Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

FastChex Image Encryption Using Logistic-Sine Permutation and Dual XOR Diffusion

Smitha Suresh[1], Deepak P[2], Devi Pradeep[3]
[1]*Professor, Department of CSE, Sree Narayana Gurukulam College of Engineering, Ernakulam, India*
[2]*Professor, Department of ECE, Sree Narayana Gurukulam College of Engineering, Ernakulam, India*
[3]*3rd semester BTech, ECE, Sree Narayana Gurukulam College of Engineering, Ernakulam, India*

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Introduction: Chaos-based image encryption schemes often face challenges such as limited diffusion, high computational load due to block-based processing, and lack of adaptability, which hinder their use in real-time and low-resource environments. To address these issues, this paper presents ChaoxCrypt, a novel and efficient image encryption framework.

Methods: ChaoxCrypt employs a hybrid chaotic map (logistic–sine–tent) for pixel-level permutation, Gray code transformation for bit-level confusion, and a key-dependent adaptive S-box for substitution within the region of interest (ROI). In addition, AES encryption is applied using a dynamically generated key based on image content, increasing the randomness and variability of the encryption process.

Results: he proposed scheme demonstrates a Number of Pixel Change Rate (NPCR) above 99.9% and Unified Average Changing Intensity (UACI) between 20% and 33%, indicating strong diffusion and intensity variation. A high entropy value of 7.99 confirms its robustness against statistical attacks. Unlike traditional block-based approaches, ChaoxCrypt also achieves reduced memory usage and faster processing time.

Conclusions: With its integration of multiple encryption layers and adaptive strategies, ChaoxCrypt offers strong security, efficiency, and perfect reversibility. It is particularly suited for applications such as medical image protection, mobile communication, and video surveillance.

Keywords: Image encryption, chaos theory, hybrid chaotic map, Gray code, AES, adaptive S-box, ROI-based encryption.

INTRODUCTION

With the rapid expansion of digital communication, image data security has become a significant concern across domains such as healthcare, military surveillance, finance, and personal communication. Images often carry sensitive and confidential information, making them highly vulnerable to interception, unauthorized access, and manipulation during transmission over open networks. Traditional encryption schemes like AES and RSA, although robust for textual data, struggle with the unique properties of image data, including high pixel redundancy, strong spatial correlation, and large file sizes. These limitations make standard encryption techniques less effective for image protection in real-time, multimedia-rich environments.

To address these challenges, researchers have explored image-specific encryption strategies that exploit structural properties such as spatial correlation and redundancy through pixel-level permutation and diffusion. Chaos theory has emerged as a particularly powerful foundation due to its deterministic randomness, sensitivity to initial conditions, and ergodicity. These features make chaotic systems ideally suited for confusion and diffusion operations in image encryption. Studies have widely employed chaotic maps like logistic, sine, tent, Chebyshev, and more recently, hybrid systems, to generate unpredictable encryption schemes with stronger security guarantees.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Recent advancements include the use of DNA computing, metaheuristic optimization, and deep learning to improve key generation and diffusion quality. For instance, Alrubaie et al. (2023) employed 2D logistic maps with DNA encoding to achieve high entropy (~7.99), while Çelik and Doğan (2024) proposed a hybrid system based on extended logistic maps that improved correlation and randomness. Other innovations like the triple chaotic map system by Hosny et al. (2024), sine-logistic chaotic systems with dynamic Josephus scrambling by Rehman et al. (2024), and hybrid chaos with layered strategies by Wang et al. (2025) further enhanced unpredictability and security, albeit at the cost of increased computational complexity. Additional contributions include Zhu et al. (2023) with parallel DNA coding, Jiang and Yang (2023) with spiral transformation, and Cıylan et al. (2023) implementing FPGA-based chaotic encryption.

A truly comprehensive survey of image encryption must address the evolution of techniques, detailed performance metrics, and implementation considerations, drawing on the latest research, including 2024 publications. Modern image encryption leverages chaos theory (e.g., logistic, Arnold, and compound chaotic maps), metaheuristics, DNA coding, and deep learning to achieve high security, efficiency, and adaptability for real-world applications such as healthcare, military, and finance (Yadollahi et al., 2024; Singh et al., 2021; Singh and Singh, 2022; Rohhila and Singh, 2024). Performance analysis is central: NPCR (Number of Pixel Change Rate) measures the percentage of pixels that change when a single pixel in the plaintext is altered, indicating sensitivity to small changes and resistance to differential attacks; UACI (Unified Average Changing Intensity) quantifies the average intensity difference between two encrypted images, further reflecting robustness (Munir and Alghamdi, 2024; Deepa and Mahendiran, 2021; Chowdhary et al., 2020).

