International Journal of Safety and Security Engineering
Vol. 16, No. 5, May, 2026, pp. 941-951
Journal homepage: http://iieta.org/journals/ijsse

A Chaos-Guided Feature Level Image Encryption Framework Based on Tinkerbell Map and Fusion Autoencoder

Christy Atika Sari[1*], Heru Lestiawan[1], Pulung Nurtantio Andono[2], Aris Marjuni[3], Agus Winarno[4], Chaerul Umam[1], Musab Iqtait[5], Md Kamruzzaman Sarker[6]

[1] Department of Informatics Engineering, Universitas Dian Nuswantoro, Semarang 50131, Indonesia
[2] Department of Computer Science Doctoral Program, Universitas Dian Nuswantoro, Semarang 50131, Indonesia
[3] Department of Master of Informatics Engineering, Universitas Dian Nuswantoro, Semarang 50131, Indonesia
[4] Department of Information System, Universitas Dian Nuswantoro, Semarang 50131, Indonesia
[5] Department of Data Science and Artificial Intelligence, Zarqa University, Zarqa 13110, Jordan
[6] Department of Computer Science, Bowie State University, Maryland 20715-9465, United States

Corresponding Author Email: christy.atika.sari@dsn.dinus.ac.id

https://doi.org/10.18280/ijsse.160501

Received: 13 March 2026
Revised: 24 April 2026
Accepted: 29 April 2026
Available online: 31 May 2026

Keywords:
autoencoder, chaotic map, feature-level encryption, image encryption, security analysis

ABSTRACT

With the increasing use of digital images in communication and storage systems, ensuring image security against various attacks has become a critical challenge. Traditional chaos-based image encryption methods mainly operate at the pixel level, which may limit their effectiveness in fully disrupting spatial correlations, particularly for complex image structures. To address this limitation, this study proposes a chaos-guided feature-level image encryption framework that integrates a fusion autoencoder with a two-dimensional Tinkerbell chaotic map. The proposed approach introduces chaotic control into the deep feature domain, followed by implicit permutation and diffusion processes, in order to enhance encryption randomness while preserving reconstruction capability. The performance of the proposed method is evaluated using standard grayscale test images, including Barbara, House, Tree, and Candy, under a controlled experimental setting. Comparative analysis is conducted by integrating multiple chaotic maps within the same fusion autoencoder architecture to ensure fair evaluation. Security performance is assessed using entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM) metrics. Experimental results show that the proposed method achieves entropy values close to the theoretical ideal (up to 7.999), NPCR values around 99.62%–99.64%, and UACI values near 33.47%, indicating strong resistance to statistical and differential attacks within the evaluated setting. In addition, noise robustness analysis under Gaussian and salt-and-pepper disturbances demonstrates that the method maintains stable reconstruction quality, with PSNR values above 29 dB and SSIM values exceeding 0.92. These results indicate that the integration of the Tinkerbell chaotic map within a feature-level autoencoder framework provides improved randomness and diffusion characteristics compared to conventional pixel-level chaos-based approaches, while maintaining reliable image reconstruction under the tested conditions.

1. INTRODUCTION

Digital technologies and communication networks led to an extensive exchange of image data across various application domains [1], ranging from multimedia systems to security-critical environments such as healthcare [2, 3], industrial monitoring [4], and intelligent surveillance [5]. Digital images often carry sensitive and high-value information, making them attractive targets for unauthorized access, interception, and tampering during storage and transmission [6-8]. Unlike textual data, images exhibit intrinsic characteristics such as high data redundancy, strong spatial correlation among neighboring pixels, and complex two-dimensional structures, which significantly reduce the effectiveness of conventional cryptographic algorithms when directly applied [9, 10]. Moreover, the increasing availability of computational resources and data-driven analysis techniques has further exposed traditional image encryption schemes to statistical analysis and learning-based attacks [11]. These challenges highlight a fundamental limitation of classical encryption approaches and emphasize the need for more adaptive image encryption mechanisms that can effectively disrupt statistical patterns while maintaining reliable image reconstruction for authorized users.

Despite the widespread adoption of chaotic systems in image encryption, chaos-based methods alone have gradually

revealed inherent limitations in addressing modern security requirements [11-13]. Most existing chaotic encryption schemes rely heavily on low-dimensional chaotic maps to generate pseudo-random sequences for pixel permutation and diffusion [14, 15]. Although such systems exhibit sensitivity to initial conditions and parameter variations, their deterministic nature and limited phase space often result in non-uniform distributions and residual statistical patterns within the encrypted images. These weaknesses can be exploited through phase space reconstruction, known-plaintext attacks, or learning-based analysis, especially when the same chaotic structure is repeatedly employed [16, 17]. Furthermore, chaos-driven encryption mechanisms typically operate at the pixel level, focusing on scrambling and diffusion without considering higher-level feature representations [18, 19]. As a result, they struggle to achieve strong diffusion performance and robustness against noise, cropping, and partial data loss when deployed in complex transmission environments. These observations indicate that relying solely on chaotic methods is no longer sufficient to provide a comprehensive and resilient image encryption solution. To overcome these limitations, recent studies have begun integrating chaotic systems with deep learning models, particularly autoencoder-based architectures, to enhance encryption strength beyond pixel-level operations. This hybrid paradigm aims to combine the randomness of chaos with the representation learning capability of deep neural networks. For instance, the study [20] proposed an image encryption method that combines a logistic chaotic system with a deep autoencoder to generate encrypted images with uniform distribution and high randomness, aiming to resist common cryptanalytic attacks. The logistic chaotic map is used to scramble pixel positions before feeding scrambled images into a deep autoencoder to produce ciphertext, and extensive experiments demonstrate strong statistical performance such as high entropy and key sensitivity. However, this approach fundamentally suffers from reliance on a one-dimensional chaotic map (logistic) whose limited chaotic range and periodic regions may reduce unpredictability and vulnerability, especially under phase space reconstruction attacks, limiting its robustness against advanced cryptanalysis.

Also study [21] introduced an encryption scheme integrating a 6D hyperchaotic system with a Vision Transformer-based autoencoder, where the autoencoder compresses images into latent representations and hyperchaotic sequences scramble and diffuse them. This method shows excellent key space, entropy, and Number of Pixels Change Rate (NPCR)/Unified Average Changing Intensity (UACI) results, suggesting strong resistance to statistical and brute-force attacks. Nonetheless, a critical limitation of this approach is that the latent compression is lossy, which can lead to information degradation and reduced fidelity upon decryption, making it less suitable for applications requiring exact reconstruction or privacy preservation in domains like medical imaging.

Last related study [22] proposed a visual image encryption and compression scheme using a CNN-based autoencoder trained with a masked dataset to learn feature representations for shared encryption and decryption. While effective in preserving confidentiality and reducing dimensionality, the core limitation is that the method relies on a pre-shared mask (secret key) that must be known to the receiver, which introduces practical key distribution and management challenges. Additionally, as the design focuses on compression alongside encryption, it does not explicitly address chaotic perturbation mechanics to enhance security, making it less robust against targeted cryptanalytic attacks compared to hybrid chaos-DL systems.

Based on the above discussion, existing image encryption approaches can be broadly categorized into three main groups. First, pixel-level chaos-based methods rely on low-dimensional chaotic maps to perform permutation and diffusion operations directly on pixel values. While effective in basic scrambling, these methods often suffer from limited phase space and residual statistical patterns. Second, hybrid approaches that combine chaotic systems with autoencoder-based architectures introduce feature representation into the encryption process, improving randomness and security. However, many of these methods either depend on low-dimensional chaotic maps or adopt lossy latent compression, which may reduce reconstruction fidelity. Third, compression-oriented schemes focus on integrating encryption with data reduction, but often require pre-shared masks or introduce additional complexity in key management.

