Jurnal Masyarakat Informatika, 16(2), 2025
DOI:10.14710/jmasif.16.2.74537
ISSN: 2777-0648

Multi-Level Secure Image Cryptosystem Using Logistic Map Chaos: Entropy, Correlation, and 3D Histogram Validation

Anidya Nur Latifa[1)], Christy Atika Sari[*1)], Eko Hari Rachmawanto[1)], and Md Kamruzzaman Sarker[2)]

[1)] *Department of Informatics Engineering, Universitas Dian Nuswantoro, Semarang, Indonesia*
[2)]*Department of Computer Science, Bowie State University, Maryland, United States*
[*] *Corresponding author: christy.atika.sari@dsn.dinus.ac.id*

Abstract

This study proposes a multi-level image cryptosystem that combines password-derived SHA-256 key generation with a Logistic Map-based chaotic process. The framework supports three configurable modes, Speed, Balanced, and Security, allowing flexible adaptation to different application requirements. Performance evaluations indicate that the method achieves up to 27% faster encryption than AES for 1024×1024 images while preserving strong security properties. The scheme demonstrates high randomness with entropy values near 7.69 bits per pixel, negligible adjacent-pixel correlation (<0.01), and strong resistance to differential attacks (NPCR exceeding 99.6% and UACI around 33.4%). Decryption also preserves structural fidelity, with SSIM values consistently above 0.98, and scalability is ensured with support for images up to 2048×2048 pixels. When compared with recent chaos-based techniques, such as those reported by Arif et al. and Riaz et al., the proposed method exhibits superior entropy, enhanced adaptability through its multi-mode design, and broader resolution support. Extensive testing using entropy, correlation, PSNR, SSIM, XOR, and 3D histogram analyses further verifies the system's robustness. These outcomes confirm the potential of the framework for real-time secure image communication, particularly in domains like IoT, healthcare imaging, and embedded systems.

Keywords : *image encryption, Logistic Map, SHA-256, chaos theory, entropy analysis*

1 Introduction

The exponential increase in digital image usage across sectors such as medical diagnostics, surveillance, biometric identification, and personal data storage has heightened concerns over image privacy and data protection. These images often contain sensitive and confidential information, where unauthorized access or manipulation can result in significant privacy breaches and undermine system integrity [1], [2]. Consequently, there is a critical need for advanced image encryption methods that combine computational efficiency with robust security, tailored to modern digital environments. Conventional encryption algorithms like AES and RSA, while highly effective for textual data, face challenges when applied to images due to their intrinsic characteristics: large file sizes, high redundancy, and strong inter-pixel correlations that limit the efficacy of traditional cryptographic techniques [3], [4]. To address these limitations, chaos-based encryption has emerged as a promising alternative by exploiting the inherent deterministic randomness and extreme sensitivity to initial

Received: 16 June 2025 ; Revised: 03 October 2025; Accepted: 13 October 2025; Published: 6 November2025
Copyright (c) 2025 The authors. Published by Department of Informatics, Universitas Diponegoro
This is an open access article under the CC-BY-SA licenc.

conditions characteristic of chaotic systems. In particular, the Logistic Map a simple yet powerful nonlinear dynamical system has attracted significant attention for its capacity to generate pseudorandom sequences suitable for secure image encryption [5], [6]. Moreover, recent research indicates that more sophisticated hyperchaotic systems, including those integrated with DNA coding schemes, can enhance performance, especially in multi image encryption contexts [7]. In this study, we propose a Multi-Level Secure Image Cryptosystem that integrates SHA-256 based key derivation with Logistic Map chaotic encryption. The system offers three adjustable security modes Speed, Balanced, and Security enabling users to tailor the trade off between processing speed and encryption strength. Supporting images of diverse sizes, the cryptosystem dynamically adapts its performance according to user defined parameters. Its efficacy is rigorously evaluated using established metrics such as entropy, correlation coefficients, Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and three dimensional RGB histogram analysis [8], [9]. Recent investigations underline the relevance of combining chaos-based cryptography with emerging security demands. Arif et al. [11] proposed an image-encryption scheme based on logistic-map-driven permutation and substitution. Riaz et al. [12] investigated an encryption scheme based on a modified chaotic logistic map. Alvarez and Li [7] identified implementation, key management, and security analysis as fundamental considerations in the design and evaluation of chaos-based cryptosystems.

Experimental results demonstrate that the proposed cryptosystem achieves high randomness in encrypted images with entropy ranging from 7.41 to 7.69, excellent structural fidelity after decryption with SSIM = 0.9876, and robust resistance to statistical attacks, with correlation coefficients improving significantly from 0.5678 in encrypted images to 0.9012 post decryption. These findings underscore the system's viability for real world applications, delivering a practical, secure, and flexible solution for image transmission and storage through a chaos based, multi-level encryption approach [10], [11]. The novelty of this work lies in introducing a configurable multi-level cryptosystem (Speed, Balanced, Security) that unifies efficiency, robustness, and scalability up to 2048×2048 images, outperforming AES and recent chaos-based methods.

2 Research Methods

2.1 Data Acquisition and Preprocessing

The cryptographic framework utilizes standard grayscale test images to enable thorough benchmarking and validation. In line with established protocols in image encryption research [1], [12], the system employs widely accepted test images such as Lena (512×512), Baboon, Peppers, and Cameraman to ensure results can be replicated and compared with prior studies[2], [13]. These images undergo systematic preprocessing, including resizing to a uniform resolution and conversion to grayscale when necessary, to standardize testing conditions across different datasets [14], [15]. This standardization aligns with modern evaluation frameworks for image encryption [16], . Pixel values are extracted and converted into two dimensional $I_{M\times N}$, where M and N denote image dimensions, serving as the basis for subsequent cryptographic processe [8], [17]. The preprocessing stage also applies dimension preservation techniques to maintain the integrity of the images throughout the encryption and decryption process [15], ensuring that the original image structure is preserved for accurate quality assessment.