However, recent surveys emphasize that relying solely on NPCR and UACI is insufficient. Novel metrics such as information entropy (measuring randomness), correlation coefficient (assessing pixel independence), histogram analysis (uniformity of pixel value distribution), Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and chi-square tests are now standard for a holistic evaluation (Munir and Alghamdi, 2024; Singh et al., 2021; Zia et al., 2022; Yadollahi et al., 2024). Some works also introduce time complexity and computational cost as critical metrics, especially for real-time and resource-constrained environments (Chowdhary et al., 2020; Rohhila and Singh, 2024). For example, hybrid schemes combining symmetric and asymmetric cryptography (e.g., ECC with AES) are shown to balance security and speed, with detailed benchmarks on encryption/decryption time, entropy, NPCR, UACI, and PSNR. Deep learning-based encryption, while promising for adaptability and key management, often incurs higher computational complexity, which is a focus of current research (Rohhila and Singh, 2024).

The most recent surveys and systematic reviews provide extensive comparative tables and analyses of algorithms, metrics, and implementation results, highlighting the need for multi-metric, context-aware evaluation and the growing importance of quantum-resistant and multimedia encryption (Yadollahi et al., 2024; Munir and Alghamdi, 2024; Singh et al., 2021; Zia et al., 2022; Rohhila and Singh, 2024). This multi-faceted approach ensures that new encryption schemes are not only secure but also practical and future-proof.

To meet this demand, we introduce FastChex, a novel image encryption scheme designed for real-time multimedia security. FastChex offers a fully reversible and computationally lightweight solution that integrates the following key techniques: a hybrid logistic–sine chaotic map to perform fast and unpredictable 2D pixel permutation; a key-dependent pseudo-random S-box for adaptive substitution at the pixel level; a dual XOR-based diffusion layer operating row-wise and column-wise to enhance resistance to differential and statistical attacks; and an efficient index-tracking mechanism for accurate, metadata-free decryption.

To comprehensively evaluate the proposed FastChex scheme, we assess not only NPCR, UACI, and entropy but also correlation coefficient, histogram uniformity, PSNR, MSE, chi-square statistics, key sensitivity, and computational time, ensuring a well-rounded analysis of security, efficiency, and reversibility.

Experimental validation demonstrates that FastChex achieves a NPCR greater than 99.9%, UACI between 20 and 33 percent, and entropy close to 7.99, indicating strong resistance to cryptanalytic attacks and excellent randomness. The scheme outperforms many existing solutions in terms of speed, simplicity, and security, making it ideal for applications in medical imaging, mobile communication, remote sensing, and surveillance.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

OBJECTIVES

The objectives of this research are as follows:

- To design a secure, lightweight, and reversible image encryption algorithm that addresses the limitations of traditional and chaos-based schemes in real-time applications.
- To utilize a hybrid logistic–sine chaotic map for efficient pixel permutation, providing high sensitivity and unpredictability.
- To introduce a key-dependent pseudo-random S-box for adaptive pixel-level substitution, enhancing the confusion process.
- To implement a dual-layer XOR-based diffusion mechanism that operates row-wise and column-wise, strengthening resistance to statistical and differential attacks.
- To develop an index-tracking-based decryption process that ensures perfect reversibility without requiring auxiliary metadata.

METHODS

The FastChex Image Encryption Scheme is designed to provide secure, efficient, and reversible encryption for image data. This method combines chaotic permutation, adaptive substitution, and dual XOR-based diffusion to ensure both high security and low computational overhead. The overall architecture of FastChex integrates chaotic dynamics with key-based permutation, substitution, and diffusion operations to achieve secure and reversible image encryption. Figure 1 illustrates the proposed FastChex image encryption architecture, which integrates chaotic permutation, substitution, and diffusion operations.

