Enhancing Image Encryption Security via Metaheuristic-Optimized Logistic Chaotic Mapping

Majid Cheshmeh Kouhi [1], Ali Nodehi [1,*], Rasul Enayatifar[2]

Abstract – In the era of widespread digital communication and sensitive data transmission, robust image encryption has become imperative to protect confidential visual information, especially in domains such as medical imaging, military communications, and secure cloud storage. Traditional chaos-based encryption methods, which often rely on static parameters for chaotic maps, suffer from predictability and vulnerability to statistical and brute-force attacks. To overcome these limitations, this paper presents an innovative and adaptive image encryption framework that integrates the logistic chaotic map with the Harmony Search (HS) metaheuristic optimization algorithm. The core contribution of this work lies in the dynamic tuning of the logistic map parameters—specifically the control parameter μ and the initial condition—based on the statistical properties of each input image. Unlike conventional approaches that employ fixed chaotic sequences, our method uses HS to optimize these parameters in real-time, thereby generating unique pseudo-random sequences tailored to every plain-image. This adaptation significantly enhances key sensitivity, cryptographic randomness, and resistance against pattern analysis. The optimization process is guided by Shannon entropy as a fitness function, ensuring that the encrypted image approaches a uniform pixel distribution, a hallmark of secure encryption. The encryption process consists of several structured phases: key generation, parameter optimization via HS, chaotic sequence generation, and diffusion-based pixel encryption. A 32-character secret key is converted into a 256-bit integer to derive the initial value for the logistic map, ensuring a vast key space of 2^{256} possibilities. Harmony Search operates by maintaining a harmony memory of candidate μ values, iteratively improvising new solutions through memory consideration, pitch adjustment, and random selection. The optimal μ* that maximizes entropy is selected to produce the final chaotic sequence used for encryption via XOR operations. Comprehensive security analyses were conducted using six standard grayscale test images at multiple resolutions. The proposed method achieved near-optimal Shannon entropy values (averaging 7.9993 for 512×512 images), indicating excellent randomness. Histogram analysis confirmed uniform distributions in cipher-images, and correlation coefficients between adjacent pixels were reduced to nearly zero, demonstrating effective removal of spatial patterns. The algorithm also exhibited strong resilience against differential attacks, with high NPCR (up to 0.995835) and UACI (up to 0.335217) values, closely approaching theoretical optima. Comparative evaluations against state-of-the-art techniques revealed superior performance in entropy, pixel decorrelation, and differential metrics, while maintaining reasonable computational efficiency (1467 ms execution time). Boxplot analysis over 30 independent runs confirmed the algorithm's stability and reliability, with very low interquartile ranges. The method's large key space and high key sensitivity further fortify it against brute-force and statistical attacks.

Keywords: Image encryption; Logistic chaotic function; Harmony search(HS); parameter tuning

1. Introduction

The widespread adoption of digital medical imaging—including computed tomography (CT), magnetic resonance imaging (MRI), and ultrasound—has transformed modern diagnostics, enabling faster and more accurate disease detection [1]. However, the transmission and storage of these sensitive images over networks expose them to growing cybersecurity threats, such as unauthorized access and data breaches. Given the confidential nature of medical records, ensuring robust encryption is not merely a technical challenge but a critical requirement for patient privacy and trust [2]. Traditional encryption methods often - struggle to balance security with computational efficiency, particularly for high-resolution medical images, necessitating more adaptive and intelligent solutions[3, 4].

