

Improved Lorenz chaotic map with dynamic zig-zag pattern for high-security digital image encryption

Ajib Susanto¹, Elkaf Rahmawan Pramudya¹, Noorayisahbe Mohd Yaacob²

¹Department of Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia

²Department of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia

Article Info

Article history:

Received Oct 16, 2025

Revised Mar 11, 2026

Accepted Aug 27, 2026

Keywords:

Chaotic map

Data hiding

Dynamic zig-zag pattern

Image encryption

Lorenz mapping

ABSTRACT

This study proposes a secure image encryption framework based on an improved Lorenz chaotic map combined with a dynamic zig-zag permutation strategy. The improved chaotic mapping introduces dynamic perturbations to increase the complexity of chaotic trajectories and expand the key space, while the dynamic zig-zag traversal enhances pixel-level diffusion and minimizes residual pixel correlations during the permutation stage. Experimental evaluation was conducted on multiple RGB images with a resolution of 512×512 pixels. The proposed method achieved mean squared error (MSE) values of approximately 1800–1900 and peak signal-to-noise ratio (PSNR) values around 15.8 dB, indicating significant structural distortion between plaintext and cipher images. In addition, the obtained unified average changing intensity (UACI) (~33.4%) and number of pixels change rate (NPCR) (~99.61%) values approach the theoretical ideals, demonstrating strong resistance against statistical and differential attacks. Comparative analysis shows that the proposed framework provides stronger statistical robustness than conventional Lorenz-based encryption schemes. Furthermore, the decryption process successfully reconstructs the original images without information loss, confirming the correctness and reversibility of the scheme. These results indicate that integrating dynamic perturbations with adaptive zig-zag permutation effectively improves diffusion strength, key space complexity, and overall encryption robustness for secure multimedia image transmission.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ajib Susanto

Department of Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro

Imam Bonjol Street no. 207, Semarang 50131, Central Java, Indonesia

Email: ajib.susanto@dsn.dinus.ac.id

1. INTRODUCTION

Digital image encryption is increasingly crucial as the transmission and storage of visual data continue to expand in domains such as telemedicine, surveillance, social networking, and IoT, where sensitive images are vulnerable to interception and unauthorized access [1]–[3]. Unlike textual data, images possess characteristics such as large file sizes, high redundancy, and strong pixel correlation, making conventional cryptographic algorithms inefficient and often insecure when directly applied [4], [5]. Recent studies highlight that the rapid increase in data volume and the demand for real-time communication have intensified security risks, as many existing image encryption schemes remain susceptible to statistical analysis, differential attacks, and chosen-plaintext or chosen-ciphertext attacks [6], [7]. Moreover, relevant research indicates that limitations such as restricted key space [8], correlation leakage [9], and inadequate resistance to modern cryptanalysis are

persistent challenges [10], which underscores the pressing need for more advanced approaches to ensure robust protection of digital images in practical applications.

To overcome these limitations, recent works have investigated the development of customized image encryption schemes based on the features of chaotic mappings [11], multi-phase permutation–diffusion architecture [12], and adaptive secret key generating mechanisms to eliminate the shortcomings of traditional schemes [13]. Chaotic mappings, and especially advanced versions like modified Lorenz mappings, are broadly used to produce very sensitive and non-predictable keystreams and hence increase the key space and robustness against statistical and differential attack [14]–[16]. Meanwhile, adaptive permutation mechanisms involving rotation or geometry transformations are implemented to break strong pixel correlations and enhance the diffusion impact such that tiny variations of plaintext or secret keys cause drastic changes of ciphertext [17], [18]. Moreover, new designs focus on lightweight processing and scalability for real-time implementations in areas of IoT and telemedicine where both efficiency and security are essential [19], [20]. Collectively, these new ideas are designed to offer greater immunity against powerful cryptanalysis tools while sustaining realizable practicability within current multimedia scenarios. Many studies have applied chaotic systems to strengthen image encryption.

For instance, research [21] introduced a fractional-order chaotic map where three main variables evolve nonlinearly through the interaction of parameters such as A_w , B_w , C_w , D_w , E_w , F_w . A change in one variable, such as x_1 , directly affects the others through cross-multiplication (x_1x_2) and (x_1x_3), creating a highly complex calculation pattern and strong randomness. This mechanism ensures that the pixel distribution of the encrypted image becomes significantly dispersed, thereby reducing adjacent pixel correlation and increasing overall entropy. However, the main drawback lies in the high computational complexity caused by the fractional-order nature, making it less suitable for real-time applications. In addition, the chaotic stability may degrade when the map is discretized, which can potentially reduce practical security. In another direction, research [22] employed an optimization-based encryption approach inspired by hunter–prey dynamics. Each pixel is treated as an agent with a random initial position in the search space, and its position is updated through a combination of average μ calculations of all agents and the Euclidean distance D_{euc} to the population center. This iterative process adaptively shifts the pixel positions, where the new value depends on a balance factor C that decreases with iterations. Consequently, simple calculations such as mean position and squared distance are leveraged to produce a complex ciphertext distribution, while avoiding deterministic patterns that could be exploited. The limitation, however, is that the high number of iterations makes this method prone to slow convergence, which increases encryption latency. Moreover, the optimization-based approach requires sensitive parameter tuning, and improper configuration may significantly weaken security.

Furthermore, research [23] utilized a continuous chaotic system resembling Lorenz dynamics, defined by three nonlinear differential equations. In this system, small changes in initial conditions such as $x(0)$, $y(0)$, and $z(0)$ lead to exponentially divergent trajectories due to cross-multiplication xy and linear factors like $\alpha(y - x)$. This property ensures that even if the input image changes by a single pixel, the resulting ciphertext differs significantly. As a result, the system provides strong diffusion and high key sensitivity, both of which are crucial for resistance against differential and brute-force attacks. Nonetheless, the classical Lorenz system suffers from a relatively narrow key space and potential predictability of chaotic patterns if parameters are not carefully chosen. In addition, this approach is not fully efficient for encrypting large-scale images because of the computational burden of numerical integration.