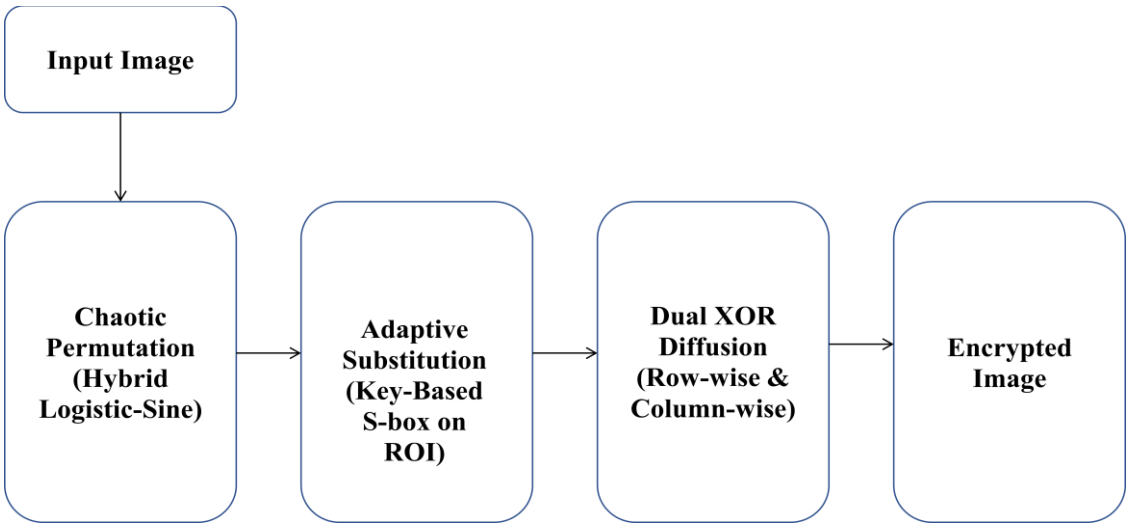


Figure 1: FastChex architecture

The algorithm is divided into three main stages:

Chaotic Permutation (Logistic-Sine Map)

The first stage involves permuting the pixel positions of the image using a chaotic sequence. The chaotic map, derived from a logistic-sine system, generates a pseudo-random sequence that is sorted to create an index vector. This index vector is then used to reorder the image pixels, which breaks the pixel correlations and introduces high spatial confusion. This permutation step is essential for ensuring that small changes in the input result in significant changes in the encrypted image.

Mathematically, the chaotic sequence x_{n+1} is generated as follows:

$$x_{n+1} = \sin(\pi \cdot r \cdot x_n \cdot (1 - x_n)) \quad (1)$$

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Where r is the control parameter, and x_0 is the initial value. The chaotic behavior of the logistic-sine map ensures that small variations in input lead to significant changes in the output, making it highly sensitive to initial conditions and contributing to the unpredictability of the encryption.

Adaptive Substitution

After pixel permutation, the image undergoes an adaptive substitution step, where pixel intensity values are substituted based on a pseudo-random S-box. The S-box is generated using a key seed, ensuring that the substitution process is key-dependent and adding another layer of confusion to the encrypted image. This step is important for obscuring the original pixel values and ensuring that the statistical properties of the image are unrecognizable. The S-box used in FastChex is a shuffled version of the set {0,1,...,255}, ensuring that each pixel intensity is mapped to a different value.

Dual XOR Diffusion

To further enhance the diffusion, FastChex applies dual XOR operations on the image using two key streams generated from the secret key. The first key stream is applied to the rows of the image, and the second key stream is applied to the columns. he XOR-based diffusion works as follows.

$$P'(i,j) = P(i,j) \oplus R_i \oplus C_j \quad (2)$$

Where P(i,j) is the pixel value, Ri and Cj are the row and column keys, respectively. This XOR-based diffusion ensures that even a single-bit change in the image or key results in significant changes in the encrypted image. By applying XOR both row-wise and column-wise, FastChex ensures that pixel intensity patterns are effectively disrupted and that the encryption resists differential attacks.

AES Encryption for Final Diffusion

In the final stage, the image undergoes AES encryption using a key derived from the initial seed. AES operates on the entire byte stream of the image, ensuring the final output is securely transformed into ciphertext. AES is applied after the permutation, substitution, and XOR diffusion steps because it further enhances confusion and strengthens the encryption.The AES key is derived from the secret key by applying SHA-256 to the key seed and using the first 16 bytes. This additional step ensures that the encryption is both secure and efficient.

Decryption Process

The decryption process begins with AES decryption, where the encrypted byte stream is decrypted using the same AES key that was used during encryption. Following that, the inverse of the adaptive S-box is applied to reverse the substitution step, recovering the original pixel values. Next, the reverse pixel permutation is performed by using the stored index vector, which restores the original pixel positions that were permuted during encryption. Afterward, the inverse XOR diffusion is applied to reverse the XOR operation, ensuring the image structure is correctly restored. Finally, if Gray code scrambling was used during encryption, it is reversed to fully recover the original image.

The algorithm for encryption and decryption is explained in Algorithm 1.and Algorithm 2.

