Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.3, June 2026, pp. 2467~2475
e-ISSN: 2548-6861

Hybrid Cryptosystem for Image Encryption Using Lorenz Attractor and Neural Network Optimization

I Wayan Rangga Pinastawa [1]*, Radinal Setyadinsa [2]*, Ihsan Tri Marseno [3]* Gybran Kalmando [4]*
* Informatika, *Universitas Pembangunan Nasional "Veteran" Jakarta.*
rangga@upnvj.ac.id [1], radinalsetyadinsa@upnvj.ac.id [2], 2110511088@mahasiswa.upnvj.ac.id [3], 2110511106@mahasiswa.upnvj.ac.id [4]

Article Info

Article history:

Received 2026-04-27
Revised 2026-05-12
Accepted 2026-05-25

Keyword:

Chaos Encryption,
Image Security,
Lorenz Attractor,
Neural Network,
RGB Image.

ABSTRACT

Image encryption is required to protect visual data from unauthorized access. This study proposes a hybrid image cryptosystem based on the Lorenz chaotic attractor combined with artificial neural network optimization for adaptive chaotic parameter generation. The proposed method applies chaotic pixel permutation and bidirectional diffusion using chained XOR and bit rotation operations to improve ciphertext randomness and differential attack resistance. Experiments were conducted on three categories of generated RGB images with a resolution of 1024×1024 pixels. Performance evaluation was carried out using entropy, correlation coefficient, NPCR, UACI, PSNR, SSIM, key sensitivity, key space, histogram analysis, and encryption time analysis. The experimental results show that both encryption methods achieved entropy values close to the theoretical maximum approx ≈7.9999 and correlation values near zero, indicating strong randomness and successful removal of spatial pixel relationships. The proposed system also achieved NPCR values of approximately 99.6% and UACI values close to 333%, demonstrating strong resistance against differential attacks. In addition, the decryption process successfully reconstructed the original images without information loss, producing infinite PSNR values and SSIM values of 1.0. The obtained key sensitivity values exceeding 99.6% and the approximate key space of 10^{45} further indicate strong dependence on secret key precision and resistance against brute-force attacks. Overall, the proposed hybrid cryptosystem demonstrated strong statistical security, stable computational performance, and effective encryption capability for high-resolution RGB images.

I. INTRODUCTION

In the era of rapid growth in digital information exchange, ensuring data confidentiality and integrity has become a crucial necessity. Images, as one of the most frequently transmitted forms of digital media, are vulnerable to unauthorized interception and manipulation[1,2]. Traditional encryption algorithms, although effective against certain attacks, often face challenges when dealing with the intrinsic redundancy, structural patterns, and large file sizes commonly found in digital images. This condition has encouraged researchers to explore more dynamic and nonlinear approaches, such as chaos-based cryptosystems, which utilize high sensitivity to initial conditions and secret keys in chaotic maps to generate highly unpredictable encryption keys. Among various chaotic systems, the Lorenz attractor and other chaos models have been widely studied due to their ability to generate complex and non-repetitive sequences, making them suitable as robust cryptographic keys[3].

Recent studies have shown that chaos-based systems have strong potential for improving image encryption security. For example, research by Sayed utilized an affine transformation of the Lorenz system to produce a more complex random number generator, enabling image encryption that is more difficult to break[4]. In addition, a Lorenz attractor-based approach was applied to RGB images by Alexan, who combined cellular automata and an S-box to improve resistance against statistical and brute-force attacks[5]. Other studies have also evaluated various chaotic maps, including the Lorenz attractor, and reported that the Lorenz attractor

was able to produce higher entropy values and lower pixel correlation compared to several other methods, indicating its potential as an effective choice for chaos-based encryption schemes [6–8].

In addition, the integration of chaos-based methods with artificial neural networks has shown promising potential in adaptive image encryption systems. Neural networks provide adaptive capabilities for chaotic parameter prediction, allowing Lorenz attractor parameters to be dynamically adjusted according to image statistical characteristics. This adaptive mechanism enables the encryption process to maintain strong cryptographic performance while producing image-dependent chaotic behavior[9,10].

Furthermore, several studies have highlighted the importance of integrating confusion and diffusion stages in chaos-based encryption schemes[11,12]. The confusion stage is intended to shuffle pixel positions so that the spatial pattern of the original image is destroyed, while the diffusion stage uses operations such as XOR to spread key information across all image pixels.

However, a major challenge in developing chaos-based encryption systems is ensuring that the algorithm remains efficient when applied to large-sized images. In addition, the adaptability of chaotic parameters to different image types requires a more dynamic approach, making the combination with technologies such as neural networks a promising solution[13–15].