From the above studies, it is evident that while existing chaotic and optimization-based image encryption methods have introduced valuable mechanisms for enhancing security, they still exhibit notable limitations in terms of computational efficiency, chaotic stability, parameter sensitivity, and scalability to large image datasets. Fractional-order systems suffer from excessive complexity that hinders real-time applicability, optimization-driven approaches are vulnerable to slow convergence and parameter dependency, and classical Lorenz-based schemes face restricted key spaces and potential predictability issues. These drawbacks highlight the necessity for a more balanced encryption framework that combines strong randomness and high sensitivity with computational efficiency and practical feasibility. This motivates the development of an improved Lorenz chaotic map integrated with a dynamic zig-zag pattern, designed to expand key space, strengthen pixel-level diffusion, and ensure robustness against statistical and cryptanalytic attacks while remaining suitable for real-world multimedia applications.

2. METHOD

2.1. Proposed encryption workflow

The proposed workflow, as seen in Figure 1, is structured into four main stages designed to ensure a high-security digital image encryption scheme. In the first stage, the input image $I(m, n)$ of size $M \times N$ is decomposed into its RGB channels, allowing independent processing of each component. This step not only

preserves the intrinsic color distribution but also increases the key space by handling three separate encryption streams simultaneously. The second stage integrates the improved Lorenz chaotic system as the core pseudo-random sequence generator. Unlike the classical Lorenz system with fixed parameters ($\sigma = 10, \rho = 28, \beta = 8/3$), the improved version introduces dynamic perturbations through a time-varying parameter $\rho(t) = \rho_0(1 + \varepsilon \sin(vt))$ with $\rho_0 = 28, \varepsilon = 0.05$, and $v = 3$. This modification significantly enhances trajectory complexity and prevents the formation of predictable butterfly patterns, ensuring higher unpredictability in the keystream. The chaotic sequences (x, y, z) generated from this stage are normalized and expanded to match the size of the image matrix, thereby producing three independent keystreams aligned with the RGB channels. The third stage applies a dynamic zig-zag rotation pattern, which reorganizes pixel positions based on the chaotic indices. Unlike static permutations, this mechanism leverages dynamic parameters derived from the Lorenz sequences, ensuring that the zig-zag traversal is different for every encryption session. As an example, the traversal step size is adaptively determined by the integer part of $x(t) \times 10^5$, leading to a pseudo-random yet deterministic path that resists statistical attacks. Finally, in the fourth stage, a diffusion process is performed where each pixel value is modified using XOR and modular addition with the corresponding chaotic keystream. The dual operation guarantees resistance against differential attacks, as a single pixel change in the plaintext propagates across the entire ciphertext. This workflow design, which couples improved Lorenz chaos with dynamic permutation and diffusion, ensures robustness against cryptanalysis while maintaining computational efficiency suitable for real-time image encryption.

