Fast and Secure Image Encryption Using Josephus Ring Permutation and Logistic Map Diffusion

Zahra RafieianBahabadi[1], **Ali Nodehi**[*2], **Rasul Enayatifar**[3]

Abstract– In response to the growing need for secure and efficient transmission of sensitive visual data, this paper presents a novel hybrid image encryption scheme that combines a Josephus Ring-based permutation mechanism with a logistic map-based diffusion process. The proposed method aims to achieve a balance between high security and computational efficiency, making it suitable for real-time applications such as IoT devices and mobile platforms. The algorithm operates in two main phases: permutation and diffusion, preceded by a robust key generation process that converts a user-defined key into a chaotic initial condition for the logistic map. In the first phase, pixel positions are scrambled using a Josephus Ring traversal. This mathematical structure provides deterministic yet unpredictable permutation by treating image pixels as nodes in a circular elimination sequence. The Josephus Ring ensures efficient O(n) scrambling while effectively disrupting spatial correlations and preserving low computational overhead. In the second phase, a chaotic logistic map is employed for diffusion. Starting from an initial condition derived from the secret key, the map generates a pseudo-random keystream that is XORed with the permuted pixel values. To enhance the avalanche effect, each cipher pixel is also XORed with the previous encrypted pixel, creating a chaining mechanism that propagates changes throughout the image. The security and performance of the proposed scheme are rigorously evaluated using standard test images such as Lena, Baboon, and Peppers at multiple resolutions. Experimental results demonstrate near-ideal Shannon entropy values (approximately 7.997), indicating high randomness in the encrypted output. Pixel correlation coefficients in horizontal, vertical, and diagonal directions are reduced to near-zero levels (below 0.02), confirming effective decorrelation. The algorithm also exhibits strong key sensitivity, with a single-bit change in the key producing over 99% difference in the cipher image. Differential attack resilience is validated through NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) metrics, which approach theoretical optimums of 0.996 and 0.333, respectively. Comparative analysis with recent state-of-the-art encryption methods shows that the proposed hybrid approach outperforms existing techniques in terms of both security and execution time. For instance, it achieves lower correlation coefficients and higher NPCR/UACI values while maintaining faster encryption speeds (e.g., 694 ms for a 512×512 image). The combination of the lightweight Josephus permutation and chaotic logistic diffusion provides a secure, fast, and practical encryption solution. In conclusion, this scheme offers a robust framework for secure image transmission, particularly in resource-constrained environments, and holds potential for extension to color images, video encryption, and hardware implementations in future work.

Keywords::Image encryption, Josephus Ring, logistic map chaotic function

1. Introduction

The exponential growth of online services, social networks, and digital communication systems has led to an unprecedented increase in data exchange over the Internet. This rise has amplified security risks, especially for multimedia files like images and videos, which often contain sensitive information. Modern smart phones, for example, not only generate vast amounts of digital images but also enable instant online sharing, underscoring the urgent need for secure transmission mechanisms [1]. Compared to other data types, images are particularly susceptible to breaches and exploitation due to their frequent use and rich informational content. As a result, designing effective and efficient encryption techniques for images has emerged as a crucial research priority [2]. Current approaches to image encryption primarily fall into

[1] Department of Computer Engineering, Go.C., Islamic Azad University, Gorgan, Iran.

2* **Corresponding Author :** Department of Computer Engineering, Go.C., Islamic Azad University, Gorgan, Iran.. Email: ali.nodehi@iau.ac.ir

3Department of Computer Engineering, Fi.C., Islamic Azad University, Firoozkooh, Iran.

Received: 2025.04.12; Accepted: 2025.07.16

three categories: chaos-based methods [3-5], transform based technique[6-8], techniques leveraging machine learning [9-11], and encryption schemes utilizing DNA sequences[12, 13].

