Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 3, August, Pp. 367-376

Improved chaotic image encryption in grayscale color space using elliptic curves and the 3d Lorenz system

Daurat Sinaga*[1,2], Cahaya Jatmoko[1,2], Erna Zuni Astuti[1,2], Eko Hari Rachmawanto[1,2], Abdussalam[1,2], Elkaf Rahmawan Pramudya[1,2], Guruh Fajar Shidik[1,2], Pulung Nurtantio Andono[1,2], Mohamed Doheir[2]
Universitas Dian Nuswantoro, Indonesia[1]
Universiti Teknikal Malaysia Melaka, Malaysia[2]

Article Info

Keywords:
3D Lorenz System, Chaotic Image Encryption, Cryptography, Elliptic Curve, Quality Measurement

Article history:
Received: February 10, 2025
Accepted: June 02, 2025
Published: August 31, 2025

Cite:
D. Sinaga, "Improved Chaotic Image Encryption on Grayscale Colorspace Using Elliptic Curves and 3D Lorenz System", *KINETIK*, vol. 10, no. 3, Aug. 2025. https://doi.org/10.22219/kinetik.v10i3.2251

*Corresponding author.
Daurat Sinaga
E-mail address:
dauratsinaga@dsn.dinus.ac.id

Abstract

Digital data, especially visual content, faces significant security challenges due to its susceptibility to eavesdropping, manipulation, and theft in the modern digital landscape. One effective solution to address these issues is the use of encryption techniques, such as image encryption algorithms, that ensure the confidentiality, integrity, and authenticity of digital visual content. This study addresses these concerns by introducing an advanced image encryption method that combines Elliptic Curve Cryptography (ECC) with the 3D Lorenz chaotic system to enhance both security and efficiency. The method employs pixel permutation, ECC-based encryption, and diffusion using pseudo-random numbers generated by the Lorenz 3D system. The results show superior performance, with an MSE of 3032 and a PSNR of 8.87 dB, as well as UACI and NPCR values of 33.34% and 99.64%, respectively, indicating strong resilience to pixel intensity changes. During testing, the approach demonstrated robustness, allowing only the correct key to decrypt images accurately, while incorrect or modified keys led to distorted outputs, ensuring encryption reliability. Future work could explore extending the method to color images, optimizing processing for larger datasets, and incorporating additional chaotic systems to further fortify encryption strength.

1. Introduction

Digital security has become one of the main concerns in the modern context [1], [2], [3]. The reason is that in applications related to healthcare, surveillance, banking, and social networking, human dependence on visual data in digital format is increasing [4], [5], [6]. Thus, a major area of concern involves the vulnerability of the digital images during transmission and storage to eavesdropping, manipulation, and theft of data [7], [8]. Compared to textual or numerical data, digital images have larger file sizes and require appropriate encryption methods that are not only secure but also efficient in managing high-dimensional data [9], [10]. Additionally, due to the redundancy in image data, some patterns can easily be predicted by an attacker, which may further present possibilities for several attacks, especially when using encryption techniques of low complexity [11]. Another challenge is the need to balance security with quality, whereby overly intricate algorithms can quickly prove counterproductive, leading to either lower quality in images or slowing down the processing.

Cryptography, in particular, has been proposed as a solid way to address these concerns, particularly through image encryption, to protect under confidentiality and integrity with respect to digital images [12], [13]. Under encryption, the process that starts with an image makes it appear illegible, aided by special algorithms that create randomness, making it a very difficult task to decrypt it without proper authority. Logically speaking, encryption involves changing the spatial representation of an image, normally in the form of pixel matrices, into a scrambled representation using known methods such as Elliptic Curve Cryptography (ECC) or chaotic systems, dictated by a particular encryption key [12], [14], [15]. Reverse decryption uses the same key to undo encryption operations and restore the image back to its original recognizable state without any critical detail being lost [16]. The decrypted image will be evaluated based on its restoration quality by measurements such as Peak Signal-to-Noise Ratio (PSNR) or Structural Similarity Index Measures (SSIM), thereby determining the recovery capacity of the original structure and details of the image after undergoing such encryption and decryption processes [17]. This approach offers the advantage of securing the image data while ensuring the recoverability of the information as accurately and reliably as intended, thereby finding a critical balance between the protection of the data and its usability.