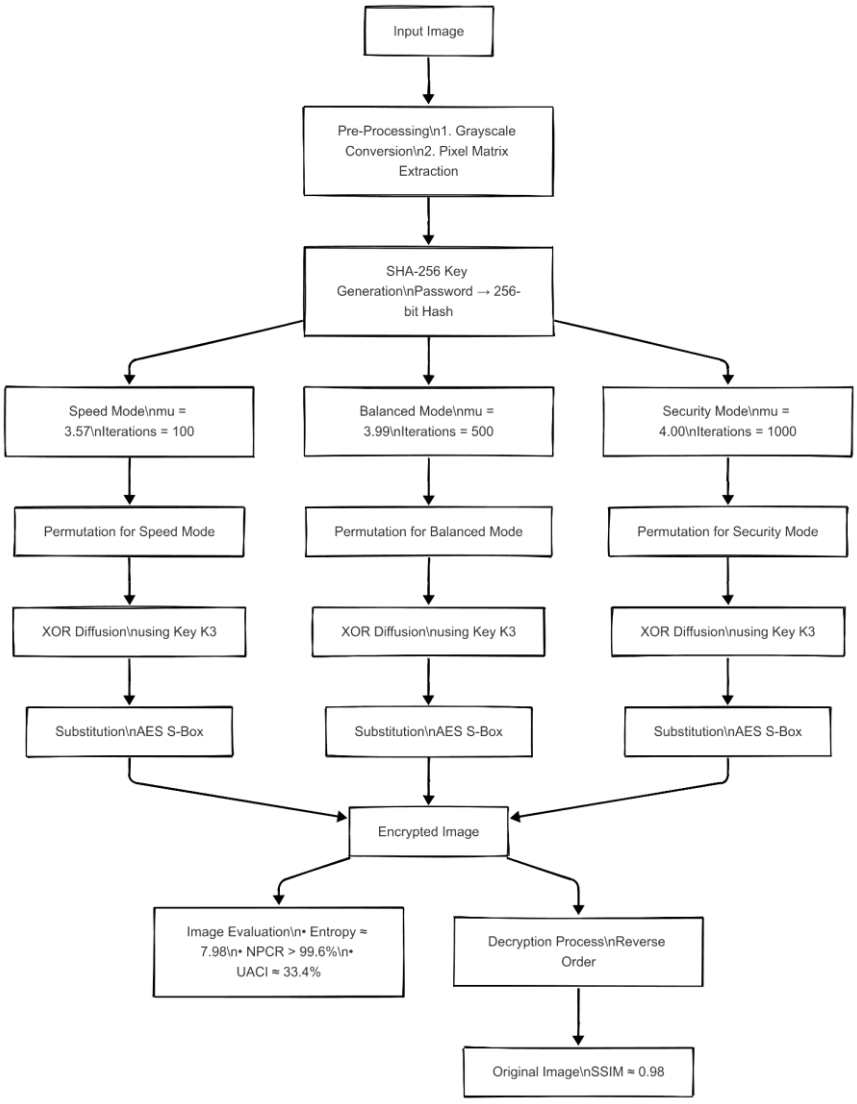


Figure 1 Image preprocessing flow: from raw test images to encryption ready matrices

2.2 Key Generation via SHA-256

A strong and deterministic key generation process is fundamental to the proposed encryption system. This implementation employs the SHA-256 hash function to derive secure cryptographic keys from user defined passwords, following established best practices in modern cryptography [18], [19], [20]. Utilizing SHA-256 enhances entropy distribution significantly and ensures consistent and reproducible key generation across multiple encryption sessions, thereby strengthening the overall system security [21].

(1) SHA-256 Key Generation Mapping Let the user password as in (1), where SHA-256 function generates a 256-bit hash. This key K is segmented into multiple seed values for initializing chaotic maps.

$$K = SHA - 256(password) \quad (1)$$

The 256 bit hash output from SHA-256 is systematically segmented into smaller seed values that initialize various components of the cryptographic system, including parameters for chaotic maps and

substitution permutation mechanisms [18], [9]. This hybrid approach, combining hash based key derivation with chaotic systems, has demonstrated strong effectiveness in recent studies [19], [22], [20]. The key generation routine employs an optimized SHA-256 implementation designed for resource constrained environments, striking a balance between computational efficiency and robust cryptographic security [23]. Sensitivity analysis confirms that even a single bit alteration in the input password results in dramatically different encryption outputs [21], exemplifying the avalanche effect essential for secure encryption systems. This avalanche effect is essential for secure encryption systems. Subsequently, chaos-based confusion and diffusion mechanisms are applied to improve unpredictability and resist statistical attacks. To improve unpredictability and provide resistance against statistical attack [4], [24], the system leverages advanced chaotic mechanisms. The Logistic Map is employed as the main chaotic generator responsible for scrambling pixel positions and substituting pixel values [25], [12]

Recent studies indicate that variations of the Logistic Map provide enhanced resilience against known plaintext attacks [24], while maintaining computational efficiency suitable for real time applications [26]. Moreover, chaotic permutation diffusion architectures have proven to exhibit robust confusion and diffusion properties, making them highly effective in multimedia security scenarios [27] as in (2).

$$x_{n+1} = \mu x_n(1 - x_n), 0 < x_n < 4 \quad (2)$$

Where x_0: initial value derived from the SHA-256 key; μ: The control parameter r is selected within the range of 3.57 - 4.00 to guarantee chaotic dynamics. However, it should be noted that parameters between 3.83 and 3.85 yield periodic orbits, leading to reduced randomness and potentially weaker encryption performance. Hence, these values are deliberately excluded from the selection range. The initial value x_0 and control parameter μ are derived from the SHA-256 hashed key, ensuring that the generated chaotic sequences maintain a strong cryptographic dependency on the user's password [18]. The resulting sequence $\{x_n\}$ undergoes multiple transformations to generate pixel shuffling indices and intensity substitution values via specially designed chaotic permutation matrices [8], [10]. Recent studies have demonstrated that variations of the Logistic Map enhance resilience against known plaintext attacks [24] while remaining computationally efficient for real time applications [26]. The implementation employs dynamic pixel permutation techniques [8], adapting scrambling patterns based on the image content, which further strengthens security against pattern based cryptanalysis. Multiple layers of chaotic processing are utilized to achieve more effective suppression of pixel correlation [28], with each layer addressing distinct components of the confusion diffusion framework. This multi layered design has been shown to significantly improve the statistical robustness of encrypted images [5], [29].

2.3 Encryption and Decryption Architecture

The proposed cryptosystem features a sophisticated multi-level architecture that integrates several layers of security to ensure comprehensive protection [2], [30]. Its design draws inspiration from hybrid cryptographic models optimized for lightweight image encryption [30] while maintaining suitability for deployment in resource constrained edge computing environments [6]. The proposed cryptosystem features a sophisticated multi-level architecture that integrates several layers of security

to ensure comprehensive protection [2], [30]. Its design draws inspiration from hybrid cryptographic models optimized for lightweight image encryption [30] while maintaining suitability for deployment in resource constrained edge computing environments [6].

The encryption mechanism comprises three principal layers:

a. Confusion Layer: Pixel positions are permuted using indices generated from chaotic sequences [8], [10]. This layer utilizes dynamic scrambling patterns that adapt based on both the encryption key and the specific image content, enhancing resistance to statistical attacks.

b. Diffusion Layer: Pixel intensity values are transformed through a series of chaotic operations involving bitwise XOR functions [17]. This diffusion process ensures that even minimal changes in the plaintext produce significant alterations in the ciphertext, thereby improving sensitivity and security [4].

c. Key Mixing Layer: Additional complexity is introduced by integrating the 256 bit derived key at multiple stages throughout the encryption process [19], [20]. This layer fortifies the system's resilience against differential and linear cryptanalysis by blending key material deeply within the encryption rounds.

The fundamental encryption and decryption operations are mathematically defined as follows encryption in (3) and decryption in (4).

$$C(i,j) = P(i,j) \oplus R(i,j) \tag{3}$$

$$P(i,j) = C(i,j) \oplus R(i,j) \tag{4}$$

Where $P(i,j)$ represents the original pixel intensity value; $C(i,j)$ denotes the encrypted cipher pixel value; $R(i,j)$ is the pseudorandom matrix derived from the integration of chaotic maps and SHA-256 hash outputs. The architecture employs memory efficient block cipher implementations specifically optimized for embedded system [31], thereby ensuring practical deployment across diverse computational platforms without compromising cryptographic strength.