Chaos-based encryption has gained prominence as a viable approach due to its inherent properties, such as sensitivity to initial conditions and pseudo-randomness. Most chaos-based techniques involve two key steps: permutation (rearranging pixel positions) and diffusion

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

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

*** Corresponding Author :** ali.nodehi@iau.ac.ir

Received: 2025.04.18; Accepted: 2025.07.16

(altering pixel values using chaotic sequences)[5, 6]. While logistic maps are widely used for their simplicity, their security is frequently undermined by fixed parameters. For instance, many algorithms set the logistic parameter $\mu \approx 3.99$ to ensure chaotic behavior, but the restricted range ($\mu \in (0,4]$) and static tuning render the keystream predictable, leaving systems vulnerable to brute-force and statistical attacks [7, 8]. To overcome these limitations, researchers have turned to evolutionary algorithms (EAs) for dynamic parameter optimization. Methods like the imperialist competitive algorithm (ICA) generate multiple cipher-images using chaotic maps (e.g., asymmetric tent maps) and refine them using fitness functions based on entropy and correlation coefficients[9]. However, these approaches often suffer from high computational costs and fail to fully adapt to the unique statistical features of individual images[10, 11]. This gap highlights the need for a more efficient and adaptive encryption framework that can tailor chaotic sequences to specific input images while maintaining low computational overhead.

Abdullah et al. [10] proposed a genetic algorithm-chaos hybrid that optimizes encryption through entropy maximization. Wang et al. [19] enhanced security through coupled map lattices with mixed multi-chaos systems. Raj et al. [20] implemented reversible logic cryptography with LFSR-based key generation for microcontroller applications. Our method advances beyond these approaches by unifying the computational efficiency of Josephus Ring permutation with the cryptographic strength of Logistic Map diffusion in a lightweight architecture.

In this study, we propose a novel metaheuristic-optimized logistic chaotic map for secure and efficient image encryption. Our approach leverages Harmony Search (HS)[12] to dynamically tune the logistic map's parameters (μ, initial conditions) based on the input image's statistical properties. Unlike conventional methods, this ensures that the pseudo-random sequences are uniquely tailored to each plain-image, significantly enhancing resistance against pattern analysis and statistical attacks. By optimizing for Shannon entropy, the cipher-image achieves near-uniform pixel distribution, while HS's balance of exploration and exploitation ensures computational efficiency—a crucial advantage for real-time applications. The proposed method is particularly suited for medical imaging systems, where patient confidentiality is paramount, as well as military communications and IoT-based video encryption, where both security and speed are critical.

The remainder of this paper is organized as follows: Section 2 provides background on chaotic maps and Harmony Search, Section 3 details the proposed encryption framework, Section 4 evaluates its security and performance through statistical tests and attack analyses, and Section 5 concludes with future research directions.

1. Background of the study

Background of the study is explained as follow:

2.1 Logistic chaotic function

The logistic map is a well-known one-dimensional chaotic system defined by the recurrence Eq. 1:

$$x_{n+1} = \mu x_n(1 - x_n) \qquad (1)$$

where $x_n \in [0,1]$ represents the state variable at step n, and $\mu \in (0,4]$ is the control parameter governing the map's behavior. Despite its simplicity, the logistic map exhibits complex dynamics, including period-doubling bifurcations and deterministic chaos. For $\mu \geq 3.57$, the system enters a chaotic regime, where infinitesimal changes in initial conditions (x_n) or μ lead to vastly divergent trajectories—a hallmark of the butterfly effect. This sensitivity makes the logistic map ideal for generating pseudo-random sequences in encryption, as small perturbations in parameters or inputs produce entirely uncorrelated outputs.

However, the logistic map's cryptographic utility is limited by two key challenges. First, its parameter range ($\mu \in (0,4]$) is narrow, and conventional encryption schemes often fix $\mu \approx 3.99$ to ensure chaos, inadvertently reducing key space and predictability. Second, the map's geometric structure (e.g., non-uniform distribution of iterates) can leak statistical patterns, making cipher-images vulnerable to attacks.

2.2 Harmony Search Algorithm: Theory and Formulation

Harmony Search (HS) is a metaheuristic optimization algorithm inspired by the musical process of improvising harmonies. The algorithm iteratively refines a set of candidate solutions (harmonies) stored in the Harmony Memory (HM) to converge toward an optimal solution. Below are the core components and equations governing HS[13]:

2.2.1 Harmony Memory Initialization

The HM is initialized with HMS (Harmony Memory Size) random solutions, each represented as a vector of D decision variables:

$$HM = \begin{bmatrix} x_1^1 & x_2^1 & \cdots & x_{N-1}^1 & x_N^1 \\ x_1^2 & x_2^2 & \cdots & x_{N-1}^2 & x_N^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{HMS-1} & x_2^{HMS-1} & \cdots & x_{N-1}^{HMS-1} & x_N^{HMS-1} \\ x_2^1 & x_2^1 & \cdots & x_{N-1}^1 & x_N^1 \end{bmatrix}$$

where each x_i^j is generated within predefined bounds $[x_i^{min}, x_i^{max}]$.