Despite these advancements, a clear gap remains in achieving a tightly integrated framework that simultaneously leverages high-dimensional chaotic dynamics and feature-level representation without compromising reconstruction quality. In particular, existing methods often treat chaotic control and deep feature learning as loosely coupled components, limiting their combined effectiveness. To address this gap, the present study proposes a chaos-guided feature-level image encryption framework that integrates the two-dimensional Tinkerbell chaotic map directly into the feature domain of a fusion autoencoder. This design enables stronger randomness and diffusion characteristics while maintaining stable reconstruction performance, distinguishing it from prior pixel-level, hybrid, and compression-based approaches.

This paper proposes a novel deep learning-based image encryption framework that integrates a two-dimensional Tinkerbell chaotic map with feature-level autoencoder fusion. Unlike logistic-based chaotic systems, the Tinkerbell map offers richer nonlinear dynamics and a larger chaotic space, significantly enhancing key sensitivity and unpredictability. In contrast to lossy latent compression strategies, the proposed framework embeds chaotic perturbations directly into the feature encoding and decoding process of a deep autoencoder, enabling secure encryption while preserving reconstruction fidelity. Furthermore, the proposed method eliminates the need for externally shared masking keys by generating encryption behavior intrinsically through chaos-guided feature fusion. By tightly coupling chaotic dynamics with deep feature representations, the proposed framework provides a more robust, adaptive, and secure image encryption solution capable of overcoming the limitations observed in existing chaos-only and hybrid encryption approaches.

2. PRELIMINARIES

2.1 Chaotic map based on Tinkerbell

Chaotic maps have been extensively utilized in cryptographic systems due to their intrinsic nonlinear behavior, sensitivity to initial conditions, and capability to generate pseudo-random sequences. In contrast to commonly used one-dimensional chaotic maps, two-dimensional chaotic systems provide higher dynamical complexity and a

substantially larger phase space, which are critical for enhancing security in modern image encryption frameworks [23]. In this study, the Tinkerbell chaotic map is employed as the core chaotic mechanism owing to its strong nonlinear coupling and rich chaotic dynamics, making it particularly suitable for feature-level encryption in deep learning–based architectures. The Tinkerbell chaotic map is defined as a discrete-time two-dimensional nonlinear dynamical system [24]. Given an initial state (x_0, y_0) and a set of control parameters (a, b, c, d), the evolution of the chaotic system is governed by the iterative equations, as calculated in Eq. (1). Here, x_n and y_n are the chaotic state variables at the n-th iteration, while a, b, c, and d are real-valued control parameters that determine the system's chaotic behavior. For appropriate parameter selections, the Tinkerbell map exhibits strong chaotic properties, including aperiodicity and ergodicity, which are essential for secure cryptographic key generation. To enhance sensitivity to initial conditions and prevent transient effects, the chaotic system is iterated for a predefined number of steps N_t, during which the initial transient states are discarded. The effective chaotic sequences are then obtained as calculated in Eq. (2). The resulting chaotic sequences X and Y typically exhibit unbounded amplitudes, which are unsuitable for direct integration with deep learning models. Therefore, a normalization operation is applied to map the chaotic values into a bounded interval. This normalization process is performed as expressed in Eq. (3).

$$\begin{aligned} x_{n+1} &= x_n^2 - y_n^2 + ax_n + by_n, \\ y_{n+1} &= 2x_n y_n + cx_n + dy_n \end{aligned} \tag{1}$$

$$X = \{x_n \mid n > N_t\}, Y = \{y_n \mid n > N_t\} \tag{2}$$

$$\begin{aligned} \hat{x}_n &= \frac{x_n - \min(\mathrm{X})}{\max(\mathrm{X}) - \min(\mathrm{X})}, \\ \hat{y}_n &= \frac{y_n - \min(\mathrm{Y})}{\max(\mathrm{Y}) - \min(\mathrm{Y})} \end{aligned} \tag{3}$$

The normalized chaotic sequences $\hat{x}_n$ and $\hat{y}_n$ are then combined to construct a composite chaotic control signal, which is used to guide feature-level transformations within the proposed encryption framework. This fusion operation is formulated as calculated in Eq. (4). In Eq. (4), C_n represents the final chaos-driven control sequence, while α is a weighting factor that balances the influence of both chaotic dimensions. This formulation enables flexible adjustment of chaotic intensity and ensures high randomness in the generated control signal. Unlike conventional chaotic encryption methods that apply chaotic sequences solely for pixel permutation or diffusion [25], the proposed approach integrates the Tinkerbell chaotic dynamics directly into the feature representation domain of a deep autoencoder.

$$\mathrm{C}_n = \alpha\hat{x}_n + (1-\alpha)\hat{y}_n, 0 < \alpha < 1 \tag{4}$$

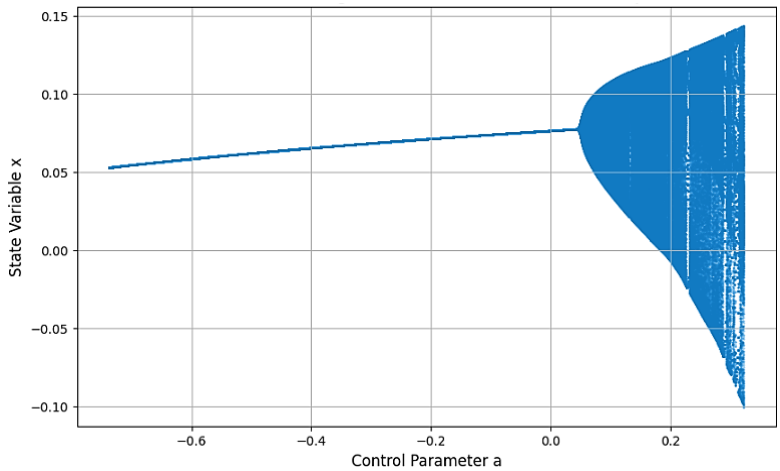

Figure 1. Bifurcation diagram of the Tinkerbell chaotic map with respect to control parameter a
Note: The diagram illustrates the transition from periodic to chaotic behavior. The initial conditions are set to $(x_0, y_0) = (0.1, 0.1)$, while the parameters $b = 0.6$, $c = 2.0$, and $d = 0.5$ are kept constant.

As seen in Figure 1, the bifurcation diagram of the Tinkerbell chaotic map with respect to the control parameter a, while the remaining parameters (b, c, d) and the initial conditions (x_0, y_0) are kept fixed. As the parameter a varies, the evolution of the state variable x_n demonstrates a clear transition from stable behavior to chaotic dynamics [26]. For lower values of a, the sequence $\{x_n\}$ converges to a narrow range, indicating periodic or quasi-periodic motion governed by stable fixed points. Mathematically, this corresponds to regions where the magnitude of the dominant eigenvalues of the system's Jacobian matrix remains less than unity, resulting in bounded and predictable trajectories. As a increases and enters the chaotic regime, the distribution of x_n becomes dense over a wider interval, as observed in Figure 1. In this region, the recurrence relation defined in Eq. (1) produces trajectories that are extremely sensitive to both initial conditions and parameter perturbations, such that $|x_n - x_n'| \to \infty$ for arbitrarily small differences in (x_0, y_0) or a after sufficient iterations. This sensitivity implies that the long-term evolution of the system cannot be predicted through linear approximation or short-term observation, which is a desirable property for cryptographic key generation. The broad chaotic interval illustrated in the bifurcation diagram confirms that the Tinkerbell map offers a richer and more stable chaotic domain compared to low-dimensional maps with narrow chaotic windows. The encryption effect of the Tinkerbell chaotic dynamics is visually demonstrated in Figure 2. As shown in Figure 2(a), the plain image exhibits strong spatial correlations, where neighboring pixel intensities p_i and p_j satisfy a high correlation coefficient $\rho(p_i, p_j) = 1$. Such correlations reflect the inherent redundancy present in natural images and

