International Journal of Safety and Security Engineering
Vol. 15, No. 7, July, 2025, pp. 1369-1377
Journal homepage: http://iieta.org/journals/ijsse

Symmetric Image Encryption Using Chaotic Logistic Map and Deep Convolutional Feature Learning

Christy Atika Sari[1*], Eko Hari Rachmawanto[1], Folasade Olubusola Isinkaye[2], Rabei Raad Ali[3]

[1] Department of Informtics Engineering, Universitas Dian Nuswantoro, Semarang, 50131, Indonesia
[2] Department of Computer Science, Ekiti State University, Ado-Ekiti, 362103, Nigeria
[3] Department of Computer Techniques Engineering, Northern Technical University, Mosul 41001, Iraq

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

https://doi.org/10.18280/ijsse.150704

Received: 5 June 2025
Revised: 11 July 2025
Accepted: 21 July 2025
Available online: 31 July 2025

Keywords:
autoencoder, chaotic mapping, convolutional feature learning, deep learning, image encryption

ABSTRACT

The rapid increase in the transmission and storage of digital images has intensified the need for encryption algorithms that ensure visual confidentiality and resilience against statistical and differential attacks. Conventional encryption approaches often struggle to eliminate residual structural information, particularly when handling highly correlated image data. To overcome these limitations, this study proposes a hybrid symmetric image encryption method that combines the unpredictability of chaotic logistic map operations with the deep representational capabilities of convolutional autoencoders. The encryption process consists of a two-stage mechanism: first, the image undergoes chaotic pixel permutation, substitution, and XOR masking; second, the result is passed through a deep convolutional network for feature-level obfuscation, further diminishing any remaining visual patterns. The proposed method was evaluated on multiple standard grayscale images using four key metrics: MSE, PSNR, UACI, and NPCR. The averaged results across all test images show an MSE of 36.23, a PSNR of 7.46 dB, a UACI of 33.50%, and an NPCR of 99.60%. These values indicate strong encryption quality and high sensitivity to plaintext variations. The integration of chaotic systems with deep learning effectively enhances security while maintaining computational efficiency, providing a robust solution for secure visual data protection in modern applications.

1. INTRODUCTION

In the modern digital environment characterized by large-scale visual data exchange, either through social media, cloud services, or surveillance systems, protection of visual content such as images has become crucial [1-3]. Digital images have special features such as high spatial correlation between pixels and predictable intensity distributions. This makes them vulnerable to various forms of cryptanalysis attacks, especially on conventional encryption systems [4-6]. A major challenge in this domain is how to design encryption algorithms that are not only capable of destroying the internal statistical regularities of the image but also have a high degree of sensitivity to small changes in the plaintext to ensure optimal diffusion and confusion [7, 8].

In response to these challenges, this paper proposes a hybrid approach that integrates a logistic map-based chaotic system with the feature abstraction capabilities of a deep convolutional neural network (CNN) [9-12]. The chaotic system acts as a random sequence generator that is used for pixel permutation, bit substitution, and XOR-based masking to produce the initial encrypted image [13-15]. The image is then processed through a CNN in the form of an autoencoder, which exhaustively extracts non-linear feature representations and masks any spatial patterns that may still be detected [16]. Thus, this two-layer approach combines the deterministic randomness of chaotic systems with the structural non-linearity power of deep learning to enhance the resistance of cipher-images to various visual and statistical attack techniques [17].

The main motivation of this research comes from the observation that although chaotic systems are characterized by high sensitivity to initial conditions and good pseudo-random properties, pure chaos-based encryption still leaves structural traces that can be exploited in visual attacks [8, 18, 19]. On the other hand, deep learning, especially CNN architecture, has the extraordinary ability to abstract semantic and spatial information through hierarchical convolution processes [20]. This study combines these two techniques with the aim to create a symmetric encryption system that is not only mathematically complex but also visually and statistically uninterpretable, even against increasingly advanced machine learning-based analysis.

Several previous studies have explored the use of chaotic systems in image encryption schemes, especially to increase the complexity of cryptography and make the decryption process difficult without a key. One of the most prominent methods was developed by Arif et al. [21], which combines chaotic logistic maps with random substitution techniques to form a symmetric encryption scheme. This approach uses a

random S-Box-based pixel permutation and substitution process controlled by chaotic sequences, resulting in a cipher-image with a uniform histogram distribution and near-maximum entropy. Although this method has been proven to be resistant to brute-force attacks and statistical attacks, their approach still relies heavily on the strength of a single-layer chaotic system, without any further obfuscation stages on the feature representation level. As a result, in some cases with finely textured images or regular patterns, latent information can still be detected through differential analysis or local spatial correlation.

Another approach was developed by Anees et al. [19], which specifically targets encryption weaknesses in handling data with high levels of autocorrelation. They proposed a chaos-based substitution scheme that adaptively replaces data bits in an image using a pseudo-random sequence of complexly initialized logistic maps. By focusing on randomizing the internal structure of pixels, this method shows significant improvements in reducing correlations between neighbouring pixels and increasing the diversity of encrypted bits. However, the power of this method is limited to the spatial domain and has not touched on the aspect of non-linear feature transformations that can disguise semantic information more deeply. In addition, the absence of a multi-layered obfuscation mechanism makes the resulting cipher-image vulnerable to advanced forms of attacks that exploit the statistical imperfections of a single encryption result.