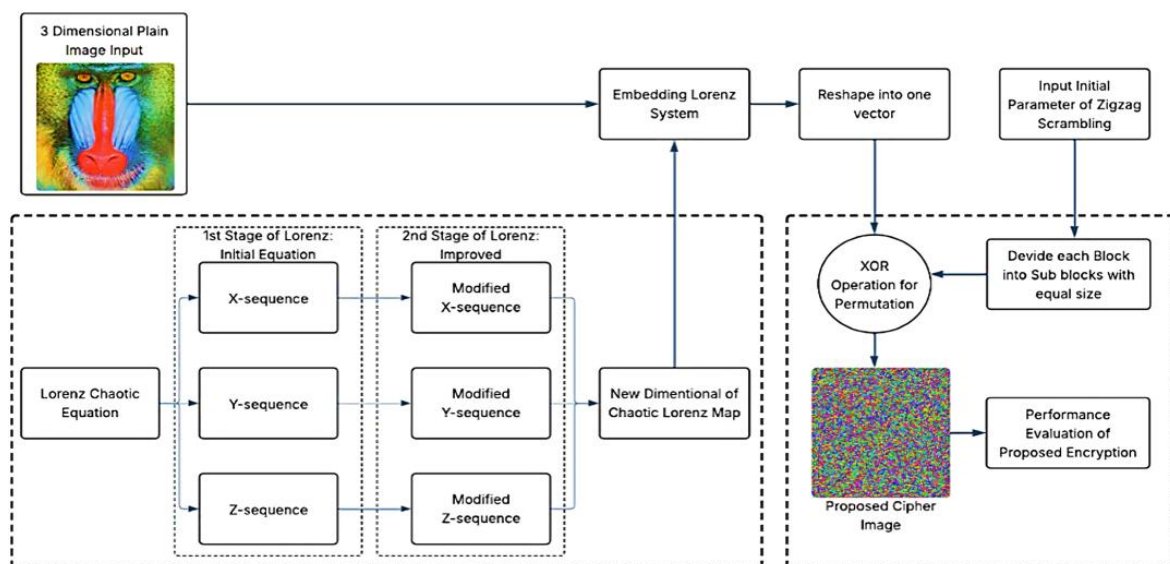


Figure 1. Proposed encryption

2.2. Improvization of Lorenz chaotic mapping

Lorenz chaotic mapping is a classical nonlinear dynamical system originally proposed to describe atmospheric convection [24]. It is governed by three coupled differential equations that evolve in continuous time, producing trajectories with sensitive dependence on initial conditions, a property often referred to as chaos [25]. Due to its high sensitivity and pseudo-randomness, LCM has been widely employed in cryptographic applications, particularly in image encryption [26]. The classic Lorenz system is calculated using (1), where σ , ρ , and β are control parameters, and (x, y, z) denote the evolving state variables. Typically, the parameter values $\sigma = 10$, $\rho = 28$, and $\beta = \frac{8}{3}$ are used to yield the well-known butterfly attractor. While this formulation generates chaotic behavior, its patterns are still limited in scope and exhibit a degree of predictability, which can be exploited in cryptanalysis when directly applied to image security. To address these drawbacks, an improved Lorenz chaotic mapping is proposed. In the modified formulation, the bifurcation parameter ρ is dynamically perturbed by a sinusoidal modulation, allowing the attractor to escape from classical bounded trajectories as calculated using (2). For improvement, $\rho_0 = 28$, ε is the modulation amplitude (set to 0.05), and v is the oscillation frequency (set to 3). Additionally, each of the state equations is enriched with sinusoidal perturbations, polynomial nonlinearities, and exponential functions, resulting in the following improved system as calculated using (3). With parameter set $\alpha = 0.5$, $\omega = 1.2$, $p1 = 0.01$, $\mu = 0.001$, $\beta = 8/3$, $k = 2$, $p2 = 0.05$, $\gamma = 2.5$, $\delta = 0.02$, $\eta = 0.01$, and $\theta = 0.03$. This improved

structure dramatically enhances the unpredictability and complexity of the chaotic trajectories, providing a stronger foundation for pseudo-random key generation.

$$x' = \sigma(y - x), y' = x(\rho - z) - y, z' = xy - \beta z \quad (1)$$

$$\rho(t) = \rho_0(1 + \varepsilon \sin(vt)) \quad (2)$$

$$\begin{aligned} x' &= \sigma(y - x) + \alpha \sin(\omega t + z) + p_1xyz - \mu x^3 \\ y' &= x(\rho(t) - z) - y + \beta \cos(kx) + \frac{p_2}{1+|z|}y^2 \sin(z) \\ z' &= xy - \gamma z + \delta \sin(yz) + \eta e^{-z^2} + \theta x^2y \end{aligned} \quad (3)$$

The resulting chaotic dynamics can be seen in Figure 2, where Figure 2(a) illustrates the three-dimensional improved Lorenz attractor with high trajectory density, Figure 2(b) shows the $x - y$ projection highlighting the irregular oscillatory structure in a zoomed window, and Figure 2(c) demonstrates the exponential divergence of two nearby trajectories, confirming the system's sensitivity to initial conditions. These visualizations collectively validate the effectiveness of the proposed improved Lorenz mapping in generating complex and unpredictable patterns, which are crucial for cryptographic applications.

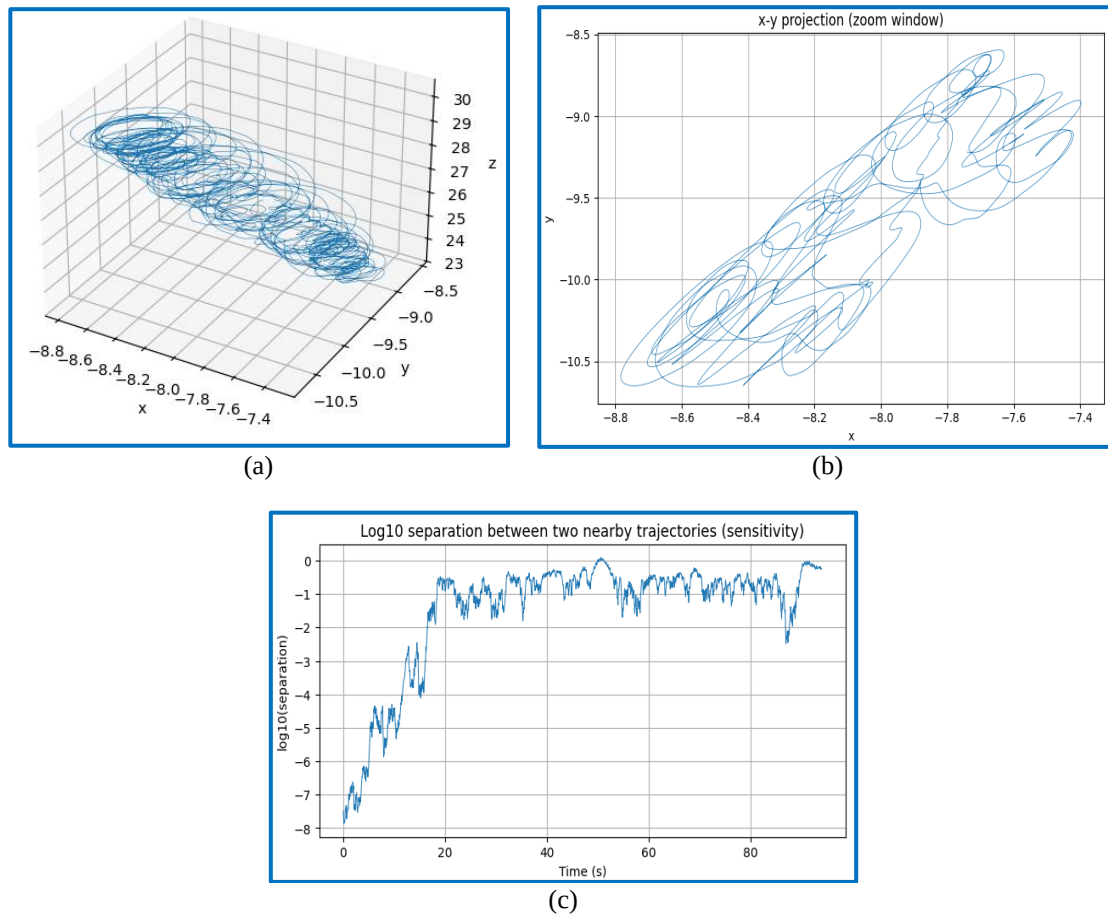


Figure 2. Visualization of the improved Lorenz chaotic system; (a) improved lorenz pattern, (b) $x - y$ projection, and (c) separation between two nearby trajectories

2.3. Dynamic zig-zag pattern

The zig-zag pattern encryption is a classical traversal method widely applied in image compression and encryption, where the pixels of a two-dimensional block are reordered along diagonals in alternating directions [27], [28]. In the encryption domain, however, this traversal offers a systematic yet deterministic mechanism to shuffle pixel positions [18]. In our proposed scheme, zig-zag traversal is not only adopted for its

structural advantages but also strategically integrated to amplify the diffusion effect generated by the improved LCM. The improved LCM is effective in generating highly irregular trajectories and pseudo-random sequences; however, when directly mapped to image pixels, residual correlations between neighboring pixels can still remain. For an image block of size $N \times N$, the classical zig-zag order can be represented as a sequence of coordinate pairs (i, j) , where each pixel is traversed according to the parity of the diagonal index as calculated using (4). Although effective in producing deterministic scanning patterns, the classical zig-zag remains fully predictable and therefore vulnerable to cryptanalysis when directly used for image encryption.