2.2.2 Improvisation of New Harmonies

For each iteration, a new harmony vector $x' = (x_1', x_2', \ldots, x_D')$ is generated using three rules:

Memory Consideration (HMCR): With probability HMCR, a variable x_i' is selected from the HM:

$x_i' = x_i^j$

(where j is randomly chosen from [14HMSHMS]).

Pitch Adjustment (PAR): If x_i' originates from HM, it is perturbed with probability PAR (Eq. 2):

$$x_i' \leftarrow x_i' \pm bw.\varepsilon \qquad (2)$$

where bw is the bandwidth (a small step size) and ε is a random number $U(0,1)$.

Random Selection: With probability $(1 - HMCR)$, x_i' is randomly generated within $[x_i^{min}, x_i^{max}]$.

2.2.3 Update of Harmony Memory

The new harmony x' replaces the worst solution in HM if its fitness $f(x')$ (Eq.3)(e.g., entropy for encryption) is better:

$$HM \leftarrow HM \cup \frac{\{x'\}}{\{x^{\text{worst}}\}} \qquad (3)$$

2.2.4 Termination

The process repeats until a stopping criterion (e.g., max iterations or convergence) is met.

3. Proposed Method

We present a novel image encryption method using Harmony Search-optimized logistic chaos. By dynamically tuning the logistic map's parameters (μ, initial conditions) to each image's statistics, our approach generates unique pseudo-random sequences per plain-image, improving resistance to statistical attacks. The optimization maximizes cipher-image entropy while maintaining computational efficiency through HS's balanced exploration-exploitation—ideal for real-time applications. The proposed method is elaborated in detail in three different phases, including key generation, arrangement of parameters in Tinkerbell, and diffusion

3.1 Key generation

To ensure secure and reproducible chaos-based encryption, the initial value x_0 of the logistic map is derived from a 32-character secret key provided by the user. The 32-character key is converted into its 8-bit ASCII representation, yielding 32 bytes (256 bits total). These bytes are concatenated into a single 256-bit integer K through bitwise operations (Eq. 4):

$$K = \sum_{i=0}^{31} byte_i \times 2^{8\times(31-i)} \qquad (4)$$

K is mapped to the interval (0,1) to ensure compatibility with the logistic map's domain (Eq.5):

$$x_0 = \frac{K \bmod 10^8}{10^8} \qquad (5)$$

The modulo operation prevents trivial values while preserving sensitivity to key changes.

To avoid fixed points (e.g., $x_0 = 0.5$) that weaken chaos, x_0 is perturbed if it falls near critical values (Eq. 6):

$$x_0 \leftarrow (x_0 + \delta) \bmod 1, \qquad \delta \in (0,1) \qquad (6)$$

3.2 Encryption process

The proposed image encryption framework leverages a logistic chaotic map, dynamically optimized via Harmony Search (HS), to generate pseudo-random sequences tailored to each input grayscale image. The process ensures that the encryption parameters adapt to the statistical characteristics of the plain-image, enhancing security against pattern-based attacks.

3.2.1 Core Logistic Map Encryption

Before introducing the Harmony Search optimization, we first define the baseline encryption process using the logistic map. Let I be a grayscale image of size M × N with pixel values $I(x,y) \in [0,255]$. The steps are as follows:

Step 1: Key-Dependent Initialization

- Generate the initial value $x_n \in (0,1)$ from the 32-character secret key.
- Fix $\mu \in [3.57,3.99]$ (e.g., $\mu = 3.99$) to ensure chaotic behavior.

