Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Lightweight Feature-Adaptive Chaotic ImageEncryption Framework via Unsupervised Statistical Feature Learning and Cryptographic Keystream Enhancement

Shima Maniyath

shima.ramesh@mvjce.edu.in

MVJ College of Engineering

Leena Kunnath

Vijaya Vittala Institute of Technology

Research Article

Keywords: image encryption, feature-adaptive encryption, unsupervised statistical feature learning, principle component analysis, chaotic maps, cryptographic keystream enhancement

Posted Date: October 8th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10744065/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Lightweight Feature-Adaptive Chaotic Image Encryption Framework via Unsupervised Statistical Feature Learning and Cryptographic Keystream Enhancement

1st Shima Ramesh Maniyath
Assistant Professor, Department of Electronics and Communication Engineering, MVJ College of Engineering, Bengaluru, India,
ramesh.shima86@gmail.com,

2nd Leena Kunnath
Professor, Department of Electronics and Communication Engineering, Vijaya Vittala Institute of Technology, Bengaluru, India
dr.leena.vvit@gmail.com

***Abstract*— Recent advancements in multimedia transmission and cloud-based storage have made secure image encryption vital for protecting sensitive visual information. Conventional chaotic image encryption schemes offer high sensitivity to initial conditions but generally lack adaptivity to heterogeneous image characteristics, whereas training-based adaptive encryption methods often require extensive datasets, high computational resources, and complex model optimization. This paper presents a lightweight feature-adaptive chaotic image encryption framework that applies unsupervised statistical feature learning through Principal Component Analysis (PCA) to derive compact image descriptors for adaptive chaotic parameter modulation. The extracted feature descriptors are used to adaptively modulate the logistic map parameters, which enables image-dependent keystream generation while preserve computational efficiency and interpretability. To improve resistance against finite-precision effects and keystream predictability, the generated keystream is further strengthened using cryptographic hashing and HMAC-based keystream enhancement. The proposed framework is evaluated using standard image encryption metrics, including entropy, NPCR, UACI, adjacent-pixel correlation, PSNR, key-sensitivity, and plaintext sensitivity analyses. Experimental results demonstrate competitive or improved diffusion, randomness, and decorrelation characteristics in comparison with representative fixed-chaotic, AES-based, and HMAC-assisted encryption baselines. The proposed framework provides an interpretable, computationally efficient, and content-adaptive encryption solution suitable for resource-constrained secure imaging applications, while offering a practical alternative to computationally intensive training-based adaptive encryption methods.**

Keywords*— *image encryption, feature-adaptive encryption, unsupervised statistical feature learning, principle component analysis, chaotic maps, cryptographic keystream enhancement

I. INTRODUCTION

The rapid growth of digital image acquisition, transmission, and cloud-based storage across applications such as medical imaging, IoT surveillance, intelligent transportation, and multimedia communication has made secure image protection an increasingly important research challenge [1], [2]. Unauthorized access, tampering, or disclosure of sensitive visual information can lead to serious privacy breaches, financial losses, and security risks. On the other hand, there is an increasing demand for image encryption techniques that can simultaneously provide strong confidentiality, computational efficiency, and robustness against emerging cryptanalytic attacks [3]-[6].

Chaotic image encryption has attracted considerable attention because, chaotic systems exhibit intrinsic properties which include sensitivity to initial conditions, pseudo-random behaviour, and non-linear dynamics, which are well suited for confusion and diffusion operations. Nevertheless, conventional chaotic encryption schemes generally employ fixed or user-defined chaotic parameters that remain independent of the statistical characteristics of the plaintext image. As a result, although different secret keys generate different ciphertexts, the encryption process itself does not adapt to variations in image texture, structural complexity, or statistical distribution. Furthermore, digital implementations of chaotic maps remain susceptible to finite-precision effects that may reduce the randomness and unpredictability of the generated keystreams [7]-[10]. Recent advances in machine learning have introduced adaptive image encryption strategies in which neural networks, auto-encoders and generative models learn image-dependent representations for encryption [11], [12]. These approaches improve content adaptively by exploiting data-driven feature extraction; however, they usually require extensive training datasets, computationally intensive optimization, and high inference complexity, which limits their applicability to real-time and resource constrained environments such as embedded IoT devices, edge imaging systems [13]-[16]. Moreover, the limited interpretability of deep learning models often makes it difficult to analyse how image characteristics influence the encryption process.

The above observations implies the need for lightweight and interpretable feature-adaptive encryption framework that can combine the computational efficiency of chaotic encryption with

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

content-aware parameter adaption while avoiding the overhead of training-based learning models. Instead of relying on deep neural networks, such a framework should extract compact statistical descriptors directly from the plaintext image and utilize them to dynamically modulate the chaotic system, thereby producing image-dependent keystreams without increasing computational complexity.

To address this challenge, this paper presents a Feature-Adaptive Chaotic Image Encryption Framework based on unsupervised statistical feature learning using Principal Component analysis (PCA). Image patches are first represented through compact PCA descriptors that can capture dominant structural and textural information. These descriptors are subsequently transformed into adaptive logistic-map parameters, allowing image-dependent chaotic keystream generation through a Feature-Adaptive Chaotic Parameter Modulation (FACPM). To further improve resistance against finite-precision effects and keystream predictability, the generated keystream is strengthened using cryptographic hashing and HMAC-based enhancement prior performing pixel-level encryption. The resulting framework therefore remains computationally efficient, interpretable and suitable for lightweight secure imaging applications. Unlike existing adaptive encryption schemes that rely on trainable neural networks or fixed chaotic parameterization, this work introduces a FACPM methodology that transforms lightweight statistical image descriptors into image-dependent chaotic dynamics, thereby enabling adaptive keystream generation without any training process.

- A lightweight feature adaptive chaotic parameter modulation framework that generates image dependent chaotic dynamics using unsupervised statistical feature descriptors without requiring any modeling training.
- An image-dependent chaotic parameter modulation strategy namely FACPM transforms compact PCA-derived statistical descriptors into adaptive chaotic parameters, enabling content-aware keystream generation without iterative learning or complex model optimization.
- A cryptographic keystream enhancement stage that strengthens the adaptive chaotic sequence against finite-precision effects and deterministic keystream predictability.
- A comprehensive experimental evaluation against representative fixed-chaotic, AES-based, and HMAC-assisted encryption schemes using entropy, NPCR, UACI, adjacent-pixel correlation, PSNR, key sensitivity, and plaintext sensitivity analyses.