This study aims to develop and evaluate a hybrid image cryptosystem that combines the Lorenz chaotic attractor with an artificial neural network for adaptive chaotic parameter prediction. The proposed system applies confusion through chaotic pixel permutation and bidirectional diffusion through chained XOR and bit rotation operations to enhance resistance against statistical and differential attacks. Unlike conventional chaos-based encryption approaches that use fixed Lorenz parameters, the proposed method dynamically predicts chaotic parameters based on image statistical characteristics. In addition, this study provides a comparative evaluation between the standard Lorenz-based method and the adaptive Lorenz + Neural Network approach using statistical analysis (entropy and correlation coefficient), differential attack analysis (NPCR and UACI), reconstruction quality analysis (PSNR and SSIM), and key security evaluation (key sensitivity and key space analysis). The proposed approach is expected to contribute to the development of adaptive and secure image encryption systems with strong randomness, high sensitivity to secret keys, and resistance against brute-force attacks for protecting digital visual information in modern communication environments.

II. METHOD

This study uses an experimental approach to design, implement, and evaluate a hybrid cryptosystem intended to secure digital images. The system utilizes the Lorenz attractor to generate chaotic keys and applies artificial neural network optimization for adaptive chaotic parameter prediction. The research workflow is presented in the following figure.

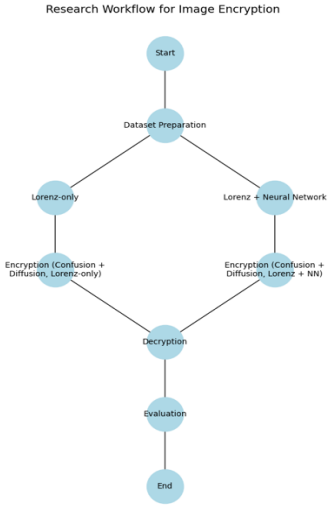

Figure 1. Research Workflow

Figure illustrates the workflow of the proposed image encryption system, which consists of dataset preparation, encryption using two approaches, decryption, and evaluation stages. The developed encryption system is chaos-based and uses the Lorenz attractor as the key generator, with additional chaotic parameter prediction using an artificial neural network in one of the approaches. Both approaches apply the same encryption mechanism, but differ in the strategy used to determine the chaotic parameters.

A. Dataset

The dataset used in this study consists of RGB digital images generated using generative image technology. The use of generated images allows controlled variations in visual patterns, color distribution, texture complexity, and object composition without dependence on a specific public dataset. Three image categories were selected, namely natural scene, synthetic object, and abstract art, to represent different statistical and structural image characteristics during encryption testing.

The natural scene category contains images with complex textures, natural color transitions, and irregular spatial structures. The synthetic object category represents images with clearer edges, more regular geometric structures, and relatively uniform object distributions. Meanwhile, the abstract art category contains highly varied color distributions and irregular visual patterns intended to evaluate encryption robustness under complex visual conditions. The use of these three categories enables the proposed cryptosystem to be evaluated across multiple image characteristics with different statistical properties.

All images were processed at high resolution (1024 × 1024 pixels) during the main evaluation stage in order to analyze the computational feasibility and encryption performance on large-sized images. Smaller image versions (thumbnails)

were additionally utilized to accelerate the initial analysis process and neural network training data generation.

The dataset was used for two main purposes. First, it was employed to evaluate the encryption and decryption performance of both the Lorenz-only and Lorenz + Neural Network methods. Second, the dataset was used to construct neural network training data through statistical feature extraction from encrypted images.

To construct the neural network training dataset, 120 encrypted image samples were generated using various Lorenz parameter combinations within predefined parameter ranges. Statistical characteristics extracted from the encrypted images, including RGB channel mean values, standard deviations, and entropy, were used as input features, while the corresponding Lorenz parameters were used as target outputs for adaptive parameter prediction.

To evaluate the generalization capability of the neural network and reduce the risk of overfitting, the generated feature dataset was divided into training and validation subsets using an 80:20 train-validation split. During the training process, both training loss and validation loss were monitored to analyze model convergence and overfitting behavior.

Although the proposed method demonstrated strong cryptographic performance across the tested image categories, this study remains limited to generated RGB images and has not yet evaluated other image modalities such as medical imaging, hyperspectral imaging, or video surveillance datasets. Therefore, broader generalization to real-world security applications requires further investigation in future work.

B. Divergence of Encryption Methods

The term divergence in this study refers to the difference in the strategy used to determine chaotic parameters between the two encryption approaches. This research applies two image encryption approaches, namely the Lorenz-based chaos method (Lorenz-only) and the hybrid Lorenz method with artificial neural network optimization (Lorenz + Neural Network). Both approaches use the Lorenz chaotic system as the generator of the encryption key sequence, which is expressed as follows:

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = x(\rho - z) - y$$
$$\frac{dz}{dt} = xy - \beta z$$

where $(\sigma), (\beta),$ and (ρ) are the control parameters of the Lorenz chaotic system. In the Lorenz-only method, the Lorenz system uses standard parameter values commonly found in the literature, namely $(\sigma) = 10$, $(\beta) = 2.667$, and $(\rho) = 28$. This approach is used as the baseline in evaluating the chaos-based encryption system[16].