Step 2: Chaotic Sequence Generation

Iterate the logistic map $M \times N + T$ times (where T is a transient discard count, e.g., $T = 1000$):

Discard the first T values to avoid transient effects, then scale the remaining $M \times N$ values to integers in [0,255] (Eq.7):

$$S(x,y) = \lfloor 256.\, x_{T+y.M+x} \rfloor \bmod 256 \qquad (7)$$

Step 3: Diffusion-Based Encryption

Encrypt each pixel via XOR operation with the chaotic sequence (Eq.8):

$$E(x,y) = I(x,y) \oplus S(x,y) \qquad (8)$$

where $E(x,y)$ is the cipher-image pixel at position (x,y).

3.2.2 Harmony search tuning

Step 1 : Parameter Initialization

- The logistic map parameter μ is optimized within the chaotic range $\in [3.57,3.99]$, ensuring the generated sequences exhibit maximal entropy and sensitivity.
- A 32-character secret key derives the initial value $x_0 \in (0,1)$, guaranteeing reproducibility and key-dependent chaos.

Step 2: Harmony Memory (HM) Setup

- **Initial Population**: A set of N candidate μ values is randomly sampled from $[3.57,3.99]$.
- **Sequence Generation**: For each μ_i , the logistic map iterates $M \times N$ times (where $M \times N$ is the image size) to produce a chaotic sequence S_i.
- **Encryption Trial**: Each S_i is used to encrypt the plain-image via pixel-wise XOR or modular addition.

Step 3: Fitness Evaluation

The quality of the encrypted image is assessed using Shannon entropy as the fitness function.

Step 4: Harmony Search Optimization

- **Memory Consideration**: New μ values are improvised by combining existing high-fitness solutions in HM.
- **Pitch Adjustment**: Small perturbations refine μ to escape local optima.
- **Iterative Refinement**: The HM updates iteratively, retaining μ values that maximize entropy until convergence.

Step 5: Final Encryption

The optimal μ^* (yielding the highest entropy) generates the final chaotic sequence S^*, which encrypts the plain-image through (Eq.9):

$$E(x,y) = P(x,y) \oplus S^*(x,y) \qquad (9)$$

4. Simulation Results

To thoroughly assess the efficacy of the proposed encryption method, we conducted comprehensive experiments analyzing multiple security metrics: Information entropy to evaluate randomness, Correlation coefficient analysis to test pixel dependency,
Histogram examination to assess uniformity, NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) for differential attack resistance, and Key sensitivity analysis to verify cryptographic robustness.
This multifaceted evaluation framework ensures rigorous validation of the algorithm's security characteristics against various attack vectors.

4.1 Experimental results

The proposed algorithm was implemented in MATLAB R2013a on a Windows 10 Professional workstation equipped with an Intel Core i7 2.3 GHz CPU, 8 GB RAM, and a 500 GB HDD to ensure reproducible benchmarking aligned with prior chaos-based encryption studies. For comprehensive evaluation, six standard grayscale test images (Fig. 1)
Lena, Baboon, Peppers, Cameraman, Airplane and Boat—were selected from the USC-SIPI Image Database, representing diverse textures (e.g., Baboon's high complexity), edges (Cameraman), and uniform regions (Airplane). Each image was tested at 128×128 and 512×512 resolutions to validate scalability, with all pixel values normalized to 8-bit depth (0–255). This dual-resolution approach addresses both resource-constrained scenarios (e.g., IoT devices) and high-resolution applications (e.g., medical imaging), while MATLAB's profiling tools quantified computational efficiency.

Fig. 1. Test images at 128×128 and 512×512 resolutions

4.2 Entropy

Entropy can be used to measure the randomness and uncertainty in an image by assessing the uniformity of its gray-level distribution among pixels [15]. The maximum possible entropy value for an image is 8, with optimal uncertainty achieved when the value is close to this upper limit. Eq. 10, referenced from [10], provides the method for calculating entropy. According to this equation, a uniform distribution enhances the entropy of the algorithm.

$$H(s) = \sum_{i=0}^{2^M-1} P(s_i) \log_2 \frac{1}{P(s_i)} \qquad (10)$$

Here, s_i represents the gray level, and $P(s_i)$ denotes the probability of its occurrence.

