Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

Original article

Parallel Bit-Level Image Encryption Using a Two-Dimensional Sine-Coupled Map and Josephus Scrambling

Khaled El Hadad*, Salah Abokhatwa

Faculty of Engineering, Garaboulli, Elmergib University, Libya
Email. *kmelhadad@elmergib.edu.ly*

Abstract
This paper presents a parallel bit-level image-encryption scheme based on a two-dimensional sine-coupled chaotic map, a plaintext-dependent SHA-256 key-derivation step, Josephus-based bit scrambling, and feedback diffusion. The image is divided into high- and low-order bit groups, which are scrambled using chaotic sequences before recombination and diffusion. Tests on three grayscale benchmark images produced ciphertext entropy above 7.9990, absolute adjacent-pixel correlation below 0.002, NPCR values from 99.5995% to 99.6116%, and UACI values from 33.4327% to 33.5168%. The reported implementation encrypted a 256 × 256 image in approximately 0.04 s. These results indicate good statistical diffusion and support further evaluation of the scheme for resource-constrained image-transmission applications.
Keywords. Image Encryption, Two-Dimensional Chaotic Map, Bit-Level Permutation, Josephus Traversal, SHA-256.

Introduction

Industrial Internet of Things (IIoT) and edge-computing devices generate and exchange large volumes of multimedia data [1,2]. Images used in industrial monitoring, healthcare, and surveillance can contain operationally sensitive or personal information [3,4]. When these data travel over open or untrusted networks, they may be intercepted or modified [5]. Protecting image confidentiality and integrity is therefore an important requirement for edge-based applications [4]. Standard ciphers such as AES can encrypt image data securely when they are used in an appropriate authenticated mode. However, image-specific schemes continue to attract research interest because images are large and highly redundant, and embedded implementations may impose strict latency and memory limits [6-8]. Any proposed alternative must therefore demonstrate both cryptographic soundness and a measurable implementation advantage over established methods. Chaos-based image-encryption methods commonly use a permutation-diffusion structure [9,11].

Permutation rearranges pixel or bit positions, whereas diffusion changes pixel values so that a small plaintext change affects many ciphertext samples. Published variants have used coupled-map lattices, cellular automata, DNA coding, and Josephus traversal [12,16]. These methods can produce favorable statistical results, but statistical randomness alone does not establish cryptographic security. Some lattice-based and cellular-automata schemes require repeated neighborhood updates that may limit throughput on constrained hardware [17,18]. Separate permutation and diffusion stages can also preserve exploitable structure when the key schedule or plaintext coupling is weak [19,20]. These concerns motivate a simpler architecture, but resistance to chosen-plaintext attacks must be demonstrated by explicit analysis rather than inferred from histogram, entropy, NPCR, or UACI results alone.

This work proposes a parallel bit-level scheme that combines a two-dimensional sine-coupled chaotic map with Josephus-based scrambling and feedback diffusion. The intended contribution is to reduce sequential processing while retaining plaintext sensitivity and statistical diffusion. The remainder of this paper is organized as follows: Section 2 details the proposed 2D-SICM chaotic map and its performance analysis; Section 3 outlines the explicit steps of the parallel bit-level encryption and decryption algorithms; Section 4 presents the experimental simulations and comprehensive security analysis; and Section 5 concludes the paper.

Two-Dimensional Sine-Coupled Chaotic Map

This study uses the two-dimensional sine-coupled map defined in (1). Figure 1 shows one phase-space trajectory for the stated parameter values. A phase portrait illustrates the trajectory but does not, by itself, establish hyperchaos; Lyapunov-exponent calculations over the claimed operating range are also required.