Elliptic Curve image encryption is a cryptographic approach that uses the mathematical properties of elliptic curves to secure image data [18]. It combines the strength of public-key cryptography with efficient computational methods, making it particularly suitable for resource-constrained environments like image encryption [19]. Banik et al. (2022) [15] highlighted the increasing need for securing digital images due to their growing prevalence in communication and data transmission. Recognizing the challenges in Abdelfatah’s block-based image encryption scheme, which combines chaotic systems and elliptic curve cryptography, the authors identified key issues that compromise its effectiveness. These issues include the grouping of multiple pixels into large integers exceeding the elliptic curve’s modulo prime, resulting in decryption errors, and the additional overhead of transferring information about the pixel grouping. To address these limitations, the authors proposed an improved algorithm that leverages the largest 512-bit elliptic curve prime modulo, alongside advanced confusion and diffusion operations derived from a chaotic system. Through security and statistical analyses, their method demonstrated enhanced robustness against cryptographic attacks, highlighting its potential to address vulnerabilities in existing encryption techniques while maintaining the integrity and confidentiality of digital image data.

Ye et al. (2022) [20] introduced a novel three-dimensional continuous chaotic system, termed ImproBsys, which transitions from ordinary chaos to hyperchaos, exhibiting more complex and unpredictable behavior with two positive Lyapunov exponents. Based on this advanced system, they have proposed an integrated double-image encryption algorithm that links compressive sensing with elliptic curve cryptography. First, they performed DWT on two equal-sized plain images and thresholded their coefficients to increase sparsity. Furthermore, they compressed the quantized matrix to reduce its data dimensions by half and then concatenated the compressed matrix to form a single new matrix. Elliptic curve cryptography is then performed on the resultant matrix for secure transmission. The researchers’ work maintains essential contributions, including the development of improved chaotic properties in the ImproBsys system, the use of compressive sensing to reduce data for transmission while integrating the chaos system to control the measurement matrix, and the presentation of a novel mathematical model that maps the initial conditions of the ImproBsys with the entropy of the plain image.

Parida et al. (2021) [19] integrated ECDH key exchange for establishing a shared session key using a variant of the ElGamal encoding scheme for encryption. Moreover, three-dimensional and four-dimensional ACM maps were employed to scramble and transform pixel values efficiently, ensuring high confusion and diffusion. Furthermore, a digital signature in a structured format is included to enable authentication of the encrypted image prior to its decryption for legitimacy. The results demonstrated the efficiency of the proposed model, where the average entropy for grayscale images was found to be 7.9993 and for the color image components was 7.99925, with an average NPCR of 99.6%, an average UACI of 33.3%, and low pixel correlation. By minimizing computational overhead through optimized point multiplication operations, the model demonstrated resilience against various types of attacks, including statistical, differential, chosen-plaintext, known-plaintext, and occlusion attacks. This proves its efficacy and robustness as a comprehensive encryption framework.

The above three works involved ECC for image encryption and thus share a common framework but differ in the specific techniques used to enhance encryption strength and diffusion. Researcher [15] focused on the limitations in Abdelfatah's block-based encryption and used a 512-bit ECC prime modulo along with advanced confusion and diffusion derived from chaotic systems. Researcher [20] proposed an innovative method that incorporates compressive sensing and error correction codes into a new three-dimensional continuous chaotic system known as ImproBsys. This method aims to reduce data size and improve data transmission efficiency while embedding more chaos to achieve higher security. On the other hand, Researcher [19] proposed a robust encryption model based on ECC that combined ECDH key exchange with improved ElGamal encoding, incorporating Arnold Cat maps for efficient pixel scrambling. In this regard, the given paper presents a fresh perspective that combines Elliptic Curve Cryptography with the three-dimensional Lorenz system to increase the complexity of the diffusion and, subsequently, the entire encryption process. In this context, the Lorenz chaotic system was integrated to enhance the unpredictability of the scheme through better distribution of the pixel value changes across the entire image. The new implementation of ECC with the Lorenz system uniquely contributes to adding more complexity to the diffusion process, further enhancing its resilience against various cryptographic attacks.

2. Research Method

In the encryption phase (red flow), the process begins by combining the secret key with the hash value of the original image, generated using the Hashing-512 algorithm. This combination is used to perform pixel permutation, scrambling the arrangement of the image's pixels to enhance data complexity and resistance to attacks. After the permutation, the data undergoes further processing using elliptic curve encryption, utilizing pseudo-random numbers generated by a 3D Lorenz system as the key. The result is then refined through an EC Diffusion algorithm, followed by additional PRNG-based diffusion, ultimately producing the encrypted or cipher image.