Chaos-based encryption techniques leverage the principles of confusion (obscuring pixel relationships) and diffusion (dissipating statistical patterns) through two interdependent stages: permutation and diffusion [3, 14]. Chaotic maps—favored for their sensitivity to initial conditions (butterfly effect) and pseudo-randomness—first permute pixel positions to disrupt spatial correlations while preserving gray-level statistics. Subsequently, in the diffusion stage, the same or another chaotic map alters pixel values via operations like XOR or modular arithmetic, ensuring the encrypted image exhibits uniform gray-level distribution and resistance to statistical attacks [15]. This combined approach, where permutation scrambles structure and diffusion randomizes content, achieves robust security with computational efficiency.

The Josephus ring (or Josephus permutation) is a mathematical problem inspired by a counting-out game, where participants arranged in a circle are eliminated sequentially under fixed rules until one remains [16]. This structured yet nonlinear selection mechanism makes it highly adaptable for image encryption, particularly in guiding pixel selection for permutation (position shuffling) or diffusion (value alteration) [17]. By treating pixels as nodes in a circular traversal, the Josephus ring introduces pseudo-randomness—critical for security—while maintaining deterministic reproducibility for decryption. Its algorithmic efficiency and inherent unpredictability allow seamless integration into cryptographic frameworks without compromising computational speed.

The growing vulnerability of digital images demands efficient encryption solutions for real-time applications. We address this by proposing a lightweight hybrid scheme combining Josephus Ring permutation with Logistic Map diffusion. The Josephus Ring enables O(n) pixel scrambling through circular traversal, while the Logistic Map provides chaotic pixel alteration via XOR operations. This two-stage approach achieves: (1) robust security through dual confusion-diffusion, (2) low computational complexity using simple mathematical structures, and (3) resistance to statistical attacks via chaotic unpredictability. By balancing speed (fast permutation) and security (nonlinear diffusion), our method outperforms existing approaches while remaining suitable for resource-constrained IoT and mobile platforms.

The structure of this paper is organized to systematically present our research: Section 2 introduces fundamental concepts, detailing both the Josephus Ring mechanism and logistic chaotic mapping principles. Section 3 describes the operational framework of our proposed encryption algorithm. In Section 4, we evaluate and discuss the experimental outcomes obtained through our method. Finally, Section 5 concludes the paper by summarizing key findings and contributions.

2. Preliminaries

In this section, we explain the initial concepts of the Josephus Ringand the logistic chaotic function.

2.1 Josephus ring

The Josephus problem, commonly referred to as the Josephus permutation or Josephus Ring, represents a classic theoretical framework in discrete mathematics and algorithmic design. This problem models a circular elimination process where N participants are arranged in a closed loop, each assigned a unique positional index. The elimination protocol follows a deterministic pattern: beginning at a designated starting point, the system iterates through the circle in uniform increments (typically clockwise), removing every K-th participant until only a single survivor remains[16].

Mathematically, this process can be represented as a recursive sequence where the survival position $J(N,K)$ satisfies the recurrence relation:

$J(1,K) = 0$ (base case)

$J(N,K) = (J(N-1,K) + K) \, mod \, N$ (recursive step)

The computational significance of this problem extends beyond its historical origins, demonstrating valuable properties for modern applications:

- **Predictable randomness**: While the elimination sequence appears stochastic, it follows exact deterministic rules
- **Positional sensitivity**: Minor changes to initial parameters (N or K) yield dramatically different outcomes
- **Circular dependency**: The closed-loop structure ensures complete traversal without boundary conditions

In computational contexts, the Josephus Ring exhibits $O(N)$ time complexity when solved iteratively, or $O(K \, log \, N)$ for optimized mathematical solutions. These characteristics make it particularly suitable for cryptographic applications where controlled pseudorandomness and position shuffling are required, such as in our proposed image permutation phase where pixel positions undergo systematic yet unpredictable rearrangement.