The reminder of the paper is organized as follows: Section 2 reviews recent literature on chaotic, machine learning –based, and hybrid image encryption techniques. Section-3 formulates the research problem and motivates the proposed approach. Section 4 presents the proposed feature-adaptive chaotic image encryption framework and its mathematical formulation. Section 5 discusses the experimental evaluation and comparative analysis. Finally section 6 concludes the paper and outlines future research directions.

II. Literature Review

Recently, securing digital images has been extensively studied, with approaches ranging from classical cryptographic algorithms to chaos-based and machine-learning driven schemes.

A. Chaotic Image Encryption

There are various classical schemes that employ logistic maps, Chebyshey maps, and hyper-chaotic systems for pixel permeation and diffusion. The authors Bhattacharjee et al. [17] presented a modified logistic map-based encryption scheme for visible and COVID-19 X-ray images, which achieves time-efficient encryption and high NPCR/UACI values. While effective on standard metrices the approach lacks adaptivity to local image features and doesn't employ ML approach for content-aware encryption. On the other hand, Setiadi and Rijati [18] combined 2D cascaded logistic maps with permutation-substitution operations for improved diffusion yet their fixed parameters limit content driven-adaption. The authors Laila et al., [19] enhanced 2D logistic maps for grayscale images which improves randomness but without ML-guided feature extraction.

Kanwal et al., [20] also incorporated a 3D-cyclic Chebyshev map with elliptic curves for stronger cryptography at high computational cost. GA and Bhanu [21] on the other hand also applied Chebyshev chaotic maps with attribute-based encryption in fog networks, yet it is not image specific. The authors Dai et al., [22] applied GAN-based double encryption with hyper-chaotic systems which offer adaptivity but require large datasets and significant computation. Mohammed et al., [23] also leveraged hyper-chaotic systems for IoT images and achieves strong diffusion but without ML-based adaptive control. Overall, existing chaotic encryption schemes provide strong confusion and diffusion characteristics. However, many conventional approaches employ fixed or key-dependent chaotic parameters that remain independent of compact statistical descriptors extracted from the plaintext image. Consequently, lightweight content-adaptive chaotic parameter modulation remains comparatively underexplored.

B. ML-Based Image Encryption

Alqahtani [24] used auto-encoders for securing medical images which provide high-quality reconstruction and encryption, but the model requires extensive training data and incurs high computational cost making it less practical for light-weight or real time systems. The authors Ahmed et al., [25] presented a DNA-based color image encryption method considering convolutional autoencoder, offering strong confusion-diffusion but relying on complex neural architectures that are difficult to interpret and energy-intensive to train. The authors Alslman et al., [15] combined autoencoder with AES for medical image protection achieving robustness but still depends on supervised deep models and heavyweight cryptographic operations. Saini and Sehrawat [26] proposed a CNN-AES multi-key scheme that improves block-level security. On the other hand, Feng et al., [27] also combined chaotic encryption with CNN-based feature extraction and enhances the adaptivity, however it relies on deep networks, lacks transparency and limits usability in constrained environment. Although learning-based encryption approaches improve content adaptivity, their

dependence on model, training, large datasets, and high computational complexity limits their applicability to lightweight and resource-constrained imaging systems.

C. Hybrid ML with Chaos

The authors Gogineni et al., [28] presented a hybrid encryption system that combines chaotic maps with autoencoder-based transformations which improve robustness but still require supervised training and significant model computation. On the other hand, Nair et al., [29] introduced a deep-learning-assisted chaotic encryption-decryption framework that demonstrates strong diffusion but rely on deep models that limit real-time deployment. Hwang et al., [30] also presented a comprehensive survey of ML techniques integrated with chaotic encryption which highlights the potential but also identify challenges such as interpretability, parameter sensitivity and computational overhead in most ML-chaos hybrids. The authors Liu [31] presented a chaos-CNN-driven compressive image encryption modeling that improves key sensitivity but make the system dependent on CNN training cycles and increased architectural complexity. Consequently, existing hybrid chaos-learning frameworks have not yet demonstrated a lightweight feature-adaptive mechanism which is capable of generating image dependent chaotic dynamics without iterative model training. From the above analysis it is evident that the principal challenge is not the generation of chaotic keystreams themselves, but the design of lightweight feature-adaptive mechanisms that enable the chaotic dynamics to respond to the statistical characteristics of the plaintext image without requiring computationally intensive model training.

The above literature indicates that existing chaotic encryption schemes predominantly employ fixed or key-dependent chaotic parameterization, whereas learning-based adaptive approaches often rely on computationally intensive training models. Consequently, a lightweight training-free framework that systematically maps compact statistical image descriptors to image-dependent chaotic parameter modulation while preserving computational efficiency and interpretability remains insufficiently explored. To address this gap, this study proposes a feature-adaptive chaotic encryption framework that employs PCA-derived statistical descriptors to dynamically generate content-dependent chaotic parameters and corresponding image-specific keystreams.

III. Research Problem

Despite significant advances in chaotic and learning-based image encryption, achieving content adaptivity, computational efficiency, and strong cryptographic security within a unified framework remains challenge. Conventional chaotic encryption schemes typically employ fixed or key-dependent chaotic parameters that do not explicitly adapt to image-specific statistical characteristics, whereas learning-based adaptive approaches require computationally intensive training and large datasets, which restricts their applicability in resource-constrained environments. Therefore, the fundamental research problem is to develop a lightweight, training-free, and interpretable image encryption framework that derives statistical image descriptors to dynamically modulate chaotic parameters and generate content-dependent keystreams while maintaining strong resistance against statistical, differential, and key-sensitivity attacks.

IV. Research Method

This section presents the mathematical formulation and algorithmic design of the proposed Feature-Adaptive Chaotic Parameter Modulation (FACPM) framework. The proposed framework establishes a deterministic mapping between compact statistical image descriptors and chaotic system parameters, which enables image-dependent keystream generation without iterative model training. Unlike conventional chaotic encryption, where chaotic parameters remain fixed or user-defined, the proposed framework adaptively modulates the chaotic dynamics according to the statistical characteristics of each plaintext image while preserving computational efficiency and interpretability. The resulting adaptive encryption process is designed to ensure the following:

a. Content-adaptive chaotic parameter modulation through PCA-derived statistical descriptors.

b. Deterministic image-dependent keystream generation without model training

c. Cryptographically strengthened keystream generation using HMAC to improve finite-precision robustness.

d. Improve confusion and diffusion by adapting chaotic dynamics to image content.