For instance, in the method proposed by Arif et al. [21], although the use of chaotic permutation and substitution achieves a uniform histogram, the encrypted images of highly textured patterns such as the "Baboon" image still exhibit residual local correlations that can be exploited through statistical or entropy-based analysis. Similarly, Anees et al. [19] showed improvement in decorrelating adjacent pixels, but their approach struggles with complex spatial patterns like those in satellite or medical images, where the single-layer chaotic masking is insufficient to completely disrupt semantic structures. These limitations underscore the need for a more robust, multi-layered encryption mechanism that operates not only on pixel-level transformation but also on deeper feature abstractions.

The main contribution of this research is the design of a symmetric encryption system based on a hybrid model that combines chaos logistic map with deep convolutional autoencoder. Different from previous approaches, this scheme can perform permutation and substitution based on chaotic sequence, and also project the initial encrypted image into a high-dimensional feature space using CNN. The result is a cipher-image that has non-deterministic characteristics, a uniform histogram distribution, and does not show any spatial structure that can be re-analyzed. This model is tested on various image datasets and quantitatively compared with previous approaches based on MSE, PSNR, NPCR, and UACI metrics. The evaluation results show significant improvements in information diffusion and resistance to differential attacks, while maintaining process efficiency that can be applied to large-scale real-time systems.

2. PRELIMINARIES

Before examining the proposed hybrid model, this section outlines the fundamental concepts that underpin the system architecture. These include the principles of chaotic encryption using logistic maps and the essential components of deep learning, especially convolutional neural networks. A clear understanding of these preliminaries is important for understanding the mechanisms and motivations behind the hybrid symmetric image encryption framework.

2.1 Logistic map encryption

The novelty of this study is the utilization of a finely tuned configuration of the logistic map parameters to maximize the chaotic behaviour essential for robust symmetric image encryption [22]. The control parameter r is carefully selected within the narrow chaotic interval, specifically in the interval from 3.89 to 4 [23]. This selection ensures high entropy and unpredictability of the generated pseudo-random sequences [24]. The sensitivity to initial conditions x_0 is intensified by treating x_0 as a high-precision key parameter constrained strictly within the interval between 0 and 1, while avoiding values close to the boundaries to prevent periodicity.

The number of iterations N is dynamically adapted based on image size and encryption complexity. This approach balances computational efficiency with cryptographic strength. The adaptive iteration count is incorporated into the key schedule. This is to enhance the key space and increase resistance to brute-force and statistical attacks. This chaotic method based logistic map is shown in Eq. (1).

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n), n = 0,1,2,3, \dots, N-1 \quad (1)$$

Based on Eq. (1), x_n is the initial condition or secret key seed, chosen within the interval $(0, 1)$, r is the control parameter ranging from 3.89 to 4, which ensures chaotic dynamics, N represents the total number of iterations to generate the pseudo-random sequence. Iterating the map from $n = 0$ up to $n = N - 1$, the chaotic sequence $\{x1, x2, \dots, xN\}$ is produced. This sequence is then normalized and quantized as needed to generate the encryption key stream or to control pixel permutation during image encryption.

2.2 Image encryption based on deep convolutional feature learning

For the purposes of amplifying the non-linearity and strength of the encrypted image obtained from the chaotic logistic map [25, 26], a deep convolutional neural network (CNN) is utilized in this research for processing and mapping the encrypted image in a complex and secure way [11, 12]. The suggested method harnesses the capacity of the CNN for abstracting high-dimensional features in a way that effectively hides any residual statistical features that might remain after the chaos-based encryption phase.

The essence of using deep convolutional feature learning lies in its ability to take advantage of local spatial correlations to learn hierarchical features from input images, even when these inputs are pre-transformed by chaotic encryption [27, 28]. Using the learned convolutional filters, the network can project the encrypted image into a space in which any structural information gained from the encrypted image will be effectively concealed thus enhancing the resistance of the ciphertext to cryptanalysis.

In this model, the encrypted image $I_e \in R^{H \cdot W \cdot C}$ (with height H, width W, and channel count C) is input to a CNN module consisting of multiple convolutional layers. Each convolutional layer performs using Eq. (2).

$$F^{(l)} = \sigma(W^{(l)} \cdot F^{(l-1)} + B^{(l)}) \quad (2)$$

Based on Eq. (2), $F^{(l)}$ is the output feature map at layer l, $F^{(0)} = I_e$ is the encrypted input image, $W^l \in R^{k \times k \times C_{in} \times C_{out}}$ is the set of learnable convolutional kernels with size $k \times k$, $B^{(l)}$ is the bias term, σ is a non-linear activation function, typically ReLU of $\sigma(x) = max(0, x)$.

The successive application of convolution, non-linear activation, and pooling layers transforms the encrypted image into a compact, high-dimensional feature space that exhibits minimal correlation to the original content. To further reduce redundancy and control spatial dimensions, pooling operations such as max-pooling are applied. The operation is defined in Eq. (3).

$$p_{i,j}^{l} = \max F_{i+m,j+n}^{(l)} \quad (3)$$

This step contributes to obfuscating localized patterns while reducing sensitivity to small perturbations, thereby making it more difficult to reverse-engineer the encrypted image. After multiple layers of convolution and pooling, the network concludes with a final encoding layer as calculated in Eq. (4).

$$E = f(F^{(l)}) \quad (4)$$

Based on Eq. (4), $F^{(l)}$ is the output of the last convolutional block, and f is either a flattening operation followed by a dense layer (for generating key vectors or secure hashes), or an upsampling+convolutional path (if aiming to reconstruct an encrypted form). The result E becomes the final encrypted output, a representation that has passed through both chaotic dynamics and deep feature transformation. This layered security makes the scheme highly resistant to known-plaintext and chosen-ciphertext attacks, while also eliminating visual cues that may leak structural hints about the original image.
Figure 1 shows the complete design for this hybrid encryption scheme. It involves chaotic logistic map encryption, deep convolutional feature learning, and deep encryption layers. The figure outlines, sequentially, the end-to-end processing starting from taking encrypted image input (host) through convolutional feature learning layers which finally leads to the last deep learning-based encryption module.