The decryption process (green flow) reverses the encryption steps, starting from the cipher image. First, the PRNG-based diffusion and EC Diffusion are undone to restore the pre-diffusion state. The encrypted data is then decrypted using the appropriate private key to reverse the elliptic curve encryption. Next, the pixel arrangement is restored using the "reverse pixel permutation" algorithm, returning the scrambled pixels to their original order. Finally, the initial diffusion algorithm is reversed using data derived from the private key, reconstructing the original image. This method ensures that only authorized users with the correct private key can decrypt the cipher image back into its original form.

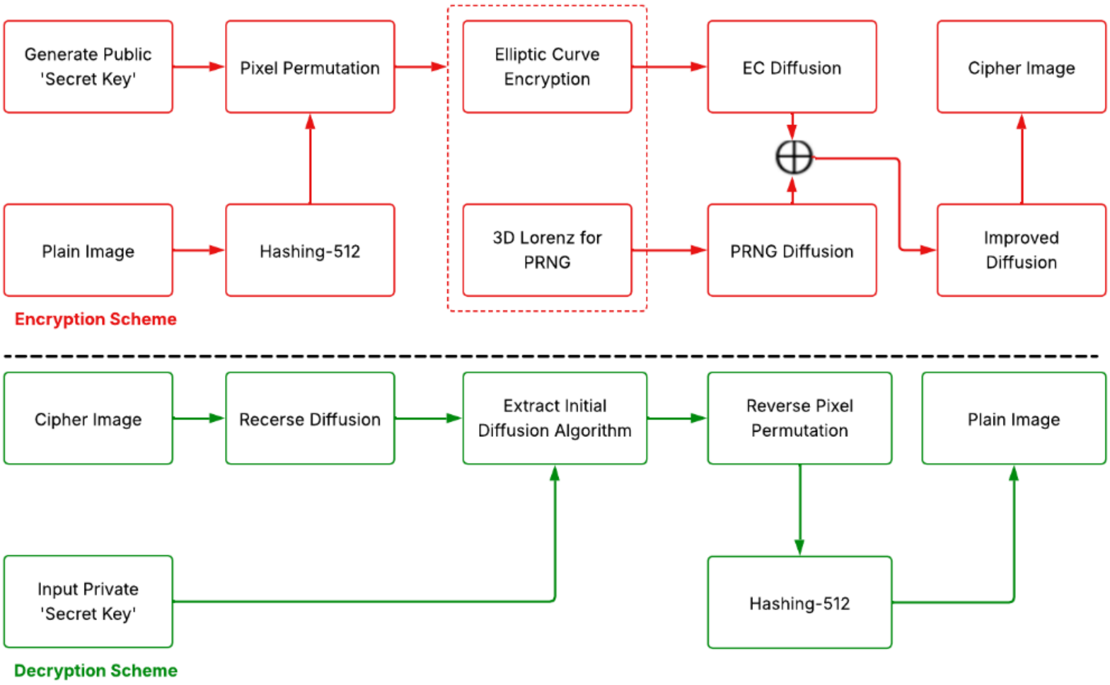


Figure 1. Procedure of Proposed Scheme

2.1 Preliminaries

In this research, the SHA-512 hashing algorithm is utilized to generate the initial values for the chaotic system [21]. This step is essential to ensure that even when two images differ by only a single pixel, the resulting chaotic parameters are significantly different, thereby enhancing the security and unpredictability of the encryption process [22]. By leveraging the cryptographic strength of SHA-512, the hash output serves as a robust and sensitive foundation for initializing chaos.

The SHA-512 hash function generates a 512-bit fixed-length output from the input data. In this research, the resulting $512 - bit$ secret key, H, is partitioned into 128 blocks, each consisting of 4 bits. These blocks are subsequently employed to initialize the chaotic system with high sensitivity to small variations in the input. The hashing process is represented mathematically in Equation 1.

$$Hashing\ (H) = h_1, h_2, h_3, \dots, h_{128} \tag{1}$$

After that, the hash result (H) is combined with the public secret key (K) to create a new set of parameters P, where the formula (K) for the public secret key in question can be seen in Equation 2. This equation defines the public secret key, which functions to randomize all the pixels in the plain image used as the secret key, with $\sigma, \rho,$ and β as predefined constants.

$$K = \begin{cases} x_{n+1} = \sigma(y_n - x_n) \\ y_{n+1} = x_n(\rho - z_n) - y_n \\ z_{n+1} = x_n y_{n-\beta z_n} \end{cases} \tag{2}$$