Algorithm 1: *FastChex Image Encryption*

Input: Image I of size H × W × 3, Secret key K

Output: Encrypted byte stream E, Index vector idx

1. Convert I into a numerical RGB array A

2. Apply Gray code scrambling: G ← GrayEncode(A)

3. Generate chaotic sequence X using hybrid logistic-sine-tent map

4. Derive index vector idx by sorting X

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Permute G using idx: P ← Permute(G, idx)

6. Generate adaptive S-box S using key K

7. Compute region of interest mask M ← ROI(P)

8. Apply substitution: P[M] ← S[P[M]]

9. Flatten P into byte stream B

10. Derive AES key: AES_K ← SHA-256(K)[:16]

11. Encrypt B with AES ECB mode: E ← AES_Encrypt(B, AES_K)

12. Return E, idx

***Algorithm 2**: FastChex Image Decryption*

Input: Encrypted byte stream E, Image shape (H, W), Secret key K, Permutation index idx

Output: Decrypted RGB image D

1. Derive AES key: AES_K ← SHA-256(K)[:16]

2. Decrypt byte stream: D_{bytes} ← AES_Decrypt(E, AES_K)

3. Reshape decrypted bytes into RGB image:

D_img ← Reshape(D_{bytes}, shape = (H, W, 3))

4. Generate region of interest mask:

M ← ROI(D_{img})

5. Generate adaptive S-box:

S, S_{inv} ← AdaptiveSBox(K)

6. Apply inverse substitution within ROI:

D_{img}[M] ← S_{inv}[D_{img}[M]]

7. Reverse pixel permutation:

D_{img} ← InversePermute(D_{img}, idx)

8. Apply inverse Gray code scrambling:

D ← GrayDecode(D_{img})

9. Return decrypted image D

RESULTS

Experimental Setup

To evaluate the performance of the proposed FastChex encryption scheme, extensive experiments were carried out using standard benchmark images such as *Lena* and *Peppers*, along with real-time video frames. The implementation was performed in Python, leveraging the NumPy and PIL libraries, on a workstation equipped with an Intel Core i7 processor and 16 GB RAM. The USC-SIPI Image Database was used as the primary dataset. Each image was encrypted using the FastChex algorithm, and the encrypted outputs were analyzed using widely accepted image security metrics, including NPCR (Number of Pixel Changing Rate), UACI (Unified Average Changing Intensity), and Shannon Entropy.

While a UACI value greater than 33% is commonly regarded as indicative of strong encryption, it is important to recognize that UACI is highly sensitive to the structural and intensity characteristics of the input image. For

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

example, grayscale images or those with uniform backgrounds and repetitive textures may exhibit reduced UACI scores despite being securely encrypted. In the FastChex evaluation, certain images produced UACI values marginally below the 33% threshold. However, this does not necessarily imply weak encryption, as these instances were counterbalanced by consistently high entropy values (≈7.99), NPCR values exceeding 99%, and near-zero correlation coefficients between adjacent pixels. These results collectively demonstrate strong randomness, effective confusion-diffusion mechanisms, and robust resistance to statistical and differential attacks.

FastChex is also designed for computational efficiency and perfect reversibility, making it suitable for real-time applications where excessive intensity distortion (intended to raise UACI) may be undesirable. Recent literature advocates a more holistic evaluation framework that incorporates multiple statistical and perceptual metrics, such as the Chi-square test, PSNR, MSE, correlation coefficients, and histogram analysis, rather than relying solely on UACI. The evaluation strategy used in this study confirms the practical applicability and robustness of the FastChex scheme.