In the Lorenz + Neural Network method, a feedforward artificial neural network, namely a Multilayer Perceptron (MLP), is used to adaptively optimize Lorenz parameters based on statistical characteristics extracted from encrypted images.

The neural network training dataset was constructed using 120 Lorenz parameter combinations generated randomly through uniform random sampling. The parameter ranges used were (σ) between 5 and 20, (β) between 0.5 and 4, and (ρ) between 20 and 45. These ranges were selected to include the standard values of the classical Lorenz system, namely $(\sigma = 10)$, $(\beta = 2.667)$, and $(\rho = 28)$, while also providing a wider exploration space during the optimization process.

Each parameter combination was applied to a representative RGB image, after which statistical features from the encrypted image were extracted as input data, while the Lorenz parameter values were used as output targets. The extracted input features consisted of the mean values of the RGB channels, the standard deviation of each channel, and the entropy of the encrypted image.

The neural network architecture consisted of one input layer with seven statistical features, two hidden layers containing 64 neurons each with ReLU activation functions, and one output layer with three linear neurons representing the Lorenz parameters, namely (σ), (β), and (ρ).

The model was trained for 40 epochs using the Adam optimization algorithm with a learning rate of 0.001, while Mean Squared Error (MSE) was employed as the loss function. During the training phase, each iteration processed data in batches of 8 samples. To evaluate the generalization capability of the model and reduce the risk of overfitting, the generated feature dataset was divided into training and validation subsets using an 80:20 train-validation split. Training loss and validation loss were monitored during the learning process to analyze model convergence and overfitting behavior.

For computational efficiency during neural network dataset generation, the encrypted training samples were produced using a reduced diffusion configuration before being applied to the full bidirectional diffusion process during the main encryption evaluation stage.

The Lorenz parameters optimized by the neural network were subsequently utilized in the image encryption process to generate adaptive chaotic behavior based on image statistical characteristics.

C. Encryption and Decryption Process

Both encryption methods apply an identical processing flow, with the main difference lying in the Lorenz parameter values used. The input image is first processed using the Lorenz chaotic system to generate a chaotic sequence that functions as the encryption key.

The first dimension of the chaotic sequence is used to construct the diffusion key, while the second dimension is utilized to generate pixel permutation indices during the confusion stage. The permutation process is performed by

sorting the chaotic sequence values to produce permutation indices, causing the spatial arrangement of image pixels to become highly randomized before the diffusion stage.

After the confusion stage, the diffusion process is carried out to modify pixel intensity values using modulo 256 arithmetic operations, chained XOR operations, and bit rotation. The proposed method applies bidirectional diffusion consisting of forward and backward diffusion stages to improve resistance against differential attacks and increase the avalanche effect.

In the forward diffusion stage, the encryption process for the iii-th pixel is expressed as follows:

$$\mathrm{C_i} = \mathrm{ROL}\left(\left((\mathrm{P_i} + \mathrm{K_i}) \bmod 256\right) \oplus \mathrm{C_{i-1}}, \mathrm{r_i}\right)$$

where $(\mathrm{P_i})$ represents the (i)-th plaintext pixel, $(\mathrm{K_i})$ is the (i)-th chaotic key, $(\mathrm{C_i})$ is the (i)-th ciphertext pixel, and (ROL) denotes the left bit rotation operation.

To further enhance diffusion propagation, a backward diffusion stage is subsequently applied in the reverse direction, which is expressed as follows:

$$C_i' = ROL\left(\left((C_i \oplus C_{i+1}') + K_i\right) mod 256, r_i'\right)$$

Where C_i' represents the ciphertext generated after the backward diffusion process.

The diffusion stage is repeated for five rounds using forward and backward bidirectional diffusion to increase sensitivity to small changes in both the plaintext image and chaotic parameters. This mechanism enables small modifications in the input image or secret key to propagate across the entire encrypted image more effectively.

The decryption process is carried out by sequentially applying the inverse operations of each encryption stage, including inverse backward diffusion, inverse forward diffusion, right bit rotation, reverse XOR operation, modulo 256 subtraction, and inverse permutation. By using the same Lorenz parameters and chaotic key sequence, the original image can be reconstructed correctly without information loss.

The reversibility of the proposed cryptosystem was further evaluated using PSNR and SSIM metrics between the original image and the decrypted image. High PSNR values and SSIM values close to 1 indicate that the decryption process successfully reconstructs the original image with negligible distortion while maintaining encryption security[17].

D. Evaluation Method

The performance evaluation of the encryption system was conducted on encrypted images to assess the security level, reconstruction quality, and computational effectiveness of the proposed cryptosystem. Several evaluation metrics were employed, including Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), information entropy, pixel correlation, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), key sensitivity analysis, key space analysis, histogram analysis, and encryption time analysis.