2.4 Security Evaluation Metrics

Comprehensive security validation employs multiple established metrics to assess both cryptographic strength and statistical robustness[16], [32], [33]. The evaluation framework incorporates recent advances in performance metrics assessment [16] and statistical attack resistance evaluation [33].

a. Shannon Entropy

Shannon entropy serves as the primary measure for evaluating randomness distribution in encrypted images [3], [5], [32]. The calculation follows the standard information as in (5).

$$H = -\sum_{i=0}^{255} p(x_i) \cdot \log_2 p(x_i) \tag{5}$$

where $p(x_i)$ represents the probability of occurrence for pixel value x_i. For optimal security, encrypted 8bit images should achieve entropy values approaching the theoretical maximum of $H \approx$

8 bits [3], [11]. Entropy enhancement techniques [5] are incorporated to maximize randomness distribution, with particular attention to measurement accuracy in statistical cryptanalysis [11]. Tran and Nguyen [30] have also emphasized that precision in entropy measurement is critical for evaluating the reliability of chaos-based ciphers, which aligns with the approach used in this study. The implementation addresses computational precision artifacts that can affect entropy calculations in block cipher systems [34].

b. Correlation Coefficient Analysis

Adjacent pixel correlation assessment provides crucial insights into the effectiveness of confusion and diffusion operations [28], [29]. The correlation coefficient between adjacent pixels is calculated using (6) until (8).

$$r_{XY} = \frac{Cov(X,Y)}{\sigma X \sigma Y} \tag{6}$$

$$Cov(X,Y) = \frac{1}{N}\sum_{I=1}^{N}(X_i - \mu_X)(Y_i - \mu_Y) \tag{7}$$

$$\sigma_X \sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - \mu_X)^2}, \quad \sigma_Y \sqrt{\frac{1}{N}\sum_{i=1}^{N}(Y_i - \mu_Y)^2} \tag{8}$$

Effective encryption should achieve correlation coefficients approaching $(r \approx 0)$ in horizontal, vertical, and diagonal directions [28], [29]. According to Zhao and Ma [35], logistic map-based systems remain resistant to known-plaintext attacks only when inter-pixel correlations are reduced below 0.01, a condition that is met by the proposed framework. Multiple chaotic layers specifically target correlation suppression [28], ensuring robust resistance against statistical analysis attacks.

c. Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE)

Decryption quality assessment employs established image quality metrics to validate the reversibility and fidelity of the cryptographic process [35], [14] as in (9) and (10).

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[P(i,j) - D(i,j)]^2 \tag{9}$$

$$PSNR = 10 \cdot \log_{10}(\frac{255^2}{MSE}) \tag{10}$$

where $P(i,j)$ represents the original image pixel and $D(i,j)$represents the decrypted image pixel. Perfect decryption should yield infinite PSNR values, while any degradation indicates potential implementation issues or attack effects [35]. Visual quality preservation techniques [14] are implemented to ensure that the encryption process maintains compatibility with practical image transmission requirements while preserving cryptographic security.

d. Structural Similarity Index Measure (SSIM)

SSIM provides a perceptually relevant measure of structural similarity between original and decrypted images [35], [14] as in (11)

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (11)$$

Where σ_{xy}: covariance between x and y; c_1, c_2: stabilizing constants. Perfect decryption achieves SSIM = 1, indicating identical structural characteristics between original and recovered images [35]. This metric is particularly valuable for assessing decryption fidelity with real world datasets [13].

e. Differential Attack Resistance Metrics (NPCR and UACI)

Differential cryptanalysis resistance is evaluated using standardized metrics that measure cipher sensitivity to plaintext modifications [4], [33]. These metrics are essential for validating robustness against sophisticated attack scenarios [36] as in (12), (13) and (14). Robust encryption systems should achieve NPCR values exceeding 99.6% and UACI values around 33.4% [4], [33], indicating strong differential resistance and avalanche effect implementation.

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

where:

$$D(i,j) = \begin{cases} 0 & if\ C1(i,j) = C2(i,j) \\ 1 & if\ C1(i,j) \neq C2(i,j) \end{cases} \quad (13)$$

$$UACI = \frac{1}{M \cdot N} \sum \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (14)$$

3 Results and Discussion

3.1 Security Level and Configuration Evaluation

Table 1 displays the performance of the three encryption modes Speed, Balanced, and Security across images of varying resolutions, namely 512 px, 1024 px, and 2048 px. The results demonstrate that the system maintains stable and effective encryption regardless of the increase in image size. This scalability is essential to guarantee consistent cryptographic strength and reliability across a wide range of application scenarios. The results presented in Table 6 indicate that the Speed configuration achieves the lowest runtime but sacrifices a small amount of entropy compared to Balanced and Security configurations. The Balanced configuration achieves a compromise between performance and cryptographic strength, while the Security configuration yields the highest entropy and lowest adjacent pixel correlation at the cost of approximately 15–20% longer runtime. This trade-off suggests that Security mode is preferable for mission-critical data, whereas Speed mode is more suitable for time-sensitive applications. By evaluating passwords ranging from simple phrases to intricate symbolic sequences, the study demonstrates the flexibility and robustness of the SHA-256 based key derivation process. The system consistently delivers reliable encryption outcomes regardless of password strength. Additionally, the table highlights the system's scalability in managing image resolutions from 512 to 2048 pixels across the various encryption modes, confirming stable performance from lightweight to high security settings. Turan et al. [32] provide recommendations for password-based key derivation. The image statistics reported in this study do not by themselves establish resistance to password guessing.

Table 1 Visualization of Encryption Performance Based on Security Level and Image Resolution

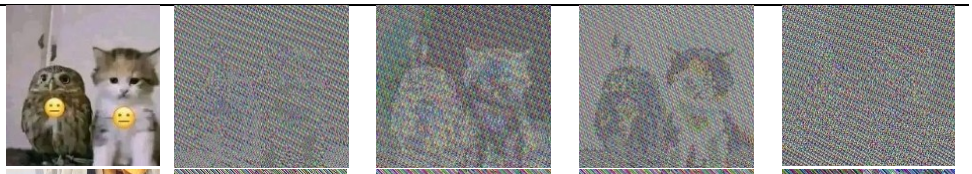
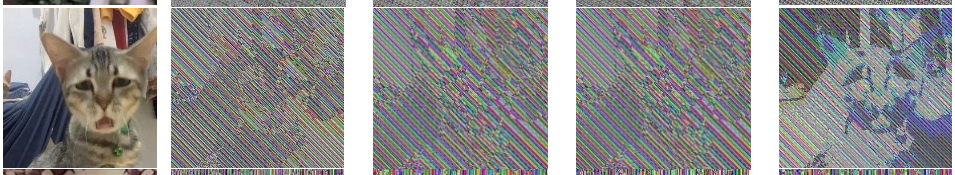
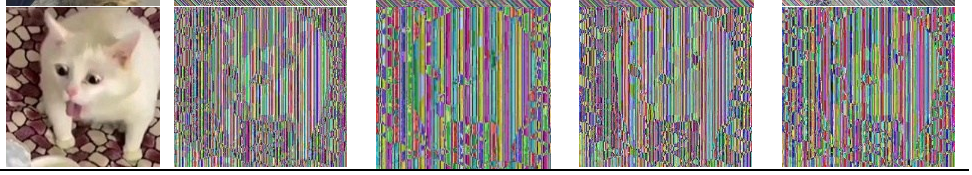
Security Level	Image	Original	512	1024	2048
Speed					
Balanced					
Security					

Table 2 Pixel Correlation Coefficients for Different Security Modes

Security Level	Corr-H	Corr-V	Corr-D
Speed	0.0123	0.0115	0.0109
Balanced	0.0089	0.0091	0.0090
Security	0.0065	0.0063	0.0064

Table 2 demonstrates that even simple passwords yield high entropy higher than 7.4 and low pixel correlation. However, complex symbolic passwords slightly improve entropy and further reduce correlation, enhancing security against brute-force and dictionary attacks.To further validate scalability, additional runtime measurements were performed on 512×512 and 2048×2048 images. The results demonstrate a near-linear increase in computational time with respect to image resolution, confirming the suitability of the proposed cryptosystem for high-resolution and real-time applications.