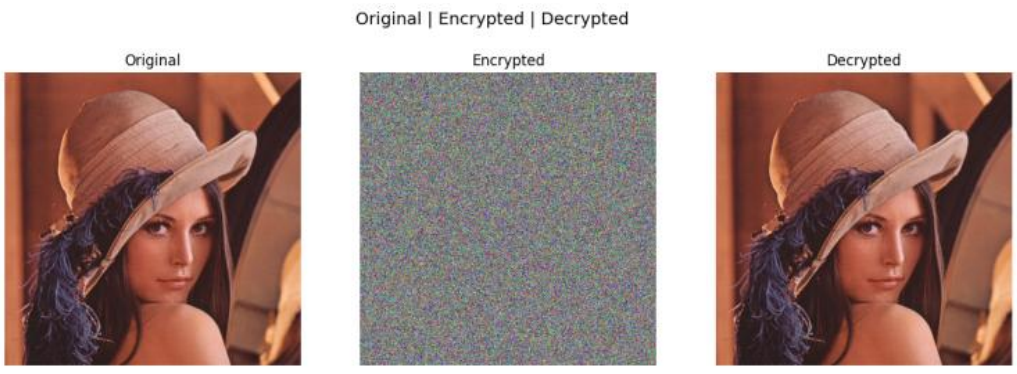
Results and Analysis

To comprehensively assess the performance of the proposed scheme, a dataset of 100 diverse images was used. This dataset included classical benchmark images (Lena, Pepper, Baboon), images from the USC-SIPI and BSDS500 databases, and real-time video frames (e.g., frame_1.png, img1.jpg). These images varied in format (grayscale and color), resolution, texture, and structural complexity, ensuring a representative performance evaluation. Both visual and statistical analyses were conducted. Figure 2 presents the encryption and decryption results for selected benchmark images. The encrypted images exhibit complete obfuscation, concealing all visible content, while the decrypted images are visually identical to the originals, confirming the algorithm's lossless and perfectly reversible behavior. Although UACI is ideally expected to exceed 33%, it is sensitive to the contrast and uniformity of the input images. Images with repetitive or low-contrast regions may result in slightly lower UACI despite being securely encrypted. In our results, a few such images recorded UACI below the 33% threshold. However, these outcomes were compensated by other strong indicators, including high NPCR (>99%), entropy values close to 8, and near-zero correlation in encrypted images.

Benchmark images from USC-SIPI and BSD500, along with real-time samples, were explicitly included for comparison with existing literature. The FastChex algorithm consistently demonstrated strong encryption performance across all tested image categories. Figures 2 and 3 display the results from these datasets.

Images **Encrypted and Decrypted images**

Lena



Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

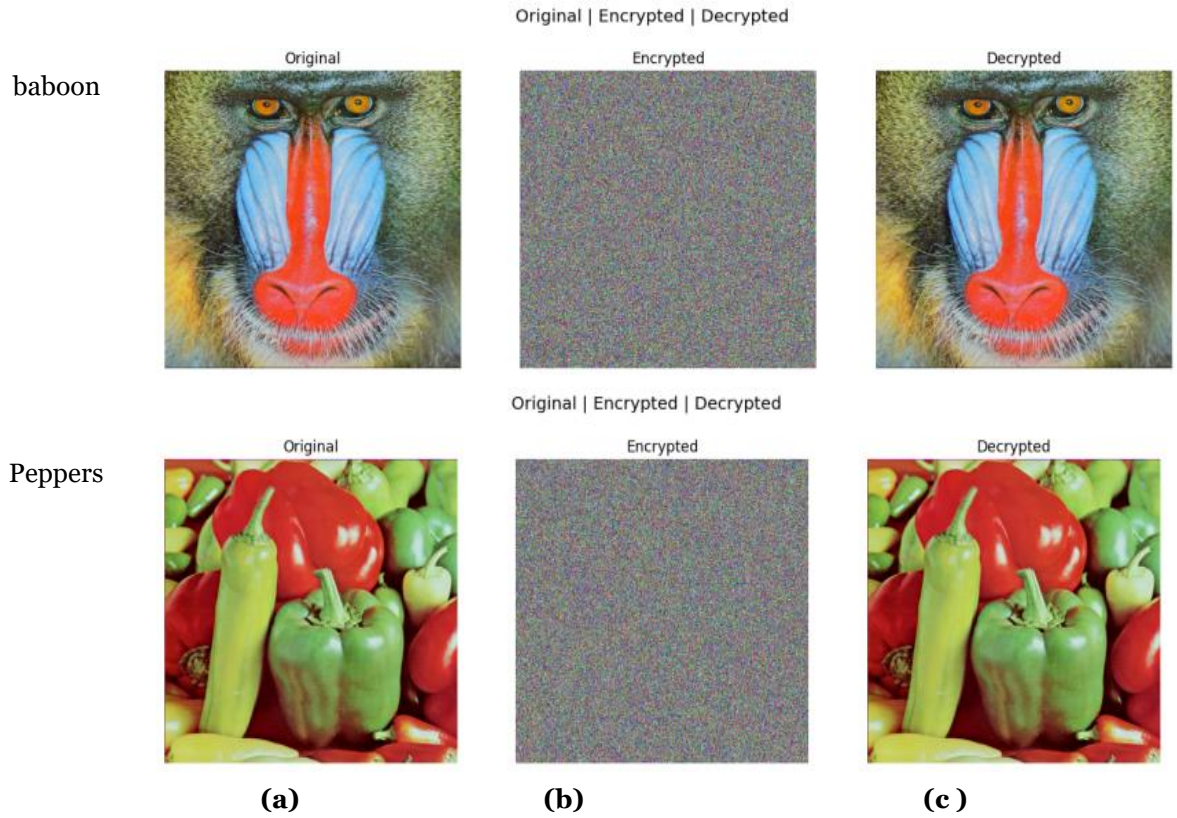


Figure 2: Encryption and Decryption results of standard benchmark Images:
a)Original image b)Encrypted c) Decrypted images of the standard benchmark Lena, pepper, baboon