NPCR is used to measure the percentage of pixel changes in the ciphertext caused by small modifications in the plaintext image, and is formulated as follows:

$$NPCR = \left(\frac{\sum D(i,j)}{M \times N}\right) \times 100$$

where $(\mathrm{D(i,j)} = 1)$ if $\left(C_1(i,j) \neq C_2(i,j)\right)$, and $(D(i,j) = 0)$ otherwise.

UACI is used to measure the average intensity difference between two ciphertext images and is expressed as follows:

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100$$

Information entropy is used to evaluate the randomness level of ciphertext pixel distribution and is calculated using the following formula:

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

Correlation between adjacent pixels is used to evaluate the ability of the encryption system to eliminate spatial relationships in the original image, and is formulated as follows:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{\mathrm{Var}(x)}\sqrt{\mathrm{Var}(y)}}$$

PSNR is used to evaluate the reconstruction quality of the decrypted image relative to the original image and is expressed as follows:

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right)$$

where *MSE* represents the Mean Squared Error between the original image and the decrypted image.

SSIM is used to measure structural similarity between the original image and the decrypted image by considering luminance, contrast, and structural information, and is expressed as follows:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Where μ_x and μ_y represent the average intensity values of the two images, σ_x^2 and σ_y^2 denote the variances, σ_{xy} is the covariance, and C_1 and C_2 are stability constants.

Key sensitivity analysis was performed by applying a very small perturbation to one of the Lorenz parameters and observing the resulting changes in the ciphertext image. The difference between the ciphertexts generated using the original and modified parameters was evaluated using the NPCR metric. High NPCR values indicate strong sensitivity of the encryption system to small changes in the secret key.

Key space analysis was conducted to estimate the total number of possible secret key combinations generated from the Lorenz chaotic parameters. Assuming that each Lorenz parameter (σ, β, ρ) is represented with a computational precision of approximately 10^{-15}, The approximate key space can be expressed as follows:

$$K_{\mathrm{space}} = (10^{15})^3 \approx 10^{45} \approx 2^{149}$$

which represents the combined precision space of the three Lorenz parameters (σ), (β), and (ρ). The obtained key space is sufficiently large to resist brute-force attacks using current computational capabilities[18].

Histogram analysis was used to evaluate the uniformity of ciphertext pixel distributions, while encryption time analysis was conducted to evaluate the computational feasibility of the proposed encryption system when processing high-resolution images.

An entropy value close to 8 indicates a highly random ciphertext distribution, while correlation values close to zero indicate successful removal of adjacent pixel relationships. High NPCR and UACI values indicate strong resistance against differential attacks. In addition, high PSNR values and SSIM values close to 1 indicate successful image reconstruction during the decryption process with minimal information loss.

All evaluation metrics were applied consistently to both the Lorenz-only and Lorenz + Neural Network methods to ensure objective and fair performance comparison.

III. Results and Discussion

This section presents the experimental results and discussion of the proposed hybrid image cryptosystem based on the Lorenz chaotic attractor and artificial neural network optimization. The experiments were conducted using three categories of generated RGB images, namely natural scene, synthetic object, and abstract art, with a resolution of 1024×1024 pixels. The evaluation focused on encryption randomness, differential attack resistance, reconstruction quality, key security, and computational performance.

A. Dataset Visualization

The proposed cryptosystem was evaluated using two approaches, namely the standard Lorenz-based encryption method (Lorenz-only) and the adaptive Lorenz + Neural Network method. Both methods applied identical confusion and bidirectional diffusion stages, while differing in the strategy used to determine the Lorenz chaotic parameters. An example of one of the generated images used in this study is shown in Figure 2.

Figure 2. Generated RGB Image Dataset

B. Lorenz Trajectory Visualization

Figure 3 presents the trajectory visualization of the Lorenz attractor used as the chaotic key generator in both the Lorenz-only and Lorenz + Neural Network methods. The butterfly-shaped trajectory pattern demonstrates the nonlinear and non-periodic behavior of the Lorenz chaotic system, which is highly sensitive to small changes in chaotic parameters and initial conditions. These characteristics are important in image cryptography because they enable the generation of complex and unpredictable key sequences for the confusion and bidirectional diffusion processes.

In the Lorenz-only method, the chaotic trajectory was generated using the standard Lorenz parameters $(\sigma = 10)$, $(\beta = 2.667)$, and $(\rho = 28)$,. Meanwhile, the Lorenz + Neural Network method utilized adaptively optimized Lorenz parameters generated by the neural network model. Although both methods preserved the fundamental chaotic structure of the Lorenz attractor, observable differences appeared in the trajectory density and orbit distribution due to the adaptive parameter optimization process. These results indicate that the neural network successfully generated alternative chaotic parameter configurations while maintaining the chaotic behavior required for secure image encryption.