The following Fig.1 illustrates the overall architecture of the proposed Feature-Adaptive Chaotic Parameter Modulation (FACPM) framework.

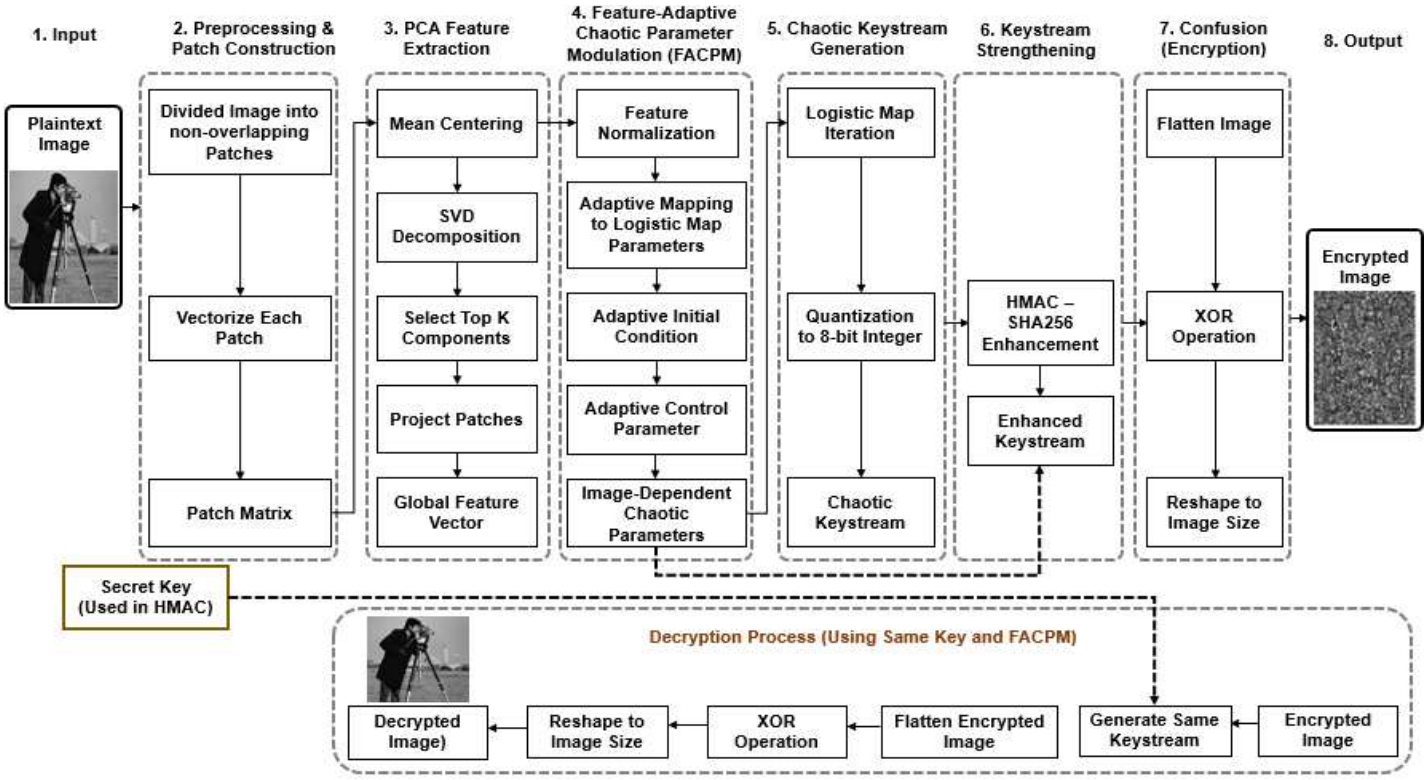


Fig. 1. Overall workflow of the proposed feature-adaptive chaotic parameter modulation (FACPM)-based image encryption framework.

A. Pre-processing and Patch Extraction

Let the input grayscale image be $I \in \mathbb{R}^{H\times W}$, whereas to embed the local content characteristics into the encryption process, the image is further partitioned into fixed size non-overlapping patches of dimension $p \times p$. Here for image dimensions of H and W, divisible by, each patch is further vectorized with the following mathematical expression as follows:

$$x_k = vec(I[i{:}\, i+p, j{:}\, j+p], \quad k = 1,2,\dots,N, \tag{1}$$

Here the total number of patches can be computed as follows:

$$N = {HW}/{p^2} \tag{2}$$

Further stacking all vectorized patches results in the patch matrix as follows:

$$X = [x_1, x_2, \dots, x_N]^T \in \mathbb{R}^{N\times p^2} \tag{3}$$

Patch-level representation preserves local spatial statistics that are generally lost when global image descriptors are used. Consequently, the derived PCA features capture local texture variability and structural information more effectively, which enables finer adaptive modulation of the chaotic parameters. Unlike, fixed chaotic-map systems that generate identical keystreams for all images, the proposed framework dynamically adapts its chaotic behaviour according to underlying texture complexity, local variance, and spatial intensity distribution of each image. This feature-adaptive modulation strengthens the confusion-diffusion process while increasing resistance against statistical and differential attacks.

B. PCA-based Unsupervised Feature Extraction

In the proposed work PCA is employed to extract compact, unsupervised statistical descriptors, from the patch matrix $X = [x_1, x_2, \dots, x_N]^T \in \mathbb{R}^{N\times p^2}$ where each row refers to the vectorized content of a local image patch. PCA transforms these high-dimensional patch vectors into a lower-dimensional latent space that captures the dominant structural variations of the plaintext image.

Mean Centring: Here each patch vector is first centered around the global patch mean which is mathematically expressed as follows:

$$\tilde{X} = X - \mu, \;\; \mu = {1}/{N} \sum_{k=1}^{N} x_k \tag{4}$$

Here mean cantering ensures that the PCA focuses on variations in texture and intensity patterns rather than absolute brightness, which stabilizes the chaotic parameter estimation. Further the system also employs singular value decomposition which is modelled as follows:

Singular Value Decomposition: PCA is further implemented via the SVD of the centered matrix:

$$\tilde{X} = USV^T \tag{5}$$

Here in the above expression (5), U contains the left singular vectors, S contains singular values arranged in descending order

and V contains the principal directions (eigenvectors of the covariance matrix). Here it has to be noted that the first K principal components capture the most informative directions:

$$W = V_{1:K} \tag{6}$$

This selection approach offers a compact subspace capturing the dominant local-texture signatures of the underlying image.