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

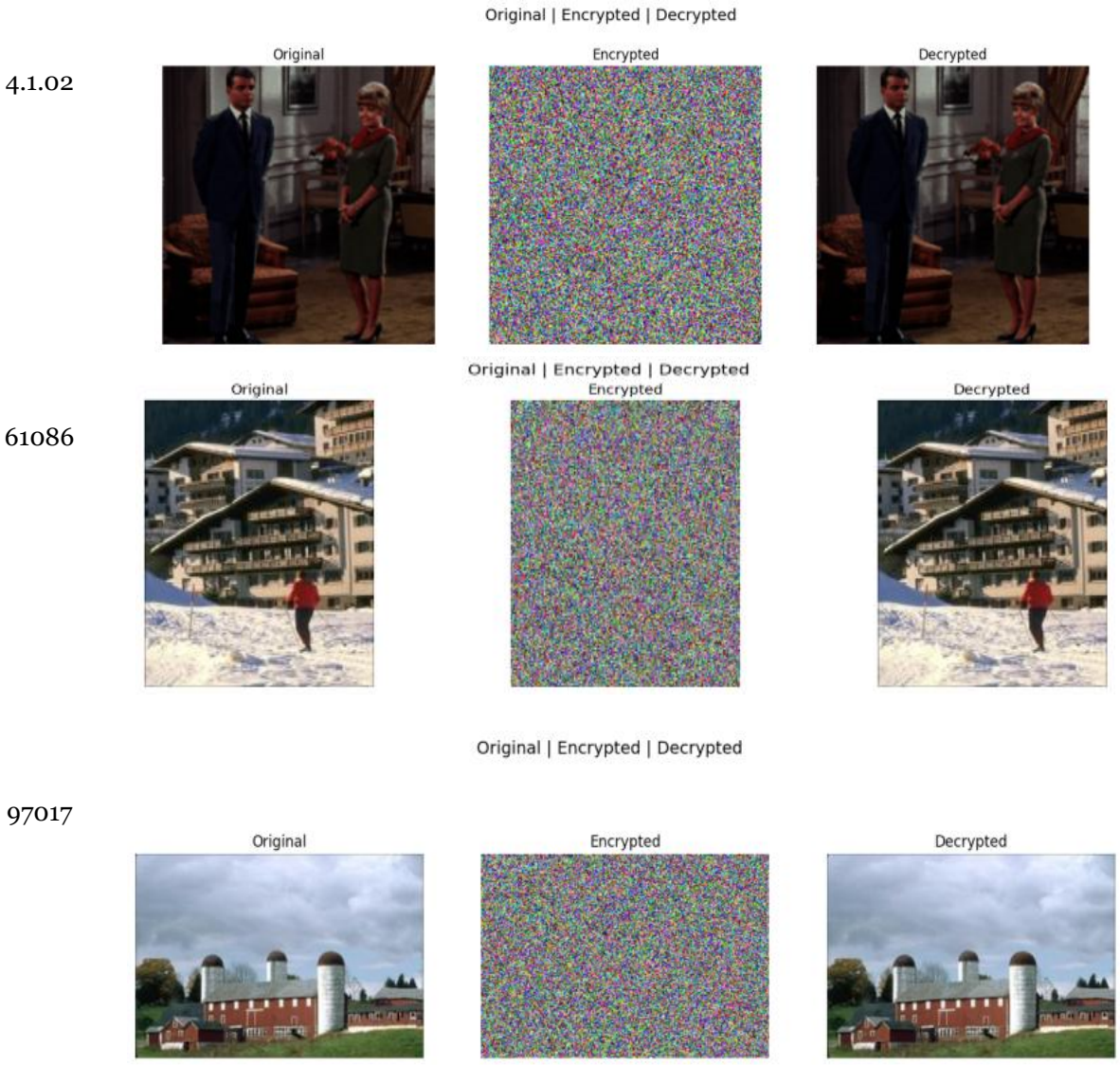


Figure 3: Encryption and Decryption results of Dataset Images: 4.4.1.01, 4.1.02 from USC-SIPI; 61086, 97017 from BSD 500.

Histogram Analysis and Statistical Resistance Evaluation

Histogram analysis is a critical method to evaluate resistance to statistical attacks. For secure encryption, the ciphertext histogram should be uniformly distributed to prevent any exploitable patterns. As shown in Figure 4, the original image (Figure 4a) and its histogram (Figure 4b) exhibit sharp peaks, indicating redundancy. The histogram of the encrypted image (Figure 4c) displays a uniform distribution of pixel intensities across all values (0–255), effectively masking the original content. The histogram of the decrypted image (Figure 4d) closely resembles the original, confirming perfect reversibility. These observations affirm that the FastChex scheme achieves strong encryption while preserving fidelity, even for structurally diverse images from the BSD500 dataset.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