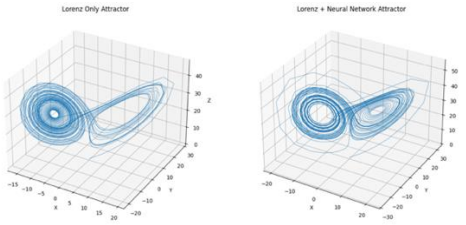

Figure 3. Comparison of Chaotic Lorenz Trajectories

C. Adaptive Lorenz Parameter Analysis

The Lorenz + Neural Network method generated adaptive chaotic parameters for each image category based on extracted image statistical characteristics. Table I presents the predicted Lorenz parameters (σ), (β), and (ρ)) produced by the neural network model during the encryption process.

The experimental results show that the predicted chaotic parameters varied slightly across different image categories while remaining within the chaotic region of the Lorenz system. For example, the predicted σ values ranged from approximately 13.79 to 13.82, while the predicted ρ values remained around 32.7. These variations indicate that the neural network successfully generated adaptive parameter configurations according to image statistical characteristics while preserving the chaotic behavior required for secure image encryption.

TABEL I
ADAPTIVE LORENZ PARAMETERS GENERATED BY THE NEURAL NETWORK MODEL FOR DIFFERENT IMAGE CATEGORIES.

Category	Sigma NN	Beta NN	Rho NN
Natural Scene	13.8122	2.5339	32.7190
Synthetic Object	13.8241	2.5084	32.7151
Abstract Art	13.7957	2.5096	32.722

D. Overfitting Analysis

The overfitting behavior of the neural network model was evaluated by monitoring both training loss and validation loss

during the training process. Figure 4 presents the training and validation loss curves obtained during 40 training epochs.

As shown in Figure 4, both the training loss and validation loss decreased rapidly during the early training stage and gradually converged as the training process progressed. The final training loss and validation loss values were approximately 23.57 and 25.13, respectively, indicating that the difference between both curves remained relatively small.

The absence of a large gap between the training and validation loss curves suggests that no significant overfitting occurred during model training. These results indicate that the neural network model was able to generalize the relationship between image statistical characteristics and Lorenz chaotic parameters effectively within the generated dataset.

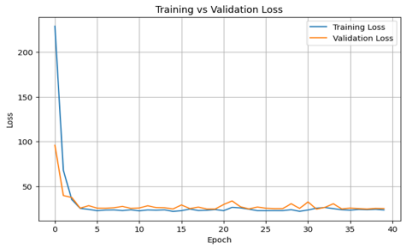

Figure 4. Training and Validation Loss Curves of the Neural Network Model.

E. Encryption-Decryption Visualization

Figure 5 presents a visual comparison between the original image, encrypted images generated using the Lorenz-only and Lorenz + Neural Network methods, and the reconstructed decrypted image for the natural scene category. The encrypted images produced by both methods exhibit highly random visual patterns without recognizable structural information from the original image. Meanwhile, the decrypted image was successfully reconstructed and visually identical to the original image, confirming the reversibility and stability of the proposed cryptosystem.

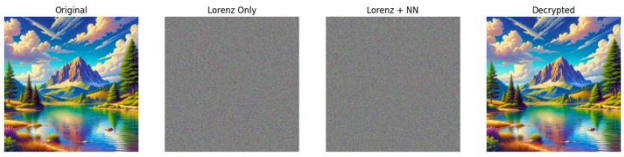

Figure 5. Comparison of Encryption and Decryption Results

F. Histogram Analysis

Histogram analysis was conducted to evaluate the pixel intensity distribution before and after the encryption process. Figure 6 presents the histogram comparison between the original image, the Lorenz-only encrypted image, and the Lorenz + Neural Network encrypted image. The histogram of the original image shows a non-uniform distribution that reflects the natural visual structure and statistical characteristics of the image content.

After the encryption process, both encryption methods produced ciphertext histograms with nearly uniform distributions across the entire intensity range (0–255)(0–255)(0–255). This indicates that the statistical properties of the original image were successfully concealed through the confusion and bidirectional diffusion processes. The uniform histogram distribution demonstrates that the encrypted images possess strong statistical randomness and reduced vulnerability to histogram-based statistical attacks.

The histogram patterns produced by the Lorenz-only and Lorenz + Neural Network methods were visually similar, indicating that both approaches successfully maintained strong ciphertext randomness. The adaptive neural network optimization primarily influenced the chaotic parameter generation process while preserving the statistical security characteristics of the Lorenz chaotic encryption system.

