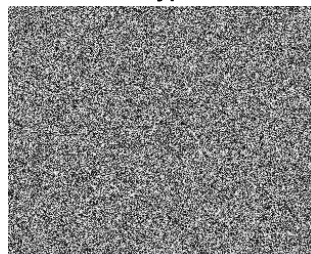
Original



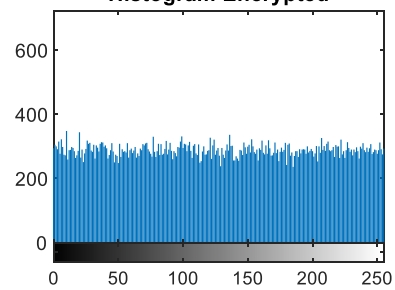
Histogram Original



Encrypted



Histogram Encrypted



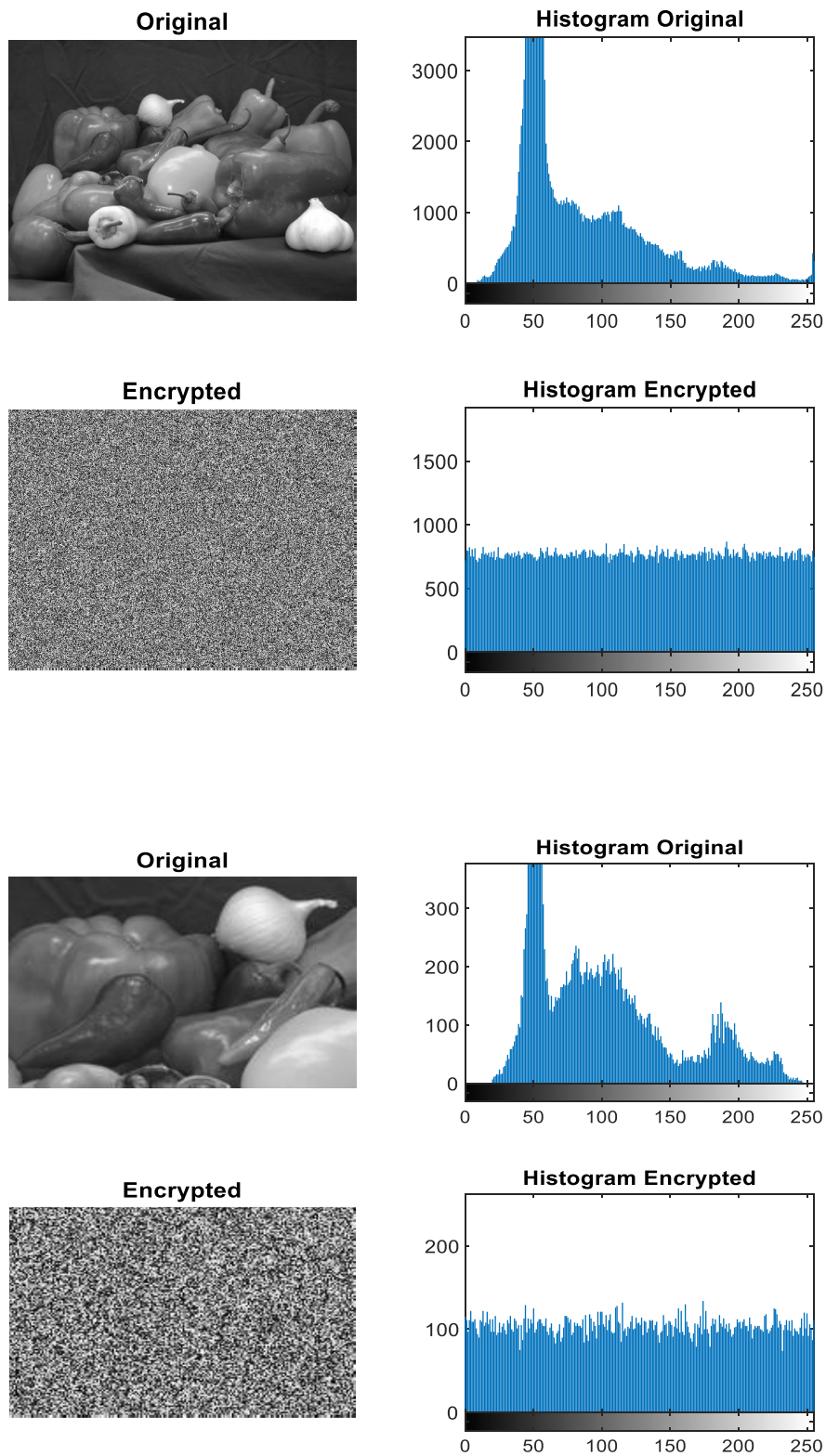


Fig. 4 – Histogram of original Gray scale and Encrypted Image.