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

Figure 1. Phase portrait of the proposed two-dimensional chaotic map for the stated parameter values

Mathematical Formulation

The map is defined by

$$\left\{\begin{array}{l} x_{i+1} = \sin(\pi \cdot \alpha \cdot (y_i + 3x_i)\,) \\ y_{i+1} = \sin\big(\pi \cdot \beta \cdot (x_{i+1} + 3y_i)\big) \end{array}\right\} \quad (1)$$

where x_{i+1} and x_{i+1} are the state variables, and α and β are control parameters. Because the sine function bounds each update, $x_{i+1}, x_{i+1} \in [-1,1]$ after the first iteration. The parameter values used in this study are α = 5.2 and β = 4.9. A broader operating region should be claimed only when it is supported by a parameter sweep. For A_i = πα(y_i + 3x_i) and B_i = πβ(x_{i+1} + 3y_i), the Jacobian is

$$J = \begin{bmatrix} \frac{\partial x_{i+1}}{\partial x_i} & \frac{\partial x_{i+1}}{\partial y_i} \\ \frac{\partial y_{i+1}}{\partial x_i} & \frac{\partial y_{i+1}}{\partial y_i} \end{bmatrix} \quad (2)$$

The four derivatives are

∂x_(i+1)/∂x_i = 3πα cos(A_i), (3)

∂x_(i+1)/∂y_i = πα cos(A_i), (4)

∂y_(i+1)/∂x_i = πβ cos(B_i)[∂x_(i+1)/∂x_i], (5)

∂y_(i+1)/∂y_i = πβ cos(B_i)[∂x_(i+1)/∂y_i + 3]. (6)

The Lyapunov exponents are estimated from the long-term product of Jacobians, not from the eigenvalues of one instantaneous Jacobian. Starting with an orthonormal basis Q_0, the tangent update J_iQ_(i−1) = Q_iR_i is computed at every iteration using QR factorization. The exponents are then estimated as λ_j = (1/L)Σ_i ln|R_i(j,j)| after discarding the transient samples. Two positive values are required before the map can be described as hyperchaotic. (Figure 1) gives a qualitative phase portrait. The final manuscript should also provide Lyapunov exponent and bifurcation plots over the tested parameter interval. These dynamical tests characterize the map but do not replace cryptanalysis of the complete cipher.

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

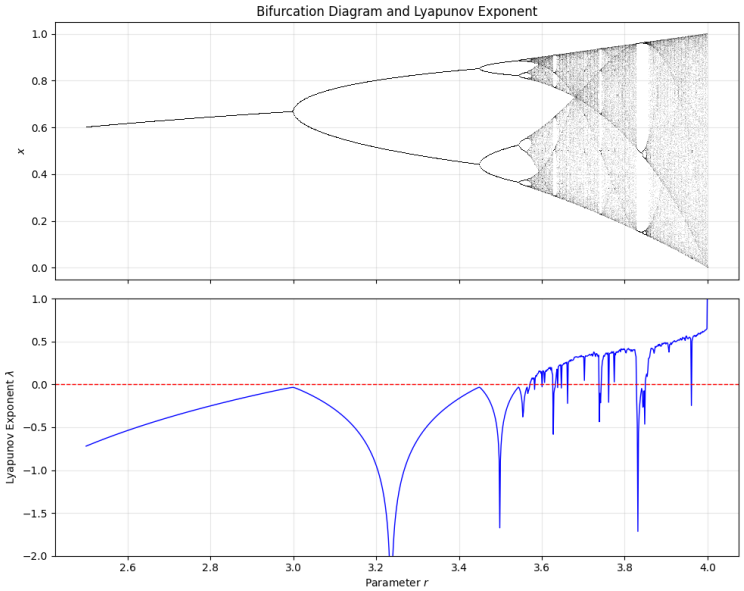

Figure 2. Bifurcation Diagram and Lyapunov exponent

Image Encryption and Decryption Scheme
Parallel Bit-Level Encryption Algorithm

The proposed encryption algorithm represents the grayscale plaintext image as an M × N matrix with 8-bit entries. The procedure contains five stages:

Step 1

Session-Key Derivation. Let K be a uniformly random 256-bit master key shared through an external secure mechanism. Generate a fresh 128-bit public nonce n for every encryption. Compute the plaintext digest h = SHA-256(P), then derive the session material S = HMAC-SHA-256(K, n || h || "image-encryption-v1"). Map separate, non-overlapping parts of S to the initial states, control values, permutation controls, and diffusion key. Transmit n and h with the ciphertext. Authenticate n, h, algorithm parameters, image dimensions, and ciphertext with a separate authentication key derived from K.