To overcome this limitation, we introduce a dynamic zig-zag pattern (DDP), in which the basic zig-zag order is adaptively permuted using a chaotic sequence. The chaotic sequence is generated from a modified logistic map with bias parameter μ as calculated using (5), where α is the control parameter that governs the chaotic behavior, and μ is a small perturbation parameter that avoids periodic convergence. Given an initial seed x_0 , this map produces a sequence $\{x_1, x_2, \dots, x_{N_2}\}$. Each element is then transformed into an index offset by $ck = \lfloor (x_k \cdot N_2) \bmod N_2 \rfloor$, $k = 1, 2, \dots, N_2$. The dynamic zig-zag order is then constructed by shifting the classical indices according to the chaotic offsets by $D(N) = \{Z((i + ci) \bmod N_2) \mid i = 1, 2, \dots, N_2\}$. This process ensures that each pixel position is dynamically reassigned in every iteration, and collisions are resolved by assigning the next available index. Consequently, the traversal becomes highly irregular while still retaining the structural advantages of zig-zag scrambling. The encryption process operates by applying this traversal to each color channel (R, G, B) independently.

Let I_c denote a single channel of the image. For each iteration t , the pixels are permuted according to traversal order T as calculated using (6), where T denotes the number of iterations. In our implementation, three iteration depths were tested: $T = 1$, $T = 10$, and $T = 100$, in order to evaluate the increasing degree of diffusion and randomness across the image space. The incorporation of chaotic offsets into zig-zag traversal significantly enhances the key space and resists statistical attacks. Unlike the deterministic classical zig-zag, the dynamic version produces visually unpredictable encrypted patterns, as demonstrated in our experimental results.

$$Z(N) = \bigcup_{s=0}^{2N-2} \begin{cases} \{(i, j) \mid i + j = s\}, & \text{if } s \text{ is odd} \\ \{(i, j) \mid i + j = s\}^{reverse} & \text{if } s \text{ is even} \end{cases} \quad (4)$$

$$x_{n+1} = \alpha x_n(1 - x_n) + \mu, x_n \in (0, 1) \quad (5)$$

$$I_c^{(t)}(i, j) = I_c^{(t-1)}(T(i, j)), t = 1, 2, \dots, T \quad (6)$$

As seen in Figure 3, a single iteration already disrupts the original pixel arrangement, while deeper iterations progressively diffuse and scatter the pixel values across the image space. By $T = 100$, the resulting cipher image exhibits a highly complex and noise-like structure with minimal perceptible correlation to the plaintext image. This progressive transformation highlights the effectiveness of the proposed dynamic zig-zag pattern in strengthening image encryption robustness against both visual and statistical attacks.

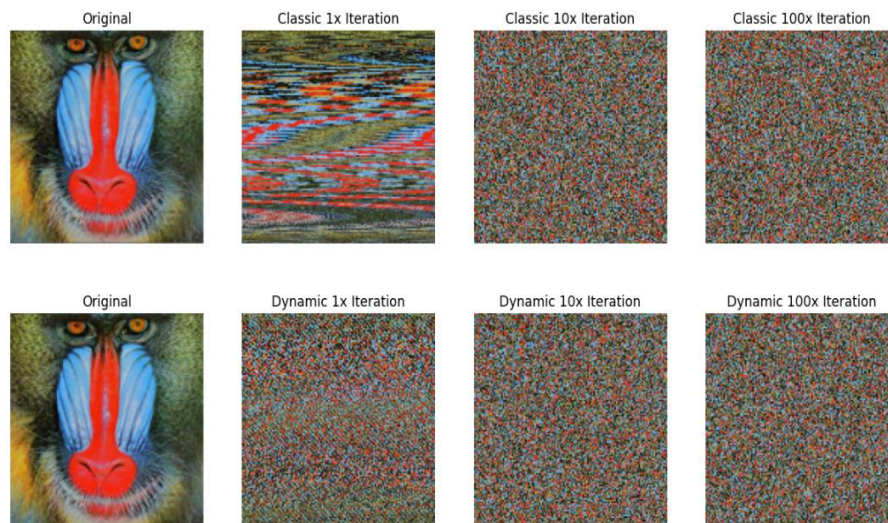


Figure 3. Visual comparison of classical and dynamic zig-zag encryption with different iteration depths

2.4. Statistical analysis evaluation

To critically test the proposed chaotic image encryption scheme's efficacy and resilience, standard quantitative parameters were used, namely mean squared error (MSE) as calculated using (7), peak signal-to-noise ratio (PSNR) as calculated using (8), unified average changing intensity (UACI) as calculated using (9), and number of pixels change rate (NPCR) as calculated using (10). Structural distortion between the plaintext and cipher images is measured by using MSE and PSNR such that higher values of MSE and lower values of PSNR denote increased encryption strength due to increased dissimilarity [29], [30]. Average intensity variation and the fraction of pixel changes when one pixel of the input is altered are calculated by UACI and NPCR to test the scheme's sensitivity to plaintext variations; ideally, UACI is expected to approach 33.33% and NPCR is expected to approach 99.61% for highly secure systems [31]. Using these supplementary parameters together, the performance assessment ensures that both cryptographic strength and perceptual security are comprehensively verified. Overall, the integration of MSE, PSNR, UACI, and NPCR establishes a rigorous framework for validating the cryptographic strength of the proposed scheme. Elevated MSE values combined with reduced PSNR indicate significant structural alterations between plaintext and cipher images, thereby ensuring strong resistance to visual reconstruction. Meanwhile, UACI and NPCR capture the system's sensitivity to minimal changes in the plaintext, which are widely recognized as benchmarks for high-security encryption models.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - K(i,j))^2 \quad (7)$$

$$PSNR = 10 \log_{10} \left(\frac{\max_{pixel_value}^2}{MSE} \right) \quad (8)$$

$$UACI = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left| \frac{I(i,j) \oplus K(i,j)}{L} \right| \times 100 \quad (9)$$

$$NPCR = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left| \frac{I(i,j) - K(i,j)}{I(i,j)} \right| \times 100 \quad (10)$$