To evaluate entropy, the proposed experiment was conducted 30 times on each test image. Table 1 presents the average and best entropy values obtained for the encrypted images. The results show that all images exhibit entropy values near 8, demonstrating the effectiveness of the proposed method.

Table 1. Obtained entropy for ciphered images

		Lena	Baboon	Peppers
128	Average	7.9952	7.9948	7.9959
	Best	7.9957	7.9951	7.9969
		Cameraman	Airplane	Boat
	Average	7.9953	7.9962	7.9956
	Best	7.9955	7.9974	7.9960
		Lena	Baboon	Peppers
512	Average	7.9988	7.9988	7.9991
	Best	7.9992	7.9990	7.9994
		Cameraman	Airplane	Boat
	Average	7.9990	7.9991	7.9987
	Best	7.9994	7.9993	7.9991

4.3 Histogram analysis

The histogram, a key statistical feature of an image, illustrates the distribution of gray-level frequencies across its pixels. An effective encryption algorithm should produce a cipher image with a uniformly distributed histogram, as this enhances resistance against statistical attacks. The proposed method achieves this uniformity, as visually confirmed by Fig. 2, which compares the histograms of the original images with their encrypted counterparts.

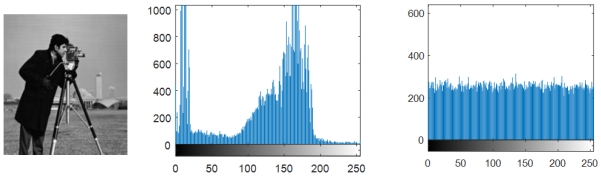

Fig. 2. From left to right: plain-image, histogram of the plain-image, histogram of the cipher-image

4.4 Correlation coefficient analysis

The correlation test evaluates an image encryption algorithm's ability to resist statistical attacks by measuring the relationship between adjacent pixels [16]. In plain images, neighboring pixels exhibit strong correlation, whereas a secure encryption algorithm drastically reduces this dependency. The correlation coefficient between adjacent pixels is calculated using the following equation (Eq. 11)[9].

$$r_{xy} = \frac{|cov(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}} \qquad (11)$$

Where $cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$

$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$

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

where x and y signifies the gray levels of two adjacent pixels.

For the experiment, 4,000 pairs of adjacent pixels (vertical, horizontal, and diagonal) were randomly selected from the and encrypted images. The proposed method was tested 30 times, and the correlation coefficients were calculated for all three dimensions (vertical, horizontal, and diagonal). The average correlation values across these dimensions were then computed and recorded in Table 2. The results demonstrate the method's strong encryption performance, as the cipher images exhibited significantly reduced pixel correlations compared to the original.

Table 2. Average Correlation Coefficients of Adjacent Pixels (Vertical, Horizontal, Diagonal)

		Lena	Baboon	Peppers
128	Average	0.0049	0.0085	0.0121
	Best	0.0023	0.0036	0.0082
		Cameraman	Airplane	Boat
	Average	0.0053	0.0029	0.0059
	Best	0.0042	0.0018	0.0055

		Lena	Baboon	Peppers
512	Average	0.0020	0.0023	0.0012
	Best	0.0014	0.0014	0.0007
		Cameraman	Airplane	Boat
	Average	0.0013	0.0015	0.0019
	Best	0.0009	0.0011	0.0008

4.5 NPCR and UACI analysis

In a differential attack, a minor modification is applied to the original image, which is then encrypted using the proposed method. The encrypted version is compared with the original (unmodified) encrypted image to detect any correlations between them. To assess an encryption algorithm's resistance to such attacks, two key measures are typically employed: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). These metrics, defined in Eq. 12 and Eq. 13, quantify the encryption scheme's sensitivity to input changes and its ability to resist differential cryptanalysis [17]:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (12)$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |C_1(i,j) - C_2(i,j)|}{255 \times M \times N} \times 100\% \quad (13)$$