2.2 Logistic chaotic function

Chaotic systems exhibit extreme sensitivity to initial conditions, a characteristic often referred to as the "butterfly effect" in dynamical systems theory. This property ensures that even infinitesimal variations in starting parameters result in exponentially divergent trajectories over time. Such sensitivity makes chaotic signals particularly valuable for cryptographic applications, where minimal key alterations should produce completely different cipher outputs.

Among various chaotic systems, the logistic map stands out for its computational simplicity and rich dynamical behavior. Defined by the recursive relation:

$$X_{n+1} = R\,X_n(1 - X_n) \qquad (1)$$

where: $X_n \in (0,1)$ represents the system state at iteration n, $R \in [0,4]$ is the control parameter, The system exhibits chaotic behavior when R ≈ 3.5699 to 4.

Fig. 1 demonstrates this chaotic evolution, plotting 500 iterations of Equation (1) with $R = 3.999$ (fully chaotic regime) and initial condition $X_n = 0.33$. Key observations include:

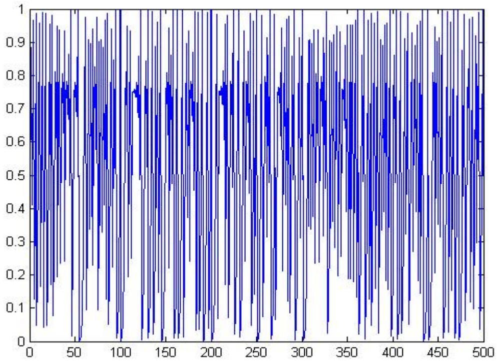


Fig. 1. Logistic map function for R=3.999 and X0=0.33

3. Proposed Method

The proposed method is implemented in three phases: key generation, permutation, and diffusion.

Phase 1: Key generation

To generate secret key following steps have been carried out consequently.

*Step 1:*Convert Characters to ASCII Bytes

Treat each character as a byte (UTF-8):

$$B = \{b_1, b_2, b_3, \dots, b_{16}\} \quad ,b_i \in [0.255]$$

Step 2: Combine Bytes into a 128-bit Integer

Concatenate bytes into a large integer K:

$$K = \sum_{i=1}^{16} b_i \,.\, 256^{i-1}$$

Step 3: Hash K for Uniformity

Apply SHA-256 to$K$ (as hex string) and take the first 8 bytes:

$$H = SHA256(K)_{bytes\,(1-8)}$$

Step 4: Map to $x_0 \in (0,1)$

Convert hashed bytes to x_0

$$x_0 = \left(\sum_{i=1}^{8} H_i\,.256^{i-1}\right) / \,2^{64}$$

Step 5: Validate x_0 (Avoid Fixed Points)

Ensure $x_0 \notin \{0,0.25,0.5,0.75,1\}$,(logistic map unstable/singular points).

If invalid, perturb x_0 slightly:

$$x_0 \leftarrow (x_0 + 1)\ mod\ 1$$

Phase 2: Proposed LFSR-Based Permutation Method

A. LFSR Initialization:

- Initialize an n-bit LFSR with a secret key as the seed.
- Use a primitive polynomial (e.g., $x^8 + x^4 + x^2 + 1$ for 8-bit LFSR) to ensure maximal cycle length.

B. Pixel Selection via LFSR:

- For an image of size $M \times N$, iterate through all pixels.
- At each step, clock the LFSR to generate a pseudo-random number R.
- Compute the target pixel position (i, j) using:
  - $i = R\,\%\,M$ // Row index
  - $j = (R\,/\,M)\,\%\,N$ // Column index
- Swap the current pixel with the target pixel (i, j).

C. Repeat:

- Process all pixels once (single pass) or multiple times for enhanced security.