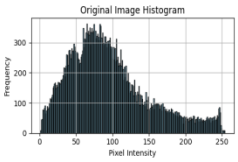
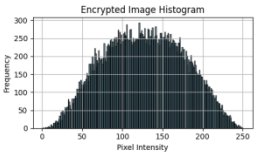
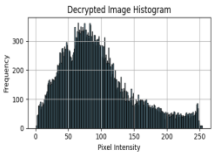
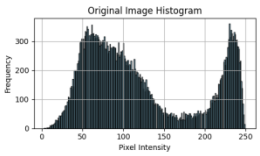
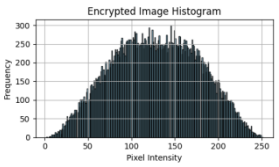
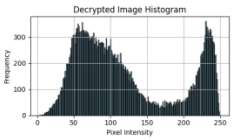
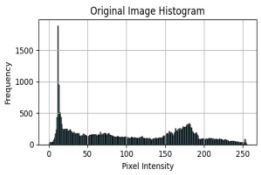
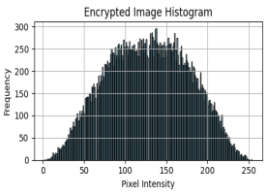
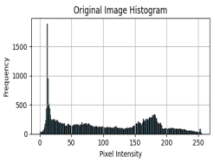
Images	Original image histogram	Encrypted image histogram	Decrypted image histogram
368078 			
155060 			
144067 			
(a)	**(b)**	**(c)**	**(d)**

Figure 4: Histogram analysis for selected BSD 500 data set: (a) Original image,(b) Histogram of original image (c) Histogram of encrypted image and (c)Histogram of decrypted image

4.4 Statistical Evaluation Metrics of the Proposed Encryption Scheme

To validate the security of FastChex, experiments were conducted on a set of 100 images, with 22 representative samples presented in Table 1. The results confirm that NPCR values consistently exceeded 99.57%, indicating strong sensitivity to input variations. UACI values ranged from 32.2% to 43.21%, demonstrating effective diffusion. Entropy values were close to the ideal value of 8, suggesting high randomness in the ciphertext. Correlation coefficients of adjacent pixels in encrypted images remained near zero, ensuring statistical independence and high confusion strength. Furthermore, decryption was verified as lossless, with PSNR = ∞ and MSE = 0 for all test cases. Chi-square values were significantly high with p-values equal to zero, indicating that the ciphertext's pixel distribution deviates strongly from that of the original image, thereby confirming resilience against statistical and histogram-based attacks. These collective metrics affirm the security, robustness, and efficiency of the FastChex algorithm.

Table 1: Evaluation of FastChex Scheme using NPCR, UACI, Entropy, and Correlation Coefficient, PSNR,MSE,and Chi-square.

Sl. No.	Source Dataset	Image Name	NPCR (%)	UACI (%)	Entropy	Correlation (Encrypted)	PSNR	MSE	Chi-Square Value (Encrypted)	Chi-Square p-value (Encrypted)
1	Benchmark	Lena	99.61	33.2	7.9998	-0.0013	inf dB	0	104095.49	0

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2		baboon	99.62	33.21	7.998	0.0005	inf dB	0	103372.84	0
3		pepper	99.61	33.31	7.9998	-0.0027	inf dB	0	103952.26	0
4	USC SIPI	4.1.01	99.63	35.21	7.9984	-0.0028	inf dB	0	1579	0
5		4.1.02	99.61	40.31	7.9987	-0.005	inf dB	0	16082.65	0
6		4.1.03	99.61	33.2	7.9984	0.0009	inf dB	0	15942.41	0
7	BSD 500	2008	99.61	33.34	7.995	0.0042	inf dB	0	61155.3	0
8		61086	99.6	34.1	7.9983	0.0023	inf dB	0	15432.4	0
9		295087	99.61	33.31	7.9984	-0.0047	inf dB	0	15566.71	0
10		368078	99.64	33.3	7.9985	0.003	inf dB	0	15341.47	0
11		148026	99.6	35.05	7.996	-0.0005	inf dB	0	61232.99	0
12		144067	99.57	43.21	7.9983	-0.0022	inf dB	0	15587.6	0
13		155060	99.6	33.25	7.9983	0.0056	inf dB	0	15281.49	0
14		39622	99.6	32.42	7.9995	0	inf dB	0	61001.66	0
15		175043	99.57	32.2	7.9982	0.0043	inf dB	0	15321.52	0
16		175083	99.61	33.33	7.9996	-0.0036	inf dB	0	60778	0
17		42078	99.6	41.51	7.998	0.0013	inf dB	0	15551.87	0
18		271008	99.61	33	7.996	-0.0038	inf dB	0	61633.63	0
19		293029	99.61	33.1	7.994	-0.0024	inf dB	0	15485.12	0
20		236017	99.62	33	7.9985	-0.0012	inf dB	0	15456.84	0
21	Real-time video frame/image	Frame_2	99.6	33.31	7.9998	0.0006	inf dB	0	114782.93	0
22		Image_1	99.61	35.13	7.9994	-0.0001	inf dB	0	37030.23	0