After generating based on Equation 2, the XOR process is carried out on the generated public key with the hashing-512 result, thus forming a pixel permutation as seen in Equation 3. This process ensures that the encryption result is more complex and difficult to predict, increasing the security of the altered image.

$$Permutedpixel\ (i,j) = K(i,j) \oplus H(i,j) \tag{3}$$

Here, $K(i,j)$ is the value generated by the public secret key, and $H(i,j)$ is the result of hashing-512. The XOR process combines the two to form scrambled pixels, enhancing the confidentiality of the resulting image. In this context, XOR does not directly permute pixel positions in a spatial sense but modifies the pixel intensity values at specific coordinates. By applying XOR between $K(i,j)$ and $H(i,j)$, the original pixel values are transformed into new, non-intuitive values based on both the cryptographic key and hash function. Since both K and H depend on secret parameters and cryptographic operations, the resulting scrambled pixels appear statistically random and uncorrelated to the original image. This transformation ensures that even small changes in the input or key produce significantly different outputs, thereby enhancing diffusion and resisting statistical or differential attacks.

2.2 Elliptic Curve Encryption

Elliptic Curve Cryptography (ECC) is a form of public-key cryptography based on the mathematical properties of elliptic curves defined over finite fields to secure data [23]. This technique provides the same level of security as traditional cryptographic methods with much smaller key sizes, resulting in faster computations and reduced memory requirements [24]. ECC relies on public-key cryptography in which a public key is used for encryption and a private key is used for decryption, allowing for secure data transmission between two parties without the need to agree on any secret keys beforehand [25]. An elliptic curve over a finite field $F_q$is defined, as can be seen in Equation 4.

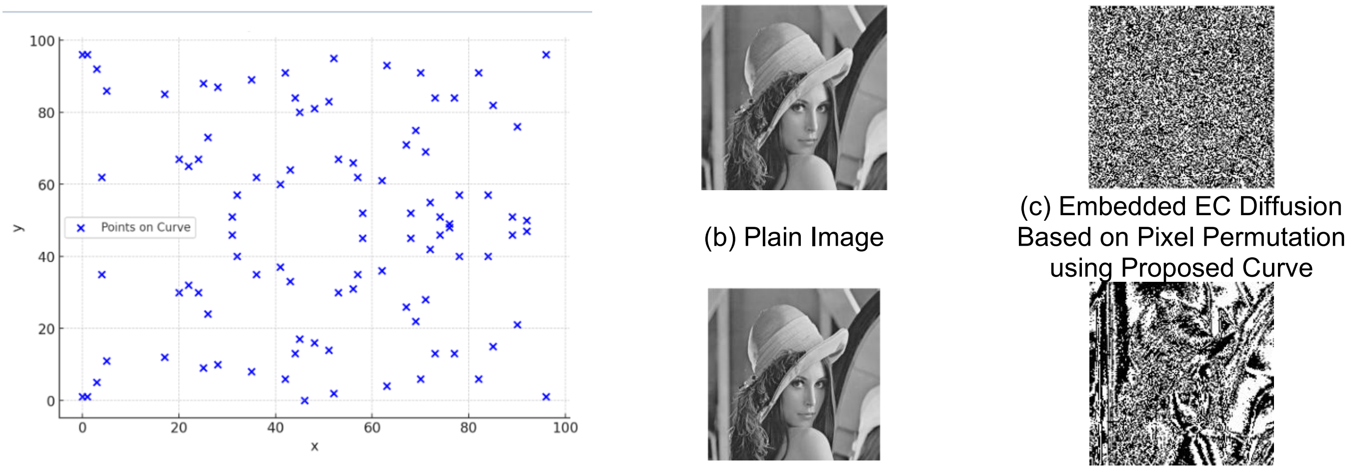
$$\sum_{a,b}^{F_q} = (\infty) \cup \{(x,y): x,y \in F_q \cdot F_q: y^2 = x^3 + ax + b \; mod \; q\} \tag{4}$$