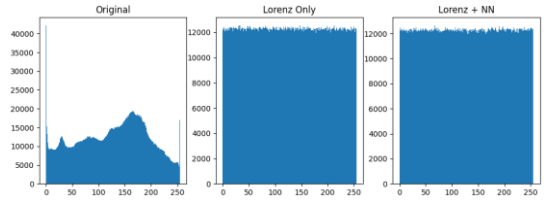

Figure 6. Histogram Comparison of Original and Encrypted Images.

G. Entropy Analysis

Table II presents a comparison of the entropy values of the original images, encrypted images, and decrypted images for both methods. The entropy values of the encrypted images in both methods reached 7.9999 or were very close to the theoretical maximum value of 8.0, indicating a highly random and unpredictable pixel intensity distribution.

The decryption process in both methods successfully restored the entropy values to their original values, indicating that the proposed encryption system is reversible. There was no difference in entropy values between the Lorenz-only and Lorenz + Neural Network methods, showing that parameter optimization using an artificial neural network does not directly affect the global randomness level of the image, but plays a greater role in sensitivity and parameter adaptability.

TABEL II
COMPARISON OF ENTROPY VALUES

Category	Entropy Lorenz	Entropy Lorenz + NN
Natural Scene	7.9999	7.9999
Synthetic Object	7.9999	7.9999
Abstract Art	7.9999	7.9999
Average	7.9999	7.9999

H. Correlation Analysis

Table III presents the pixel correlation analysis results for the encrypted images generated using the Lorenz-only and Lorenz + Neural Network methods. The encrypted images produced by both approaches achieved correlation values very close to zero across all tested image categories. The average correlation values obtained using the Lorenz-only

and Lorenz + Neural Network methods were approximately −0.0008 and −0.0014, respectively.

The very low correlation values indicate that neighboring pixels in the ciphertext images became statistically independent after the confusion and bidirectional diffusion processes. This demonstrates that both encryption methods successfully removed spatial dependencies between adjacent pixels, thereby increasing resistance against statistical analysis attacks.

Although the differences between both methods were relatively small, the Lorenz-only method achieved slightly lower absolute correlation values on average. However, both approaches consistently produced correlation values extremely close to zero, indicating highly effective pixel decorrelation performance. These findings suggest that the adaptive neural network optimization primarily contributed to dynamic chaotic parameter generation while maintaining the strong decorrelation capability of the Lorenz chaotic encryption system.

TABEL III
PIXEL CORRELATION COMPARISON OF BOTH METHODS

Image	Encryption Correlation (Lorenz)	Encryption Correlation (Lorenz + NN)
Natural Scene	-0.000669	-0.001578
Synthetic Object	-0.000788	-0.000931
Abstract Art	-0.000944	-0.001560
Average	-0.000800	-0.001356

I. NPCR & UACI Analysis

Table IV presents the NPCR and UACI results obtained from the differential attack analysis for both encryption methods. The Lorenz-only and Lorenz + Neural Network methods consistently achieved NPCR values of

approximately 99.6% and UACI values close to 33% across all tested image categories. These values are close to the ideal cryptographic criteria for secure image encryption systems, indicating strong resistance against differential attacks and a significant avalanche effect.

For natural scene images, the Lorenz-only method produced slightly higher NPCR and UACI values compared to the Lorenz + Neural Network method. This indicates that the standard Lorenz parameters were already highly effective for images with complex natural textures and color variations.

For synthetic object images, the Lorenz + Neural Network method produced a slightly higher UACI value (33.4838%) compared to the Lorenz-only method (33.4563%), indicating improved intensity diffusion performance under adaptive parameter optimization. However, the NPCR values of both methods remained highly comparable and very close to the ideal value.

For abstract art images, both methods again demonstrated very similar NPCR and UACI performance, with only minor differences between the Lorenz-only and Lorenz + Neural Network approaches. These findings indicate that the final bidirectional diffusion mechanism successfully enhanced differential attack resistance in both encryption methods.

Overall, the experimental results demonstrate that both methods achieved highly secure differential attack performance after the implementation of the enhanced bidirectional diffusion process. The adaptive neural network optimization primarily contributed to dynamic chaotic parameter generation and parameter adaptability rather than dramatically increasing NPCR and UACI values beyond the already strong performance of the Lorenz chaotic encryption system.

TABEL IV
NPCR AND UACI COMPARISON OF BOTH METHODS

Category	NPCR Lorenz	NPCR Lorenz + NN	UACI Lorenz	UACI Lorenz + NN
Natural Scene	99.6094	99.6057	33.4577	33.4558
Synthetic Object	99.6118	99.6082	33.4563	33.4838
Abstract Art	99.6111	99.6077	33.4745	33.4622
Average	99.6108	99.6072	33.4628	33.4673

J. PSNR & SSIM Analysis

Reconstruction quality analysis was conducted using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) to evaluate the reversibility of the proposed cryptosystem. Table V presents the PSNR and SSIM results obtained between the original images and the decrypted images for all tested image categories.