Step 2

Chaotic-Sequence Generation. Iterate the sine-coupled map after quantizing all states with the declared numeric representation. Discard T_0 transient samples, then convert subsequent states to integer control sequences with the stated extraction rule.

Step 3

Bit-Group Decomposition. Express every grayscale pixel as eight bits. Form a high-order group from bits 7–4 and a low-order group from bits 3–0.

Step 4

Josephus Bit Permutation. Use domain-separated session controls to generate the start position, step size, and direction for each group. Apply the permutation independently to the high- and low-order groups. The implementation must state whether these operations run concurrently or are only algorithmically independent.

Step 5

Recombination, Feedback Diffusion, and Authentication. Recombine the permuted groups into S_i and compute the ciphertext recurrence in (7), using a session-dependent initial feedback byte C_0. Finally, compute an authentication tag over the complete header and ciphertext. Decryption must reject the input if tag verification fails.

$$C_i = S_i \oplus K_i \oplus C_{i-1} \qquad (7)$$

This flowchart tracks the data flow through all five mathematical steps outlined in the encryption pipeline:

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

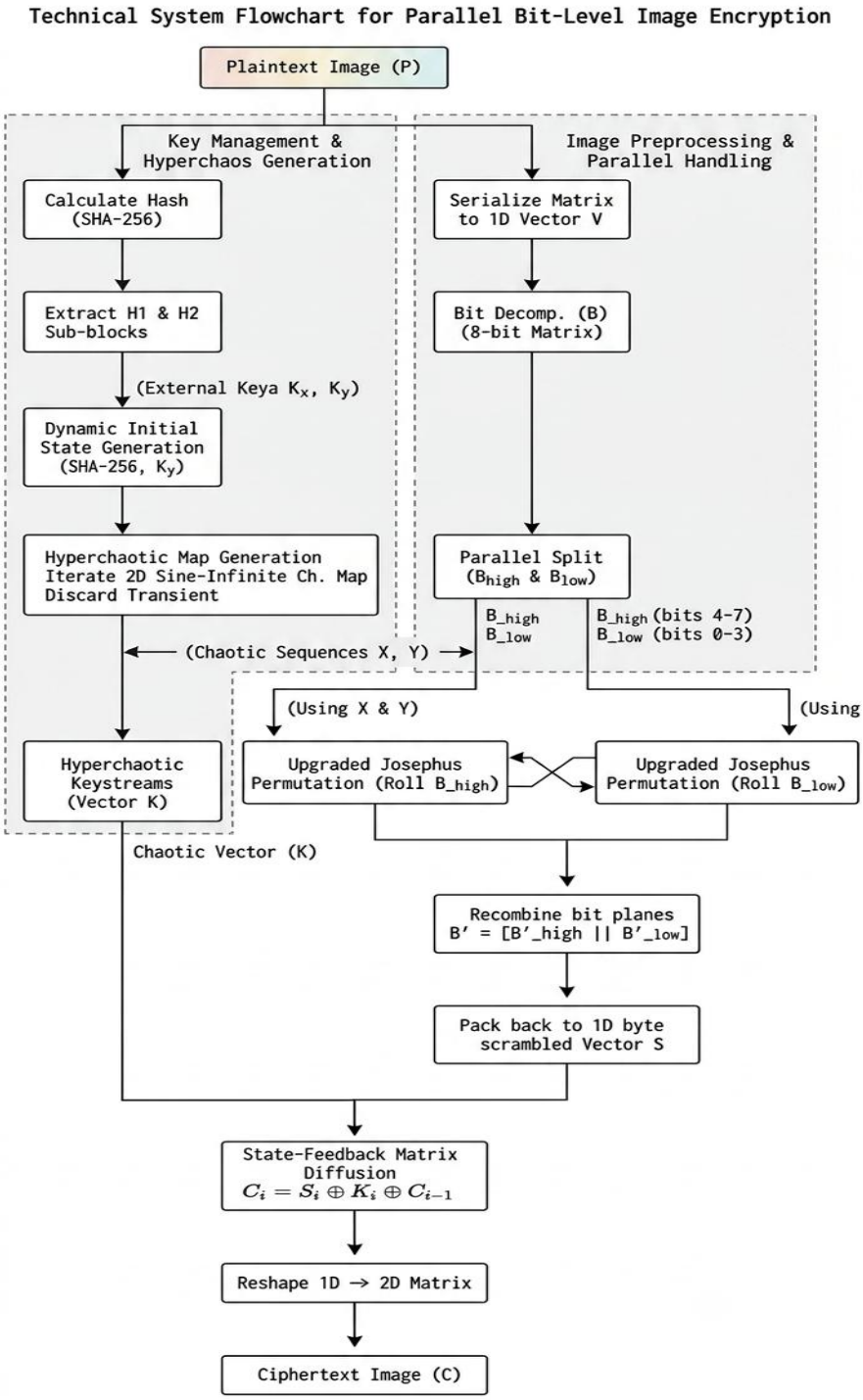

Figure 3. Flowchart for Parallel Bit-Level Image Encryption

Parallel Bit-Level Decryption Algorithm

Decryption first verifies the authentication tag. It then reads the transmitted nonce n and plaintext digest h, derives the same session material from the secret master key K, and applies the inverse operations. This removes the circular dependence in which the receiver would otherwise need the unknown plaintext before deriving the decryption sequence.

Step 1

Verify the tag and regenerate the session material from K, n, and h.

Step 2

Recover S_i with S_i = C_i ⊕ K_i ⊕ C_(i−1).

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

Step 3
Separate S into the scrambled high- and low-order bit groups.

Step 4
Apply the inverse Josephus permutations in reverse order.

Step 5
Recombine the recovered groups to obtain P and verify that SHA-256(P) = h. A mismatch causes decryption failure. Technical System Flowchart for Parallel Bit-Level Image Decryption.