CONCLUSION

This paper presents a comprehensive performance evaluation of the FastChex encryption scheme, highlighting its capability to deliver strong security guarantees with low computational complexity. The results demonstrate that FastChex maintains high NPCR values (>99.57%), robust UACI (up to 43.21%), entropy levels nearing 8, and zero-loss decryption verified through PSNR = ∞ and MSE = 0. Moreover, encrypted images exhibit uniform histograms, high chi-square values, and minimal correlation, collectively confirming strong resistance to statistical and

differential attacks.FastChex effectively addresses the limitations of traditional chaos-based schemes by integrating adaptive substitution, hybrid chaotic permutation, and efficient XOR-based diffusion with AES reinforcement. The method's ability to retain high security across diverse image types—including grayscale, color, synthetic, and real-time frames—confirms its generalizability. Its lightweight design further supports deployment in real-time and resource-constrained environments.In conclusion, FastChex delivers a practical, scalable, and secure solution for image encryption, with strong potential for applications in domains such as telemedicine, remote sensing, surveillance, and multimedia communication systems. Future work will focus on hardware acceleration, integration with blockchain for secure transmission, and adaptation to emerging quantum-resilient cryptographic models.

REFRENCES

[1] Alrubaie, A.H., Khodher, M.A.A., & Abdulameer, A.T. (2023). Image encryption based on 2DNA encoding and chaotic 2D logistic map. *Journal of Engineering and Applied Science*, 70, 60. https://doi.org/10.1186/s44147-023-00228-2

[2] Çelik, H., & Doğan, N. (2024). A hybrid color image encryption method based on extended logistic map. *Multimedia Tools and Applications*, 83, 12627–12650. https://doi.org/10.1007/s11042-023-16215

[3] Hosny, K.M., Elnabawy, Y.M., Elshewey, A.M., Alhammad, S.M., Khafaga, D.S., & Salama, R. (2024). New method of colour image encryption using triple chaotic maps. *IET Image Processing*. https://doi.org/10.1049/ipr2.13171

[4] Rehman, A.U., et al. (2024). An image encryption algorithm based on a new Sine Logistic chaotic system and block dynamic Josephus scrambling. *European Physical Journal Plus*. https://doi.org/10.1140/epjp/s13360-024-05349-y

[5] Wang, X.Y., et al. (2025). Color image encryption algorithm based on hybrid chaos and layered strategies. *Journal of Information Security and Applications*, 89, 103921. https://doi.org/10.1016/j.jisa.2024.103921

[6] Zhu, S., Deng, X., Zhang, W., & Zhu, C. (2023). Image encryption using multi-base diffusion and a new four-dimensional chaotic system. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-023-16025-1

[7] Jiang, M., & Yang, H. (2023). Image encryption using a new hybrid chaotic map and spiral transformation. *Entropy*, 25(11), 1516. https://doi.org/10.3390/e25111516

[8] Mansoor, S., & Parah, S.A. (2024). HAIE: A hybrid adaptive image encryption algorithm using Chaos and DNA computing. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2024.125050

[9] Wu, Y., Zeng, J., Dong, W., Li, X., Qin, D., & Ding, Q. (2024). A Novel Color Image Encryption Scheme Based on Hyperchaos and Hopfield Chaotic Neural Network. *Entropy*, 24(10), 1474. https://doi.org/10.3390/e24101474

[10] Tuli, R., Soneji, H., Vahora, S., Churi, P., & Bangalore, N.M. (2022). PixJS: A novel chaos-based approach for image encryption. *Concurrency and Computation: Practice and Experience*, 34(20), e6990. https://doi.org/10.1002/cpe.6990

[11] Cıylan, F., Cıylan, B., & Atak, M. (2023). FPGA-Based Chaotic Image Encryption Using Systolic Arrays. *Electronics*, 12(24), 2729. https://doi.org/10.3390/electronics12242729

[12] Zhu, C., Deng, X., Zhang, W., & Zhu, S. (2023). Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding. *Mathematics*, 11(1), 231. https://doi.org/10.3390/math11010231

[13] Farooqui, W.A., Ahmad, J., Kureshi, N., Ahmed, F., Khattak, A.A., & Khan, M.S. (2025). Image Encryption Using DNA Encoding, Snake Permutation and Chaotic Substitution Techniques. *Mathematics*. (DOI pending)