2.3 Performance measurement

To measure the effectiveness and stability of security provided by the suggested deep learning image encryption model, statistical and quantitative metrics are utilized [29]. The performance assessment focuses on quantifying distortion, imperceptibility, and sensitivity of the encryption algorithm to small changes in the plaintext. The key metrics used are MSE, PSNR, UACI, and NPCR [29, 30]. These metrics provide critical information about visual degradation, quality of encryption, and sensitivity of the implemented cryptosystem.

2.3.1 Mean Squared Error (MSE)

MSE measures the average squared difference between the original image and its encrypted counterpart. A higher MSE value indicates a greater level of distortion, which is desirable in image encryption. The MSE calculation process is seen in Eq. (5).

$$\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - K(i,j))^2 \quad (5)$$

2.3.2 Peak Signal-to-Noise Ratio (PSNR)

PSNR is computed from the MSE and reflects the encryption strength in terms of pixel-wise similarity. Lower PSNR indicates better encryption strength, as the encrypted image should be dissimilar to the original. The PSNR calculation process is seen in Eq. (6).

$$10 \log 10 \left(\frac{\max\_pixel\_value^2}{MSE}\right) \quad (6)$$

2.3.3 Unified Average Changing Intensity (UACI)

UACI evaluates the average intensity difference between two ciphered images generated from slightly different plaintexts as seen in Eq. (7). This metric measures differential attack resistance.

$$\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) \oplus K(i,j)}{L}\right| \quad (7)$$

2.3.4 Number of Pixels Change Rate (NPCR)

NPCR measures the percentage of differing pixels between two cipher images when the original image has a slight variation as indicated in Eq. (8). High NPCR values indicate strong diffusion properties.

$$\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) - K(i,j)}{I(i,j)}\right| \quad (8)$$

Based on Eqs. (5)-(8), the effectiveness and security level of the proposed encryption model are supported by the methodology detailed in the next section and further validated by the experimental results presented thereafter.

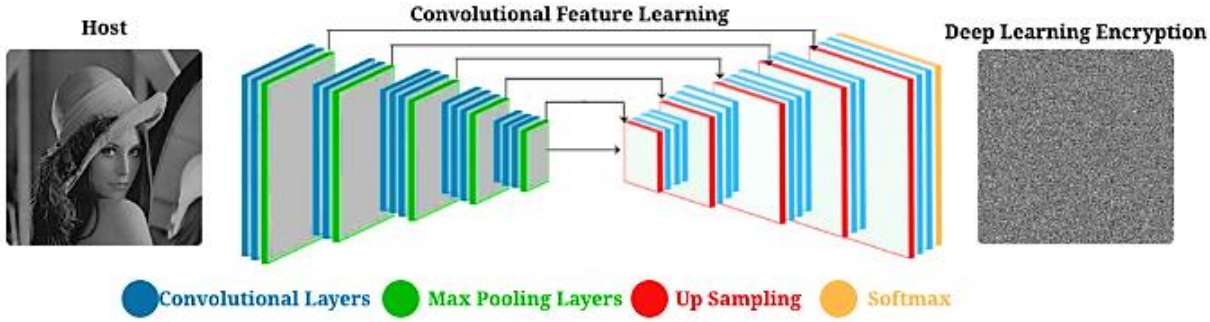


Figure 1. Improvement hiding networks

3. METHODOLOGY

As illustrates in Figure 1, the proposed image encryption framework is organized into three main stages: chaotic encryption, deep learning-based improvement, and decoding. In the first stage, the logistic map drives pixel permutation, bit substitution, and XOR operations to produce the first encrypted image. This encrypted output is then passed to a deep learning autoencoder in the second stage for feature-level encryption refinement. Finally, a decoder network reconstructs the ciphered image, which is later decrypted through inverse logistic operations to restore the original image.

As seen in Figure 2, the encryption process begins with a plain image I and a predefined secret key, set as "$atika\_sari$". To ensure secure and unpredictable key generation for the chaotic system, the SHA-512 hashing algorithm is applied to this secret key. The secret key is processed using SHA-512 to generate a 512-bit hash value as calculated in Eq. (9).

$$H = SHA - 512("atika\_sari") \tag{9}$$

This hash H is then segmented and mapped to initialize the logistic map parameters. For instance: Initial value $x0$ and Control parameter $r \in (3.57,4.0]$ are derived from selected segments of the hash by normalizing them into the range required for chaotic behavior.