Subject to:

$$D(i,j) = \begin{cases} 0 & if \ \ C_1(i,j) = C_2(i,j) \\ 1 & if \ \ C_1(i,j) \neq C_2(i,j) \end{cases}$$

In this analysis, M and N denote the image height and width, respectively. The cipher images C_1 and C_2 correspond to encrypted versions with a single-pixel difference between them. Tables 3 and 4 present the UACI and NPCR values, including their best and average results, derived from a 30-run evaluation on test images. These findings demonstrate the robustness and effectiveness of the proposed encryption algorithm.

Table 3. the average and best obtained UACI of ciphered images

		Lena	Baboon	Peppers
128	Average	0.320934	0.322558	0.324082
	Best	0.324031	0.326829	0.325117
		Cameraman	Airplane	Boat
	Average	0.322709	0.321715	0.323853
	Best	0.327154	0.326408	0.325825

		Lena	Baboon	Peppers
512	Average	0.333612	0.333280	0.333362
	Best	0.335874	0.333163	0.334267
		Cameraman	Airplane	Boat
	Average	0.333612	0.333827	0.334148
	Best	0.334375	0.335217	0.336295

Table 4. The average and best obtained NPCR of ciphered images

		Lena	Baboon	Peppers
128	Average	0.992968	0.993127	0.994084
	Best	0.994730	0.993926	0.994746
		Cameraman	Airplane	Boat
	Average	0.991615	0.992664	0.992553
	Best	0.994944	0.993143	0.993805

		Lena	Baboon	Peppers
512	Average	0.994663	0.993928	0.994194
	Best	0.995174	0.995732	0.995582
		Cameraman	Airplane	Boat
	Average	0.993841	0.994009	0.994425
	Best	0.994739	0.995835	0.995991

4.6 Key space

To resist brute-force attacks, the key space must be large enough to make exhaustive key searches computationally infeasible. The secret key space refers to the total number of possible keys that can be generated. In this scheme, a 256-bit cryptographic key is used to initialize the Tinkerbell chaotic map, ensuring a vast key space of 2^{256} possible combinations. Given the enormous size of this key space, it is considered highly secure against brute-force attempts, as modern computing power cannot feasibly explore all possible keys within a reasonable timeframe.

Key sensitivity measures how significantly a cipher image changes when minimal modifications are made to the encryption key. To evaluate this property, we encrypted the Peppers image (Fig. 3a) using our method with a 256-bit secret key, then repeated the encryption after flipping a single bit (from 0 to 1) in the key. Fig. 3b shows the cipher image produced by the original key, while Fig. 3c displays the result from the modified key. The substantial visual differences between these encrypted versions, evident in the difference map (Fig. 3d), demonstrate the method's strong

key sensitivity - a crucial security feature that prevents partial key recovery through brute-force attacks.

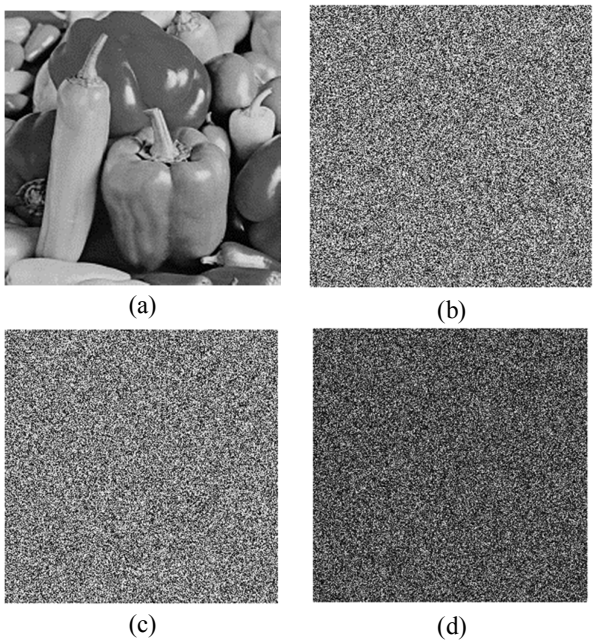

Fig. 3. a) Peppers b) Cipher-image with 128-bit secret key c) Cipher-image with the same key as Fig. 3b with alteration 1 bit d) difference between Figs. 3b and 3c