represent a structural weakness from a cryptographic perspective. If not properly disrupted, these correlations can be exploited through statistical analysis or chosen-plaintext attacks. After applying the Tinkerbell-based encryption process, the cipher image shown in Figure 2(b) displays a noise-like appearance with no visually discernible structures. This indicates that the permutation and diffusion processes driven by the chaotic sequence have effectively transformed the original pixel distribution $P(p)$ into a cipher distribution $P(c)$ that approaches uniformity. From a mathematical standpoint, the encryption aims to minimize spatial correlations such that $\rho(c_i, c_j) \to 0$ for adjacent cipher pixels, while simultaneously increasing entropy toward its theoretical maximum.

(a) Plain image (b) Cipher of Tinkerbell map

Figure 2. Encryption result using Tinkerbell chaotic map

2.2 Chaotic feature key generation

The plaintext image is first processed using the SHA-256 hashing algorithm, which produces a fixed-length 256-bit hash value [27]. Due to the avalanche property of SHA-256, even a minimal variation in the plaintext image results in a significantly different hash output. This characteristic ensures that feature keys generated for two visually similar images remain completely independent, even when identical chaotic parameters are employed. The SHA-256 hash of I is denoted as h = SHA256(I) [27, 28]. In order to introduce spatial dependency between the image content and the chaotic initialization, a plaintext-related offset parameter p is calculated by Eq. (5). Based on Eq. (5), im (i) is the grayscale intensity value of the i-th pixel obtained through raster scanning of the plaintext image. The hash vector h is subsequently segmented into multiple disjoint blocks, each of which is used to perturb the initial conditions of the Tinkerbell chaotic map. Based on the offset parameter p, four 64-bit segments are selected from the hash vector and combined with user-defined secret values $\{b_1, b_2, b_3, b_4\}$ to generate the chaotic initial states. This process is calculated using Eq. (6). The plaintext-dependent components derived from the SHA-256 hash are embedded into the key initialization parameters or securely transmitted alongside the ciphertext, allowing the receiver to reconstruct the same chaotic sequences without requiring access to the original plaintext. Where $h_{m:n}$ is the hash segment extracted from position m to n. Using the initial conditions and parameters defined in Eq. (6), the Tinkerbell chaotic map is iterated according to Eq. (1) to generate chaotic sequences $\{x_n\}$, and $\{y_n\}$. After removing transient states, the resulting sequences are normalized and fused to form a chaos-guided control sequence whose length matches the total number of elements in the encoded feature tensor. Consequently, the generated feature key exhibits strong sensitivity to both the secret parameters and the plaintext image, ensuring that the same secret key produces entirely different feature keys when applied to different images.

$$p = \mathrm{mod}\left(\sum_{i=1}^{WH} i \cdot \mathrm{im}(i), 256\right) \tag{5}$$

$$\begin{cases} x_0 = \dfrac{\mathrm{mod}\left(h_{p:p+64} \oplus b_1, 2^{64}\right)}{2^{64}}, \\ y_0 = \dfrac{\mathrm{mod}\left(h_{p+65:p+128} \oplus b_2, 2^{64}\right)}{2^{64}}, \\ a = \dfrac{\mathrm{mod}\left(h_{p+129:p+192} \oplus b_3, 2^{64}\right)}{2^{64}}, \\ b = \dfrac{\mathrm{mod}\left(h_{p+193:p+256} \oplus b_4, 2^{64}\right)}{2^{64}}, \end{cases} \tag{6}$$

2.3 Autoencoder network configuration

The autoencoder provides a deterministic and hierarchical mapping between the image domain and a latent feature domain, enabling multi-scale feature extraction and reconstruction while preserving essential spatial and structural information. This backbone serves as a foundational representation framework and, by itself, does not perform any encryption-specific operations. The backbone architecture follows a symmetric encoder–decoder configuration composed of convolutional, deconvolutional, residual, and dense connectivity components. The encoder progressively transforms the input image into higher-dimensional feature representations by reducing spatial resolution while increasing channel depth. Conversely, the decoder performs the inverse transformation, reconstructing the image from encoded features through a mirrored sequence of operations.

This symmetric design ensures dimensional consistency and supports stable reconstruction across multiple feature scales. As seen in Figure 3, the autoencoder backbone is organized into four primary functional modules that define the overall flow of feature representations throughout the network. The Feature Extraction Module (FEM) operates along the encoding pathway and performs hierarchical feature extraction using convolutional and residual operations, capturing progressively abstract representations from the input image. The Feature Decoding Module (FDM) is employed along the decoding pathway and reconstructs spatial details through deconvolutional and residual transformations.

In addition, Feature Fusion Enhancement Modules (FFEM) are incorporated to facilitate multi-scale feature interaction and refinement without altering spatial resolution, while Feature Fusion Decoding Modules (FFDM) support effective feature fusion and detail recovery during the reconstruction process. The detailed layer-wise parameter configuration of the autoencoder backbone is summarized in Table 1, which demonstrates a carefully designed balance between representational capacity and computational complexity. Here, Table 1 shows that the backbone begins with a convolutional input layer employing a 5 × 5 kernel to map the single-channel grayscale image into 32 feature channels, requiring only 832 learnable parameters. This initial expansion enables effective capture of low-level spatial patterns while maintaining a lightweight parameter footprint. Subsequent convolutional layers with 3 × 3 kernels progressively increase the channel dimensionality from 32 to 256, reflecting a deliberate design choice to enhance representational capacity as spatial resolution decreases. The cumulative parameter count of the convolutional and residual blocks within the FEM reaches approximately 3.7×10^6, indicating a moderate-depth

encoder capable of extracting rich hierarchical features without excessive computational burden. In the decoding pathway, the FDM mirrors the encoder structure through a sequence of deconvolutional layers and residual blocks. As summarized in Table 1, these layers progressively reduce the channel dimensionality from 256 back to 32 while restoring spatial resolution. The total number of learnable parameters within the FDM is approximately 2.5×10^6, which is slightly lower than that of the encoder, reflecting the reduced complexity required for reconstruction compared to feature abstraction. This asymmetric parameter distribution contributes to stable reconstruction performance while avoiding unnecessary redundancy in the decoder.