Adaptive PCA Feature Vector: The projected representation of each patch onto the PCA subspace is estimated as:

$$z_k = \tilde{x}_k W \tag{7}$$

Here the global PCA descriptor of the image is also obtained as the mean activation over all patches:

$$\mathfrak{f} = {}^{1}/_{N} \sum_{k=1}^{N} z_k \tag{8}$$

This feature vector is low dimensional, stable and compact making it suitable for driving adaptive encryption parameters. Unlike deep-learning feature extractors, PCA requires only, matrix, centering, one-pass SVD, small-dimensional projections where the computational cost is approximately $O(N.p^2)$ which makes it suitable for embedded systems, IoT imaging devices and edge encryption schemes. PCA is adopted as it offers deterministic, reproducible, and interpretable feature extraction without iterative model training. Consequently, the proposed framework achieves content-adaptive chaotic parameter modulation while maintain low computational complexity. This approach makes it more suitable for resource constrained secure imaging applications than training based deep learning (DL) approaches.

C. Feature-Adaptive Chaotic Parameter Modulation (FACPM)

The FACPM constitutes the core contribution of the proposed framework. Instead of employing fixed or manually selected chaotic parameters, FACPM establishes a deterministic mapping between compact statistical image descriptors extracted by PCA and the parameters governing the chaotic system. Consequently, the generated chaotic dynamics become dependent on the structural characteristics of the plaintext image while remains completely deterministic for identical inputs. Here the modulation process consists of four sequential stages which are (i) extraction of compact patch-level statistical descriptors using PCA, (ii) normalization of the extracted feature vector to obtain a stable numerical representation, (iii) deterministic transformation of the normalized features into the initial condition of x_0 and control parameter r of the logistic map, and (iv) generation of an image-dependent chaotic keystream for subsequent confusion-based encryption. The complete mapping can be summarized as $I \to X \to \mathfrak{f} \to \ddot{\mathfrak{f}} \to (\mathrm{x}_0, \mathrm{r}) \to K \to E$. Here I refers to the plaintext image and X represents the patch matrix, $\mathfrak{f}$ represents the PCA feature vector whereas $\ddot{\mathfrak{f}}$ is the normalized feature vector. $(\mathrm{x}_0, \mathrm{r})$ refers to the adaptively modulated chaotic parameters, and K is the generated keystream, and E denotes the encrypted image. Since the parameters are directly derived from statistical image characteristics, different plaintext images naturally generate different chaotic trajectories even under identical secret keys. This feature modulation significantly increases plaintext sensitivity while also preserve the computational efficiency of conventional chaotic encryption.

D. Adaptive Chaotic Parameter Computation

Let the feature vector of an image is denoted as $\mathfrak{f} \in \mathbb{R}^K$. To ensure compatibility with chaotic maps and avoid numerical instability the feature vector is further normalized as follows:

$$\hat{\mathfrak{f}} = {\mathfrak{f} - min(\mathfrak{f})}\Big/{max(\mathfrak{f}) - min(\mathfrak{f}) + 10^{-12}} \tag{9}$$

This normalization approach scales the features to range of $[0,1]$ while the small constant 10^{-12} prevents division by zero. Using these normalized features, the parameters of the logistic map are derived adaptively to increase the sensitivity of the chaotic sequence to the image content. Here in the proposed framework the initial condition x_0 and control parameter r are computed as follows:

Adaptive Initial Condition:

$$\mathrm{x}_0 = 0.1 + 0.8\left({}^{1}/_{\mathrm{K}} \sum_{\mathrm{i}=1}^{\mathrm{K}} \hat{\mathfrak{f}}^{\mathrm{i}}\right) \tag{10}$$

Adaptive Control Parameter:

$$\mathrm{r} = 3.6 + 0.399\left({}^{1}/_{\mathrm{K}} \sum_{\mathrm{i}=1}^{\mathrm{K}} \left|\hat{\mathfrak{f}}^{\mathrm{i}}\right|\right) \tag{11}$$

Here x_0 and r are dynamically adjusted based on the statistical distribution of the image features. This adaptiveness in the proposed framework ensures that even slight variations in the image content produce significantly different chaotic sequences, which enhance security against chosen-plaintext and brute-force attacks. By linking the logistic map parameters directly to the image characteristics, the encryption becomes highly sensitive to input variations providing robust diffusion and confusion in the encrypted output. Here the mapping constants are selected to constrain the adaptive parameters within the chaotic operating region of the logistic map ($3.6<\mathrm{r}<3.999$), which ensures stable chaotic behaviour while preventing non-chaotic operating regions.

E. Chaotic Keystream Generation

After deriving the adaptive parameters x_0, r for logistic map, the chaotic sequence is generated by iterating the logistic map equation:

$$\mathrm{x}_{\mathrm{n}+1} = \mathrm{r}\mathrm{x}_{\mathrm{n}}(1 - \mathrm{x}_{\mathrm{n}}) \tag{12}$$

Where $n = 0,1,2, \ldots . HW - 1$, and HW is the total number of pixels in the image. The recursive iteration produces a sequence of real numbers in the range of $(0,1)$ that is highly sensitive to initial condition and control parameter, ensuring that even small changes in the image or key produce drastically different sequences. To make this sequence suitable for digital encryption, the chaotic values are quantized to 8-bit integers:

$$k_n = \lfloor (x_n - \lfloor x_n \rfloor) \times 256 \rfloor \quad (13)$$

This step converts the continuous chaotic values into discrete values in the range of $[0,255]$ which can be directly applied to pixel-level encryption. Finally, the generated keystream vector for the entire image is defined as follows:

$$K = [k_1, k_2, \ldots, k_{HW}] \quad (14)$$

This serves as the encryption mask applied to the image pixels. Due to strong dependence of K on the adaptive parameters the keystream inherits high sensitivity to the image features which significantly enhances resistance against cryptanalysis attacks such as known-plaintext or chosen-plaintext attacks.

a. Keystream Strengthening via HMAC

The generated keystream K is subsequently strengthened using HMAC-SHA256 before encryption to improve its cryptographic robustness. This cryptographic post-processing mitigates finite-precision effects and reduces the predictability associated with pure logistic-map sequences, thereby enhancing the security of the generated keystream. Mathematically the HMAC-enhanced keystream can be represented as follows:

$$\mathrm{K}' = \mathrm{HMAC}_{\mathrm{SHA256}}(\mathrm{secret}_{\mathrm{key}}, \mathrm{K}) \quad (15)$$

This enhanced K' is then subsequently used in the XOR-based confusion encryption which is further also highlighted in equation (17).