The experimental results show that all decrypted images achieved infinite PSNR values and SSIM values of 1.0 for both encryption methods. These findings indicate that the decryption process successfully reconstructed the original images without information loss or structural distortion.

The obtained PSNR and SSIM results confirm that the proposed encryption and decryption processes are fully reversible and stable. In addition, the perfect reconstruction performance demonstrates that the implementation of the confusion and bidirectional diffusion mechanisms did not introduce irreversible modifications to the encrypted image data.

TABEL V
PSNR AND SSIM RESULTS OF DECRYPTED IMAGES

Image	PSNR	SSIM
Natural Scene	Inf	1.0
Synthetic Object	inf	1.0
Abstract Art	inf	1.0
Average	inf	1.0

K. Computational Performance Analysis

Computational performance analysis was conducted to evaluate the practical feasibility of the proposed encryption system when processing high-resolution RGB images. Table VI presents the encryption time comparison between the Lorenz-only and Lorenz + Neural Network methods for all tested image categories.

The experimental results show that both methods required relatively similar encryption times, with average encryption times of approximately 53.39 seconds for the Lorenz-only method and 54.27 seconds for the Lorenz + Neural Network method. The slightly higher computational time observed in the Lorenz + Neural Network method was mainly caused by the additional neural network parameter optimization process before chaotic sequence generation.

Despite the additional optimization stage, the computational overhead introduced by the neural network remained relatively small compared to the overall encryption process. These findings indicate that the proposed hybrid cryptosystem is capable of maintaining strong cryptographic performance while preserving acceptable computational efficiency for high-resolution 1024×1024 RGB image encryption.

TABEL VI
ENCRYPTION TIME COMPARISON BETWEEN THE LORENZ-ONLY AND LORENZ + NEURAL NETWORK METHODS.

Image	Enc Time Lorenz (s)	Enc Time Lorenz + NN (s)
Natural Scene	54.0195	54.1270
Synthetic Object	52.0569	53.5843
Abstract Art	54.0802	55.1011
Average	53.3855	54.2708

L. Key Security Analysis.

Key sensitivity analysis was conducted by applying small perturbations to the Lorenz chaotic parameters during the encryption process. Table VII presents the key sensitivity results obtained using NPCR measurements between ciphertext images generated from the original and modified chaotic parameters.

The experimental results show that all image categories achieved key sensitivity values exceeding 99.6%. These findings indicate that very small modifications in the chaotic parameters produced substantially different ciphertext outputs, demonstrating strong dependence on secret key precision and high resistance against key-related attacks.

In addition, the proposed cryptosystem achieved an approximate key space of 10^{45}, which is sufficiently large to resist brute-force attacks using current computational capabilities. These results confirm that the proposed Lorenz-based cryptosystem possesses strong key security characteristics suitable for secure image encryption applications.

TABEL VII
KEY SENSITIVITY ANALYSIS RESULTS OF THE PROPOSED CRYPTOSYSTEM

Image	Enc Time Lorenz (s)
Natural Scene	99.6053
Synthetic Object	99.6145
Abstract Art	99.6124
Average	99.6107

IV. CONCLUSION

Based on the experimental results obtained from the three image categories, namely natural scene, synthetic object, and abstract art, it can be concluded that the Lorenz attractor is highly effective as a chaotic key generator for secure image encryption due to its nonlinear dynamics and high sensitivity to chaotic parameters. Both the Lorenz-only and Lorenz + Neural Network methods consistently produced entropy values of approximately 7.9999 and correlation values very close to zero, indicating strong ciphertext randomness and successful removal of spatial relationships between adjacent pixels.

The proposed bidirectional diffusion mechanism significantly improved differential attack resistance, as demonstrated by NPCR values of approximately 99.6% and UACI values close to 33% for both encryption methods. These values are close to the ideal cryptographic criteria for secure image encryption systems and indicate a strong avalanche effect against small plaintext modifications.

The experimental results also showed that the Lorenz-only and Lorenz + Neural Network methods achieved relatively comparable cryptographic performance across all tested image categories. Although the adaptive neural network optimization did not significantly outperform the standard Lorenz method in all evaluation metrics, the neural network successfully generated alternative chaotic parameter configurations while preserving the strong security characteristics of the Lorenz chaotic system. This demonstrates that the neural network primarily contributed to adaptive chaotic parameter optimization and dynamic chaotic behavior rather than solely maximizing a specific cryptographic metric.

In addition, the proposed cryptosystem successfully reconstructed the original images during the decryption process without information loss, as indicated by infinite PSNR values and SSIM values of 1.0 across all experiments. The obtained key sensitivity values exceeding 99.6% and the approximate key space of 10^{45} further indicate strong dependence on secret key precision and high resistance against brute-force attacks.