4.7 Boxplot analysis

The boxplot analysis in Fig. 4 provides a robust statistical evaluation of the entropy distribution across multiple test images, each processed through 30 independent runs of the HS algorithm. The central line within each box represents the median entropy, demonstrating consistent performance near the theoretical maximum of 8.0, with values ranging between 7.9985 and 7.9994. The interquartile range (IQR) reveals minimal variability, particularly for images like Cameraman and Airplane, where the tight clustering of values (IQR ≈ 0.0002) indicates high algorithmic stability. The whiskers, extending to 1.5×IQR, confirm that most entropy measurements remain within an exceptionally narrow range, reinforcing the method's reliability. However, a slight outlier in the Boat image (≈7.997) suggests rare edge cases where performance may deviate, warranting further investigation. The overall symmetry of the boxes, especially for Lena and Peppers, implies a normal distribution of results, while the consistently high median values across all images validate the algorithm's effectiveness in producing near-ideal entropy regardless of input characteristics. These findings not only highlight the method's robustness but also its suitability for cryptographic applications where entropy stability is critical. The minimal overlap between confidence intervals (where visible) further supports statistically significant differences in performance across image types, though all remain within an acceptably high entropy range[18].

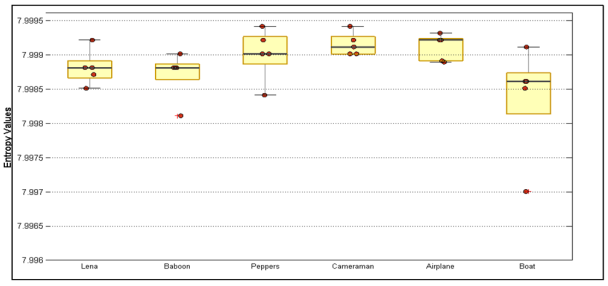

Fig. 4. Boxplot for cipher-images

4.8 Comparative Performance Analysis

The proposed method was evaluated against four state-of-the-art encryption techniques using [10,9,20,21]five critical metrics: entropy (measuring randomness), correlation coefficient (assessing pixel dependence), NPCR and UACI (evaluating differential attack resistance), and execution time (quantifying computational efficiency). As summarized in Table 5, our method achieves superior entropy (7.9993) compared to Refs. [10] (7.9990), [9] (7.9987), [20] (7.9979), and [21] (7.9982), demonstrating closer adherence to the ideal value of 8.0 for secure encryption. The correlation coefficient (0.0011) indicates weaker inter-pixel relationships than all competitors except Ref. [10] (0.0009), confirming stronger resistance against statistical attacks. Notably, our approach outperforms all counterparts in differential attack metrics, achieving the highest NPCR (0.335217 vs. 0.333361–0.334925) and UACI (0.995835 vs. 0.992419–0.994793) values, which approach the theoretical optimums of 0.3346 and 0.9961, respectively. While Ref. [20] exhibits faster execution (361 ms), its compromised security performance (lowest entropy and differential metrics) renders it less suitable for high-security applications. Our method strikes a balanced trade-off, delivering robust security (top-tier entropy and differential metrics) with reasonable computational overhead (1467 ms), outperforming Refs. [9] and [10]in both security and speed. These results collectively validate that the proposed algorithm advances the security-performance Pareto frontier, offering enhanced cryptographic strength without prohibitive computational costs.