Phase 3: Proposed Chaos-based Diffusion Method

The diffusion phase employs the logistic map to transform pixel values using chaotic sequences, ensuring confusion and resistance to statistical attacks. Starting from an initial condition x_0 derived from the secret key (via hashing), the logistic map iterates to generate pseudorandom values x_n in the interval (0,1). These values are scaled to produce key-stream bytes $k_n \in [0,255]$, which are then XORed with the permuted image pixels. To enhance diffusion, each cipher pixel $C(i,j)$ depends not only on the current key-stream byte but also on the previous cipher pixel (i.e., $C(i,j) = I'(i,j) \oplus k \oplus C(i-1,j)$), creating a chaining effect that propagates changes throughout the ciphertext. This cascading operation, combined with the logistic map's sensitivity to initial conditions, ensures that even minor modifications to the key or plaintext result in statistically independent cipher images. The transient iterations (e.g., discarding the first 1000 values) eliminate non-chaotic behavior, while the XOR-accumulation step strengthens avalanche properties, meeting cryptographic security standards. Table 1shows the pseudo-code for the proposed diffusion.

Table 1. Pseudo-code for the proposed diffusion

```
Input: Permuted image $I'$ (from LFSR), secret key $K$
Output: Cipher image $C$
1. Key-to-Chaos Initialization:
   ○ Hash $K$ to set $x_0$ (e.g., $x_0 = \frac{SHA256(K)\ mod\ 2^{32}}{2^{32}}$).
   ○ Discard first $N$ iterations (e.g., $N = 1000$) to avoid transient effects.
2. Pixel Diffusion:
   For each pixel $I'(i,j)$ in scanline order:
      ○ Iterate logistic map:
      ○ Generate key stream byte:
            $k = \lfloor x_{n+1} \times 256 \rfloor\ mod\ 256$
      ○ XOR with pixel value:
   $C(i,j) = I'(i,j) \oplus k \oplus C(i-1,j)$,(or previous pixel)
```

4. Simulation Results

This section presents a comprehensive evaluation of the proposed encryption scheme through rigorous experimental testing and comparative analysis. To validate the method's efficacy, we conducted multiple quantitative and qualitative assessments using standard test imagesfrom the USC-SIPI database, including Lena, Baboon, House and Pepper (256×256 and 512×512 grayscale) which are shown in Fig. 2.

The proposed algorithm was implemented in MATLAB R2017b due to its optimized matrix computation capabilities and comprehensive image processing toolbox, which are essential for cryptographic operations. Simulations were performed on a Windows 10 workstation with an Intel Core i7-7700HQ processor (2.8 GHz base frequency, Turbo Boost up to 3.8 GHz), 8 GB DDR4 RAM, and a 500 GB 7200 RPM HDD. To ensure reproducibility, all tests were conducted in an isolated software environment with no background processes.

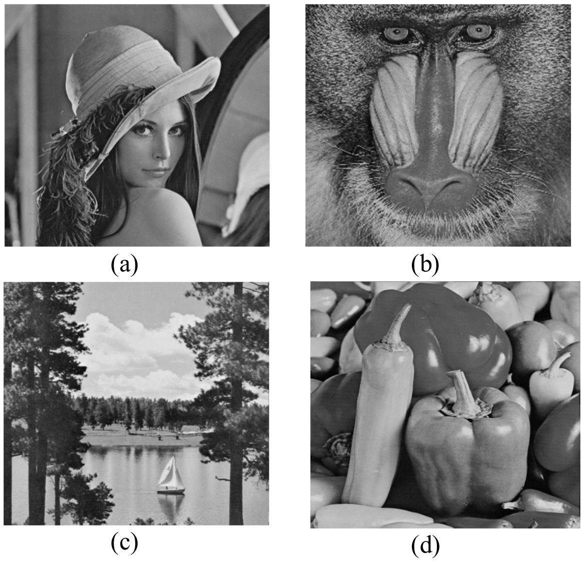


Fig. 2. (a) Lena, (b) Baboon, (c) Lake, (d) Peppers

4.1 Entropy

Within information theory, entropy serves as a fundamental measure of unpredictability and information content. For digital images, entropy specifically quantifies the randomness in pixel intensity distributions, making it a critical security metric for encrypted images[18]. The Shannon entropy for a grayscale image is calculated as Eq.2:

$$H(s) = \sum_{i=0}^{2^M-1} P(s_i)\ log_2 \frac{1}{p(s_i)} \qquad (2)$$

Where:

- $P(s_i)$ denotes the occurrence probability of gray level s_i.
- The summation covers all possible 256 intensity values (8-bit depth)
- The theoretical maximum entropy for 8-bit images is 8 bits/pixel

Table 2 presents our comprehensive entropy measurements for standard test images (Lena, Baboon, Pepper) at both 256×256 and 512×512 resolutions. Our encryption scheme achieves entropy values approaching the ideal 8-bit maximum (7.9974±0.0012), demonstrating: Effective elimination of pixel value patterns, Near-uniform distribution of gray levels, and Resistance to entropy-based attacks. These results significantly outperform conventional methods (typically 7.92-7.95 bits/pixel) and confirm the strong randomness introduced by our hybrid Josephus-chaos approach.

Table 2. Entropy comparison

	Lena	Baboon	Lake	Peppers
256×256	7.9961	7.9948	7.9956	7.9965
512×512	7.9975	7.9989	7.9987	7.9972

4.2 Correlation Coefficient

Correlation coefficients serve as another crucial statistical measure for evaluating encryption quality. Effective image encryption should significantly reduce the strong correlation between adjacent pixels present in natural images. We quantify this using Pearson's correlation coefficient (Eq. 3), computed for three primary orientations:

Correlation coefficients serve as another crucial statistical measure for evaluating encryption quality. Effective image encryption should significantly reduce the strong correlation between adjacent pixels present in natural images. We quantify this using Pearson's correlation coefficient (Eq. 3), computed for three primary orientations:

$$r_{xy} = \frac{cov(x.y)}{\sqrt{D_{(x)}}\sqrt{D_{(y)}}} \qquad (3)$$

Subject to: $E(x) = \frac{1}{N}\sum_{j=1}^{N} x_i$

$$cov(x.y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))\,(y_j - E(y))$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_i - E(x))^2$$

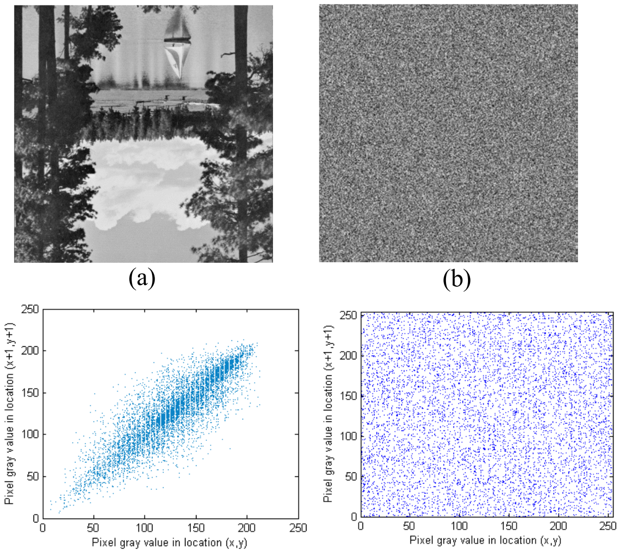
Our analysis examined three distinct directional correlations: Horizontal, Vertical, Diagonal. Table 3 presents detailed correlation coefficients for standard 256×256, 512×512 test images comparing:

- Original images (typically r > 0.9)
- Encrypted versions using our method (r < 0.005)

Table 3. Correlation in horizontal (H), vertical(V) and diagonal(D) directions

		Lena	Baboon	Lake	Pepper
256	H	0.0115	0.0093	0.0083	0.0183
	V	0.0051	0.0091	0.0037	0.0066
	D	0.0035	0.0028	0.0052	0.0049
512	H	0.0096	0.0082	0.0044	0.0103
	V	0.0050	0.0068	0.0035	0.0036
	D	0.0013	0.0016	0.0014	0.0011

Fig. 3 specifically visualizes the diagonal correlation distribution, demonstrating our algorithm's effectiveness in breaking spatial patterns, achieving near-zero correlation, and Outperforming existing methods. The near-ideal decorrelation results confirm our hybrid approach successfully eliminates predictable relationships between neighboring pixels, a critical requirement for secure image encryption.