The elliptic curve over a finite field F_q is defined as the set of points $\{\infty\} \cup \{(x,y)\}$, including the point at infinity (∞) and all $(x,y) \in F_q \cdot F_q$ that satisfy the equation $y^2 = x^3 + ax + b \; mod \; q$, where a and b are constants. For the curve to be valid and non-singular, the discriminant $4a^3 + 27b^2 \; mod \; q$ must not be zero. The point at infinity serves as the identity element for the elliptic curve group under addition. Following Equation 4, the sum of two distinct points $K_1 = (x_1, y_1)$ and $L_1 = (x_2, y_2)$ on an elliptic curve over a finite field, where $K_1 \neq L_1$, is calculated using the following steps: compute the slope λ in Equation 5 and compute the resulting point $R = K_1 + L_1 = (x_3, y_3)$ in Equation 6.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \; mod \; q \tag{5}$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \; mod \; q \\ y_3 = \lambda(x_1 - x_3) - y_1 \; mod \; q \end{cases} \tag{6}$$

If the points K_1 and L_1 are inverses of each other $(x_1 = x_2 \; and \; y_1 = -y_2)$, their sum results in the point at infinity (∞), which serves as the identity element on the elliptic curve.



(b) Plain Image

(c) Embedded EC Diffusion Based on Pixel Permutation using Proposed Curve

(a) Proposed Curve

(d) Decrypted Image Using Proposed Curve

(e) Slightly Modified Curve

Figure 2. Elliptic Curve Processing

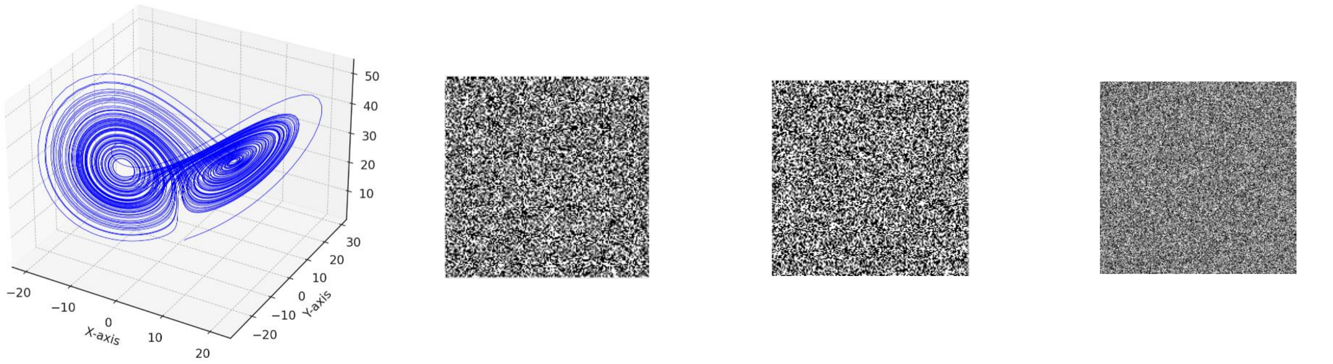
Based on Figure 2, the proposed elliptic curve in (a) generates a set of coordinate points that serve as the basis for public key generation in the encryption process. These points are derived from valid solutions to the elliptic curve equation over a finite field, as described in Equation 4. The plain image shown in (b) undergoes a diffusion process where pixel values are scrambled using the coordinates derived from the curve, as illustrated in (c). This operation ensures that the output image has a randomized appearance, making it resistant to visual interpretation and statistical analysis. When the correct curve and key parameters are applied, the original image can be successfully recovered, as shown in (d). However, in (e), a slight modification to the curve parameters leads to significant distortion in the decrypted image, indicating a high sensitivity of the encryption system to parameter accuracy.

2.3 3D Lorenz PRNG

This method utilizes the dynamics of the Lorenz system, a well-known chaotic system, to generate sequences of pseudo-random numbers with high unpredictability [26]. The Lorenz system is described by three coupled, nonlinear differential equations characterized by parameters σ, ρ, and β, which control the behavior of the chaotic attractor [27], [28]. The PRNG equation can be seen in Equation 7.

$$\frac{dx}{dt} = \sigma\,(y - x), \qquad \frac{dy}{dt} = x\,(\rho - z) - y, \qquad \frac{dz}{dt} = xy - \beta z \tag{7}$$

In this context, initial conditions $x0$, $y0$, and $z0$ are set as seeds, and the system evolves over discrete time steps using numerical integration methods, such as the Runge-Kutta method. The outputs $x(t), y(t)$, and $z(t)$ are used to derive random-like sequences, which are then scaled or transformed to meet specific application requirements. The results of proposed encryption using Elliptic Curve and 3D Lorenz can be seen in Figure 3. The system operates with predefined parameters $\sigma = 10, \rho = 28, and\ \beta = 8/3$, which are standard values commonly used to exhibit chaotic behavior. These parameters influence the Lorenz attractor's dynamics, ensuring the generation of pseudo-random sequences with high entropy. The parameter σ governs the rate of change in the x-dimension, ρ determines the divergence in the y-dimension, and β affects the behavior in the z-dimension.