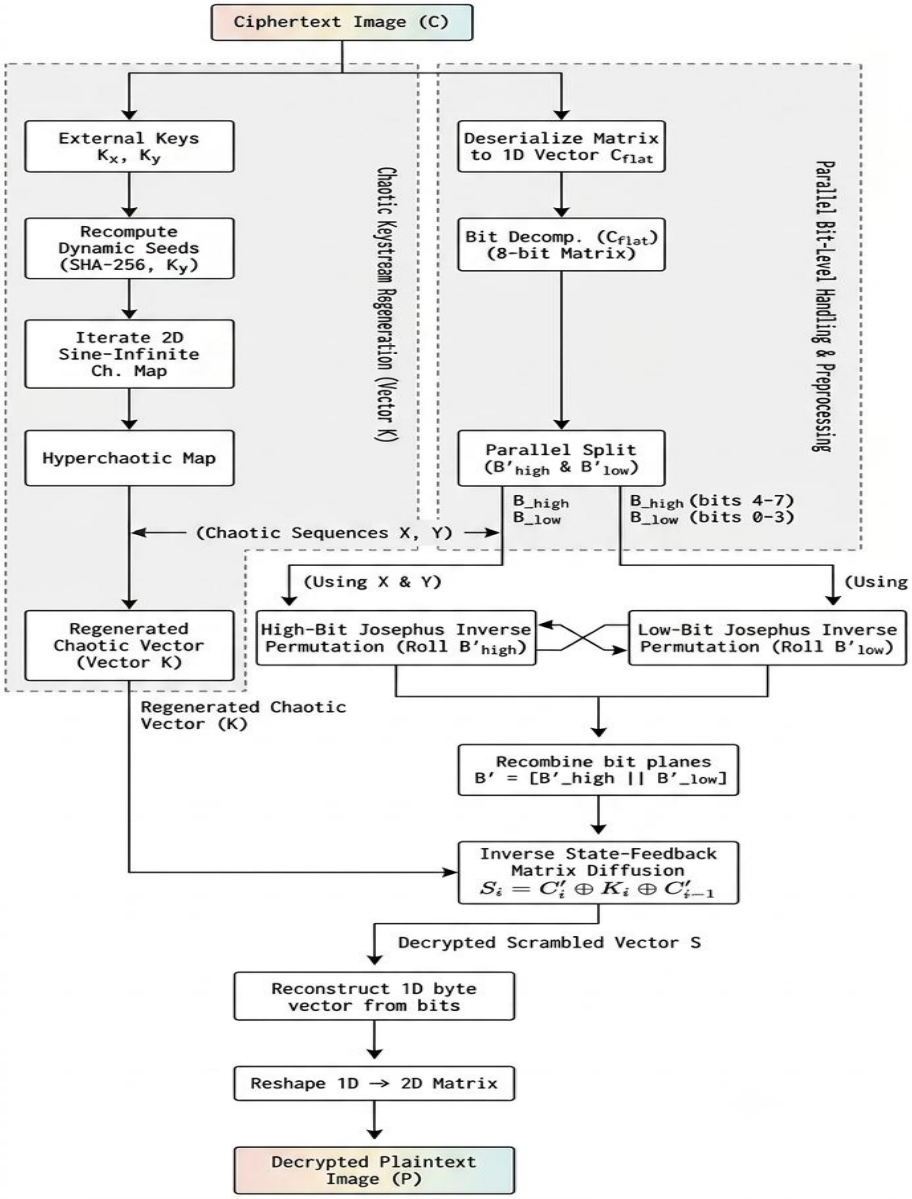

Figure 4. Flowchart for Parallel Bit-Level Image Decryption

Threat Model and Security Scope
The adversary is assumed to know the complete algorithm and all public parameters and to observe or modify transmitted ciphertexts. The adversary may also request encryptions of chosen images and may know some plaintext-ciphertext pairs. Only the uniformly random master key K remains secret. Under this model, histogram, entropy, correlation, NPCR, and UACI tests measure statistical behavior; they do not prove semantic security. The authentication tag is required to detect modification and prevent unauthenticated chosen-ciphertext processing.

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلوم
https://alqalam.utripoli.edu.ly/index.php/AR

Key Space, Precision, and Nonce Requirements

A uniformly generated 256-bit master key gives a nominal key space of 2^256. This statement does not include user-chosen passwords, which require a password-based key-derivation function. The nonce must never repeat under the same master key. The paper must specify floating-point or fixed-point precision, integer extraction, modulo operations, and parameter quantization, because finite precision can shorten chaotic periods or create equivalent session states.

Experimental Results and Security Analysis

The scheme was evaluated on three grayscale benchmark images: Airplane (512 × 512), Twin (403 × 383), and Cameraman (800 × 570). All image sources, preprocessing steps, software versions, random seeds, and source code should be archived with the final paper.

Histogram and Chi-Square Analysis

A ciphertext histogram should not retain obvious features of the plaintext histogram. Histogram uniformity was assessed with the chi-square statistic:

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - v)^2}{v} \qquad (8)$$

At α_s = 0.01 and 255 degrees of freedom, the upper chi-square critical value is approximately 310.46. A ciphertext histogram is considered consistent with uniformity when the statistic does not exceed this threshold. The paper should report the statistic for each image rather than only a range.