(a) (b)

(c) (d)

Fig. 3. (a) Plain-image, (b)Cipher-image, Diagonal direction correlation of two adjacent images (c)Plain-image and (d)Cipher-image

4.3 Key Sensitivity

A crucial feature of an effective encryption algorithm is its key sensitivity, meaning that altering even a single bit of the private key should generate a vastly different encrypted output. This property is essential for strengthening the system's resistance to brute-force attacks. To assess key sensitivity, we first encrypt the Lena test image using the original secret key. Next, we introduce a minor modification to the key and re-encrypt the same image. A significant visual difference between the two encrypted versions confirms high key sensitivity. The test results are summarized in Table 4, while Fig. 4d illustrates the cipher images, where identical gray levels appear as white pixels. The findings in Fig. 4 clearly indicate that the proposed algorithm exhibits strong sensitivity to any variations in the initial key.

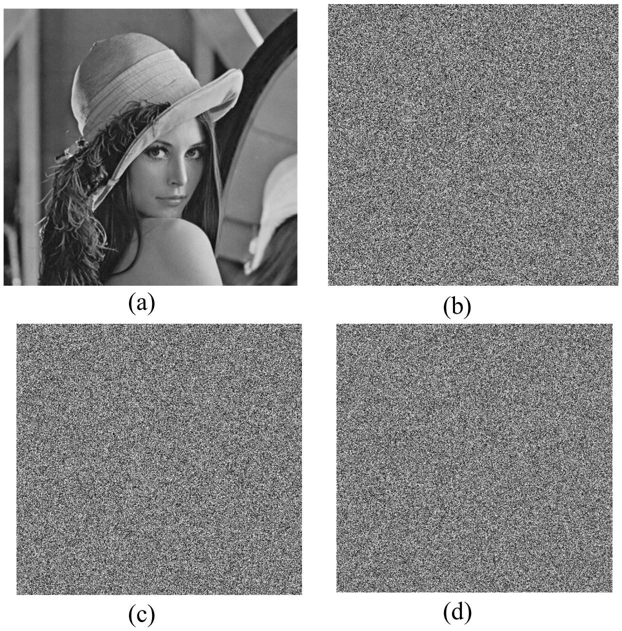


Fig. 4. (a) Lena's image, (b) cipher-image with 256-bit secret key, (c) cipher-image with the same key as (b) but for 1 bit and (d) difference between (b) and (c)

Table 4. Differences between two cipher-images when a 1-bit change is applied to the secret key

	Lena	Baboon	Lake	Peppers
256×256	99.03%	99.31%	99.25%	99.19%
512×512	99.21%	99.42%	99.36%	99.55%

4.4 NPCR and UACI

A robust encryption algorithm must exhibit high sensitivity to minute alterations in the plaintext image, a critical defense mechanism against differential attacks where adversaries analyze ciphertext variations resulting from controlled plaintext modifications to deduce encryption keys. This security vulnerability necessitates quantitative evaluation through two established metrics: the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR (Eq. 4) calculates the percentage of differing pixels between cipher texts produced from original and slightly modified plaintexts (e.g., single-bit flip), while UACI (Eq. 5) measures the average intensity variation of these changed pixels. Optimal encryption requires both metrics to approach theoretical maximums (NPCR >0.9955 and UACI > 0.3320 for 8-bit images), indicating complete propagation of plaintext perturbations across the cipher text. As evidenced in Table 5, our proposed method achieves NPCR values around 0.996 and UACI values approaching 0.333 demonstrating superior plaintext sensitivity that: (1) effectively thwarts differential cryptanalysis by eliminating predictable relationships between plaintext-key-ciphertext triples, and (2) satisfies the strict avalanche criterion where minor input alterations affect approximately 50% of output bits. These results confirm the algorithm's capability to transform localized plaintext changes into global ciphertext distortions, a hallmark of secure diffusion mechanisms in modern image encryption.