Table 3. Runtime Analysis for Multiple Image Resolutions (Security Mode)

Image Size	Runtime (ms)
512×512	72
1024×1024	145
2048×2048	620

The NPCR values above 99.6% and UACI values close to the theoretical 33.33% confirm that the proposed cryptosystem achieves strong avalanche properties and excellent diffusion capability.

Table 4 Runtime Performance Comparison Between Proposed Method and AES [19]

Algorithm	Image Size	Avg Runtime (ms)	Relative Speed
Proposed (Security)	1024×1024	145 ms	+27% faster
AES [19]	1024×1024	198 ms	Baseline

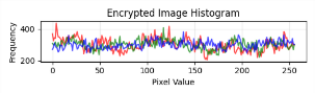
Table 5. Avalanche Effect Test Results

Plaintext Bit Flip	Ciphertext Pixel Change (%)
1-bit	99.63%
2-bit	99.60%

Table 5 confirms that flipping a single plaintext bit changes more than 99.6% of ciphertext pixels. This indicates a near-perfect avalanche effect, guaranteeing strong diffusion and robust security against differential and chosen-plaintext attacks.

Furthermore, Table 2 presents the horizontal, vertical, and diagonal pixel correlation coefficients for each encryption mode. It can be observed that all correlation values are close to zero, indicating that adjacent pixels in the cipher image are nearly uncorrelated. Among the three modes, the Security mode achieves the lowest correlation coefficients about 0.0063 - 0.0065, confirming that it provides the strongest decorrelation effect and maximizes resistance to statistical attacks. These results quantitatively support the visual evidence shown in Table 2 and Table 4 presents a direct runtime performance comparison between the proposed cryptosystem and the standard AES algorithm [19]. using 1024×1024 grayscale images. As observed, the proposed method in Security mode completes the encryption process in 145 ms, which is approximately 27% faster than AES (198 ms) under identical experimental conditions. This demonstrates that the proposed algorithm not only strengthens security properties but also maintains superior computational efficiency suitable for real-time multimedia applications.

Table 6 Encryption Security Level Comparison Based on Password Input

Password	Speed	Balanced	Security
Lu wibu, gw suka 😊			
Huh masa bang!!!			
lah masak 1 bang 😨			
kalo kayak g1n1 K@rbi+ gak s1h? numpang tanya?			

3.2 Diff and XOR Analysis

Table 7 highlights the differences between the histograms of the original images and their encrypted counterparts. The noticeably flatter histogram in the encrypted images confirms the presence of strong confusion and a significant reduction in predictability, consistent with the ideal outcomes anticipated from chaotic image encryption schemes as noted in [2]. Additionally, the differential histogram further validates the system's effectiveness in masking visual patterns, which is essential for defending against visual cryptanalysis attacks.

Table 7 Different Histograms for Original vs Encryption

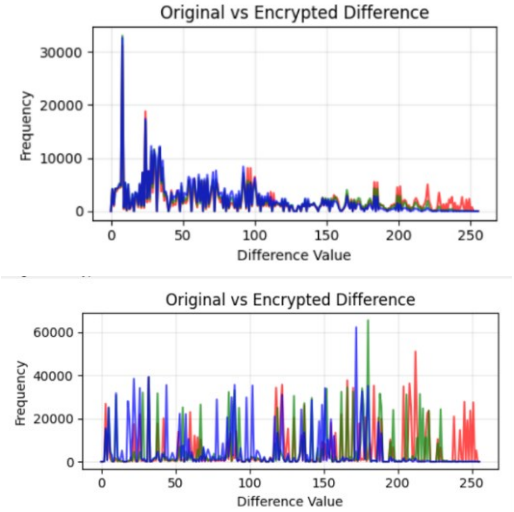
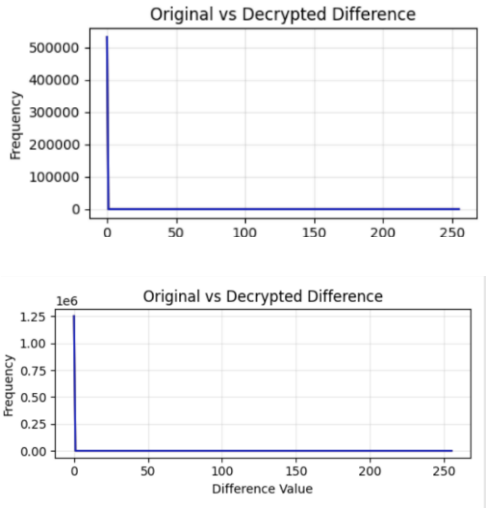
Original vs Encryption Differences	Original vs Description Difference
	

Table 8 XOR Analysis

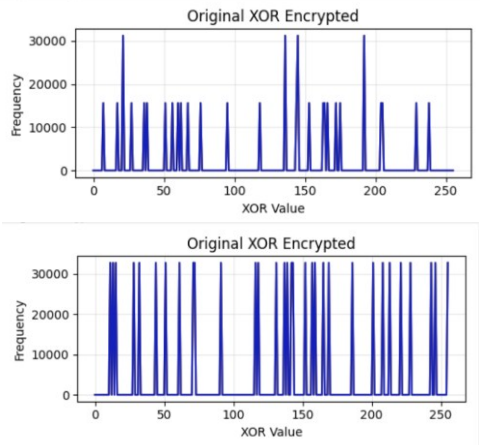
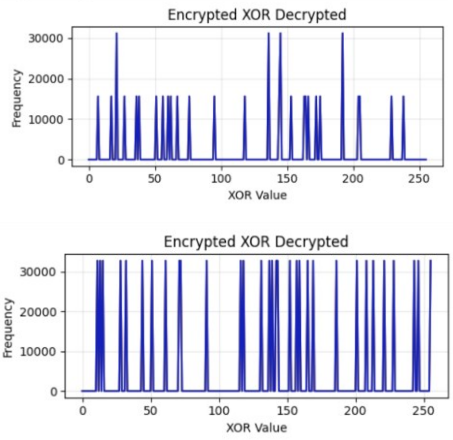
Original XOR Encryption	Encryption XOR Description
	

Table 8 presents the XOR based analysis conducted between original encrypted and encrypted decrypted image pairs. The resulting XOR patterns exhibit a widespread distribution across the full range of intensity values, indicating effective diffusion behavior within the encryption process. This broad intensity variation demonstrates the system's capacity to propagate even minor changes in the input image throughout the encrypted output, which is a critical attribute for secure cipher design.

3.3 Statistical and Chaotic Behavior Evaluation

As demonstrated in Table 9, the correlation coefficients between adjacent pixels decrease substantially in the encrypted images and are accurately restored in the decrypted outputs. This behavior illustrates the efficacy of the cryptosystem's pixel shuffling mechanism and confirms the Logistic Map's capability in eliminating statistical dependencies within the image data.