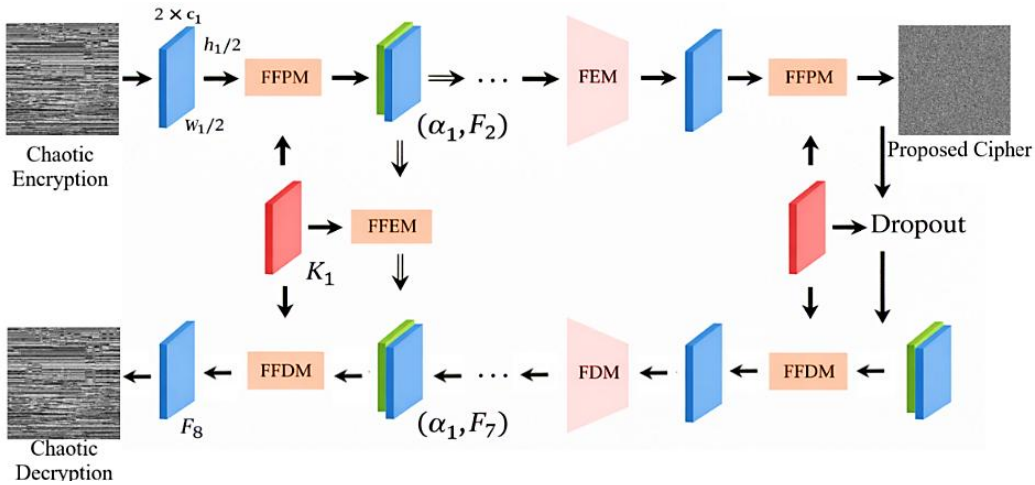

Figure 3. Our architecture model

Table 1. Parameter layer initialization

Module/Layer	Number	Kernel Size	Input Channel	Output Channel	Parameters	Total Parameters
Conv (Input)	1	5 × 5	1	32	832	832
Deconv	1	3 × 3	32	32	9,248	9,248
Conv	1	3 × 3	32	1	289	289
Conv + Res Block (FEM)	-	-	-	-	-	3,706,944
Conv	1	3 × 3	32	64	92,352	
Conv	1	3 × 3	64	128	369,024	
Conv	1	3 × 3	128	256	1,475,328	
Res Block	2	3 × 3	256	256	1,770,240	
Deconv + Res Block (FDM)	-	-	-	-	-	2,545,056
Deconv	1	3 × 3	256	256	1,770,240	
Deconv	1	3 × 3	256	128	590,208	
Deconv	1	3 × 3	128	64	147,648	
Deconv	1	3 × 3	64	32	36,960	
Res Block (FFPM)	-	-	-	-	-	20,920,896
Res Block	4 × 2	3 × 3	64	64	73,856	
Res Block	3 × 2	3 × 3	128	128	295,168	
Res Block	3 × 2	3 × 3	256	256	1,180,160	
Res Block	3 × 2	3 × 3	512	256	1,901,312	
Res Block (FFDM)	-	-	-	-	-	19,253,120
Res Block	3 × 2	3 × 3	256	256	1,180,160	
Res Block	3 × 2	3 × 3	256	256	1,180,160	
Res Block	3 × 2	3 × 3	128	128	295,168	
Res Block	4 × 2	3 × 3	64	64	73,856	
Dense Block (FFEM)	-	-	-	-	-	32,996,784
Dense Conv	2	3 × 3	64	64	3,319,680	
Dense Conv	2	3 × 3	128	128	5,753,088	
Dense Conv	2	3 × 3	256	256	11,947,008	
Dense Conv	2	3 × 3	256	256	11,947,008	

The autoencoder is trained prior to the encryption process to learn stable grayscale image reconstruction and is not optimized specifically for the test images used in the evaluation. The training data consist of grayscale images resized to a fixed input resolution and are split into training and validation sets using an 80:20 ratio. The network is trained using the Adam optimizer with a learning rate of 1×10^{-4}, a mini-batch size of 16, and Mean Squared Error (MSE) as the reconstruction loss function, for a total of 50 epochs while monitoring validation performance. After training, all learned parameters, including convolutional, deconvolutional, residual, and dense block weights, are kept fixed and used as a feature transformation backbone during both encryption and decryption stages, ensuring that the reported performance is attributed to the proposed chaos-guided feature-level encryption mechanism rather than task-specific retraining.

The FFEM implemented using dense connectivity contributes the largest share of parameters, with approximately 3.3×10^7 learnable weights. This substantial parameter allocation enables extensive feature reuse and strengthens information flow among intermediate representations. In contrast, the FFDM, composed of stacked residual blocks with decreasing channel dimensions, contains approximately 1.9×10^7 parameters, supporting effective feature refinement and detail recovery during image reconstruction.

3. PROPOSED METHODOLOGY

This section presents the proposed chaos-guided feature-level image encryption methodology. Building upon the chaotic key generation mechanism and the autoencoder backbone introduced in the previous section, the proposed approach integrates plaintext-dependent chaotic control with deep feature representations to achieve secure image encryption. The methodology is organized into two main stages: the encryption stage, which describes how the plaintext image is transformed into a cipher image, and the decryption stage, which explains the corresponding inverse process for accurate image recovery.

3.1 Encryption stages

The proposed encryption process begins by establishing a strong dependency between the plaintext image and the chaotic control mechanism. The plaintext image is first processed using the SHA-256 hashing algorithm, where the resulting hash value is segmented and combined with a user-defined secret key parameter [29]. This operation ensures that even minimal changes in the plaintext image or secret key lead to significantly different chaotic initialization parameters. The generated parameters are then used to initialize the two-dimensional Tinkerbell chaotic map, from which two coupled chaotic sequences, namely the x-sequence and y-sequence, are produced [30]. These sequences are subsequently normalized and mapped through a mod-based operation to generate a bounded chaotic feature control key, which serves as the primary control signal for the feature-level encryption process. Following chaotic key generation, the plaintext image is transformed from the pixel domain into a hierarchical feature representation using the autoencoder backbone. As seen in Figure 4, the encoder extracts multi-level feature maps through the FEM, enabling the capture of both local textures and global structural information. The chaotic feature control key then interacts with these feature maps through two complementary mechanisms: feature diffusion, guided by the x-sequence, and feature shuffling, guided by the y-sequence. These operations are embedded within the FFEM, where chaotic perturbations are injected directly into the feature representation, implicitly realizing permutation and diffusion without explicitly manipulating pixel positions or intensities. The chaos-guided features are subsequently propagated through the decoding pathway and refined by the FFDM, resulting in a cipher image with noise-like appearance, low spatial correlation, and high randomness. This design ensures that encryption is achieved at the feature level while maintaining compatibility with reliable decryption using the same chaotic control key.

3.2 Decryption stages

The proposed decryption process mirrors the encryption stage in a symmetric and deterministic manner, ensuring accurate reconstruction of the original image when the correct secret key is provided. During decryption, the chaotic feature control key is not generated from the plaintext image. Instead, it is reconstructed using the same secret key parameters and the transmitted key-dependent values generated during the encryption stage. These parameters are used to initialize the Tinkerbell chaotic map, producing identical chaotic sequences as those used in the encryption process. After normalization and mapping, the regenerated chaotic feature control key remains fully synchronized with its encryption counterpart.

Following chaotic key regeneration, the cipher image is processed through the decoding pathway of the autoencoder backbone, as seen in Figure 5. The cipher image first enters the FFDM, where chaos-guided feature fusion is applied to reverse the feature-level perturbations introduced during encryption. The reconstructed features are then propagated through the FDM, which progressively restores spatial resolution and structural coherence across multiple decoding stages. Through successive decoding and fusion operations, the feature representations are refined and transformed back into the image domain, yielding the recovered image. Owing to the deterministic nature of the autoencoder backbone and the strict synchronization of the chaotic feature control key, the proposed decryption process achieves reliable and lossless image reconstruction, while any mismatch in secret key or chaotic parameters results in severe reconstruction degradation.