Subsequently, encryption uses a chaos logistic map system to perform three main processes: pixel permutation, bit substitution, and XOR masking. The main formula for the logistic map can be found in Eq. (1), and to convert this sequence to a usable form (integer array), Eq. (10) is used.

$$K[i] = \lfloor (S[i] \times 10^6)\ mod 256 \rfloor, i = 1,2, \dots, M \times N \tag{10}$$

The arrangement of pixel positions is randomized based on the ascending index order of $I = argsort(S)$, then perform a permutation of the $M \times N$ dimensional image P, and the calculation is seen in Eq. (11).

$$P'(i,j) = P(row(I_k), col(I_k)), k = (i-1) \times N + j \tag{11}$$

With $row(k) = \frac{k}{N}, col(k) = k mod N$, Each pixel $p \in [0,255]$ is represented as 8-bit and undergoes chaotic key based substitution K as calculated in Eq. (12).

$$pi' = SBox(pi \oplus Ki) \tag{12}$$

SBox can be defined statically or dynamically from a chaotic sequence as calculated in Eq. (13), so that the substitution result for the ith pixel is calculated in Eq. (14).

$$SBox[i] = (K[i] + mod(i,256)) mod 256 \tag{13}$$

$$p_1'' = SBox\ (p_i') \tag{14}$$

The final step of this phase is the XOR operation to provide additional complexity as calculated in Eq. (15). The final image resulting from this stage is called the First Encrypted Image.

$$C(i,j) = P''(i,j) \oplus K(i,j) \tag{15}$$

In the last phase of proposed methods, the first encrypted image is fed into a convolutional autoencoder network. The encoder conceals the image structure by transforming it into deep feature representations through convolutional layers. This enhances security by disrupting visual patterns in the image. The output from the autoencoder is then processed by the neural network decoder to restore the ciphered structure. Although it does not directly recover the original image, this intermediate form is now ready for final decryption through reverse logistic map operations. Here, the reverse logistic map operations in question include Inverse XOR, inverse substitution, and inverse permutation using the same logistic map sequence.