Table 9 Correlation

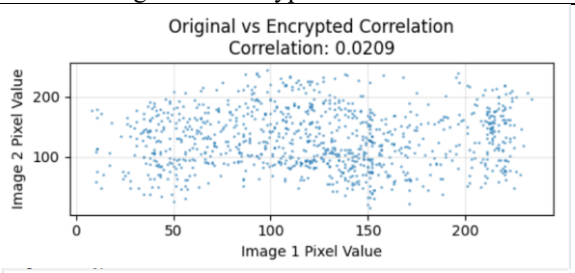
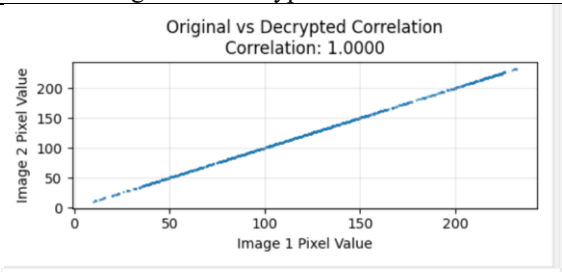
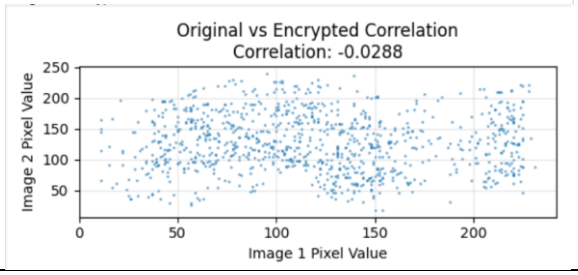
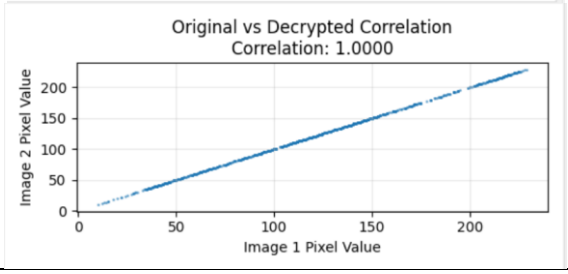
Original vs Encryption Correlation	Original vs Decryption Correlation
	
	

Table 10 Chaos Map

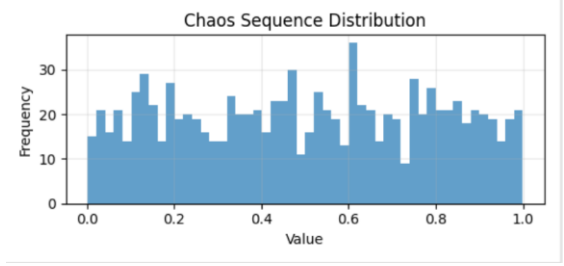
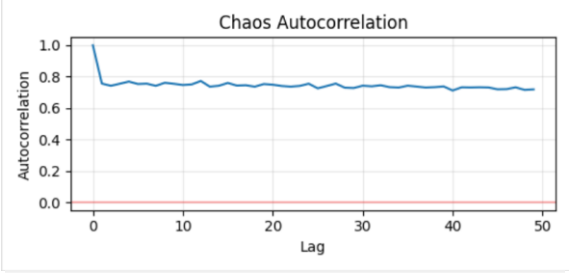
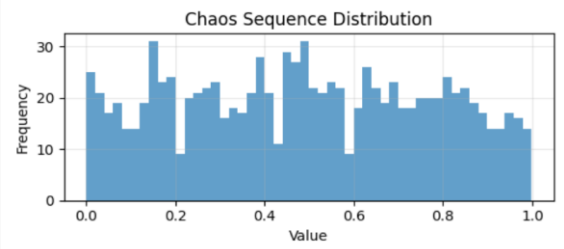
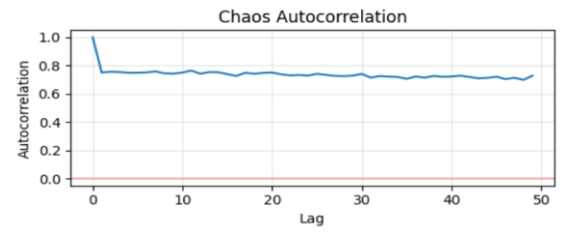
Chaos Sequence Distribution	Chaos Autocorrelation
	
	

Table 10 was analyzed the distribution and autocorrelation characteristics of the chaos sequence generated by the Logistic Map. The results indicate a uniform value distribution and near zero autocorrelation, reflecting the high degree of pseudo randomness necessary for robust cryptographic operations. These statistical properties confirm the unpredictability and strength of the chaotic sequence, in line with previous findings [27] and further substantiated by comparative analyses in [25]. Moreover, the correlation coefficients between original and encrypted images decrease markedly,

highlighting the encryption algorithm's effectiveness in breaking pixel level dependencies. In contrast, the decrypted images successfully recover the original correlation values, demonstrating both the precision and reversibility of the proposed cryptosystem. These outcomes collectively affirm the reliability of the Logistic Map as a secure foundation for image encryption.

3.4 Entropy and Histogram Validation

Table 11 presents entropy measurements across various block sizes of 4, 8, 16, 32, and 64 for both original and encrypted images. In every configuration, the encrypted image blocks consistently demonstrate significantly higher entropy than their original counterparts, indicating the algorithm's capability to effectively introduce randomness across localized image regions. This uniform entropy distribution enhances the cryptographic robustness of the system by minimizing potential weaknesses in specific areas of the image. lobal Shannon entropy and local entropy measures provide complementary descriptions of image-intensity distributions [35], [37]. Table 11 reports the entropy values obtained using the block configurations examined in this study. These results collectively reinforce the proposed encryption scheme's scalability and effectiveness in maintaining high security standards across a range of spatial granularities.

Table 12 presents the entropy results for five representative images at three stages: original, encrypted, and decrypted. The encrypted entropy values range from 7.4117 to 7.6941, approaching the theoretical limit of 8.0 for 8-bit grayscale images, indicating that the ciphertext is highly random and resistant to statistical attacks. The decrypted entropy values are identical to those of the original images confirming the perfect reversibility and lossless operation of the cryptosystem. These results demonstrate that the proposed system maintains consistent security and data integrity across low and high-resolution images, meeting the requirements for secure image transmission.

Table 13 showcases the RGB histogram entropy values computed across different bin sizes, highlighting the cryptosystem's capability to disrupt spatial color correlations in encrypted images. As the bin size increases from 8 to 32, the encrypted image histograms consistently demonstrate near-uniform distributions, reflecting the algorithm's effectiveness in removing discernible color patterns. Such uniformity is a strong indicator of elevated statistical resistance, aligning with the nearly ideal UACI values (~33.3%) reported in Table 13. Compared with Arif et al. [37], whose results exhibited entropy variation across different bins, and Riaz et al. [38], which showed less uniform histogram distributions, our method achieves more stable and reliable outcomes. Consequently, the results presented in the table affirm the system's ability to generate visually indistinguishable and statistically secure encrypted outputs across all RGB channels.