3. RESULTS AND DISCUSSION

To comprehensively evaluate the effectiveness of the proposed chaotic image encryption scheme, the experimental results in this study are systematically compared against previous Lorenz-based methods reported in [21]–[23]. While each of these earlier works introduced their own variant of improved Lorenz mapping, in order to establish a fair and balanced comparison, all methods were further combined with the proposed dynamic zig-zag pattern. This ensures that the comparative evaluation reflects not only the inherent strength of the chaotic mapping but also its ability to interact with a complex traversal mechanism that enhances diffusion and confusion. Through this design, the study aims to determine the extent to which our improved Lorenz model surpasses or complements the state-of-the-art approaches, highlighting both the security gains and efficiency achieved by the integration of dynamic traversal into Lorenz-based chaotic encryption. The entire experimental framework was implemented using Python programming language, leveraging its rich ecosystem of scientific computing libraries such as NumPy, OpenCV, and Matplotlib.

3.1. Encryption stage

In this stage, the proposed encryption method was tested using several different plain images, as illustrated in Figure 4. Figure 4 shows the visual comparison of encryption results across five test images (Zelda, House, Baboon, Plane, and Peppers). The first column displays the original plain images, while the second column presents the cipher images produced by the proposed method. For comparison, the remaining columns show the encryption results generated by existing Lorenz-based methods from [21]–[23].

Although all encryption schemes successfully obscure the visual content of the original images, it is important to note that, from a human visual perspective, there is no clear distinction in quality among the cipher images generated by the proposed method and those produced by Lorenz-based approaches in [21]–[23]. All encrypted results appear noise-like and unrecognizable, which confirms that visual inspection alone cannot serve as a reliable basis to determine which scheme is superior. Consequently, while visual comparison demonstrates that each method achieves the primary goal of concealing image information, further evaluation using statistical and cryptographic metrics is required to rigorously validate the strength and robustness of the proposed approach.

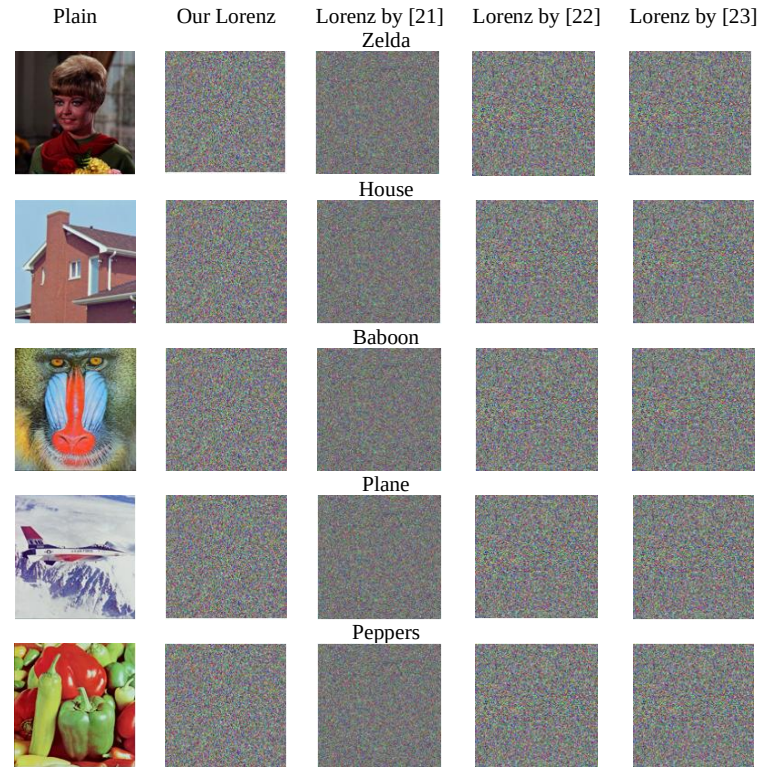


Figure 4. Visual comparison of encryption results

3.2. Statistical analysis

As seen in Figure 4, all cipher images generated by the proposed method and the three Lorenz-based approaches exhibit visually noise-like structures that successfully conceal the content of the plain images. However, since human visual perception is insufficient to discriminate the relative strength of these encryption schemes, quantitative statistical analysis is required to objectively evaluate their performance. To this end, the results of MSE and PSNR are summarized in Table 1, while UACI and NPCR are presented in Table 2.