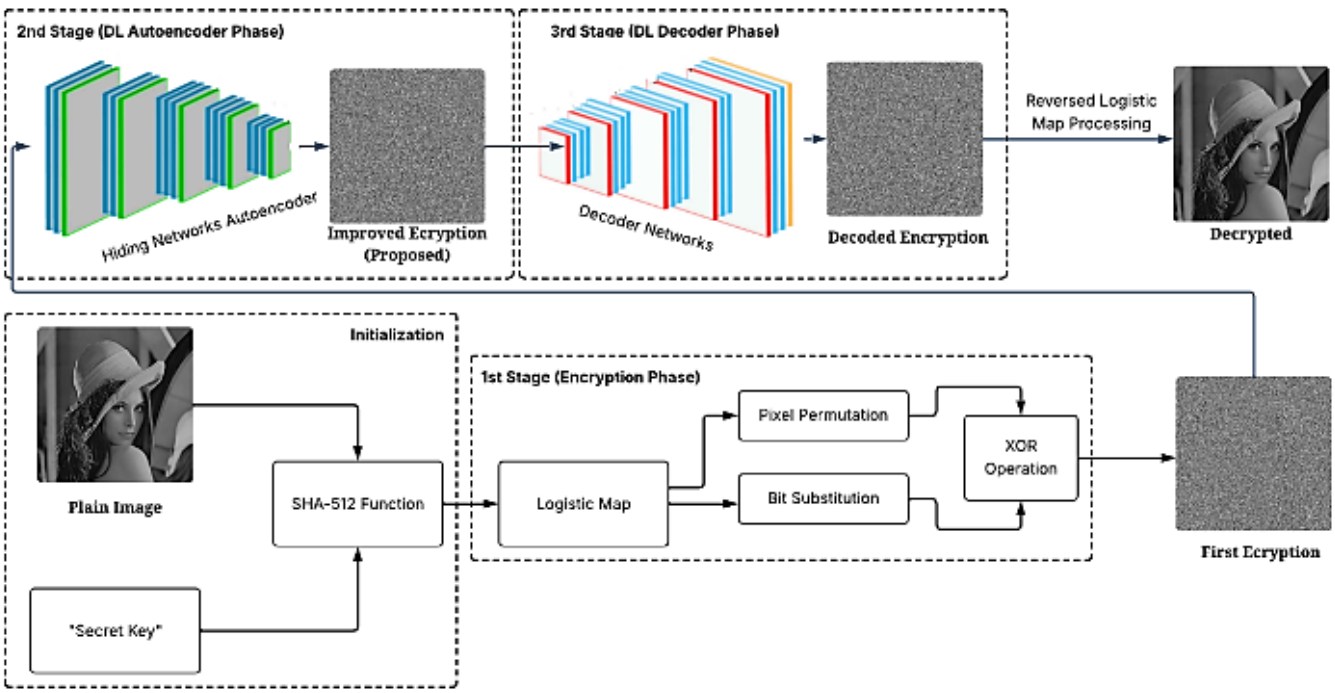


Figure 2. Research methodology

4. RESULTS AND DISCUSSION

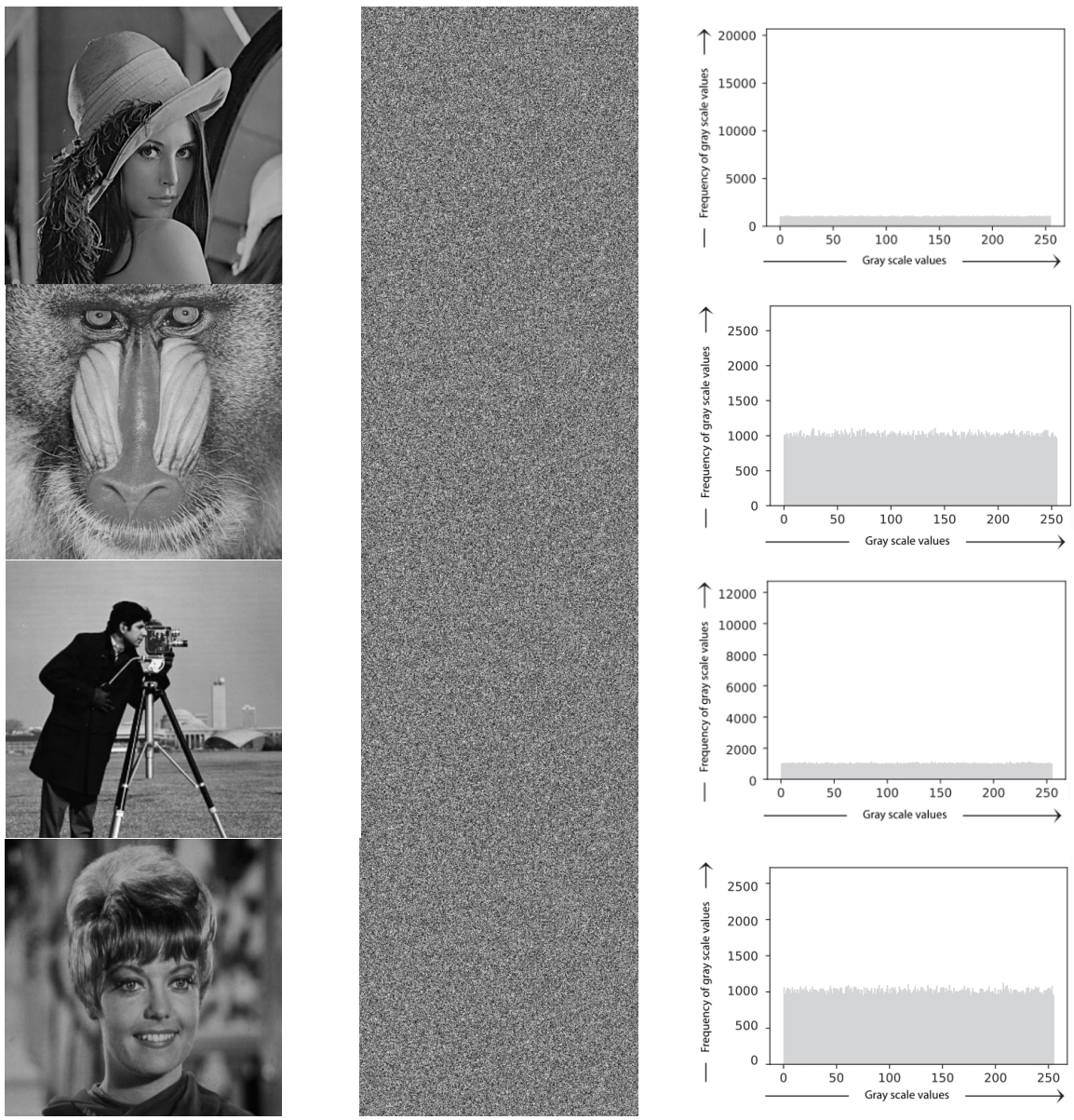
In this section, all experiments and metric evaluations were implemented using Python programming, and executed on a system with the following specifications: AMD Ryzen 5 7600 processor, NVIDIA RTX 4060 Ti GPU, 32 GB RAM, and 2 TB ROM. The computational power of this system ensures efficient execution of chaotic sequence generation and deep neural network operations, supporting rapid encryption and decryption processes. The dataset used consists of standard grayscale images commonly adopted in image encryption literature, including Lena, Baboon, Cameraman, and Zelda. These images were selected to ensure diversity in texture, structure, and complexity from highly detailed and textured images (e.g., Baboon) to smoother images with clearer edges (e.g., Cameraman). All images were resized to 256 × 256 pixels to maintain uniformity during the encryption process.

4.1 Visual experiment

Figure 3 provides the result of the encryption using the proposed approach. Precisely, the original 256 × 256 grayscale plaintext image is the one given in Figure 3(a), while the encrypted image, with a visually arbitrary pattern lacking any recognizable structure, is given in Figure 3(b). Also, the histogram of the encrypted image is shown in Figure 3(c), where the horizontal axis represents the grayscale values ranging from 0 to 250 and the vertical axis indicates the corresponding frequencies. As a note, the first row is the image of Lena, the second row is the image of the Baboon, row 3 is the image of the Cameraman, and row 4 is the image of Zelda.

4.2 Quality of visual measurement

Four quantitative metrics were utilized in the evaluation: MSE, PSNR, UACI, and NPCR metrics. Each of the metrics was calculated according to its respective formula. MSE as defined in Eq. (5), PSNR as specified in Eq. (6), UACI as defined in Eq. (7), and NPCR as defined in Eq. (8). The resulting values, which describe the level of distortion, the strength of the encryption, and the sensitivity to slight changes in the input, are presented in Tables 1 and 2.