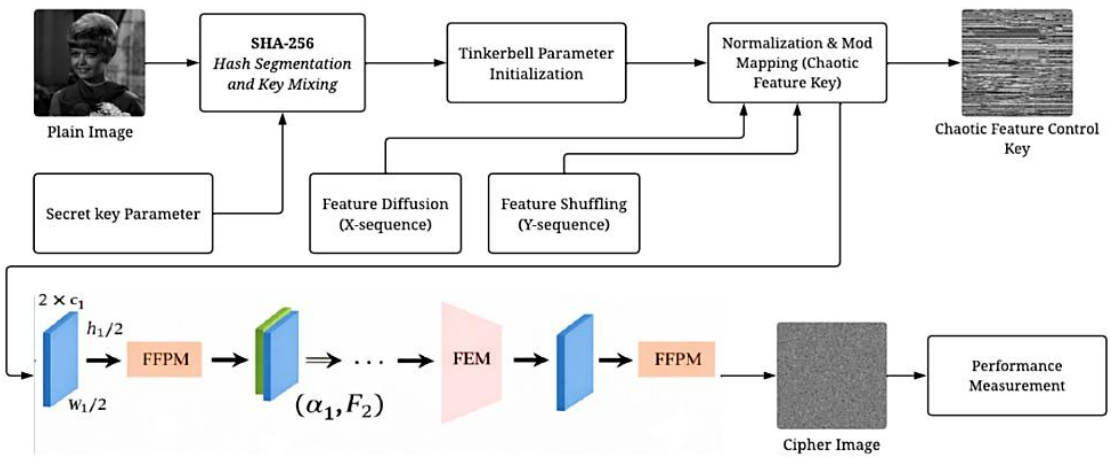

Figure 4. Proposed encryption

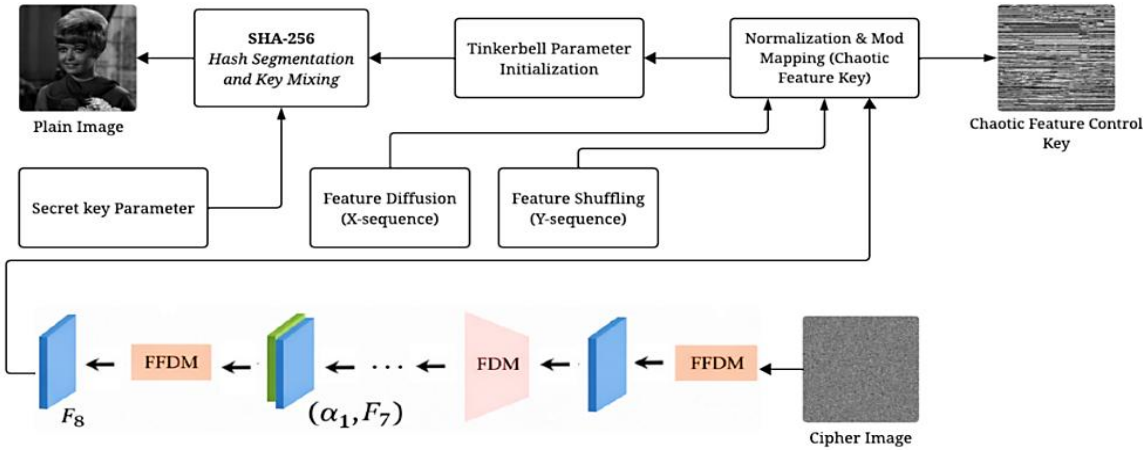

Figure 5. Proposed decryption

4. RESULTS AND DISCUSSION

This section presents the experimental evaluation and performance analysis of the proposed chaos-guided feature-level image encryption method. Comprehensive experiments are conducted to assess the effectiveness, security, and robustness of the proposed scheme. The results are discussed in detail through quantitative metrics and visual analysis, and comparisons with existing encryption methods are provided to demonstrate the advantages and practical feasibility of the proposed approach.

4.1 Experimental results

All experiments are conducted using standard grayscale test images (Barbara, House, Tree, and Candy), which are widely used due to their diverse structural characteristics. Each image is resized to a unified resolution without additional preprocessing to ensure consistent evaluation. To maintain fair comparison, all methods, including different chaotic maps, are tested within the same experimental framework under identical conditions, including image inputs, resolution, and processing pipeline. It should be noted that the evaluation is limited to these representative grayscale images, and therefore the results are interpreted within this experimental scope and may not fully generalize to more complex image types such as color or large-scale datasets.

To visually demonstrate the effectiveness of the proposed encryption scheme, a set of standard grayscale test images is employed, namely barbara.tiff, house.tiff, tree.tiff, and candy.tiff. The corresponding encryption and decryption results are illustrated in Figure 6. As seen in Figure 6(a), the plain images are arranged from top to bottom in the following order: barbara.tiff, house.tiff, tree.tiff, and candy.tiff. These images are selected to represent diverse image characteristics, including high-frequency textures (Barbara), strong geometric structures (House), complex natural contours (Tree), and clustered object patterns (Candy), thereby providing a comprehensive evaluation of the proposed method under different visual conditions. The encryption results using the Tinkerbell chaotic map alone, as shown in Figure 6(b), still exhibit residual structural patterns, particularly in texture-rich images, indicating limitations of pixel-level chaos encryption. In contrast, the proposed method in Figure 6(c) produces uniformly noise-like cipher images with no visible structures, demonstrating more effective disruption of spatial correlations. The decrypted results in Figure 6(d) closely resemble the original images, confirming accurate and reliable reconstruction when the correct key is applied.

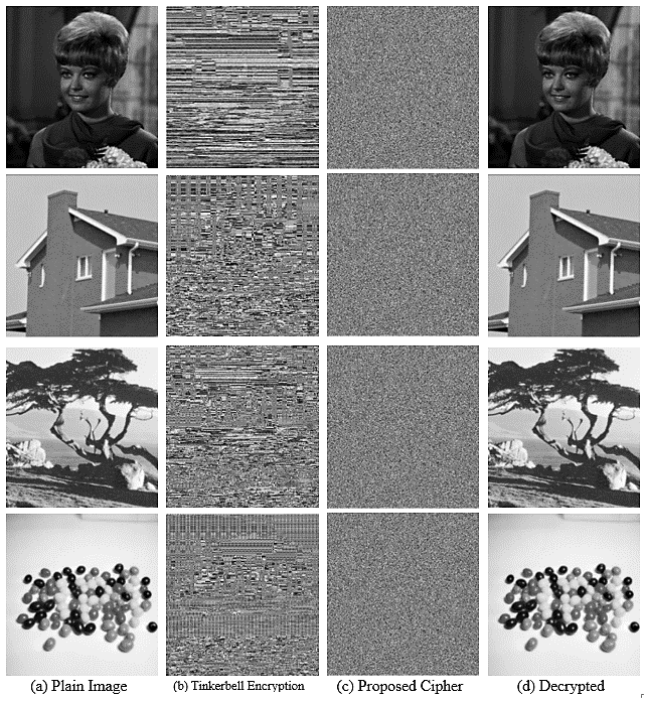

Figure 6. Visual comparison of encryption and decryption results on standard test images

4.2 Entropy analysis

In this subsection, entropy analysis is conducted to evaluate the effectiveness of the proposed encryption method in disrupting the statistical characteristics of the original images. The entropy values of the plain images, Tinkerbell-based encrypted images, and the proposed cipher images are compared to provide a quantitative assessment of encryption performance. The comparison results as seen in Figure 7. As observed, the entropy values produced by the Tinkerbell-based encryption remain slightly below the ideal value of 8 bits for all test images, indicating that residual statistical patterns still exist when chaotic encryption is applied directly. In contrast, the proposed cipher consistently achieves entropy values that are closer to the theoretical ideal value, with values of 7.999

for Barbara, House, and Tree, and 7.998 for Candy. This improvement demonstrates that the proposed chaos-guided feature-level encryption more effectively randomizes pixel intensity distributions. The observed increase in entropy confirms that embedding chaotic control signals into the deep feature domain significantly enhances statistical randomness compared to conventional chaos-based encryption. The consistently high entropy across different image types further indicates that the proposed method is robust against statistical attacks and maintains stable encryption performance regardless of image content complexity.