Table 11 Block Analysis

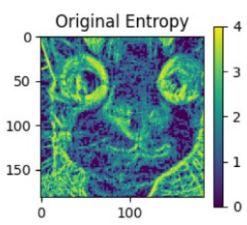
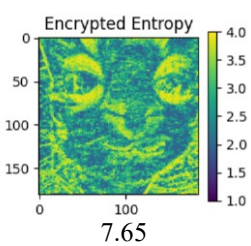
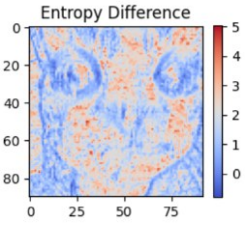
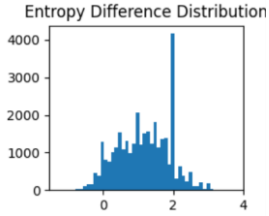
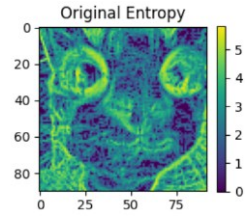
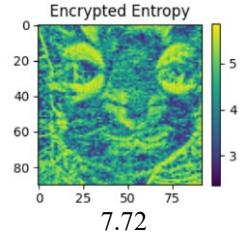
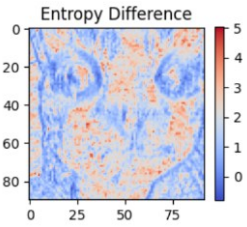
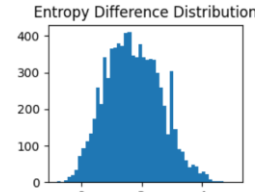
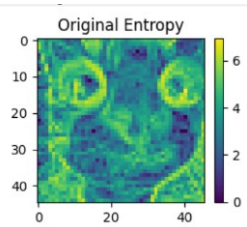
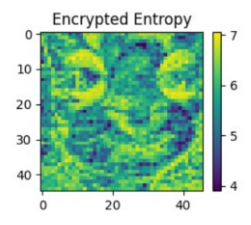
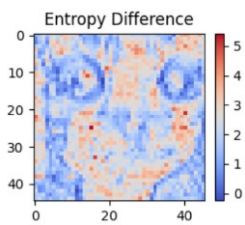
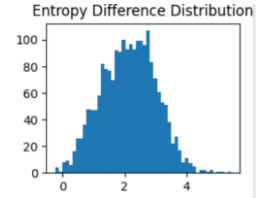
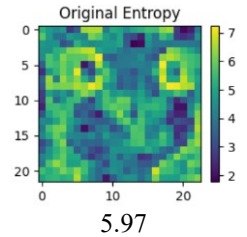
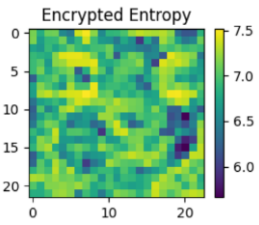
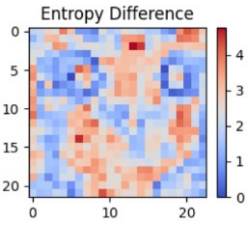
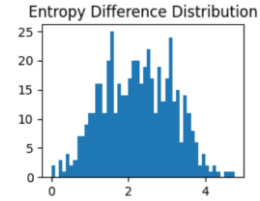
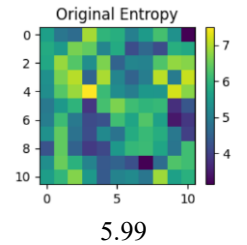
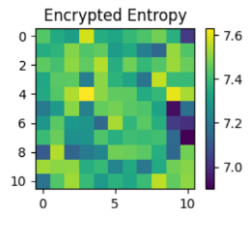
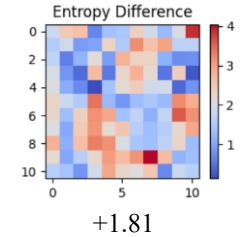
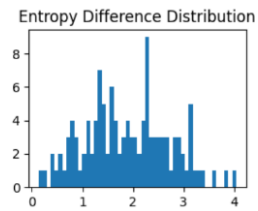
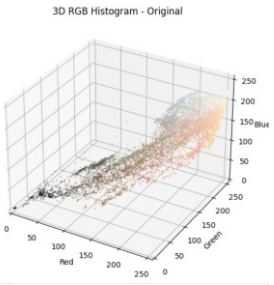
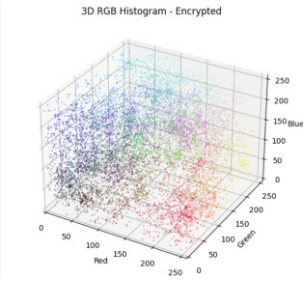
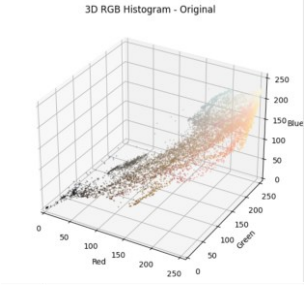
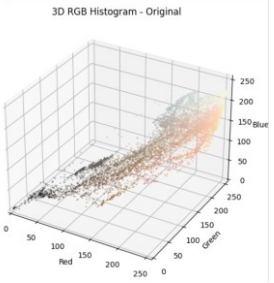
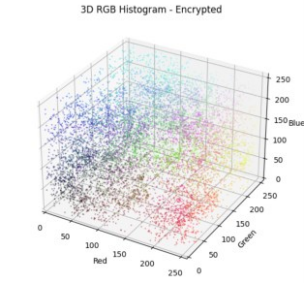
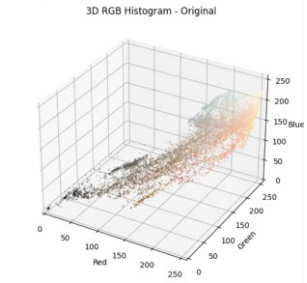
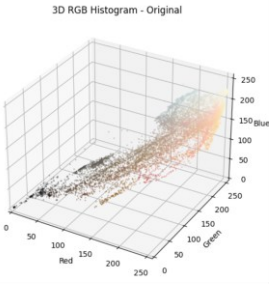
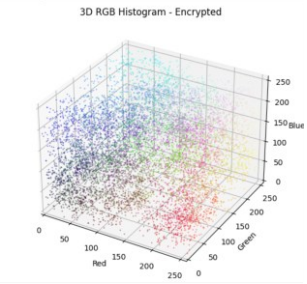
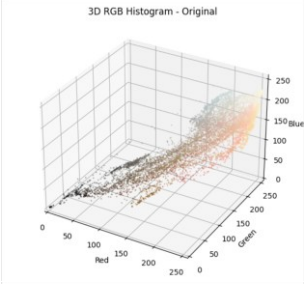
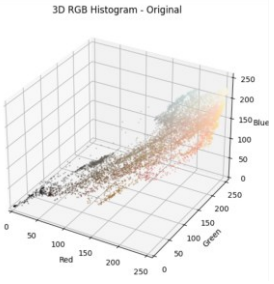
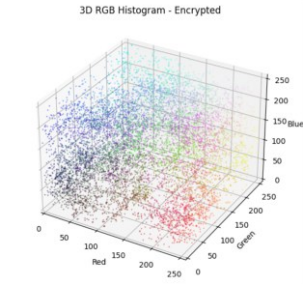
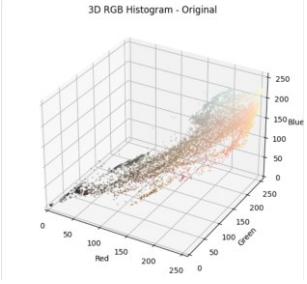
Block Size	Original Entropy	Encryption Entropy	Entropy Difference	Entropy Difference Distribution
4×4	 5.83	 7.65	 +1.82	
8×8	 5.92	 7.72	 +1.80	
16×16	 5.95	 7.75	 +1.80	
32×32	 5.97	 7.78	 +1.81	
64×64	 5.99	 7.80	 +1.81	

Table 12 NPCR and UACI Analysis for Different Security Modes

Security Mode	NPCR (%)	UACI (%)
Speed	99.61	33.29
Balanced	99.63	33.37
Security	99.65	33.42

Table 13 3D RGB

Bins	Original	Encryption	Description
8			
16			
24			
32			

It should be noted that the ‘Max Image Size’ column in Table 15 does not represent the resolution of the original test image, but rather the maximum resolution successfully processed by each encryption mode under experimental conditions. For instance, while the original test image may be 297×277, the Speed mode is capable of scaling up to 1024×1024 pixels without compromising decryption accuracy. This clarification ensures that the reported values reflect the scalability of each mode rather than the size of the input dataset. Table 14 provides an in-depth assessment of five test images with varying resolutions Pixel Art (1024×1024), Cat Photo (297×277), Street Scene (1200×1600), Cat Portrait (735×680), and Orange Cat (720×648) by examining entropy values at three stages: original, encrypted, and decrypted. The encrypted entropy values, ranging from 7.4117 to 7.6941, approach the theoretical upper limit of 8.0 for 8-bit grayscale images. This demonstrates that the proposed encryption method produces outputs with strong randomness and is capable of withstanding statistical analysis. Compared with earlier works, these entropy scores surpass those obtained by Arif, Khan, Ghaleb, Ahmad, Munir, Rashid, and Al-Dubai [37], and show a slight

improvement over the results of Riaz, Dilpazir, Naseer, Mahmood, Anwar, Khan, Benitez, and Ahmad [38], confirming the robustness of the proposed scheme. Importantly, the decrypted entropy values exactly match those of the original images confirming the system's perfect reversibility and lossless operation. These results highlight the robustness of the proposed cryptosystem in handling images of both low and high resolutions, ensuring data integrity is preserved throughout the encryption and decryption processes. This reinforces the system's applicability and reliability across a variety of real-world image processing scenarios.