F. XOR-Based Confusion Encryption

Once the chaotic keystream K is generated, the encryption process further introduces confusion by combining the keystream with image pixels. First the original image be $I \in \mathbb{R}^{H \times W}$ is reshaped into one-dimensional vector:

$$I_{\mathrm{f}} = vec(I) \quad (16)$$

Here the function vector stacks all pixel values sequentially into a column vector. The actual encryption is performed using the bitwise XOR operation between the image vector and the chaotic keystream which is analytically modeled as follows:

$$E_{\mathrm{f}} = I_{\mathrm{f}} \oplus K \quad (17)$$

This operation in expression (16) ensures that each pixel is masked by the corresponding keystream value, providing strong confusion since a small change in K or I_{f} results in a completely different E_{f}. Finally, the encrypted vector is reshaped back to the original image dimensions:

$$E = reshape(E_{\mathrm{f}}, H, W) \quad (18)$$

This mathematical expression produces the final encrypted image E. By leveraging the adaptive chaotic keystream and XOR operation, this scheme achieves high sensitivity to both the image content and the key making it robust against both statistical and differential attacks.

G. Decryption Process

The decryption process exploits the symmetry of the XOR operation. Since XOR is its own inverse, applying the same keystream K used during encryption to the encrypted image E perfectly recovers the original image:

$$D = E \oplus K \quad (19)$$

Here D refers to the decrypted image, this property ensures that the decryption is straightforward and computationally efficient the accuracy of the decryption relies entirely on using the exact chaotic keystream K which depends on the adaptive parameters x_0 and r derived from the original image features. Any small derivation in the keystream or parameters would result in a completely different decrypted image, providing an inherent sensitivity that strengthens the encryption against brute-force or key-guessing attacks. After integrating the HMAC strengthening the keystream used in XOR can be replaced with enhanced keystream K'. Finally, the proposed framework evaluates the effectiveness of the proposed approach using standard security and performance metrics. The following analytical algorithm design shows the step-by-step computing process involved in the proposed FACPM Chaotic Encryption Framework.

Algorithm 1: Feature-Adaptive Chaotic Parameter Modulation (FACPM) for Image Encryption

Input: Image I (H×W), patch size p, PCA dimension K
Output: Encrypted image E

Begin
1: Divide I into N = (HW / p²) patches → X
2: Compute mean μ and centered matrix $\tilde{X}$ = X − μ
3: Perform SVD: $\tilde{X}$ = U S V^T
4: Select first K principal components: W = V[1: K]
5: Compute adaptive feature vector f = mean ($\tilde{X}$ W)
6. FACPM Normalizes statistical descriptors → $\hat{\mathrm{f}}$
7: FACPM adaptively computes logistic parameters:

$$x_0 = 0.1 + 0.8\left(\tfrac{1}{K}\sum_{i=1}^{K}\hat{f}^i\right)$$

$$r = 3.6 + 0.399\left(\tfrac{1}{K}\sum_{i=1}^{K}\left|\hat{f}^i\right|\right)$$

8: Initialize x = x0
9: For n = 1 to HW do:
x = r * x * (1 - x)
k[n] = floor ((x - floor(x)) * 256)
10: Flatten image: If = vec(I)
11: Encrypt: E_{f}= If XOR k
12: Reshape E_{f} → encrypted image E
Return E

The overall computational complexity of the proposed FACPM framework is dominated by patch extraction and PCA computation. Let N denotes the number of image patches and $p \times p$ is the patch size. Patch extraction and feature matrix construction require $O(N.p^2)$, while PCA performed using SVD on the patch matrix also requires approximately $O(N.p^2)$ for the selected low-dimensional subspace. Adaptive parameter computational is linear in the number of retained principal components $(O(K))$, whereas chaotic keystream generation,

HMAC enhancement, and XOR-based encryption each require linear time with respect to the number of image pixels $(O(HW))$. Therefore the overall complexity of the proposed framework is $O(N.p^2 + HW)$. It clearly demonstrates that the proposed method remains computationally efficient and suitable for real-time and resource constrained secure imaging applications. It has to be noted that the proposed FACPM Chaotic Encryption framework is fully applicable to high-dimensional color images. In this approach the RGB patches can be treated either independently or jointly, whereas PCA is performed on multi-dimensional patch vectors and chaotic seeds are generated adaptively using PCA coefficients.

V. Results and Discussion

This section evaluates the security performance of the proposed Feature-Adaptive Chaotic Parameter Modulation (FACPM) framework implemented in Python 3.10.15 on an Intel Core i5-8250U processor with 12 GB RAM. The proposed framework is assessed using standard image-encryption security metrics which include entropy, adjacent-pixel correlation, NPCR, UACI, and PSNR over multiple 256×256 grayscale benchmark images. The results are further compared with representative fixed-chaotic, AES-based and HMAC-assisted and PCA-only encryption baselines to validate the effectiveness of the feature adaptive chaotic parameter modulation.

A. Visual Outcome Interpretation

Here the histogram comparison in Fig.2 shows that the original image has distinct intensity peaks due to its structured gradient and shapes which makes it statistically predicable. In contrast the encrypted image exhibits a nearly uniform and flattened histogram which indicates that pixel values are evenly dispersed across all gray levels. The near-uniform histogram demonstrates that the adaptive chaotic parameter modulation effectively distributes pixel intensities across the complete gray-level range.

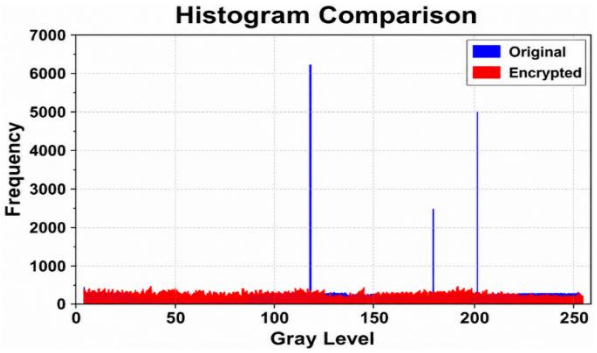


Fig. 2. Histogram comparison of the plaintext and FACPM-encrypted images.

This behaviour confirms that the image-dependent histogram keystream generated by FACPM suppresses statistical redundancy. The encrypted image in exhibits an approximately uniform gray-level distribution, which implies more effective statistical randomization and strong resistance against histogram-based cryptanalysis.