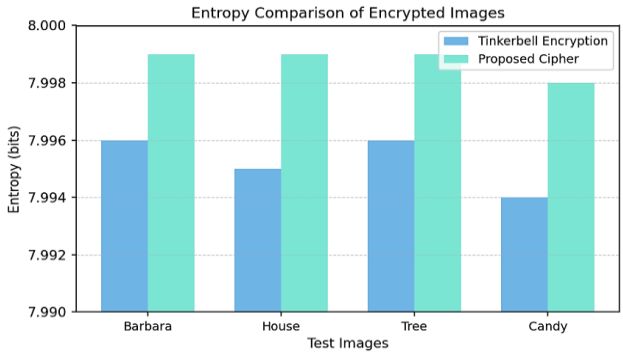

Figure 7. Value of entropy

4.3 Number of Pixels Change Rate and Unified Average Changing Intensity analysis

An effective image encryption scheme should exhibit high NPCR and UACI values, indicating that a minimal change in the input image leads to significant differences in the resulting cipher image. The comparison of NPCR values between the Tinkerbell-based encryption and the proposed method is seen in Figure 8. As seen in Figure 8, the proposed cipher consistently achieves higher NPCR values across all test images. Specifically, the proposed method attains NPCR values of 99.64% for Barbara, 99.63% for House, 99.62% for Tree, and 99.62% for Candy, which are all very close to the theoretical ideal value of 99.6%. In contrast, the Tinkerbell-based encryption produces slightly lower NPCR values ranging from 99.42% to 99.48%. This improvement indicates that the proposed encryption scheme exhibits stronger sensitivity to plaintext changes, effectively amplifying minor pixel variations into widespread differences in the cipher image. As seen in Figure 9, the proposed cipher achieves consistently higher UACI values compared to the Tinkerbell-based encryption. The proposed method yields UACI values of approximately 33.47% for Barbara, House, and Tree, and 33.46% for Candy, which are very close to the ideal theoretical value of 33.46%. Meanwhile, the UACI values obtained using the Tinkerbell-based approach remain lower, ranging from 33.25% to 33.28%. These results demonstrate that the proposed scheme induces stronger average pixel intensity changes.

4.4 Differential noise attack

Evaluating the robustness of an image encryption scheme against noise perturbations is an important aspect of security analysis. A robust encryption method should preserve its randomness characteristics and resist information leakage even when the encrypted data is corrupted by noise. In this subsection, differential noise attacks are conducted by introducing different noise models to both the plain images and the corresponding cipher images. The impact of Gaussian noise and salt-and-pepper noise at different intensity levels is analyzed to assess the resilience of the proposed encryption scheme. The experimental results provide insight into how well the encrypted images maintain statistical security under noisy conditions.

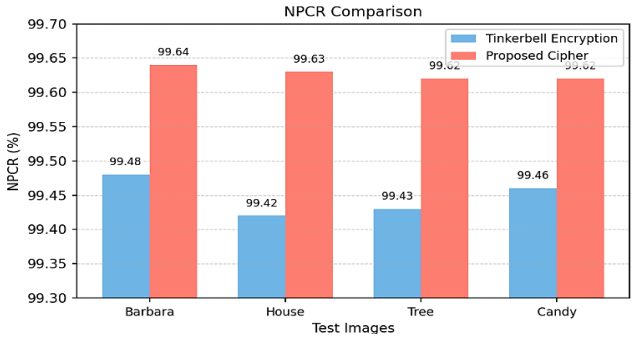

Figure 8. Value of Number of Pixels Change Rate (NPCR)

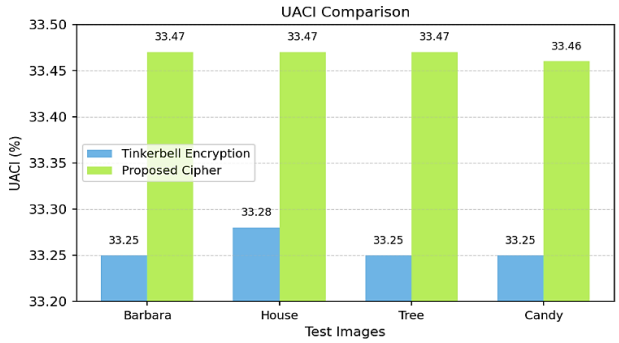

Figure 9. Value of Unified Average Changing Intensity (UACI)

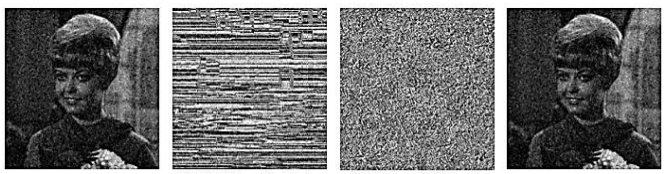

Figure 10. Gaussian noise attack

4.4.1 Gaussian noise attack

To evaluate the robustness of the proposed encryption scheme under additive noise interference, a Gaussian noise attack with a noise intensity of 10% is conducted in this experiment. Gaussian noise is commonly used to model random disturbances introduced during image acquisition or transmission processes. An effective encryption scheme should maintain its security properties and enable reliable decryption even when the encrypted data is corrupted by such noise. As shown in Figure 10(a), the plain image corrupted by 10% Gaussian noise remains visually recognizable, indicating that Gaussian noise alone is insufficient to hide image details. The Tinkerbell-based encrypted image in Figure 10(b) still exhibits residual directional patterns, reflecting limited robustness to noise at the pixel level. In contrast, the proposed cipher shown in Figure 10(c) maintains a uniformly random, noise-like appearance with no visible structures. The decrypted image in Figure 10(d) closely matches the original

plain image, demonstrating that the proposed scheme ensures reliable image recovery even under Gaussian noise interference.

4.4.2 Salt and peppers noise attack

In addition to Gaussian noise, salt-and-pepper noise is considered to further evaluate the robustness of the proposed encryption scheme against impulse noise disturbances. Salt-and-pepper noise introduces random occurrences of extreme pixel values, typically represented by black and white dots, and is commonly encountered during image transmission or sensor malfunction. Similar to the Gaussian noise attack, a noise density of 10% is applied in this experiment. As shown in Figure 11(a), the plain image corrupted by 10% salt-and-pepper noise remains visually recognizable, indicating that impulse noise alone does not sufficiently conceal image content. The Tinkerbell-based encrypted image in Figure 11(b) exhibits residual structural patterns and uneven noise distribution, reflecting limited robustness against impulse noise. In contrast, the proposed cipher in Figure 11(c) preserves a uniformly random, noise-like appearance with no discernible structures. The decrypted result in Figure 11(d) closely matches the original plain image, demonstrating that the proposed method maintains both encryption security and reliable image recovery under salt-and-pepper noise conditions. As seen in Table 2, the proposed cipher demonstrates stable reconstruction quality under both Gaussian and salt-and-pepper noise attacks. For all test images, the Peak Signal-to-Noise Ratio (PSNR) values under 10% Gaussian noise remain above 30 dB, indicating that the decrypted images preserve a high level of visual fidelity despite noise corruption. Correspondingly, the Structural Similarity Index Measure (SSIM) values consistently exceed 0.94, confirming strong structural similarity between the decrypted images and their original counterparts.