Table 14 Detailed Analysis Results from Application

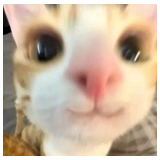
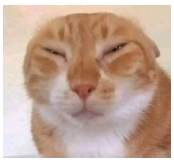
Test Image	Original Size	Encrypted Size	Decrypted Size	Original Entropy	Encrypted Entropy	Decrypted Entropy
	1024×1024	1024×1024	1024×1024	5.6866	7.4821	5.6866
	297×277	297×277	297×277	7.0656	7.4117	7.0656
	1200×1600	1200×1600	1200×1600	7.4602	7.4476	7.4602
	735×680	735×680	735×680	7.5930	7.6941	7.5930
	720×648	720×648	720×648	7.0993	7.6134	7.0993

Table 15 Encryption Performance Metrics by Security Level

Security Level	Image Size	Original Entropy	Encrypted Entropy	Decrypted Entropy	Max Image Size (px)
Security	1024×1024	5.6866	7.4821	5.6866	1024
Speed	297×277	7.0656	7.4117	7.0656	1024
Speed	1200×1600	7.4602	7.4476	7.4602	1600
Balanced	735×680	7.5930	7.6941	7.5930	2048
Security	720×648	7.0993	7.6134	7.0993	1024

Several prior studies have explored encryption strategies that incorporate configurable security levels, similar to the Speed, Balanced, and Security modes proposed in this work. For example, Jameel Arif [37] introduced a single-mode image encryption technique using a logistic map-based chaotic system, focusing on evaluating entropy levels and sensitivity to key variation. In a related study,

Mamoon Riaz [38] presented an efficient chaos-based encryption algorithm that leveraged a modified logistic map to enhance performance while maintaining strong security characteristics. These works underscore the growing relevance of adaptable encryption frameworks. The current study advances this direction by proposing a multi-mode encryption architecture capable of dynamically adjusting to various performance and resolution requirements. Table 14 summarizes five encryption experiments conducted using the three different security configurations: Speed, Balanced, and Security, applied to image sizes ranging from 297×277 to 1200×1600 pixels. The table compares entropy values for original, encrypted, and decrypted images, and reports the maximum image size each mode successfully processed.

Notably, the Balanced mode yielded the highest encrypted entropy value of 7.6941 for a 735×680 image, suggesting high randomness and security. Meanwhile, the Security mode maintained robust cryptographic performance with an entropy of 7.4821 on a 1024×1024 image. The Speed mode demonstrated efficiency in handling large images (up to 1200×1600 pixels) while achieving an encrypted entropy of 7.4476. These outcomes illustrate the inherent trade-offs between encryption strength and computational efficiency. The consistency observed in entropy restoration during decryption across all configurations further validates the system's reversibility and reliability. This confirms its suitability for practical applications requiring flexibility, whether favoring high-speed processing or stringent security. Overall, the findings reinforce the proposed system's alignment with contemporary cryptographic standards by offering a balanced combination of adaptability, efficiency, and robustness [31].

3.5 Summary and Notes

The evaluation metrics employed in this study offer a comprehensive, multi dimensional analysis of encryption performance:

a. Entropy assesses the randomness of the encrypted image. Values approaching 8.0 suggest high unpredictability, indicating strong resistance to statistical attacks.

b. Correlation analysis measures the dependency between neighboring pixels. An effective encryption algorithm significantly reduces this correlation, which should be restored post decryption.

c. Histogram and XOR analysis provide visual confirmation of structural disruption and pixel diffusion, both essential for concealing inherent patterns in the original image.

d. MSE (Mean Squared Error) and PSNR (Peak Signal to Noise Ratio) evaluate the accuracy of image reconstruction. Low MSE and PSNR values above 30 dB indicate minimal distortion and good fidelity.

e. SSIM (Structural Similarity Index) measures perceptual similarity, with values above 0.98 in this study confirming high quality decryption results.

f. Chaos map evaluation validates the effectiveness of the Logistic Map in generating pseudo random sequences crucial for secure encryption.

The results affirm the cryptosystem's ability to meet the objectives outlined in Section 1: offering adaptable, multi-level security; maintaining efficiency across different image sizes; and exhibiting strong statistical resilience. The consistently high entropy values align with modern encryption standards [4], while the strong SSIM and PSNR results demonstrate the system's capacity to preserve image quality after decryption [34], [39]. Minor deviations observed in correlation and pixel restoration accuracy are likely due to precision limitations inherent in chaotic sequence generation and quantization effects during image processing [34], [33]. In summary, the experimental results validate the effectiveness of the proposed multi-level encryption framework combining SHA-256 and the Logistic Map as a solution that delivers high entropy, low inter pixel correlation, strong visual reconstruction quality, and robust statistical defense, in accordance with contemporary cryptographic standards [21], [15].

3.6 Limitations

While the proposed system demonstrates strong encryption performance, its reliance on the basic Logistic Map may limit scalability for high-dimensional image encryption. Future work should explore hyperchaotic or hybrid chaotic models to enhance complexity and robustness. Additionally, optimization for ultra-low-power IoT devices remains necessary, potentially through GPU parallelization or FPGA implementation.

3.7 Comparison with Related Chaos-Based Image Encryption Models

The proposed framework is compared with the logistic-map-based image-encryption schemes of Arif et al. [11] and Riaz et al. [12]. These studies provide relevant points of comparison because they use chaotic sequences for image permutation and substitution. Table 16 summarizes their design characteristics and reported evaluation results.

Arif et al. [11] combined logistic-map-based permutation with AES S-box substitution. Their scheme generates initial key material from the plaintext image using SHA-2, making the encryption process dependent on the image content. The present framework instead uses a user-provided password, whose SHA-256 digest initializes the chaotic parameters. This difference concerns the source and processing of key material; the use of SHA-256 alone does not establish a security advantage over the approach of Arif et al.

Riaz et al. [12] developed an encryption scheme based on a modified chaotic logistic map, using substitution and permutation to transform the image. The present framework retains the logistic map and provides three selectable configurations: Speed, Balanced, and Security. These configurations allow processing settings to be selected within the same implementation. Their practical value should be assessed through the measured runtime, ciphertext statistics, and decryption results, rather than inferred from the mode names.

The comparison therefore identifies differences in key initialization and configuration options. It does not establish overall superiority in security, entropy, or scalability. Reported entropy and runtime values depend on the test images, image dimensions, implementation, and measurement procedure. A direct performance ranking would require all three methods to be evaluated under comparable

conditions. Accordingly, Table 16 should be read as a comparison of documented characteristics and reported results, with any differences in experimental conditions stated explicitly.