(a) Plain image (b) Proposed encrypted (c) Histogram assessment

Figure 3. Results of visual encryption

Table 1. Quality assessment (MSE and PSNR)

Plain Image	Proposed Method		Arif et al. [21]		Anees et al. [19]	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	37.911	7.339 dB	39.374	9.237 dB	39.510	9.373 dB
Baboon	38.436	7.615 dB	39.679	9.542 dB	39.634	9.497 dB
Cameraman	30.557	7.166 dB	32.531	8.415 dB	31.796	7.68 dB
Zelda	38.125	7.727 dB	39.023	8.886 dB	38.758	8.621 dB

Table 2. Quality assessment (UACI and NPCR)

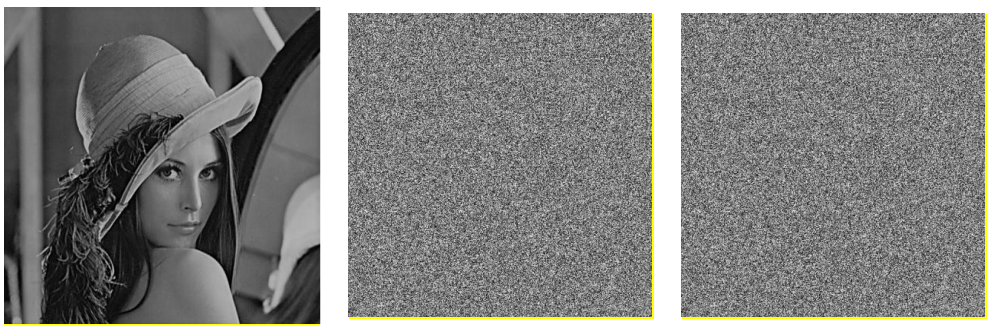
Plain Image	Proposed Method		Arif et al. [21]		Anees et al. [19]	
	UACI	NPCR	UACI	NPCR	UACI	NPCR
Lena	33.50	99.60	33.48	99.61	0.00011	0.00038
Baboon	33.50	99.60	33.43	99.60	0.00025	0.00152
Cameraman	33.49	99.60	33.48	99.60	0.00105	0.00038
Zelda	33.50	99.60	33.54	99.61	0.00013	0.00038

Table 3. Autoencoder architecture

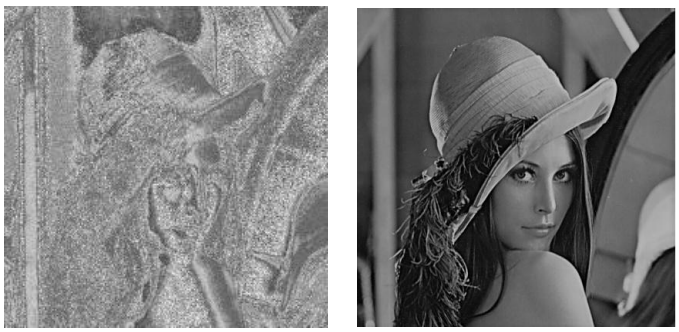
Layer Name	Type	Kernel Size	Stride	Output Shape	Activation
Input	Input layer	-	-	(256,256,1)	-
Conv1	Conv2D	3×3	1	(256,256,32)	ReLU
Conv2	Conv2D	3×3	2	(128,128,64)	ReLU
Conv3	Conv2D	3×3	2	(64,64,128)	ReLU
Bottleneck	(Latent)	3×3	2	(32, 32,256)	ReLU

Table 4. Dencoder architecture

Layer Name	Type	Kernel Size	Stride	Output Shape	Activation
Deconv1	Conv2DTranspose	3×3	2	(64,64,128)	ReLU
Deconv2	Conv2DTranspose	3×3	2	(128,128,64)	ReLU
Deconv3	Conv2DTranspose	3×3	2	(256,256,32)	ReLU
Output	Conv2D	3×3	1	(256,256,1)	Sigmoid



(a) Plain image (b) Our methods (c) Arif et al. [21]



(d) Anees et al. [19] (e) Decrypted

Figure 4. Visualization comparison

UACI and NPCR are critical metrics in evaluating the sensitivity and security robustness of an encryption algorithm against differential attacks. A high UACI value, ideally around 33%, indicates that even a minor change in the plaintext (e.g., flipping one pixel) leads to a significant average change in the encrypted image's pixel intensities. Similarly, a high NPCR value, typically above 99%, signifies that most pixels in the cipher-image will change in response to slight variations in the

input. These characteristics demonstrate that the proposed method achieves strong diffusion and confusion properties, making it highly resistant to statistical or differential cryptanalysis.

4.3 Deep learning parameter

To improve the encryption process via deep feature transformation, a convolutional autoencoder model was utilized. This model consists of an encoder to obtain deep hierarchical features from the input encrypted image, and a decoder responsible for the generation of the transformed cipher form. The encoder compresses the spatial information hierarchically to a latent space, while the decoder expands it subsequently, maintaining the encrypted features. This structure ensures that the key patterns become masked at the feature level, and thus the security of the encryption system improves. The configurations of the encoder and decoder layers utilized in the proposed approach are described in detail in Tables 3 and 4, respectively.

4.4 Visual comparison stages

To confirm the effectiveness of the new hybrid encryption approach, a comparative illustration is given in Figure 4. This figure represents a chain of images giving different phases and encryption methodologies. Particularly, the original plain image is given in Figure 4(a) while the encrypted result obtained from the proposed chaotic-deep learning approach has been illustrated in Figure 4(b). To make the comparison easier, Figures 4(c) and 4(d) give the results of encryption achieved by the conventional schemes proposed by Arif et al. [21] and Anees et al. [19], respectively. Finally, the decrypted image after applying the inverse logistic map and decoding process is illustrated in Figure 4(e). This confirms the successful reconstruction and validates the proposed method's reversibility and integrity.