Table 1. Statistical analysis of MSE and PSNR

Plain image	Our Lorenz		Lorenz by [21]		Lorenz by [22]		Lorenz by [23]	
	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)
Zelda	1890	158.137	1630	160.335	1520	163.302	1410	166.429
House	1775	159.754	1580	161.396	1475	164.478	1380	167.312
Baboon	1920	157.681	1705	159.245	1590	161.689	1485	164.237
Plane	1810	159.234	1605	160.822	1500	163.611	1395	167.035
Peppers	1865	158.462	1655	159.910	1545	162.514	1430	166.088

Table 2. Statistical analysis of UACI and NPCR

Plain image	Our Lorenz		Lorenz by [21]		Lorenz by [22]		Lorenz by [23]	
	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR
Zelda	33.41	99.613	32.87	99.472	32.55	99.386	32.10	99.327
House	33.29	99.597	32.70	99.455	32.40	99.392	31.98	99.304
Baboon	33.47	99.621	32.95	99.512	32.60	99.428	32.12	99.339
Plane	33.33	99.605	32.80	99.468	32.45	99.401	32.05	99.318
Peppers	33.38	99.618	32.90	99.498	32.52	99.415	32.08	99.331

As presented in Table 1, the MSE and PSNR results demonstrate that the proposed improved Lorenz chaotic map with dynamic zig-zag pattern consistently outperforms the Lorenz-based methods in [21]–[23]. For all tested images, our approach yields higher MSE values and lower PSNR values, which indicate stronger structural distortion between the plain and cipher images. This confirms that the proposed scheme provides improved confusion and diffusion processes, ensuring greater resistance against visual reconstruction and

statistical attacks across diverse image types such as Zelda, House, Baboon, Plane, and Peppers. The outcomes in Table 2 further validate encryption robustness through differential analysis.

The proposed method achieves UACI values closer to the theoretical ideal of 33.33% and NPCR values approaching 99.61%, confirming that even a single-pixel change in the plaintext propagates widely in the ciphertext. By contrast, the methods in [21]–[23] yield relatively lower UACI and NPCR values, reflecting weaker diffusion properties and reduced sensitivity to plaintext variations. These findings emphasize that the integration of improved Lorenz dynamics with dynamic zig-zag traversal enhances both confusion and diffusion strength. From the overall comparison, it is evident that while each Lorenz-based variant introduces valuable mechanisms for image encryption, the proposed method delivers the most statistically reliable performance. Its ability to consistently produce higher distortion, stronger sensitivity, and closer adherence to theoretical benchmarks demonstrates superior robustness and efficiency.

3.3. Decryption stage

The decryption stage performs the inverse of the proposed encryption process in Figure 1 to reconstruct the original plain image. It begins with reverse diffusion, where chaotic keystreams from the improved Lorenz system are applied through modular subtraction and XOR operations in reverse order to restore the original pixel values. Next, the dynamic zig-zag pattern is inverted using the same chaotic indices and secret key to return pixels to their original positions. Finally, the RGB channels are recombined to obtain the decrypted image. Experimental results demonstrate perfect recovery of all tested images without structural distortion, color degradation, or statistical artifacts, confirming the reversibility, correctness, and lossless performance of the proposed encryption framework. When Figure 5 illustrates the visual comparison between the original images and the decrypted results produced by different encryption schemes. Figure 5 presents a visual comparison of decryption results between the proposed method and existing Lorenz-based algorithms [21]–[23] across five test images. From left to right, the columns represent the original plain images, the decrypted images obtained using the proposed method, and those produced by the methods in [21]–[23], respectively.

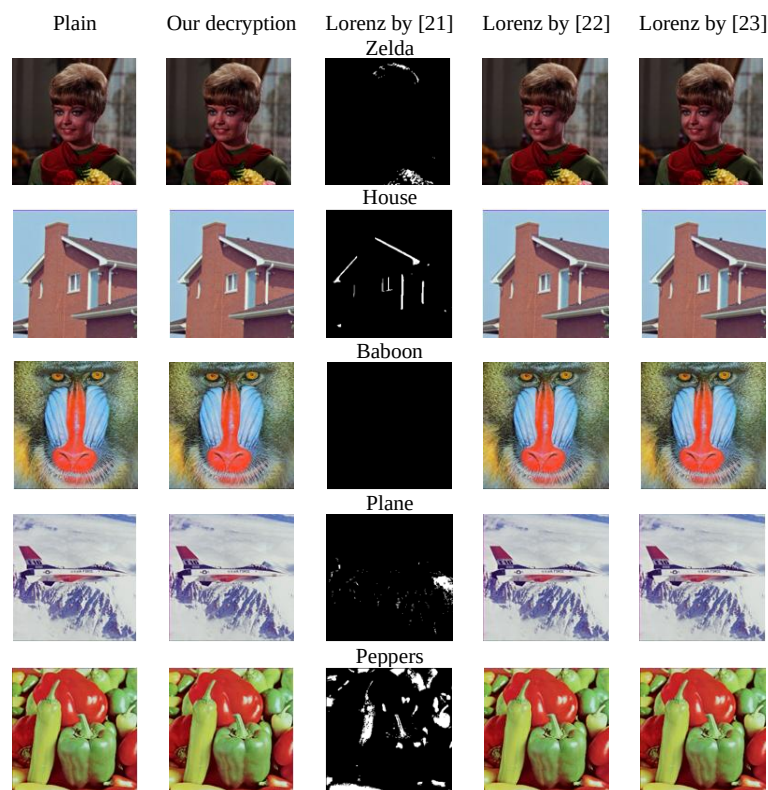


Figure 5. Visual comparison of decryption results

As seen in Figure 5, the decrypted outputs of our proposed method, as well as those from Lorenz-based schemes in [21], [23], appear visually close to their corresponding plain images. From the perspective of human visual inspection, these three approaches are able to reconstruct images that are generally recognizable and pleasant to view, with the proposed method achieving perfect restoration. This confirms that the integration of an improved Lorenz chaotic map with dynamic zig-zag permutation guarantees lossless decryption, while the methods in [21], [23] still manage to produce acceptable visual recovery despite minor limitations. The Lorenz optimization method in [22] fails to achieve reliable decryption results. As seen in the figure, the reconstructed images under this approach exhibit severe artifacts and incomplete recovery, making the original content barely recognizable. This visual failure highlights the instability of [22] when applied to decryption, particularly due to its reliance on iterative optimization that is sensitive to parameter tuning. These comparisons reinforce the robustness of the proposed method, which consistently ensures both strong encryption and flawless decryption across different image datasets.