(a) 3D Lorenz PRNG ($\sigma = 10, \rho = 28, and\ \beta = 8/3$)

(b) Embedded EC Diffusion

(c) Proposed Encryption (Elliptic Curve + 3D Lorenz)

(d) Proposed Encryption in 10x Iteration

Figure 3. Proposed Encryption Processing

2.4 Performance Evaluation

Commonly, MSE, PSNR, UACI, and NPCR are the metrics used to measure the efficiency of any encryption approach. The performance indicator respectively, as stated in Equations 8, 9, 10, and 11. The MSE calculates the average squared difference between the original and encrypted images, which provides an idea of the distortion caused by the encryption process— the higher the value of MSE, the better the encryption performance of the approach can be ensured [29]. The PSNR is derived from MSE and is used to evaluate the perceptual quality of the encrypted image. According to the literature, a low PSNR indicates a much stronger encryption effect [30]. The UACI describes the average change in intensity between two encrypted images that differ by a single pixel in the plaintext image, reflecting the algorithm's sensitivity to small changes in input [31]. In the case of NPCR, the percentage of different pixel positions between the original and encrypted images is measured; hence, it shows the ability of the encryption scheme to spread changes throughout the entire image in case of any change, and this value will be calculated. Essentially, the higher values of UACI and NPCR indicate resistance against differential attacks, demonstrating efficiency and strength in the proposed encryption system.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - K(i,j))^{2} \tag{8}$$

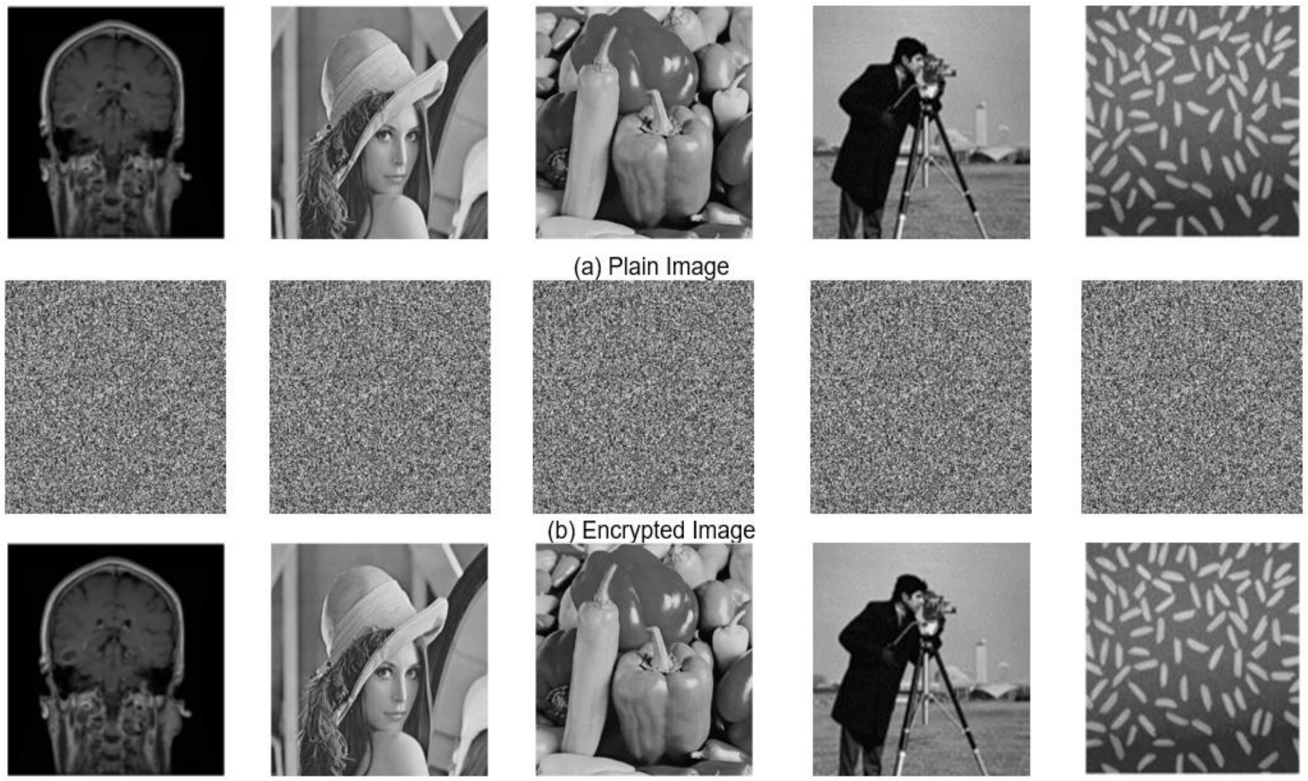
$$PSNR = 10\log 10\left(\frac{\max \_pixel\_value^{2}}{MSE}\right) \tag{9}$$