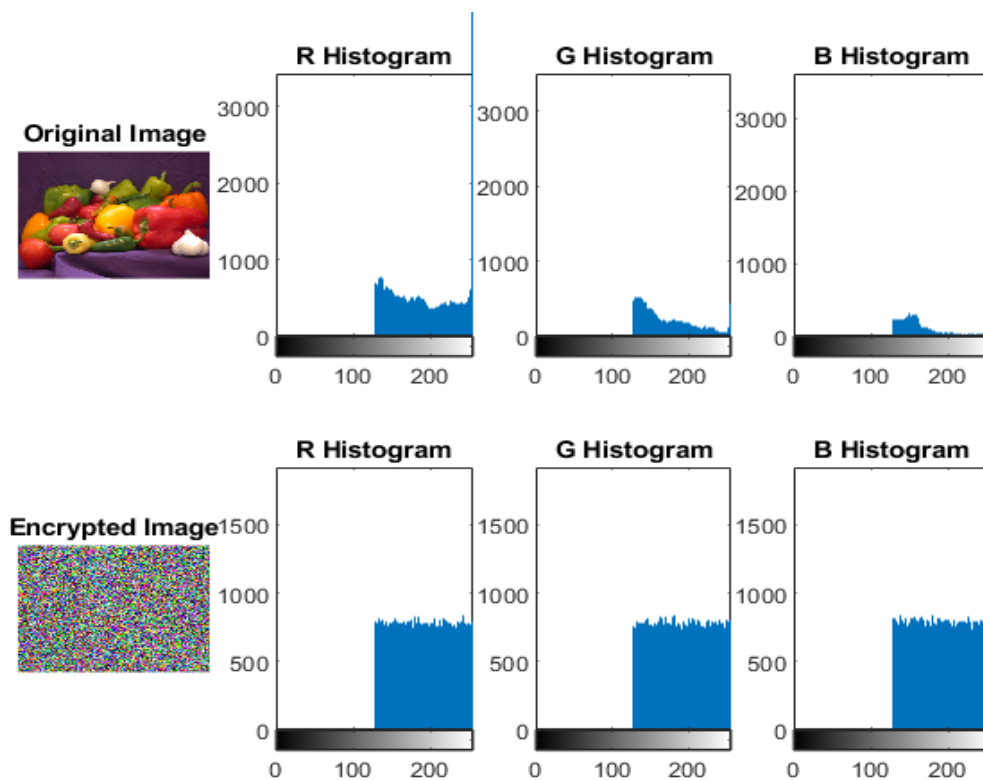


Fig. 5 – Histogram of Original Color and Encrypted Image .

4.4. Statistical Analysis

This section discusses the evaluation of the randomness and strength of security level for encrypted image by statistical analysis.

4.4.1. Entropy Analysis

We get the entropy value of encrypted image 7.9970 This value is close to the ideal 8 in case of an 8-bits grayscale image, meaning that the image random enough and it is not vulnerable for statistic attacks.

4.4.2. correlation

The neighboring pixel correlation coefficients were computed in the horizontal, vertical and diagonal directions. The original image has a high correlation values ($H = 0.9335$, $V = 0.9592$, $D = 0.9087$), which illustrate that neighboring pixels are highly similar to one another. As shown in Table 1, the correlation values start to approach zero after encryption ($H = 0.0004$, $V = 0.0023$, $D = 0.0044$). It indicates that the proposed method eliminates correlation between image adjacent pixels, which leads to a more secure encrypted image.

4.4.3. Key Space Analysis

In the proposed scheme, the secret keys are derived from plaintext-dependent features, including pixel sum, mean, variance, entropy, and maximum intensity in addition to an four external secret parameter (k_1, k_2, k_3, k_4). Which are used to generate the initial conditions of the chaotic system. Assuming a computational precision of (10^{-14}) , each external key parameter can take approximately (10^{14}) possible values. Therefore, the total key space is $(10^{14})^4 = 10^{56}$ which is approximately equivalent to 2^{186} , which is significantly larger than (2^{100}) . This large key space indicates that the proposed encryption scheme is secure against brute-force attacks.