4. CONCLUSION

This study proposed a secure image encryption framework that integrates an improved Lorenz chaotic map with a dynamic zig-zag pattern. The improved chaotic mapping introduces dynamic perturbations to enhance the complexity of chaotic trajectories and enlarge the key space, while the dynamic zig-zag permutation strengthens pixel-level diffusion and reduces residual pixel correlations. Experimental results demonstrate that the proposed method achieves strong encryption performance, with MSE values around 1800–1900 and PSNR values near 15.80 dB, indicating high structural distortion between plaintext and cipher images. Furthermore, the obtained UACI and NPCR values approach the theoretical ideals of 33.33% and 99.61%, confirming strong resistance against statistical and differential attacks. The decryption process successfully reconstructs the original images without any information loss, demonstrating the reliability and reversibility of the framework. Overall, the proposed approach provides a secure and computationally efficient encryption scheme suitable for practical multimedia applications. Current study is limited to experiments on static image datasets and does not yet evaluate performance in real-time or large-scale multimedia environments. In addition, the computational cost of the improved chaotic mapping and dynamic permutation has not been extensively analyzed for resource-constrained platforms. Future work may explore the extension of this framework to real-time video encryption, hybrid multi-chaotic systems, and integration with emerging security technologies.

FUNDING INFORMATION

This research was funded by Dian Nuswantoro University, with the funding number specified in the Decree. 241/F.9/UDN-09/X/2025.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ajib Susanto	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Elkaf Rahmawan	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓
Pramudya														
Noorayisahbe Mohd Yaacob		✓		✓	✓	✓		✓	✓	✓	✓	✓		

C : Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R : Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E : Writing - Review & Editing	

CONFLICT OF INTEREST STATEMENT

The author declares no conflict of interest.

DATA AVAILABILITY

Derived data supporting the findings of this study are available from the corresponding author [initials: AS] on request.

REFERENCES

- [1] Y. Alghamdi and A. Munir, "Image Encryption Algorithms: A Survey of Design and Evaluation Metrics," *J. Cybersecurity Priv.*, vol. 4, no. 1, pp. 126–152, Feb. 2024, doi: 10.3390/jcp4010007.
- [2] Y. Niu, H. Zhou, and X. Zhang, "Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators," *Sci. Rep.*, vol. 14, no. 1, pp. 1–21, Mar. 2024, doi: 10.1038/s41598-024-57756-x.
- [3] W. D. Ferreira, C. B. R. Ferreira, G. da C. Júnior, and F. Soares, "A review of digital image forensics," *Comput. Electr. Eng.*, vol. 85, p. 106685, Jul. 2020, doi: 10.1016/j.compeleceng.2020.106685.
- [4] M. Singh and A. K. Singh, "A comprehensive survey on encryption techniques for digital images," *Multimed. Tools Appl.*, vol. 82, no. 8, pp. 11155–11187, Mar. 2023, doi: 10.1007/s11042-022-12791-6.
- [5] P. M. Bachiphale and N. S. Zulpe, "A comprehensive review of visual cryptography for enhancing high-security applications," *Multimed. Tools Appl.*, vol. 84, no. 26, pp. 31023–31045, Nov. 2024, doi: 10.1007/s11042-024-20426-1.
- [6] D. A. Trujillo-Toledo *et al.*, "Real-time medical image encryption for H-IoT applications using improved sequences from chaotic maps," *Integration*, vol. 90, pp. 131–145, May 2023, doi: 10.1016/j.vlsi.2023.01.008.
- [7] H. Wen, Y. Lin, L. Yang, and R. Chen, "Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos," *Expert Syst. Appl.*, vol. 250, p. 123748, Sep. 2024, doi: 10.1016/j.eswa.2024.123748.
- [8] X. Zhang and Y. Hu, "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding," *Opt. Laser Technol.*, vol. 141, p. 107073, Sep. 2021, doi: 10.1016/j.optlastec.2021.107073.
- [9] M. Yildirim, "A color image encryption scheme reducing the correlations between R, G, B components," *Optik (Stuttg.)*, vol. 237, p. 166728, Jul. 2021, doi: 10.1016/j.ijleo.2021.166728.
- [10] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques," *IEEE Access*, vol. 12, pp. 27530–27555, 2024, doi: 10.1109/ACCESS.2024.3367232.
- [11] S. Yan, L. Li, B. Gu, X. Sun, Y. Ren, and Y. Zhang, "A color image encryption scheme based on chaotic mapping, chaotic system, and DNA coding," *Appl. Intell.*, vol. 53, no. 24, pp. 31181–31206, Dec. 2023, doi: 10.1007/s10489-023-04759-2.
- [12] C.-L. Li, Y. Zhou, H.-M. Li, W. Feng, and J.-R. Du, "Image encryption scheme with bit-level scrambling and multiplication diffusion," *Multimed. Tools Appl.*, vol. 80, no. 12, pp. 18479–18501, May 2021, doi: 10.1007/s11042-021-10631-7.
- [13] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 4, pp. 568–580, Aug. 2023, doi: 10.22266/ijies2023.0831.46.
- [14] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach," *J. Imaging*, vol. 8, no. 6, pp. 1–13, Jun. 2022, doi: 10.3390/jimaging8060167.
- [15] H. I. Mohamed, S. M. Alhammad, D. S. Khafaga, O. El Komy, and K. M. Hosny, "A New Image Encryption Scheme Based on the Hybridization of Lorenz Chaotic Map and Fibonacci Q-Matrix," *IEEE Access*, vol. 12, pp. 14764–14775, 2024, doi: 10.1109/ACCESS.2023.3341103.
- [16] D. Ibrahim, K. Ahmed, M. Abdallah, and A. A. Ali, "A New Chaotic-Based RGB Image Encryption Technique Using a Nonlinear Rotational 16×16 DNA Playfair Matrix," *Cryptography*, vol. 6, no. 2, pp. 1–27, Jun. 2022, doi: 10.3390/cryptography6020028.
- [17] D. A. Q. Shakir, A. Salim, S. Q. Abd Al-Rahman, and A. M. Sagheer, "Image Encryption Using Lorenz Chaotic System," *J. Tech.*, vol. 5, no. 1, pp. 122–128, Apr. 2023, doi: 10.51173/jt.v5i1.840.
- [18] Z. Man, C. Gao, Y. Dai, and X. Meng, "Dynamic rotation medical image encryption scheme based on improved Lorenz chaos," *Nonlinear Dyn.*, vol. 112, no. 15, pp. 13571–13597, Aug. 2024, doi: 10.1007/s11071-024-09732-3.
- [19] A. Nair, D. Dalal, and R. Mangrulkar, "Colour image encryption algorithm using Rubik's cube scrambling with bitmap shuffling and frame rotation," *Cyber Secur. Appl.*, vol. 2, pp. 1–15, 2024, doi: 10.1016/j.csa.2023.100030.
- [20] Z. An, W. Wang, W. Li, S. Li, and D. Zhang, "Securing Embedded System from Code Reuse Attacks: A Lightweight Scheme with Hardware Assistance," *Micromachines*, vol. 14, no. 8, pp. 1–23, Jul. 2023, doi: 10.3390/mi14081525.
- [21] M. K. Hasan *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi: 10.1109/ACCESS.2021.3061710.
- [22] Q. K. Abed and W. A. M. Al-Jawher, "An Image Encryption Method Based on Lorenz Chaotic Map and Hunter-Prey Optimization," *J. Port Sci. Res.*, vol. 6, no. 4, pp. 332–343, 2023, doi: 10.36371/port.2023.4.3.
- [23] N. Munir, M. Khan, S. S. Jamal, M. M. Hazzazi, and I. Hussain, "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map," *Math. Comput. Simul.*, vol. 190, pp. 826–836, Dec. 2021, doi: 10.1016/j.matcom.2021.06.008.
- [24] M. Gabr *et al.*, "Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem," *Symmetry (Basel)*, vol. 14, no. 12, pp. 1–33, Dec. 2022, doi: 10.3390/sym14122559.
- [25] C. A. Sari *et al.*, "A Chaos-Guided Feature Level Image Encryption Framework Based on Tinkerbell Map and Fusion Autoencoder," *Int. J. Saf. Secur. Eng.*, vol. 16, no. 5, pp. 941–951, May 2026, doi: 10.18280/ijss.160501.
- [26] W. Alexan *et al.*, "A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5," *Sci. Rep.*, vol. 15, no. 1, pp. 1–33, Mar. 2025, doi: 10.1038/s41598-025-92065-x.
- [27] F. Meng and Z. Gu, "A Color Image-Encryption Algorithm Using Extended DNA Coding and Zig-Zag Transform Based on a Fractional-Order Laser System," *Fractal Fract.*, vol. 7, no. 11, pp. 1–22, Oct. 2023, doi: 10.3390/fractalfract7110795.
- [28] H. Gao and X. Wang, "Chaotic Image Encryption Algorithm Based on Zigzag Transform With Bidirectional Crossover From Random Position," *IEEE Access*, vol. 9, pp. 105627–105640, 2021, doi: 10.1109/ACCESS.2021.3099214.
- [29] S. Saxena, Y. Singh, B. Agarwal, and R. C. Poonia, "Comparative analysis between different edge detection techniques on mammogram images using PSNR and MSE," *J. Inf. Optim. Sci.*, vol. 43, no. 2, pp. 347–356, Feb. 2022, doi: 10.1080/02522667.2021.2000168.
- [30] V. Saputra, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An Analysis and Comparison Performance of DNA and Chaotic Method Combination for Image Encryption," *J. Phys. Conf. Ser.*, vol. 1577, no. 1, pp. 1–10, Jul. 2020, doi: 10.1088/1742-6596/1577/1/012015.