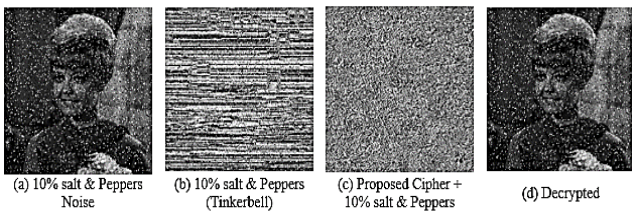

Figure 11. Salt & peppers noise attack

Table 2. PSNR and SSIM values under noise attacks

Plain	Attack	Proposed Cipher	
		PSNR (dB)	SSIM
Barbara	10% of Gaussian	31.25	0.9457
	10% of Salt & Peppers	29.84	0.9312
House	10% of Gaussian	30.92	0.9421
	10% of Salt & Peppers	29.37	0.9284
Tree	10% of Gaussian	30.18	0.9365
	10% of Salt & Peppers	28.96	0.9217
Candy	10% of Gaussian	31.04	0.9442
	10% of Salt & Peppers	29.58	0.9336

Note: Peak Signal-to-Noise Ratio (PSNR); Structural Similarity Index Measure (SSIM)

When subjected to 10% salt-and-pepper noise, a moderate reduction in PSNR and SSIM is observed across all images, which is expected due to the impulsive nature of this noise type. Nevertheless, the PSNR values remain close to 29 dB, while SSIM values stay above 0.92, indicating that the proposed method maintains robust reconstruction performance even under severe impulse noise conditions. These results demonstrate that the proposed encryption framework not only ensures strong security but also exhibits resilience against common noise attacks during transmission.

Beyond numerical proximity to theoretical values, the observed improvements can be attributed to the integration of chaos-driven perturbation within the feature domain. Unlike the Tinkerbell-only scheme, which operates at the pixel level, the proposed method applies diffusion and shuffling on hierarchical feature representations, enabling more effective disruption of spatial dependencies across multiple scales. This explains the consistent increase in entropy, NPCR, and UACI, indicating stronger resistance to statistical and differential attacks in practice. In terms of reconstruction, the reported PSNR values in the range of 29–31 dB under noise conditions indicate that the essential structural information of the image is preserved, while minor degradations remain perceptually acceptable. Therefore, the term “reliable reconstruction” in this study refers to the ability of the method to maintain visually consistent and structurally accurate outputs under controlled noise disturbances, rather than implying perfect or lossless recovery in all conditions.

4.5 Result comparison with other methods

To ensure a transparent and controlled comparison, all evaluated chaotic maps are reimplemented within the same fusion autoencoder framework proposed in this study. The overall architecture, training configuration, input images, resolution, and processing pipeline are kept identical for all methods. Only the chaotic map formulation and its corresponding control parameters are adopted from the respective studies, while the integration mechanism, including feature-level fusion, permutation, and diffusion stages, is unified under the proposed framework. This design isolates the effect of the chaotic system itself and avoids discrepancies arising from differences in model architecture or training strategy. Therefore, the comparison presented in Table 3 should be interpreted as a controlled internal evaluation under a unified framework rather than a direct reproduction of each original method in its native implementation.

Table 3. Comparison with other methods

Study	Plain	Entropy	NPCR	UACI
Logistic Map [31]	Barbara	7.996	99.58	33.29
	House	7.995	99.56	33.27
	Tree	7.996	99.57	33.28
	Candy	7.995	99.55	33.26
Honon Map [32]	Barbara	7.997	99.60	33.34
	House	7.996	99.59	33.32
	Tree	7.996	99.58	33.31
	Candy	7.996	99.58	33.30
Arnold Map [33]	Barbara	7.997	99.61	33.36
	House	7.997	99.60	33.35
	Tree	7.996	99.59	33.33
	Candy	7.996	99.59	33.32
Tinkerbell Map (Our)	Barbara	7.999	99.64	33.47
	House	7.999	99.63	33.47
	Tree	7.999	99.62	33.47
	Candy	7.998	99.62	33.46

Note: Number of Pixels Change Rate (NPCR); Unified Average Changing Intensity (UACI)

As seen in Table 3, all chaos-based methods achieve

entropy values close to the theoretical ideal value of 8 bits, indicating strong randomness in the encrypted images. However, the proposed method based on the Tinkerbell map consistently attains the highest entropy values across all test images, reaching 7.999 for Barbara, House, and Tree, and 7.998 for Candy. This demonstrates that the Tinkerbell-driven chaotic control introduces more effective randomness into the feature domain when combined with the fusion autoencoder. In terms of differential attack resistance, the proposed method also outperforms the other chaotic maps. The NPCR values obtained using the Tinkerbell map range from 99.62% to 99.64%, which are consistently higher than those achieved by the Logistic, Henon, and Arnold maps. Similarly, the UACI values of the proposed method reach up to 33.47%, closely approaching the theoretical ideal value of 33.46%. Although the competing chaotic maps exhibit strong diffusion characteristics, their NPCR and UACI values remain slightly lower, indicating comparatively weaker sensitivity to plaintext variations. Overall, the comparative analysis confirms that while the fusion autoencoder architecture provides a strong and stable encryption backbone for all chaotic maps, the choice of chaotic system plays a critical role in determining the final security performance. The superior results achieved by the Tinkerbell map demonstrate that its complex dynamical behavior and higher sensitivity to initial conditions offer enhanced randomness and diffusion when embedded within the proposed fusion autoencoder framework. These findings validate the effectiveness of the proposed method and highlight the advantage of combining feature-level encryption with an appropriately selected chaotic system.

5. CONCLUSIONS

This study introduced a chaos guided feature level image encryption framework that combines a fusion autoencoder with a two-dimensional chaotic system. The proposed approach is able to disrupt spatial correlations more effectively than conventional pixel level chaos-based encryption methods. Experimental evaluations show that the encrypted images exhibit entropy values very close to the theoretical ideal, together with consistently high NPCR and UACI scores, indicating strong resistance to statistical and differential attacks. A fair comparative study, conducted by integrating different chaotic maps within the same fusion autoencoder architecture, demonstrates that the Tinkerbell map offers the most favorable security performance among the tested chaotic systems. Furthermore, noise robustness experiments under Gaussian and salt and pepper disturbances confirm that the proposed method preserves a noise like cipher appearance while allowing accurate image reconstruction, as reflected by stable PSNR and SSIM values. Future work will explore extensions to color images and video data, as well as the development of more lightweight architectures and alternative chaotic systems to further improve efficiency and practicality in real-world secure image transmission scenarios. In addition, future research will include a more comprehensive security analysis, including key sensitivity evaluation, key space analysis, and robustness under incorrect-key decryption conditions. Furthermore, computational efficiency, runtime performance, and resource requirements will be systematically evaluated to assess the feasibility of the proposed method in real-time and large-scale deployment scenarios.

ACKNOWLEDGMENT

This research has been funded by Universitas Dian Nuswantoro and Intelligent Distributed Surveillance and Security (IDSS) based on Decree No. 032/F.9/UDN-09/II/2026.