4.4.4. Key Sensitivity Analysis

One of the major requisites for any secured encryption system is key sensitivity which means even a change at one bit number should result in different cipher image. In this paper, strong sensitivity is evaluated by changing the secret key (one parameter with a change of 10^{-14}) slightly and then obtaining encrypted images. Based on it, Key Sensitivity Ratio (KSR) is used to measure the difference between two cipher images. The calculated value indicates that the Key Sensitivity Ratio = 0.9963, which is close to the ideal value of 1. It indicates that over 99.6% of the pixels in encrypted images change with only a small modification in key A high sensitivity indicates that the proposed encryption scheme is extremely reactive to changes in key. The first one is that key generation depends on the plaintext and also the permutation and diffusion processes are tightly coupled; this leads to such behaviors. This means that if the key is altered even slightly, it will cascade all the way through the encryption process to create a cipher image that looks completely different. So, the given method has very good resistance to brute-force and differential attacks which try to exploit similarity of keys. The visual results in Fig.6 clearly demonstrate that a slight modification in the secret key leads to a completely different cipher image, which is further confirmed by the high Key Sensitivity Ratio of 0.9963.

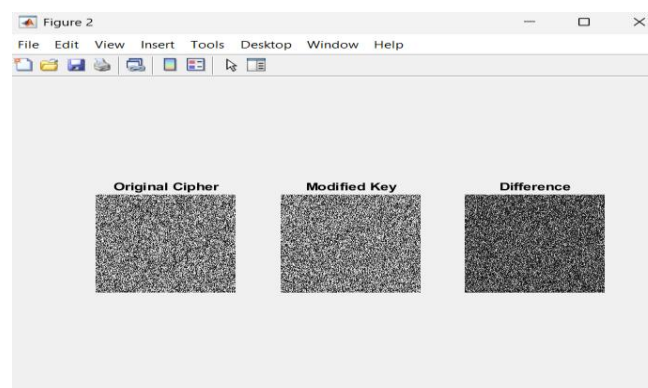


Fig. 6 – demonstrate that a slight modification in the secret key leads to a completely different cipher image.

4.4.5. Computational Complexity and Runtime Analysis

The evaluate complexity of the proposed encryption regards particularly to operations made on every pixel of the input images. As the algorithm does bit-plane decomposition, Zigzag permutation and chaotic sequence generation followed by pixel-wise XOR-diffusion, hence the overall computational complexity may be given as $O(N \times M)$, where N and M define the input image dimensions. MATLAB built-in timing functions were used to measure the time taken by the encryption/decryption algorithm. The encryption time is approximately 0.1967 seconds, while the decryption time is 0.0452 seconds. The total elapsed time is approximately 0.1934 seconds on a gray image of the size 256×256 . These data indicate that the proposed algorithm is computationally efficient. The linear computational complexity guarantees scalability with larger images. Furthermore, the scheme maintains an acceptable trade-off between security and computational cost, which is ideal for real-time applications of image encryption.

4.4.6. Comparison with AES

To verify the computational performance of the suggested encryption scheme, a comparison with the Advanced Encryption Standard (AES) was performed. The experimental results show that AES has faster execution, with encryption and decryption times of 0.0136 seconds and 0.0107 seconds, respectively. On the contrary, it only takes 0.1967 second during encryption and 0.0452 second in decryption for our method. This explains the difference in execution time which is expected since AES is a mature encryption standard with lots of optimizations on general-purpose data security. But the proposed scheme is a plaintext-dependent key-generation and chaotic operator, which leads to additional computational complexities. Although the proposed method has a marginally increased execution time, its improved security features make it highly efficient in terms of image encryption. More precisely, the chaotic maps and bit-plane level processing enhance the robustness of response to small changes in the input image while also increasing resistance against statistical and differential attacks. Therefore, while AES demonstrates superior speed, the proposed scheme achieves a better balance between security and performance for image-specific encryption applications.

4.5. Differential Attack Analysis

To evaluate the robustness of the proposed encryption scheme against differential attacks, the NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) metrics were computed. Based on the test result, we get NPCR 99.6323% and UACI 33.3974%. A high value of NPCR shows that the change in the original image refers to a great change in the encrypted image, and UACI is closely related to its theoretical best value of 33%, confirming strong diffusion capability.

Table 1 - Comparison of the proposed scheme with recent image encryption methods

Reference	Entropy	NPCR (%)	UACI (%)	Correlation			Key Space	KSR
				H	V	D		
Proposed Method	7.9970	99.6323	33.3974	0.00078	0.0013	0.0012	2^{199}	0.9963
Ref [8]	7.9971	99.6094	33.4635	0.0029	0.0085	0.0064	2^{186}	-
Ref [9]	7.9973	-	-	0.90824	0.94008	0.95927	-	-
Ref [10]	-	99.6051	33.4452	-	-	-	-	-
Ref [11]	7.9974	99.6735	33.2765	0.0018	0.0020	0.0001	2^{199}	-
Ref [12]	7.9993	99.6048	33.4706	0.0009	0.0023	0.0018	2^{384}	-