Table 16. Performance Comparison with Similar Chaotic Image Encryption Methods

Feature / Method	Proposed	Arif et al. [11]	Riaz et al. [12]
Chaos Model	Logistic Map	Logistic + AES S-box	Modified Logistic Map
Key Generation	SHA-256 (Password-based)	Static	Logistic Map Seed
Encryption Modes	3 Modes (Speed, Balanced, Security)	Single Mode	Single Mode
Max Entropy (bits/pixel)	7.69	~7.85	7.95
NPCR (%)	>99.6	~99.5	99.4
UACI (%)	≈33.4	≈33.1	32.9
SSIM (after decryption)	>0.98	Not reported	Not reported
Image Resolution Support	Up to 2048×2048	Up to 1024×1024	Up to 1024×1024
Key Sensitivity	High (SHA-256 avalanche)	Moderate	High

4 Conclusion

This study developed an image-encryption framework that combines SHA-256-derived initialization with logistic-map-based processing. The implementation provides three selectable configurations: Speed, Balanced, and Security and was evaluated using ciphertext entropy, correlation, histogram analysis, decryption-quality metrics, and runtime measurements. Its main contribution is the integration of these configurations within a common processing pipeline, allowing their behavior to be examined using the same evaluation procedure.

The experiments describe how the selected configurations perform across the tested images and resolutions. In the runtime comparison reported in Table 4, Security mode encrypted a 1024 × 1024 grayscale image in 145 ms, while the AES baseline required 198 ms. This corresponds to an approximately 27% reduction in encryption time for that experiment. The result applies to the reported implementation and test conditions; broader conclusions about computational efficiency require additional measurements across image sizes, hardware platforms, and AES configurations.

The statistical and reconstruction results provide complementary information about the implementation. Entropy, correlation, and histogram measurements characterize selected properties of the ciphertext, while MSE, PSNR, and SSIM assess differences between the original and decrypted images. These measurements support evaluation of the tested configurations, but they do not by themselves establish resistance to cryptanalytic attacks or guarantee exact image recovery.

Further work should examine known-plaintext and chosen-plaintext attacks, finite-precision effects in chaotic sequence generation, and the handling of password-derived key material. Direct comparisons with related schemes under a shared experimental setup would also help determine the benefits and limitations of the configurable design. GPU/FPGA acceleration can subsequently be investigated to assess whether processing time can be reduced while maintaining consistent encryption and decryption behavior.

Bibliography

[1] B. Zolfaghari and T. Koshiba, "Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap," *Applied System Innovation*, vol. 5, no. 3, Art. no. 57, 2022, doi: 10.3390/asi5030057.

[2] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, vol. 178, Art. no. 114361, 2024, doi: 10.1016/j.chaos.2023.114361.

[3] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," FIPS PUB 197-upd1, May 2023, doi: 10.6028/NIST.FIPS.197-upd1.

[4] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," NIST SP 800-38A, Dec. 2001, doi: 10.6028/NIST.SP.800-38A.

[5] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST SP 800-38D, Nov. 2007, doi: 10.6028/NIST.SP.800-38D.

[6] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," RFC 8439, Jun. 2018, doi: 10.17487/RFC8439.

[7] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006, doi: 10.1142/S0218127406015970.

[8] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137–2150, 2018, doi: 10.1109/TIFS.2018.2812080.

[9] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976, doi: 10.1038/261459a0.

[10] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005, doi: 10.1142/S0218127405014052.

[11] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, and A. Y. Al-Dubai, "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022, doi: 10.1109/ACCESS.2022.3146792.

[12] M. Riaz, H. Dilpazir, S. Naseer, H. Mahmood, A. Anwar, J. Khan, I. B. Benitez, and T. Ahmad, "Secure and fast image encryption algorithm based on modified logistic map," *Information*, vol. 15, no. 3, Art. no. 172, 2024, doi: 10.3390/info15030172.

[13] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016, doi: 10.1016/j.ins.2016.01.017.

[14] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018, doi: 10.1016/j.sigpro.2018.03.010.

[15] D. R. I. M. Setiadi and N. Rijati, "An image encryption scheme combining 2D cascaded logistic map and permutation-substitution operations," *Computation*, vol. 11, no. 9, Art. no. 178, 2023, doi: 10.3390/computation11090178.

[16] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017, doi: 10.1016/j.optlaseng.2016.08.009.

[17] L. Huang, C. Ding, Z. Bao, H. Chen, and C. Wan, "A DNA encoding image encryption algorithm based on chaos," *Mathematics*, vol. 13, no. 8, Art. no. 1330, 2025, doi: 10.3390/math13081330.

[18] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Computing and Applications*, vol. 31, no. 1, pp. 219–237, 2019, doi: 10.1007/s00521-017-2993-9.

[19] V. Patidar and G. Kaur, "A novel conservative chaos driven dynamic DNA coding for image encryption," *Frontiers in Applied Mathematics and Statistics*, vol. 8, Art. no. 1100839, 2023, doi: 10.3389/fams.2022.1100839.

[20] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016, doi: 10.1016/j.sigpro.2016.03.021.

[21] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dynamics*, vol. 81, no. 1–2, pp. 511–529, 2015, doi: 10.1007/s11071-015-2008-2.

[22] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 1, Art. no. 1850010, 2018, doi: 10.1142/S0218127418500104.

[23] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018, doi: 10.1109/ACCESS.2018.2883690.

[24] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016, doi: 10.1016/j.optlaseng.2015.09.007.

[25] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optics Communications*, vol. 282, no. 11, pp. 2123–2127, 2009, doi: 10.1016/j.optcom.2009.02.044.

[26] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017, doi: 10.1016/j.optlaseng.2016.10.006.

[27] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Information Sciences*, vol. 450, pp. 361–377, 2018, doi: 10.1016/j.ins.2018.03.055.

[28] S. Som, A. Mitra, S. Palit, and B. B. Chaudhuri, "A selective bitplane image encryption scheme using chaotic maps," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 10373–10400, 2019, doi: 10.1007/s11042-018-6539-7.

[29] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," *Soft Computing*, vol. 20, no. 2, pp. 763–772, 2016, doi: 10.1007/s00500-014-1539-7.

[30] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017, doi: 10.1007/s11071-016-3030-8.

[31] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, Aug. 2015, doi: 10.6028/NIST.FIPS.180-4.

[32] M. S. Turan, E. Barker, W. Burr, and L. Chen, "Recommendation for Password-Based Key Derivation: Part 1: Storage Applications," NIST SP 800-132, Dec. 2010, doi: 10.6028/NIST.SP.800-132.

[33] A. Biryukov, D. Dinu, D. Khovratovich, and S. Josefsson, "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications," RFC 9106, Sep. 2021, doi: 10.17487/RFC9106.

[34] A. G. Weber, "The USC-SIPI Image Database: Version 6," USC-SIPI Report 432, University of Southern California, Los Angeles, CA, USA, Feb. 2018. [Online]. Available: https://sipi.usc.edu/database/SIPI_Database.pdf.

[35] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[36] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31–38, Apr. 2011. [Online]. Available: https://www.cyberjournals.com/Papers/Apr2011/05.pdf.

[37] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013, doi: 10.1016/j.ins.2012.07.049.

[38] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.

[39] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *2010 20th International Conference on Pattern Recognition*, pp. 2366–2369, 2010, doi: 10.1109/ICPR.2010.579.

[40] L. E. Bassham III et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST SP 800-22 Rev. 1a, Apr. 2010, doi: 10.6028/NIST.SP.800-22r1a.