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j)\ \oplus K(i,j)}{L}\right| \times 100 \tag{10}$$

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j)-K(i,j)}{I(i,j)}\right| \times 100 \tag{11}$$

3. Results and Discussion

In this work, the implementation and execution of the suggested algorithm are performed in Python programming within a Google Colab environment, which is quite efficient and agile for code development and testing. Test cases remain exactly the same since the image dataset used for conducting experiments consists of grayscale images with a resolution of 512 x 512 pixels. Computations were performed on a system with a Ryzen 5 7600X processor, an NVIDIA RTX 3060 GPU, a 2 TB SSD, and 32 GB of RAM. The aforementioned configuration provides decent performance regarding computationally intensive applications related to chaotic system calculations, encryption, and image processing. The results of this study were evaluated using four different plain images: MRI, Lena, Peppers, Cameraman, and Rice, all in JPG format. These images were selected to represent a diverse set of textures and visual details, providing a robust assessment of the encryption algorithm's performance. The initial stage of this section involved the encryption process, where each plain image was transformed into its corresponding cipher image. The outcomes of this encryption process can be seen in Figure 4.



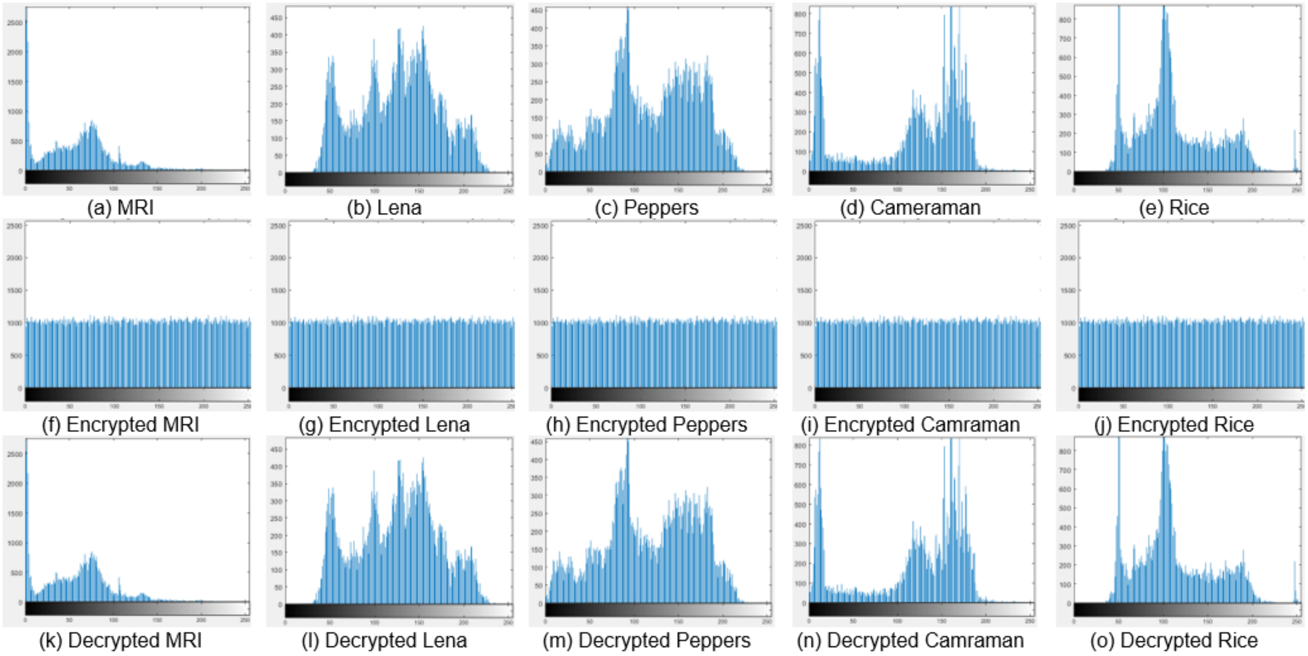
(a) Plain Image

(b) Encrypted Image

(c) Decrypted Image

Figure 4. Proposed Encryption and Decryption

Figure 5 presents the results of the histogram analysis on the encryption and the decryption processes. Figure 5(a) allows viewers to see the distribution of the pixel intensity across different steps. In more concrete terms, Figure 5(a) illustrates the histogram of the plain image before encryption, revealing the intrinsic distribution of pixel intensity in the plain image. Figure 5(b) shows that the histogram of the encrypted image is uniformly distributed, reflecting effectiveness about the randomness in the encryption process. Furthermore, Figure 5(c) displays the histogram of the decrypted image, which is almost identical to that of the original plain image. Indeed, this proves the correctness of the reversible decryption process.


(a) MRI (b) Lena (c) Peppers (d) Cameraman (e) Rice

(f) Encrypted MRI (g) Encrypted Lena (h) Encrypted Peppers (i) Encrypted Camraman (j) Encrypted Rice

(k) Decrypted MRI (l) Decrypted Lena (m) Decrypted Peppers (n) Decrypted Camraman (o) Decrypted Rice

Figure 5. Analysis of Histogram