Experimental evaluation results presented through quantitative metrics such as MSE, PSNR, NPCR, and UACI show that the proposed encryption approach is capable of generating cipher-images with high distortion and low correlation to the plaintext. High MSE and low PSNR values indicate significant visual transformation success between the original and encrypted images, while NPCR values above 99% and UACI above 33% confirm the system's robustness against differential attacks, including attacks on slightly modified plaintexts. These advantages are further strengthened through histogram visualization and spatial comparison, where the encrypted images show even intensity distribution and loss of regular patterns. Compared with the methods of Arif et al. [21] and Anees et al. [19], the proposed system is able to maintain a better level of security, especially in terms of spatial randomization and resistance to visual analysis-based decryption. Further analysis shows that the application of convolutional autoencoders makes a significant contribution in obscuring the remaining spatial information from chaos-based encryption results. CNN is able to extract non-linear features and project images into high-dimensional abstract representations, thus strengthening the second layer of protection that pure chaotic systems do not have. This can be seen from the visual comparison between the proposed method and previous approaches, where the encrypted images in this method are more random, do not display pattern structures, and are more resistant to segmentation or recovery processes based on machine learning. Thus, the use of deep learning as an additional obfuscation component is a crucial aspect that distinguishes this research from methods that only rely on chaos transformation.

The main contribution of this research lies in the integration of two different but complementary approaches, namely logistic map-based chaotic systems and deep learning techniques through autoencoders. This hybrid scheme not only improves the quality of encryption from a statistical perspective, but also creates a model that is adaptive, scalable, and has high flexibility in handling various types of images, such as complex textured and highly correlated images. This combination produces a cipher-image that is difficult to reconstruct without a key, while enriching the key space and expanding the space of encryption possibilities. In addition, while maintaining computational efficiency and lightweight network structure, this model allows for application in real-time systems, such as image transmission in IoT networks or video surveillance security in the public domain.

5. CONCLUSIONS

This study proposes a symmetric image encryption scheme based on a hybrid approach that combines a chaotic logistic map system with a deep convolutional autoencoder. In the initial stage, the image is secured through permutation, substitution, and masking processes using pseudo-random sequences generated from the logistic map. Furthermore, the initial encrypted image is further processed by a convolutional autoencoder network to deepen the spatial structure obscuration and increase the complexity of the cipher-image. This two-stage approach effectively combines deterministic randomness with the non-linear capabilities of deep learning, creating an encryption system that is resilient to statistical and differential attacks. Experimental results show that the proposed method has superior performance compared to previous methods, both in terms of MSE and PSNR values that indicate the optimal distortion level, as well as in security metrics such as NPCR and UACI that are close to the ideal maximum value. Histogram visualization and correlation tests prove that the original image structure is successfully obfuscated completely, and the resulting cipher-image does not provide explicit information that can be exploited by attackers. In addition, the maintained processing efficiency indicates that this method has the potential to be implemented in real-time systems or applications with limited resources.

For further research, model development can be focused on expanding the key space through a combination of multi-chaotic systems or higher-dimensional chaos algorithms such as Chen or Lorenz. Additionally, the use of advanced deep learning models such as the Transformer architecture can be explored to further enhance semantic-level obfuscation beyond the spatial domain. Implementing Vision Transformer (ViT) or Swin Transformer could offer improved abstraction of image features and stronger resistance to deep reconstruction attacks. Furthermore, the extension of this approach to dynamic visual data such as encrypted video frames or real-time image streams in IoT edge devices is a promising direction to improve the practical security of intelligent surveillance systems and data-sensitive applications.

ACKNOWLEDGEMENT

This research has been supported by Universitas Dian Nuswantoro, Indonesia based on Decree No. 459/KEP/UDN-01/IV/2023.

REFERENCES

[1] Otoum, Y., Gottimukkala, N., Kumar, N., Nayak, A. (2024). Machine learning in metaverse security: Current solutions and future challenges. ACM Computing Surveys, 56(8): 1-36. https://doi.org/10.1145/3654663

[2] Stefanidou, A., Cani, J., Papadopoulos, T., Radoglou-Grammatikis, P., Sarigiannidis, P., Varlamis, I., Papadopoulos, G.T. (2024). Leveraging digital twin technologies for public space protection and vulnerability assessment. In 2024 IEEE International Conference on Big Data (BigData), Washington, DC, USA, pp. 2836-2845. https://doi.org/10.1109/BigData62323.2024.10825359

[3] Ma, R., Furuya, K. (2024). Social media image and computer vision method application in landscape studies: A systematic literature review. Land, 13(2): 181. https://doi.org/10.3390/land13020181

[4] Rao, B.S. (2020). Dynamic histogram equalization for contrast enhancement for digital images. Applied Soft Computing, 89: 106114. https://doi.org/10.1016/j.asoc.2020.106114

[5] Abu-Faraj, M.A., Al-Hyari, A., Obimbo, C., Aldebei, K., Altaharwa, I., Alqadi, Z., Almanaseer, O. (2023). Protecting digital images using keys enhanced by 2D chaotic logistic maps. Cryptography, 7(2): 20. https://doi.org/10.3390/cryptography7020020

[6] Kamil Khudhair, S., Sahu, M., K.R., R., Sahu, A.K. (2023). Secure reversible data hiding using block-wise histogram shifting. Electronics, 12(5): 1222. https://doi.org/10.3390/electronics12051222

[7] Razi, Q., Piyush, R., Chakrabarti, A., Singh, A., Hassija, V., Chalapathi, G.S.S. (2025). Enhancing data privacy: A comprehensive survey of privacy-enabling technologies. IEEE Access, 13: 40354-10385. https://doi.org/10.1109/ACCESS.2025.3546618

[8] Li, L. (2024). A novel chaotic map application in image encryption algorithm. Expert Systems with Applications, 252: 124316. https://doi.org/10.1016/j.eswa.2024.124316