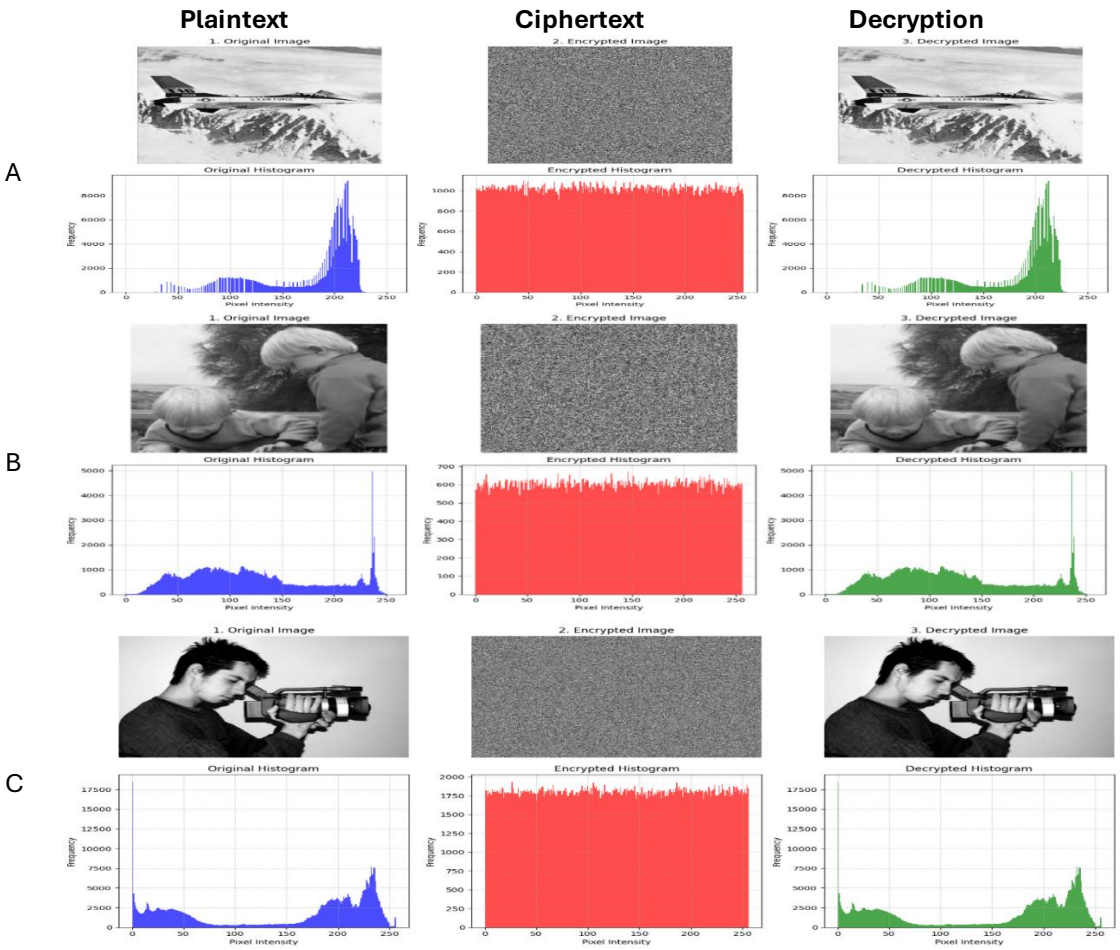

Figure 5. Encryption and decryption visual results and histogram analysis for standard benchmark images: (a) Airplane, (b) twins, and (c) Cameraman

Adjacent-Pixel Correlation Analysis

To evaluate spatial redundancy, $N = 10{,}000$ adjacent pixel pairs were extracted. The correlation coefficient r_{xy} is calculated via:

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{N}(y_i-\bar{y})^2}} \quad (9)$$

(Table 1) shows absolute ciphertext correlation below 0.002 in the tested directions. This supports spatial decorrelation for the sampled image pairs. Confidence intervals and results over repeated random pair selections should be reported because one sample of 10,000 pairs does not characterize variability.