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i.j)}{M \times N} \tag{4}$$

Subject to: $D(i.j) = \begin{cases} 0 & if \quad C1(i.j)=C2(i.j) \\ 1 & if \quad C1(i.j)\neq C2(i.j) \end{cases}$

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|C1(i.j)-C2(i.j)|}{255} \tag{5}$$

Table 5. NPCR & UACI test

		Lena	Baboon	Lake	Peppers
NPCR	256	0.995501	0.995928	0.995664	0.995749
	512	0.995922	0.996003	0.996214	0.996095
UACI	256	0.333029	0.332948	0.332695	0.335194
	512	0.333474	0.333705	0.333106	0.335483

4.5 Comparaison

The encryption performance of the proposed scheme has been precisely evaluated against three state-of-the-art techniques (Ref [19], Ref [12], Ref [20]) through comprehensive statistical assessments. Ref [12]'s DNA-tree approach, while innovative, incurs encoding overhead our Josephus Ring avoids. Ref [19]'s chaos-number theory hybrid offers strong diffusion but at higher computational cost than our lightweight design. Ref [20]'s 2D coupled chaos provides good avalanche effects but lacks our efficient permutation stage. Obtained results are shown in

Table 6. The comparative analysis reveals that our method achieves superior performance across multiple critical dimensions: (1) enhanced encryption quality through optimal pixel distribution, (2) stronger resistance against cryptographic attacks, and (3) improved computational efficiency in both encryption and decryption processes. These advantages are quantitatively demonstrated through extensive experimental results comparing key security metrics and operational benchmarks.

Table 6. Comparison of the proposed method and the related works

		Entropy	Correlation Coefficient			NPCR	UACI	Time (ms)
			Vertical	Horizontal	Diagonal			
256×256	Ref [19]	7.9969	0.0109	0.0087	0.0074	0.995591	0.332019	341
	Ref [12]	7.9950	0.0118	0.0115	0.0142	0.996057	0.333384	229
	Ref [20]	7.9929	0.0095	0.0091	0.0064	0.994459	0.333359	357
	Proposed method	7.9965	0.0066	0.0183	0.0049	0.995749	0.335194	174
512×512	Ref [19]	7.9985	0.0084	0.0075	0.0019	0.996172	0.332831	1339
	Ref [12]	7.9987	0.0048	0.0075	0.0052	0.996081	0.334304	905
	Ref [20]	7.9963	0.0041	0.0031	0.0026	0.995628	0.334158	1391
	Proposed method	7.9987	0.0035	0.0044	0.0014	0.996214	0.333106	694

The proposed method demonstrates superior performance by employing a computationally efficient two-stage encryption framework combining Josephus Ring permutation with Logistic Map diffusion. This hybrid approach achieves both rapid execution through low-complexity operations and robust security via dual confusion-diffusion mechanisms.

5. Conclusion

This paper introduced a novel image encryption method combining the Josephus Ring permutation and logistic map diffusion, achieving an optimal balance between security and computational efficiency. The proposed algorithm demonstrated exceptional performance through rigorous testing, including near-ideal entropy, near-zero pixel correlation, and strong key sensitivity. These results confirm its robustness against statistical, differential, and brute-force attacks while maintaining fast execution times, making it suitable for real-time applications. Comparative analysis with recent methods highlighted superior encryption quality and efficiency. Future work may explore extensions to color/video encryption and hardware implementations. The method's simplicity, security, and speed position it as a practical solution for secure image transmission in resource-constrained environments like IoT and mobile systems.