B. Comparative Analysis of Security Metrices

The UACI comparison parameter clearly in Fig.3 clearly shows that the proposed FACPM-Based Adaptive Encryption achieves highest UACI which is approx. 40.81% indicating superior sensitivity to plaintext changes compared to Fixed Chaotic (Approx. 33.18%), Traditional AES (Approx. 24.53%) and PCA-only (6.56%). Critically this result suggests that the proposed method offer stronger diffusion and better resists differential attacks which outperforms conventional AES and static chaotic schemes while PCA alone is clearly insufficient for secure encryption.

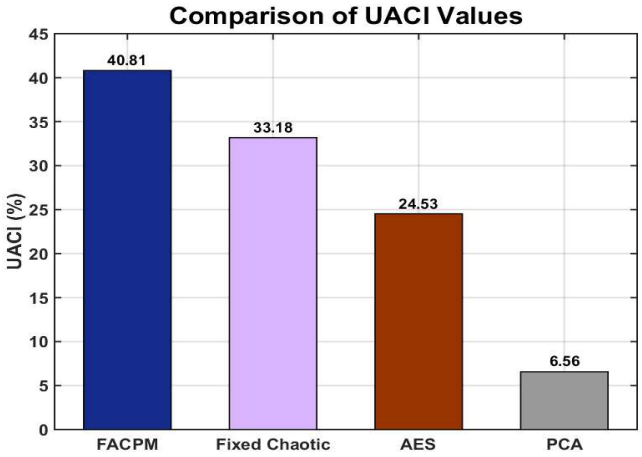


Fig. 3. Comparison of UACI values obtained using FACPM and representative baseline encryption methods.

The highest UACI (≈40.81%), demonstrate that adaptive chaotic parameter modulation significantly improves diffusion by generating distinct keystreams for different plaintext characteristics. The correlation comparison (Fig.4) clearly shows that the proposed FACPM method achieves the lowest correlation (-0.33) which demonstrates superior decorrelation capability compared to all other techniques. On the other hand, the Fixed Chaotic approach also shows weak correlation (-0.07) whereas AES exhibits a moderate positive correlation (0.51). In contrast standard PCA produce the highest correlation (0.91) confirming that it preserves strong linear relationships. These results highlight the effectiveness of the proposed FACPM model in minimizing correlation and ensuring improved randomness or feature independence.

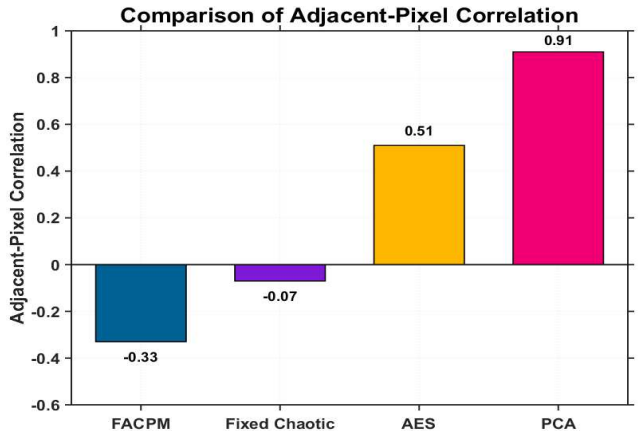


Fig. 4. Comparison of adjacent-pixel correlation coefficients for different image encryption methods. Lower correlation indicates stronger statistical decorrelation and higher encryption security

It is observed in the Fig.5 that the proposed FACPM framework achieves the lowest adjacent-pixel correlation (-0.33) which implies that adaptive modulation of chaotic parameters effectively destroys spatial dependency between neighbouring pixels. This demonstrates the effectiveness of feature-driven chaotic dynamics. The negative correlation obtained by FACPM implies effective elimination of the strong spatial dependency present in natural images which also demonstrates superior confusion capability in comparison with fixed chaotic and conventional encryption schemes.

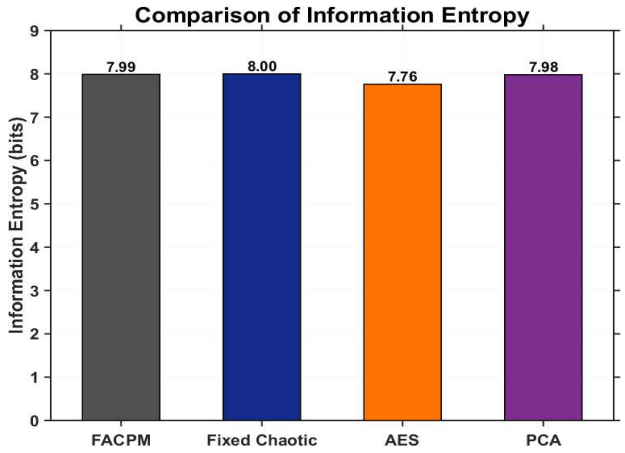


Fig. 5. Comparison of information entropy achieved by different image encryption methods. Values closer to the theoretical maximum of 8 bits indicate higher randomness and stronger resistance against statistical attacks.

The entropy analysis (Fig.6) reveals that the proposed method (7.99 bits) and Fixed Chaotic model (8.00 bits) achieve entropy values very close to the ideal value of 8 bits, indicating highly uniform and unpredictable encrypted outputs. In comparison AES exhibits a lower entropy of 7.76 bits, suggesting relatively less randomness. The PCA-based method also maintains high entropy (7.98) reflecting strong diffusion characteristics. Overall, the results confirm that proposed FACPM approach ensures near-optimal randomness enhancing encryption strength and resistance against statistical attacks. The entropy achieved by FACPM (7.99 bits) approaches the theoretical optimum of 8 bits, which confirms that adaptive chaotic parameter modulation produces highly random ciphertext distributions while preserve computational simplicity.

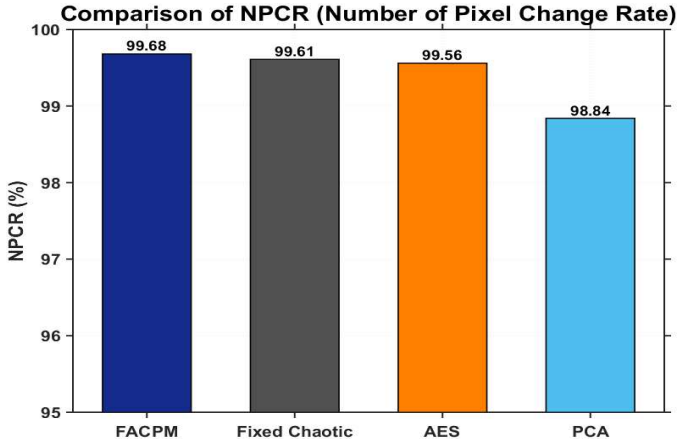


Fig. 6. Comparison of the Number of Pixels Change Rate (NPCR) achieved by the proposed FACPM framework and existing image encryption methods.