Although the proposed cryptosystem demonstrated strong statistical security and differential attack resistance, this study has not yet evaluated advanced cryptanalytic attacks such as chosen-plaintext attacks, known-plaintext attacks, or deep-learning-based cryptanalysis. In addition, the experiments were limited to generated RGB images and did not include real-world datasets such as medical images, hyperspectral images, or video surveillance data. Therefore, further investigation is required to evaluate the robustness of the proposed system in broader real-world security scenarios.

Overall, the proposed Hybrid Lorenz–Neural Network cryptosystem demonstrated strong statistical security, effective differential attack resistance, high reconstruction accuracy, and stable computational performance for 1024×1024 RGB image encryption. Future work may further evaluate the proposed approach using larger datasets,

different image modalities, and modern cryptanalytic attack scenarios to investigate broader real-world security applications.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Universitas Pembangunan Nasional "Veteran" Jakarta for the financial support provided, which enabled this research to be conducted and published.

REFERENCES

[1] Sambhaji Marutirao Shedole, V Santhi. A Comprehensive Study on Digital Watermarking for Security Threats and Research Directions. International Journal of Data Informatics and Intelligent Computing 2025;4:54–72. https://doi.org/10.59461/ijdiic.v4i1.160.

[2] Chennamma HR, Madhushree B. A comprehensive survey on image authentication for tamper detection with localization. Multimed Tools Appl 2023;82:1873–904. https://doi.org/10.1007/s11042-022-13312-1.

[3] Dinu A. From Chaos to Security: A Comparative Study of Lorenz and Rössler Systems in Cryptography. Cryptography 2025;9:58. https://doi.org/10.3390/cryptography9030058.

[4] Sayed WS, Radwan AG, Fahmy HAH, Elsedeek A. Trajectory control and image encryption using affine transformation of lorenz system. Egyptian Informatics Journal 2021;22:155–66. https://doi.org/10.1016/j.eij.2020.07.002.

[5] Alexan W, Elbeltagy M, Aboshousha A. RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System. Symmetry (Basel) 2022;14. https://doi.org/10.3390/sym14030443.

[6] Satre SM, Joshi B. Quantum image cryptography based on continuous chaotic maps. Microsystem Technologies 2024. https://doi.org/10.1007/s00542-024-05764-2.

[7] Ahuja B, Doriya R, Salunke S, Hashmi MF, Gupta A, Bokde ND. HDIEA: high dimensional color image encryption architecture using five-dimensional Gauss-logistic and Lorenz system. Conn Sci 2023;35. https://doi.org/10.1080/09540091.2023.2175792.

[8] Masood F, Ahmad J, Shah SA, Jamal SS, Hussain I. A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map. Entropy 2020;22:274. https://doi.org/10.3390/e22030274.

[9] Guitouni Z, Machhout M. Implementation of Chaotic Neural Key Generation Algorithm For IoT Devices. International Journal of Electrical Engineering and Computer Science 2024;6:232–8. https://doi.org/10.37394/232027.2024.6.27.

[10] Alloun Y, Azzaz MS, Kifouche A. A new approach based on artificial neural networks and chaos for designing deterministic random number generator and its application in image encryption. Multimed Tools Appl 2024;84:5825–60. https://doi.org/10.1007/s11042-024-19136-5.

[11] Shibeeb AK, Ahmed MH, Mohammed AH. A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation. Karbala International Journal of Modern Science 2021;7. https://doi.org/10.33640/2405-609X.3117.

[12] Andono PN, Setiadi DRIM. Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption. IEEE Access 2022;10:115143–56. https://doi.org/10.1109/ACCESS.2022.3218886.

[13] Zhang B, Liu L. Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics 2023;11:2585. https://doi.org/10.3390/math11112585.

[14] Rezaei B, Mobasseri M, Enayatifar R. A secure, efficient and super-fast chaos-based image encryption algorithm for real-time applications. J Real Time Image Process 2023;20:30. https://doi.org/10.1007/s11554-023-01289-5.

[15] Mansoor S, Parah SA. HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing. Multimed Tools Appl 2023;82:28769–96. https://doi.org/10.1007/s11042-023-14542-7.

[16] Rangga Pinastawa IW, Pradana MG, Maulana N. Dual Layer Chaotic Image in Audio Steganography System Using LSB Embedding for Secure Multimedia Communication. 2025 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), IEEE; 2025, p. 1383–8. https://doi.org/10.1109/ICIMCIS68501.2025.11327291.

[17] Al Najjar Y. Comparative Analysis of Image Quality Assessment Metrics: MSE, PSNR, SSIM and FSIM. International Journal of Science and Research (IJSR) 2024;13:110–4. https://doi.org/10.21275/SR24302013533.

[18] Feng W, Wang Q, Liu H, Ren Y, Zhang J, Zhang S, et al. Exploiting Newly Designed Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map for High-Performance Multi-Image Encryption. Fractal and Fractional 2023;7:887. https://doi.org/10.3390/fractalfract7120887.