[9] Cahyo, N.R.D., Sari, C.A., Rachmawanto, E.H., Jatmoko, C., Al-Jawry, R.R.A., Alkhafaji, M.A. (2023). A comparison of multi class support vector machine vs deep convolutional neural network for brain tumor classification. In 2023 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, pp. 358-363. https://doi.org/10.1109/iSemantic59612.2023.10295336

[10] Gupta, J., Pathak, S., Kumar, G. (2022). Deep learning (CNN) and transfer learning: A review. Journal of Physics: Conference Series, 2273(1): 012029. https://doi.org/10.1088/1742-6596/2273/1/012029

[11] Ali, A., Pasha, M.F., Ali, J., Fang, O.H., Masud, M., Jurcut, A.D., Alzain, M.A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. Sensors, 22(2): 528. https://doi.org/10.3390/s22020528

[12] Lata, K., Cenkeramaddi, L.R. (2023). Deep learning for medical image cryptography: A comprehensive review. Applied Sciences, 13(14): 8295. https://doi.org/10.3390/app13148295

[13] Roy, M., Chakraborty, S., Mali, K. (2023). An optimized image encryption framework with chaos theory and EMO approach. Multimedia Tools and Applications, 82(20): 30309-30343. https://doi.org/10.1007/s11042-023-14438-6

[14] Barik, R.C., Hu, Y.C., Samal, T., Pati, R. (2024). Dynamics of quantum mechanical schrodinger wave function and chaos for biomedical image encryption scheme. Multimedia Tools and Applications, 83(11): 32813-32834. https://doi.org/10.1007/s11042-023-16775-y

[15] Guo, Y., Jing, S., Zhou, Y., Xu, X., Wei, L. (2020). An image encryption algorithm based on logistic-fibonacci cascade chaos and 3D bit scrambling. IEEE Access, 8: 9896-9912. https://doi.org/10.1109/ACCESS.2019.2963717

[16] Berahmand, K., Daneshfar, F., Salehi, E.S., Li, Y., Xu, Y. (2024). Autoencoders and their applications in machine learning: A survey. Artificial Intelligence Review, 57(2): 28. https://doi.org/10.1007/s10462-023-10662-6

[17] Wan, S., Lei, T.C. (2022). A development of a robust machine for removing irregular noise with the intelligent system of auto-encoder for image classification of coastal waste. Environments, 9(9): 114. https://doi.org/10.3390/environments9090114

[18] Chaudhary, N., Shahi, T.B., Neupane, A. (2022). Secure image encryption using chaotic, hybrid chaotic and block cipher approach. Journal of Imaging, 8(6): 167. https://doi.org/10.3390/jimaging8060167

[19] Anees, A., Siddiqui, A.M., Ahmed, F. (2014). Chaotic substitution for highly autocorrelated data in encryption algorithm. Communications in Nonlinear Science and Numerical Simulation, 19(9): 3106-3118. https://doi.org/10.1016/j.cnsns.2014.02.011

[20] Cahyo, N.R.D., Al-Ghiffary, M.M.I. (2024). An image processing study: Image enhancement, image segmentation, and image classification using milkfish freshness images. International Journal of Engineering Computing Advanced Research, 1(1): 11-22.

[21] 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

[22] Mfungo, D.E., Fu, X., Wang, X., Xian, Y. (2023). Enhancing image encryption with the Kronecker XOR product, the Hill Cipher, and the sigmoid logistic map. Applied Sciences, 13(6): 4034. https://doi.org/10.3390/app13064034

[23] Zelinka, I., Diep, Q.B., Snášel, V., Das, S., Innocenti, G., Tesi, A., Schoen, F., Kuznetsov, N.V. (2022). Impact of chaotic dynamics on the performance of metaheuristic optimization algorithms: An experimental analysis. Information Sciences, 587: 692-719. https://doi.org/10.1016/j.ins.2021.10.076

[24] Agilandeeswari, L., Prabukumar, M., Alenizi, F.A.

(2023). A robust semi-fragile watermarking system using Pseudo-Zernike moments and dual tree complex wavelet transform for social media content authentication. Multimedia Tools and Applications, 82(28): 43367-43419. https://doi.org/10.1007/s11042-023-15177-4

[25] Wang, M., Wang, X., Wang, C., Zhou, S., Xia, Z., Li, Q. (2023). Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and two-way Josephus traversing. Digital Signal Processing, 132: 103818. https://doi.org/10.1016/j.dsp.2022.103818

[26] Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., Blažauskas, T. (2019). An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. Entropy, 21(7): 656. https://doi.org/10.3390/e21070656

[27] Liu, X., Xiao, D., Liu, C. (2020). Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. Quantum Information Processing, 19(8): 239. https://doi.org/10.1007/s11128-020-02739-w

[28] Gupta, N., Vijay, R. (2022). Hybrid image compression-encryption scheme based on multilayer stacked autoencoder and logistic map. China Communications, 19(1): 238-252. https://doi.org/10.23919/JCC.2022.01.017

[29] Sara, U., Akter, M., Uddin, M.S. (2019). Image quality assessment through FSIM, SSIM, MSE and PSNR—A comparative study. Journal of Computer and Communications, 7(3): 8-18. https://doi.org/10.4236/jcc.2019.73002

[30] Chicco, D., Warrens, M.J., Jurman, G. (2021). The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation. PeerJ Computer Science, 7: e623. https://doi.org/10.7717/peerj-cs.623