REFERENCES

[1] Singh, M., Singh, A.K. (2023). A comprehensive survey on encryption techniques for digital images. Multimedia Tools and Applications, 82(8): 11155-11187. https://doi.org/10.1007/s11042-022-12791-6

[2] Ali, G., Mijwil, M.M. (2024). Cybersecurity for sustainable smart healthcare: State of the art, taxonomy, mechanisms, and essential roles. Mesopotamian Journal of CyberSecurity, 4(2): 20-62. https://doi.org/10.58496/MJCS/2024/006

[3] Newaz, A.I., Sikder, A.K., Rahman, M.A., Uluagac, A.S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3): 1-44. https://doi.org/10.1145/3453176

[4] Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T.H., Liu, Y. (2023). A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. IEEE Internet of Things Journal, 10(17): 14965-14987. https://doi.org/10.1109/JIOT.2023.3263909

[5] Bhagat, D., Hanwate, A., Salunkhe, R.V., Jagyasi, T., Sardare, P., Sahu, M. (2025). Future perspectives on surveillance systems. In Modern Advancements in Surveillance Systems and Technologies, IGI Global Scientific Publishing, pp. 349-370. https://doi.org/10.4018/979-8-3693-6996-8.ch014

[6] Aparna, H., Madhumitha, J. (2023). Combined image encryption and steganography technique for enhanced security using multiple chaotic maps. Computers and Electrical Engineering, 110: 108824. https://doi.org/10.1016/j.compeleceng.2023.108824

[7] Xie, W.Q., Zhang, X.P., Liu, X.L., Xu, C.Y., et al. (2023). Real-time perception of rock–machine interaction information in TBM tunnelling using muck image analysis. Tunnelling and Underground Space Technology, 136: 105096. https://doi.org/10.1016/j.tust.2023.105096

[8] Huang, X., Dong, Y., Ye, G., Yap, W.S., Goi, B.M. (2023). Visually meaningful image encryption algorithm based on digital signature. Digital Communications and Networks, 9(1): 159-165. https://doi.org/10.1016/j.dcan.2022.04.028

[9] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. International Journal of Information Security, 21(4): 917-935. https://doi.org/10.1007/s10207-022-00588-5

[10] Mahalakshmi, K., Nagarajan, S. (2025). Comprehensive review and analysis of image encryption techniques. IEEE Access, 13: 109783-109813. https://doi.org/10.1109/ACCESS.2025.3578158

[11] Zhang, B., Liu, L. (2023). Chaos-based image encryption: Review, application, and challenges. Mathematics, 11(11): 2585.

https://doi.org/10.3390/math11112585
[12] Kaçar, S., Çavuşoğlu, Ü., Jahanshahi, H. (2024). Chaos-based image encryption. In Intelligent Fractal-Based Image Analysis, pp. 47-71. https://doi.org/10.1016/B978-0-44-318468-0.00009-X
[13] Abba, A., Teh, J.S., Alawida, M. (2024). Towards accurate keyspace analysis of chaos-based image ciphers. Multimedia Tools and Applications, 83(33): 79047-79066. https://doi.org/10.1007/s11042-024-18628-8
[14] Arif, J., Khan, M.A., Ghaleb, B., Ahmad, J., Munir, A., Rashid, U., Al-Dubai, A.Y. (2022). A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution. IEEE Access, 10: 12966-12982. https://doi.org/10.1109/ACCESS.2022.3146792
[15] Khurana, N., Dua, M. (2025). A novel one-dimensional Cosine within Sine chaotic map and novel permutation–diffusion based medical image encryption. Nonlinear Dynamics, 113(5): 4839-4859. https://doi.org/10.1007/s11071-024-10429-w
[16] Shakir, D.A.Q., Salim, A., Abd Al-Rahman, S.Q., Sagheer, A.M. (2023). Image encryption using Lorenz chaotic system. Journal of Techniques, 5(1): 122-128. https://doi.org/10.51173/jt.v5i1.840
[17] Zhang, H., Feng, X., Sun, J., Yan, P. (2025). Chaotic image security techniques and developments: A review. Mathematics, 13(12): 1976. https://doi.org/10.3390/math13121976
[18] Hassanzadeh, K., Ahmadi-Kandjani, S., Kheradmand, R., Mortazavi, S.A. (2025). Approach to optical encryption: Merging ghost imaging with chaos theory. Optics Express, 33(13): 28301-28319. https://doi.org/10.1364/OE.558183
[19] Zhang, Q., Wang, H., Li, X., Zhang, S., Liu, J. (2025). A multi-branch feature enhancement-based detection and hierarchical chaotic encryption fusion method for sensitive targets in remote sensing images. Scientific Reports, 16(1): 3103. https://doi.org/10.1038/s41598-025-32992-x
[20] Sang, Y., Sang, J., Alam, M.S. (2022). Image encryption based on logistic chaotic systems and deep autoencoder. Pattern Recognition Letters, 153: 59-66. https://doi.org/10.1016/j.patrec.2021.11.025
[21] Maity, A., Chen, Y.L., Alexan, W., Lip Yee, P., Dhara, B.C. (2026). Image encryption with 6D hyperchaotic system and vision transformer autoencoder. Scientific Reports, 16(1): 4243. https://doi.org/10.1038/s41598-025-34378-5
[22] Madani, M., Bourennane, E.B. (2025). Visually image encryption and compression using a CNN-based auto encoder. International Journal of Computer Networks and Communications, 17(2): 113-123. https://doi.org/10.5121/ijcnc.2025.17207
[23] Pal, P.K., Kumar, D., Agarwal, V. (2024). Efficient image encryption using the Tinkerbell map in conjunction with linear feedback shift registers. Multimedia Tools and Applications, 83(15): 44903-44932. https://doi.org/10.1007/s11042-023-17236-2
[24] Biswas, G., Pradhan, C. (2024). Implementation of novel framework for image encryption using Tinkerbell 3D cat map. In International Conference on Data Mining and Information Security, Singapore, pp. 111-123. https://doi.org/10.1007/978-981-96-6063-6_9
[25] Kumbhakar, D., Adhikari, S., Karforma, S. (2025). CTEA: Chaos based tiny encryption algorithm using ECDH and TinkerBell map for data security in supply chain management. Multimedia Tools and Applications, 84(13): 12371-12394. https://doi.org/10.1007/s11042-024-19443-x
[26] Cheshmeh Kouhi, M., Nodehi, A., Enayatifar, R. (2025). Parameter tuning of Tinkerbell chaotic function via particle swarm optimization for enhanced image encryption security. Journal of Computer Virology and Hacking Techniques, 21(1): 17. https://doi.org/10.1007/s11416-025-00551-7
[27] Suman, R.R., Mondal, B., Mandal, T. (2022). A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256. Multimedia Tools and Applications, 81(19): 27089-27110. https://doi.org/10.1007/s11042-021-11460-4
[28] Rahul, B., Kuppusamy, K., Senthilrajan, A. (2023). Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm. Multimedia Tools and Applications, 82(28): 43729-43758. https://doi.org/10.1007/s11042-023-15289-x
[29] Wang, K., Wu, X., Wang, H., Kan, H., Kurths, J. (2021). New color image cryptosystem via SHA-512 and hybrid domain. Multimedia Tools and Applications, 80(12): 18875-18899. https://doi.org/10.1007/s11042-021-10511-0
[30] Dhopavkar, T.A., Nayak, S.K., Roy, S. (2022). IETD: A novel image encryption technique using Tinkerbell map and Duffing map for IoT applications. Multimedia Tools and Applications, 81(30): 43189-43228. https://doi.org/10.1007/s11042-022-13162-x
[31] Long, B., Chen, Z., Liu, T., Wu, X., He, C., Wang, L. (2024). A novel medical image encryption scheme based on deep learning feature encoding and decoding. IEEE Access, 12: 38382-38398. https://doi.org/10.1109/ACCESS.2024.3371888
[32] Hu, Y., Wu, H., Zhou, L. (2023). Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion. Alexandria Engineering Journal, 73: 385-402. https://doi.org/10.1016/j.aej.2023.04.060
[33] Satre, S.M., Joshi, B. (2025). Enhancing the power of advanced Arnold Cat Map for secure quantum image cryptography. SN Computer Science, 6(5): 503. https://doi.org/10.1007/s42979-025-04030-0