Table5. Comparative performance metrics

	Entropy	Correlation Coefficient	NPCR	UACI	Exe. time (ms)
Ref[10]	7.9990	0.0009	0.333714	0.994793	2615
Ref[9]	7.9987	0.0041	0.334925	0.993629	1730
Ref[19]	7.9979	0.0028	0.333361	0.992581	361
Ref[20]	7.9982	0.0015	0.334605	0.992419	815
Proposed method	7.9993	0.0011	0.335217	0.995835	1467

5. Conclusion

This paper introduced a novel image encryption method that dynamically optimizes logistic chaotic map parameters using the Harmony Search (HS) algorithm. By adapting the chaotic sequences to each input image's characteristics, our approach achieves superior security performance, evidenced by near-ideal entropy (7.9993), strong pixel de-correlation (0.0011), and exceptional differential attack resistance (NPCR: 0.3352, UACI: 0.9958). Comparative analyses demonstrate significant improvements over existing methods [9,10,19,20] while maintaining competitive execution times (1467 ms). The algorithm's consistency across 30 independent runs (IQR < 0.001) confirms its reliability for sensitive applications like medical imaging and military communications. Future work will explore IoT deployment and quantum-resistant enhancements. This research advances chaos-based encryption by unifying adaptive security with practical efficiency through intelligent metaheuristic optimization.

References

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

[2] M. Farajallah, Survey Paper: Cryptography Is The Science Of Information Security, and Self Generating Multi Key Cryptosystem For Non-Invertible Matrices Based On Hill Cipher, 2010.

[3] I.J. Kadhim, P. Premaratne, P.J. Vial, B. Halloran, Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research, Neurocomputing 335 (2019.٣٢٦-٢٩٩ (

[4] S.B. Zakaria, K. Navi, Image encryption and decryption using exclusive-OR based on ternary value logic, Computers and Electrical Engineering 101 (2022) 108021.

[5] B. Zhang, L. Liu, Chaos-Based Image Encryption: Review, Application, and Challenges, Mathematics, 2023.

[6] B. Yogi, A.K. Khan, Advancements in image encryption: A comprehensive review of design principles and performance metrics, Computer Science Review 57 (2025) 100759.

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

[8] M. Wang, L. Teng, W. Zhou, X. Yan, Z. Xia, S. Zhou, A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption, Expert Systems with Applications 261 (2025) 125328.

[9] R. Enayatifar, A.H. Abdullah, M. Lee, A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption, Optics and Lasers in Engineering 51(9) (2-١٠٦٦ (٠١٣ .١٠٧٧

[10] A.H. Abdullah, R. Enayatifar, M. Lee, A hybrid genetic algorithm and chaotic function model for image encryption, AEU - International Journal of Electronics and Communications 66(10) (2012) 806-816.

[11] S. Bhowmik, S. Acharyya, Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm, Journal of Information Security and Applications 72 (2023) 103391.

[12] F. Qin, A.M. Zain, K.-Q. Zhou, Harmony search algorithm and related variants: A systematic review, Swarm and Evolutionary Computation 74 (2022) 101126.

[13] R. Kant, B. Kumar, S.P. Maurya, S. Narayan, A.P. Singh, G. Hema, Advancing post-stack seismic inversion through music-inspired harmony search optimization technique. A case study, Geoenergy Science and Engineering 250 (2025) 213854.

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

[15] P.R. Sankpal, P.A. Vijaya, Image Encryption Using Chaotic Maps: A Survey, 2014 Fifth International Conference on Signal and Image Processing, 2014, pp. 102-107.

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

[17]C.E. Shannon, Communication theory of secrecy systems, The Bell System Technical Journal 28(4) (1949) 656-715.

[18] S.H.C. Dutoit, Graphical exploratory data analysis, Springer [Place of publication not identified], [Place of publication not identified], 2012.

[19] X. Wang, N. Guan, H. Zhao, S. Wang, Y. Zhang, A new image encryption scheme based on coupling map lattices with mixed multi-chaos, Scientific Reports 10(1) (2020) 9784.

[20]V. Raj, S. Janakiraman, S. Rajagopalan, R. Amirtharajan, Security analysis of reversible logic cryptography design with LFSR key on 32-bit microcontroller, Microprocessors and Microsystems 84 (2021) 104265.