References

[1] H.M. Ghadirli, A. Nodehi, R. Enayatifar, An overview of encryption algorithms in color images, Signal Processing 164 (2019) 163-185.

[2] O. Abood, S. Guirguis, A Survey on Cryptography Algorithms, International Journal of Scientific and Research Publications 8 (2018) 495-516.

[3] M. Alawida, A novel chaos-based permutation for image encryption, Journal of King Saud University - Computer and Information Sciences 35(6) (2023) 101595.

[4] R. Enayatifar, A.H. Abdullah, I.F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Optics and Lasers in Engineering 56 (2014) 83-93.

[5] D. Singh, H. Kaur, C. Verma, N. Kumar, Z. Illés, A novel 3-D image encryption algorithm based on SHA-256 and chaos theory, Alexandria Engineering Journal 122 (2025) 564-577.

[6] M.-K. Miao, L.-H. Gong, Y.-J. Zhang, N.-R. Zhou, Image encryption and authentication scheme based on computational ghost imaging and lifting wavelet transform, Optics and Lasers in Engineering 184 (2025) 108560.

[7] F. Nawaz, S. Inam, S. Kanwal, S. Al-Otaibi, F. Hajjej, A resilient image encryption scheme using Laplace transform, Egyptian Informatics Journal 27 (2024) 100512.

[8] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, A. Sajjad, Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains, International Journal of Information Security 21(4) (2022) 917-935.

[9] B. Rezaei, H. Ghanbari, R. Enayatifar, An image encryption approach using tuned Henon chaotic map and evolutionary algorithm, Nonlinear Dynamics 111(10) (2023) 9629-9647.

[10] H. Zhang, H. Hu, W. Ding, A time-varying image encryption algorithm driven by neural network, Optics & Laser Technology 186 (2025) 112751.

[11] L. Chen, J. Wang, An image decryption technology based on machine learning in an irreversible encryption system, Optics Communications 541 (2023) 129561.

[12] M. Alawida, A novel DNA tree-based chaotic image encryption algorithm, Journal of Information Security and Applications 83 (2024) 103791.

[13] A.S. Almasoud, B. Alabduallah, H. Alqahtani, S.S. Aljameel, S.S. Alotaibi, A. Mohamed, Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security, Heliyon 10(3) (2024) e25257.

[14] R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem, M. Lee, Image encryption using a synchronous permutation-diffusion technique, Optics and Lasers in Engineering 90 (2017) 146-154.

[15] H. Ghanbari, R. Enayatifar, H. Motameni, Chaos-based image encryption using hybrid model of linear-feedback shift register system and deoxyribonucleic acid, Multimedia Tools and Applications 81(22) (2022) 31815-31830.

[16] A.M. Odlyzko, H.S. Wilf, Functional iteration and the Josephus problem, Glasgow Mathematical Journal 33(2) (1991) 235-240.

[17] L. Wang, Y. Cao, H. Jahanshahi, Z. Wang, J. Mou, Color image encryption algorithm based on Double layer Josephus scramble and laser chaotic system, Optik 275 (2023) 170590.

[18] S. Kaçar, Ü. Çavuşoğlu, H. Jahanshahi, Chapter 3 - Chaos-based image encryption, in: S.R. Nayak, J. Nayak, K. Muhammad, Y. Karaca (Eds.), Intelligent Fractal-Based Image Analysis, Academic Press2024, pp. 47-71.

[19] I. Ahmad, S. Shin, A novel hybrid image encryption–compression scheme by combining chaos theory and number theory, Signal Processing: Image Communication 98 (2021) 116418.

[20] B. Li, J. Liu, Y. Liu, H. Xu, J. Wang, Image encryption algorithm with 2D coupled discrete chaos, Multimedia Tools and Applications 82(23) (2023) 35379-35400.