Fig.6 compares the NPCR performance of the proposed FACPM framework with Fixed Chaotic, AES and PCA-based encryption methods. FACPM achieves the highest NPCR (~99.68%), followed by Fixed Chaotic (99.61%), AES (99.56%) and PCA (98.84%). Since higher NPCR value indicate stronger diffusion and greater sensitivity to plaintext modifications, the proposed FACPM framework demonstrates superior resistance to differential attacks and produces a near-ideal avalanche effect. Although NPCR values are comparable across the evaluated methods, the proposed FACPM simultaneously maintains high entropy, lower correlation, and improved UACI indicating that adaptive chaotic parameter modulation enhances overall security rather than optimizing a single metric.

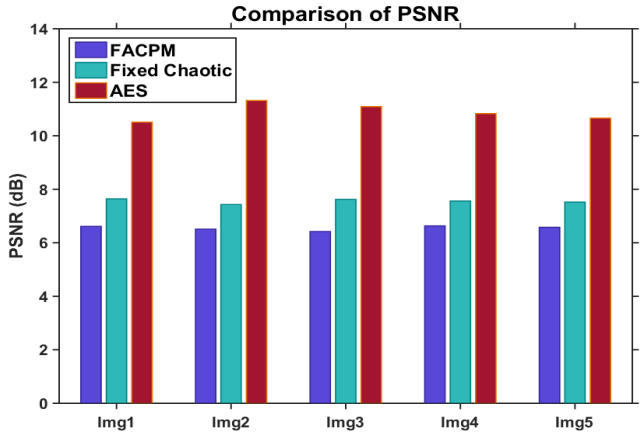


Fig. 7. PSNR comparison of FACPM and baseline encryption methods over five benchmark grayscale images. Lower PSRN indicates stronger visual distortion in the encrypted domain and improved confidentiality

The PSNR comparison (Fig.7) indicates that the AES-like method achieves the highest reconstruction quality, followed by the Fixed Chaotic approach, whereas the proposed FACPM method produces lower PSNR values across all five test images. Although lower PSNR reflects higher distortion in the encrypted domain, this characteristic directly translates into stronger security, as it becomes significantly harder for an attacker to infer any visual information from the encrypted output. The consistently reduced PSNR of the Adaptive ML-driven method therefore demonstrates its superior ability to obscure image content, offering enhanced confidentiality compared to the other techniques while still maintaining functional reconstruction performance in the decryption phase. The lower PSNR values correspond to greater visual distortion between plaintext and ciphertext images which implies stronger concealment of image content. Since PSNR is evaluated between the original and encrypted images, lower values imply improved confidentiality while decrypted image remains identical to the original. The experimental analysis also shows that the image encryption is highly secure and sensitive: the ciphertexts have near-ideal randomness (entropy ≈ 8), extremely low correlation with the original (Corr ≈ 0), and strong diffusion (NPCR ~99.6%, UACI ~40.81%). The scheme is also highly key- and plaintext-sensitive, as flipping a key bit or changing one pixel drastically

alters the encrypted output. The proposed FACPM employs a cryptographically strengthened keystream generated through adaptive chaotic parameter modulation and HMAC-SHA256, which resulted in a sufficiently large effective keyspace to resist practical brute-force attacks.

C. *Quantitative Evaluation Across Adaptive, Chaotic, And HMAC Models*

Across the evaluated test images, the proposed Feature-Adaptive Chaotic Parameter Modulation (FACPM) framework consistently achieves high information entropy (≈7.997), strong diffusion (NPCR ≈99.68%) and high pixel-change uniformity (UACI ≈40.81%). The correlation values remain closer to zero which clearly demonstrates effective decorrelation of adjacent pixel intensities after encryption. These results collectively indicate that FACPM provides near-ideal randomness, strong diffusion, and effective statistical concealment while maintain performance comparable to conventional fixed-chaotic and cryptographically strengthened encryption schemes. Overall, the experimental evaluation confirms that adaptive modulation of chaotic parameters using PCA-derived statistical descriptors improves content adaptivity while preserve computational efficiency.

VI. CONCLUSION

The study presents a Feature-Adaptive Chaotic Parameter Modulation (FACPM) framework for adaptive chaotic image encryption that demonstrates strong security characteristics across multiple quantitative evaluation metrics. The proposed method consistently achieved near-optimal entropy, high NPCR, and enhanced UACI values, which implies improved randomness, diffusion, and sensitivity, to plaintext modifications in comparison with Fixed Chaotic, AES-based, and PCA-based methods. Correlation analysis further confirms the framework's effective decorrelation capability, supressing residual structural information in the encrypted images. Overall, the experimental results demonstrates that deterministic feature-adaptive chaotic parameter modulation using PCA-derived statistical descriptors offer an interpretable, computationally efficient, and content-adaptive encryption strategy with strong resistance against statistical and differential attacks. Future work will focus on extending the adaptive framework to video and multimodal data, integrating lightweight architectures for real-time deployment, and exploring transformer-based or self-supervised models to further strengthen key sensitivity and diffusion characteristics. Additionally, hardware acceleration and FPGA/GPU-based optimization will be investigated to support scalable and energy-efficient encryption for edge and IoT environments.

Declarations

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

The data can be made available on reasonable request to the authors.

Funding

Not Applicable.

Ethical Approval

Not Applicable.

REFERENCES

[1] K. G. Salim, S. M. K. Al-alak, and M. J. Jawad, "Improved image security in internet of thing (IOT) using multiple key AES," *Baghdad Sci. J.*, vol. 18, no. 2, p. 0417, 2021, doi: 10.21123/bsj.2021.18.2.0417.

[2] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A novel image steganography method for industrial internet of things security," *IEEE Trans. Industr. Inform.*, vol. 17, no. 11, pp. 7743–7751, 2021, doi: 10.1109/tii.2021.3053595.

[3] A. Mishra, B. B. Gupta, and K. Mishra, "Security Threats and Countermeasures for Digital Images in Smart Systems," in *Digital Forensics and Cyber Crime Investigation*, CRC Press, 2024, pp. 153–167.