Table 1: Adjacent Pixel Correlation Coefficients Before and After Encryption

Image Name	Direction	Plaintext	Ciphertext
Airplane	Horizontal	0.9412	-0.0004
	Vertical	0.9701	0.0011
	Diagonal	0.9125	-0.0009
Twin	Horizontal	*0.9238*	0.0014
	Vertical	*0.9105*	-0.0018
	Diagonal	*0.8992*	0.0003
Cameraman	Horizontal	0.9314	-0.0008
	Vertical	0.9542	0.0012
	Diagonal	0.9088	-0.0005

Information Entropy Analysis

Information entropy evaluates the uncertainty and randomness of an information source. The global Shannon entropy $H(m)$ of an 8-bit image is defined as:

$$H(m) = -\sum_{i=0}^{255} P(m_i)\log_2 P(m_i) \quad (10)$$

where p(m_i) is the observed probability of gray level m_i. For an 8-bit source, the maximum entropy is 8 bits per pixel. Values close to 8 indicate a nearly uniform marginal histogram, but they do not establish independence between samples or cryptographic security.

Table 2. Information Entropy

Image Name	Dimensions	Entropy (Plain)	Entropy (Cipher)
Airplane	512×512	6.7142	7.9994
Twin	403×383	7.1044	7.9991
Cameraman	800×570	7.0097	7.9997

The global ciphertext entropy values in (Table 2) exceed 7.9990. Local entropy should also be reported as a mean, standard deviation, and confidence interval across a declared number of randomly selected or non-overlapping blocks.

Differential Attack Analysis (NPCR and UACI)

Resistance against differential attacks is evaluated using the Number of Changing Pixel Rate (NPCR) and Unified Average Changing Intensity (UACI):

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (11)$$

$$\text{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |C_1(i,j)-C_2(i,j)|}{255 \times M \times N} \times 100\% \quad (12)$$

For independent uniformly random 8-bit images, the expected NPCR and UACI values are approximately 99.6094% and 33.4635%, respectively. Acceptance should be based on image-size-specific confidence intervals rather than closeness to the expected means alone.

Table 3. NPCR and UACI Performance Evaluation

Image Name	Dimensions	NPCR (%)	UACI (%)
Airplane	512×512	99.5995	33.4327
Twin	403×383	99.6087	33.5168
Cameraman	800×570	99.6116	33.5162

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

The values in (Table 3) are close to the theoretical expectations. The final experiment should repeat the one-bit plaintext change at randomly selected locations for at least 100 trials per image and report the mean, standard deviation, minimum, maximum, and pass rate against the chosen significance limits.

Processing Speed and Computational Efficiency

Runtime must be measured on a declared processor, memory configuration, operating system, language version, and thread count. After warm-up, each image size should be encrypted and decrypted repeatedly. Report the median, mean, standard deviation, and throughput in MB/s. Baseline methods must use the same platform and optimization settings. Until those details are supplied, the reported 0.04 s result should be treated as preliminary rather than proof of real-time suitability.

Conclusion

This paper presented a parallel bit-level image-encryption design that combines a two-dimensional sine-coupled map, domain-separated session-key derivation, Josephus scrambling, feedback diffusion, and ciphertext authentication. The reported tests on three grayscale images produced entropy above 7.9990, absolute adjacent-pixel correlation below 0.002, NPCR from 99.5995% to 99.6116%, and UACI from 33.4327% to 33.5168%. These results indicate strong statistical diffusion for the selected images. A publication-ready validation still requires reproducible Lyapunov-exponent and bifurcation analyses, repeated differential tests with confidence limits, finite-precision and equivalent-key analyses, and a controlled speed comparison.