5. Conclusion

A hybrid chaotic system based image encryption scheme using the bit-plane decomposition is proposed in this paper along with a Zigzag permutation-based framework and a cumulative XOR-based diffusion mechanism. The new method based on the plaintext to generate key according to statistical characteristics of original image, it improves sensitive key and has better resistant to brute-force attack as well as known-plain text attack. The stronger pseudo-random behaviors and higher sensitivity to initial conditions come from the application of enhanced Logistic chaotic map, and also the decomposition of bit-planes and ordinary Zigzag transformation perform very well in terms of increasing confusion by destroying spatial correlations between pixels. In addition, the cumulative XOR-based diffusion stage guarantees that minor variations in plaintext result in big differences in ciphertext, reaching an avalanche effect. Experiments Results indicate that the proposed method is effective. The entropy of encrypted images, 7.9970, is close to the theoretic maximum of 8 bits for an 8-bit image which indicates high degrees of randomness. Furthermore, the correlation coefficients are pushed near 0 in all directions, indicating that statistical dependencies have been eliminated. The differential attacks resistance for the scheme is also good, NPCR = 99.63% and UACI = 33.39%, which approaches optimal values in literature. In summary, the suggested encryption algorithm balances security strength with computational performance well. It has excellent statistical properties, high sensitivity to plaintext changes and good resistance against common cryptanalytic attacks making it suitable for encryption of images in secure transmission as well as storage applications.

References

- [1] S. Rohith, K. H. Bhat, and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register," in *2014 International conference on advances in electronics computers and communications*, 2014, pp. 1-6: IEEE.
- [2] A. Dinu and M. J. M. Frunzete, "Image encryption using chaotic maps: development, application, and analysis," vol. 13, no. 16, p. 2588, 2025.
- [3] S. Wang, Q. Peng, B. J. O. Du, and L. Technology, "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," vol. 148, p. 107753, 2022.
- [4] H. Wen, Y. J. J. o. K. S. U.-C. Lin, and I. Sciences, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," vol. 35, no. 7, p. 101612, 2023.
- [5] Z. Zhang, J. Tang, F. Zhang, H. Ni, J. Chen, and Z. J. I. A. Huang, "Color image encryption using 2D sine-cosine coupling map," vol. 10, pp. 67669-67685, 2022.
- [6] B. Zhang and L. J. M. Liu, "Chaos-based image encryption: Review, application, and challenges," vol. 11, no. 11, p. 2585, 2023.
- [7] S. Jadoon, L. Pan, S. Huda, K. H. J. M. T. Khan, and Applications, "A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms," vol. 85, no. 3, p. 210, 2026.

-
- [8] J. Zheng and T. J. I. I. P. Lv, "Image encryption algorithm based on cascaded chaotic map and improved Zigzag transform," vol. 16, no. 14, pp. 3863-3875, 2022.
 - [9] Y. Wan, S. Wang, B. J. M. T. Du, and Applications, "A bit plane image encryption algorithm based on compound chaos," vol. 82, no. 14, pp. 22103-22121, 2023.
 - [10] J. Xu, K. Liu, Q. Huang, Q. Li, and L. J. P. S. Huang, "A plaintext-related and ciphertext feedback mechanism for medical image encryption based on a new one-dimensional chaotic system," vol. 99, no. 12, p. 125220, 2024.
 - [11] Y. Niu, H. Zhou, and X. J. S. R. Zhang, "Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators," vol. 14, no. 1, p. 7033, 2024.
 - [12] X. Zhang, Y. Liu, M. Liu, Y. J. J. o. K. S. U. C. Niu, and I. Sciences, "Image encryption algorithm based on Zigzag transformation and roulette wheel rotation mechanism," vol. 37, no. 8, p. 239, 2025.
 - [13] L. Kurz and M. Hafed Benteftifa, *Analysis of variance in statistical image processing*. 1997.
 - [14] A. J. M. S. i. C. S. Lesne, "Shannon entropy: a rigorous notion at the crossroads between probability, information theory, dynamical systems and statistical physics," vol. 24, no. 3, p. e240311, 2014.
 - [15] C. Y. Wong *et al.*, "Image contrast enhancement using histogram equalization with maximum intensity coverage," vol. 63, no. 16, pp. 1618-1629, 2016.
 - [16] M. Ausloos, *The logistic map and the route to chaos: From the beginnings to modern applications*. Springer Science & Business Media, 2006.
 - [17] C. Fu, B.-b. Lin, Y.-s. Miao, X. Liu, and J.-j. J. O. c. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," vol. 284, no. 23, pp. 5415-5423, 2011.
 - [18] R. Candra, S. Madenda, S. A. Sudiro, M. J. J. o. T. Subali, Electronic, and C. Engineering, "The implementation of an efficient zigzag scan," vol. 9, no. 2, pp. 95-98, 2017.
 - [19] X. Wang and H.-l. J. N. D. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," vol. 83, no. 1, pp. 333-346, 2016.