[4] A. Bhardwaj, S. Bharany, A. Osman Ibrahim, A. Almogren, A. Ur Rehman, and H. Hamam, "Unmasking vulnerabilities by a pioneering approach to securing smart IoT cameras through threat surface analysis and dynamic metrics," *Egypt. Inform. J.*, vol. 27, no. 100513, p. 100513, 2024, doi: 10.1016/j.eij.2024.100513.

[5] A. S. Nadhan and I. Jeena Jacob, "Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications," *Biomed. Signal Process. Control*, vol. 88, no. 105511, p. 105511, 2024, doi: 10.1016/j.bspc.2023.105511.

[6] H. R. Chennamma and B. Madhushree, "A comprehensive survey on image authentication for tamper detection with localization," *Multimed. Tools Appl.*, vol. 82, no. 2, pp. 1873–1904, 2023, doi: 10.1007/s11042-022-13312-1.

[7] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2585, 2023, doi: 10.3390/math11112585.

[8] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimed. Tools Appl.*, vol. 81, no. 18, pp. 25497–25518, 2022, doi: 10.1007/s11042-022-12595-8.

[9] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, 2022, doi: 10.1007/s10207-022-00588-5.

[10] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H.-N. Lee, "A systematic literature review on chaotic maps-based image security techniques," *Comput. Sci. Rev.*, vol. 54, no. 100659, p. 100659, 2024, doi: 10.1016/j.cosrev.2024.100659.

[11] K. Panwar, S. Kukreja, A. Singh, and K. K. Singh, "Towards deep learning for efficient image encryption," *Procedia Comput. Sci.*, vol. 218, pp. 644–650, 2023, doi: 10.1016/j.procs.2023.01.046.

[12] E. Abdellatef, E. A. Naeem, and F. E. A. El-Samie, "DeepEnc: deep learning-based CT image encryption approach," *Multimedia Tools and Applications*, vol. 83, pp. 11147–11167, 2024.

[13] Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 9, pp. 4915–4929, 2022, doi: 10.1109/TNNLS.2021.3062754.

[14] S. Arumugam and K. Annadurai, "An efficient machine learning based image encryption scheme for medical image security," *J. Med. Imaging Health Inform.*, vol. 11, no. 6, pp. 1533–1540, 2021, doi: 10.1166/jmihi.2021.3470.

[15] Y. Alslman, E. Alnagi, A. Ahmad, Y. AbuHour, R. Younisse, and Q. Abu Al-haija, "Hybrid encryption scheme for medical imaging using AutoEncoder and advanced encryption standard," *Electronics (Basel)*, vol. 11, no. 23, p. 3967, 2022, doi: 10.3390/electronics11233967.

[16] K. Panwar, A. Singh, S. Kukreja, K. K. Singh, N. Shakhovska, and A. Boichuk, "Encipher GAN: An end-to-end color image encryption system using a deep generative model," *Systems*, vol. 11, no. 1, p. 36, 2023, doi: 10.3390/systems11010036.

[17] S. Bhattacharjee, M. Gupta, and B. Chatterjee, "Time efficient image encryption-decryption for visible and COVID-19 X-ray images using modified chaos-based logistic map," *Appl. Biochem. Biotechnol.*, vol. 195, no. 4, pp. 2395–2413, 2023, doi: 10.1007/s12010-022-04161-7.

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

[19] D. Abu Laila *et al.*, "Enhancing 2D logistic chaotic map for gray image encryption," in *Risk Assessment and Countermeasures for Cybersecurity*, IGI Global, 2024, pp. 170–188.

[20] S. Kanwal, S. Inam, S. Al-Otaibi, J. Akbar, N. Siddiqui, and M. Ashiq, "An efficient image encryption algorithm using 3D-cyclic chebyshev map and elliptic curve," *Sci. Rep.*, vol. 14, no. 1, p. 29626, 2024, doi: 10.1038/s41598-024-77955-w.

[21] T. Ga and S. M. S. Bhanu, "Chebyshev chaotic map with attribute-based encryption on session-based data-sharing in fog environment. Peer-to-Peer Networking and Applications," vol. 18, 2025.

[22] L. Dai, L. Hu, L. Chen, C. Wang, and F. Lin, "An image double encryption based on improved GAN and hyper chaotic system," IEEE Access, vol. 12, pp. 135779–135798, 2024, doi: 10.1109/access.2024.3462547.

[23] Mohammed, R.A., Khodher, M.A.A.A. and Alabaichi, A, "Image encryption in IOT using hyper-chaotic system," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 6, pp. 101–112, 2023, doi: 10.22266/ijies2023.1231.09.

[24] F. Alqahtani, "AI-powered image security: Utilizing autoencoders for advanced medical image encryption," *Comput. Model. Eng. Sci.*, vol. 141, no. 2, pp. 1709–1724, 2024, doi: 10.32604/cmes.2024.054976.

[25] F. Ahmed *et al.*, "A DNA based colour image encryption scheme using A convolutional autoencoder," *ACM Trans. Multimed. Comput. Commun. Appl.*, 2022, doi: 10.1145/3570165.

[26] A. Saini and R. Sehrawat, "An intelligent and efficient CNN-AES framework for image block encryption with a multi-key approach," *Eng. Res. Express*, vol. 7, no. 1, p. 015206, 2025, doi: 10.1088/2631-8695/ada3af.

[27] L. Feng, J. Du, C. Fu, and W. Song, "Image encryption algorithm combining chaotic image encryption and convolutional neural network," *Electronics (Basel)*, vol. 12, no. 16, p. 3455, 2023, doi: 10.3390/electronics12163455.

[28] V. Gogineni, H. Challa, A. Chinta, and S. Tupakula, "Enhancing Image Security: A Hybrid Approach Integrating Chaos-Based Encryption and Autoencoder-Based Transformation," in *International Conference on Artificial Intelligence on Textile and Apparel*, Singapore; Singapore: Springer Nature, 2024, pp. 377–386.

[29] B. V. Nair, V. S. Vismaya, S. S. Muni, and A. Durdu, "Deep learning and chaos: A combined approach to image encryption and decryption," *arXiv [cs.CR]*, 2024. doi: 10.48550/arXiv.2406.16792.

[30] J. Hwang *et al.*, "Machine learning in chaos-based encryption: Theory, implementations, and applications," *IEEE Access*, vol. 11, pp. 125749–125767, 2023, doi: 10.1109/access.2023.3331320.

[31] L. Liu, "Optimization of Key-Driven Compressive Image Encryption Algorithm Based on Chaos-CNN Hybrid Network," *Journal of Commercial Biotechnology*, vol. 30, no. 3, pp. 1035–1046, 2025.