References

1. Basir R, et al. Fog Computing Enabling Industrial Internet of Things: State-of-the-Art and Research Challenges. Sensors. 2019;19(4807):1–29.
2. Zhukabayeva T, et al. An Impact-Aware and Taxonomy-Driven Explainable Machine Learning Framework with Edge Computing for Security in Industrial IoT–Cyber Physical Systems. Comput Model Eng Sci. 2025;145(2):2573–99.
3. Sarosh P, Parah SA, Bhat GM. An efficient image encryption scheme for healthcare applications. Multimed Tools Appl. 2022;81(5):7253–70.
4. Wu Y, Che L, Wang Y. Efficient and secure content-based image retrieval with deep neural networks in the mobile cloud computing. Comput Secur. 2023;128:103163.
5. Khan PW, Byun Y. A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entropy. 2020;22(2):175.
6. Huo M, Zheng Y, Huang J. Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency. PLoS One. 2025;20(7):e0328297.
7. Kareem SM. DES and AES algorithms for image Encryption: Review. Al-Qadisiyah J Pure Sci. 2022;27(1):1–10.
8. Sharma A, Kumar R. Machine Learning-Fused Hybrid Image Encryption Framework Using Hardware-Optimized AES Algorithm. J Signal Process Syst. 2023;94(2):215–30.
9. Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic maps. Chaos Solitons Fractals. 2004;21(3):749–61.
10. Zhang L, Liao X, Wang Y. An image encryption approach based on chaotic maps. Chaos Solitons Fractals. 2005;24(3):759–65.
11. Wang X, Zhang D, Bao Z. A novel chaotic image encryption scheme using permutation-diffusion architecture. Nonlinear Dyn. 2015;81(1–2):1–12.
12. Li T, Xu W, Li G, Song X. A mixed coupled map lattice based on enhanced Chebyshev maps for chaotic image encryption. Eur Phys J Plus. 2025;140(9):931.
13. Deng C, Wang Q, Yu S, Chen B, Li DD-U. Cryptanalysis of an image encryption algorithm based on cellular automata and chaotic skew tent map. Multimed Tools Appl. 2025;84(11):9431–46.
14. Shraida GK, Youni HA. An Efficient Color-Image Encryption Method Using DNA Sequence and Chaos Cipher. Comput Mater Contin. 2023;75(2):2641–54.
15. Liu H, Wang X, Kadir A. Image encryption using Josephus traversing and coupled map lattices. Signal Processing. 2013;93(6):1462–70.
16. Zhang Y, Zhou J. Sinusoidal-Quadratic Map Coupled Map Lattices for chaotic image encryption. Multimed Tools Appl. 2020;79(9–10):6057–78.
17. Al-Saidi NMG, Younus D, Natiq H, Ariffin MRK, Asbullah MA, Mahad Z. A New Hyperchaotic Map for a Secure Communication Scheme with an Experimental Realization. Symmetry (Basel). 2020;12(11):1881.
18. Elwakil A, Al-Mashaqbeh MA, Natiq H. Modeling and dynamical behaviors of a hyperchaotic map based on dual-memristor circuit without inductor. AEU - Int J Electron Commun. 2026;206:156195.
19. Li C, Lin D, Lü J. Cryptanalysis of a chaotic image encryption algorithm based on permutation-diffusion structure. Commun Nonlinear Sci Numer Simul. 2012;17(12):5113–27.

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*

Alq J Sci. 2026;2(9):863-871
https://doi.org/10.69667/ajs.26904
Alqalam Journal of Science
مجلـــة القلم للعلـوم
https://alqalam.utripoli.edu.ly/index.php/AR

20. Abbes A, Ouannas A. Fractional Memristive-Based Grassi-Miller Map: Hidden Hyperchaos and Complexity. In: Chaos and Control of Fractional Order Discrete Time Memristive Systems: Analytical Approaches and Numerical Simulations. Springer; 2026. p. 225–50.

Received: *08-07-2026 -* ***Accepted:*** *06-09-2026 -* ***Published:*** *14-09-2026*