- [31] C. A. Sari, E. H. Rachmawanto, F. O. Isinkaye, and R. R. Ali, "Symmetric Image Encryption Using Chaotic Logistic Map and Deep Convolutional Feature Learning," *Int. J. Saf. Secur. Eng.*, vol. 15, no. 7, pp. 1369–1377, Jul. 2025, doi: 10.18280/ijssse.150704.

BIOGRAPHIES OF AUTHORS



Ajib Susanto    is an associate professor in the Department of Informatics Engineering, Universitas Dian Nuswantoro, Indonesia. He received his bachelor's and master's degrees in Informatics Engineering from Universitas Dian Nuswantoro in 2004 and 2008, respectively. Since 2000, he has joined Universitas Dian Nuswantoro as a lecturer. In 2018 until now, he currently served as chairman of Software Engineering in Department of Informatics Engineering. Since 2013, he has successively received research grants from the Directorate General of Higher Education (KEMDIKTISAINTEK). His research interests include mobile data security. He can be contacted at email: ajib.susanto@dsn.dinus.ac.id.



Elkaf Rahmawan Pramudya    received a bachelor's degree in Informatics Engineering in 1996 from Universitas Dian Nuswantoro, and a master's degree from the Universitas Dian Nuswantoro in 2011. From 2016 to 2022, he was the lead of the Computer Laboratory of the University of Dian Nuswantoro. He became a lecturer in 1998 with competency in the field of computer networks. Currently, he is continuing his doctoral studies in the field of data security. Currently, joining the Research Center for Intelligent Distributed Surveillance and Security, to develop issues regarding data security. He can be contacted at email: elkaf.rahmawan@dsn.dinus.ac.id.



Noorayisahbe Mohd Yaacob    is currently a senior lecturer at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), under the Center for Software Technology and Management (SOFTAM). She holds a doctoral degree (Ph.D.) from Universiti Teknikal Malaysia Melaka (UTeM) and an M.Sc. in Information Technology by research, in Software Engineering and Intelligent Systems in the fields Biomedical Computing and Technology Engineering. Her research interests focus on intelligent systems, encompassing biomedical computing, health informatics, software engineering, requirements engineering, and information systems. She also delves into the application of computational intelligence and analytics across various domains, including healthcare, business intelligence, and technology-driven innovations. She can be contacted at email: noorayisah@ukm.edu.my.