The following histograms represent the distribution of pixel intensity for various states of an image: original-, (a)-(e), encrypted (f)-(j), and decrypted (k)-(o). Original images exhibit very distinct peaks and changes in their intensity values, due to the features and other subtleties inherent in each. For example, "MRI" and "Lena" (a) and (b), respectively, show apparent peaks due to the non-uniform distribution of intensity values in natural or medical images. On the other hand, encrypted histograms are uniformly distributed across all pixel values, without any particular pattern in sight. This means that encryption has truly randomized pixel values, resulting in the absence of any 'visible' pattern, which makes these images resistant to statistical attacks. Finally, decrypted histograms, as depicted in (k)-(o), are reasonably identical to the original histograms, proving that the decryption process does restore the original images with minimal loss and distortion. This indicates the efficiency of the encryption and decryption algorithm in terms of image integrity with guaranteed safety.

Next, the image quality was measured to assess the extent of changes that occurred in the encrypted and decrypted images. The results of this image quality measurement can be seen in Table 1.

Table 1. Performance Measurement

Researcher	Methods	Plain Image	MSE	PSNR	UACI	NPCR
[23]	Elliptic Curve and Affine Hill Cipher	Peppers	4409	7.4121 dB	33.31	99.63
[19]	Elliptic Curve and Multidimensional Chaotic Maps	Lena	-	27.897 dB	33.34	99.63
		Peppers	-	27.903 dB	33.31	99.63
Our Study	Elliptic Curve and 3D Lorenz	MRI	4888	5.1157 dB	33.33	99.64
		Lena	3298	7.6977 dB	33.33	99.63
		Peppers	4765	7.1332 dB	33.33	99.63
		Cameraman	3787	7.6219 dB	33.33	99.63
		Rice	3032	8.8711 dB	33.34	99.64

Based on Table 1, the performance of several image encryption methods is compared using evaluation metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), and Number of Pixel Change Rate (NPCR). Previous research by [19] used a combination of Elliptic Curve and Affine Hill Cipher, while research by [15] utilized Elliptic Curve with Multidimensional Chaotic Maps. This research introduces a new approach that combines Elliptic Curve and 3D Lorenz. The results show that this research method provides lower MSE and higher PSNR for some images, such as Rice (MSE: 3032, PSNR: 8.8711 dB), compared to other methods. The UACI and NPCR values for all methods are relatively consistent, around 33.3 for UACI and 99.6 for NPCR, indicating high effectiveness in detecting changes in pixel intensity as well as encryption sensitivity to data changes. Thus, this new approach delivers competitive performance, especially in producing high-quality encrypted images. The final step of this research is the decryption test using the correct, slightly modified, and incorrect curve/key, which is shown in Figure 6. Figure 6 (a) shows the original image (plain image); the results of Figure 6 (b) show the slightly modified key by altering the original elliptic curve parameter a by a very small margin, i.e., $\Delta a = \pm 1$ over the finite field F_q. Figure 6 (c) shows the results with the incorrect key, and Figure 6 (d) shows the results with the correct key.

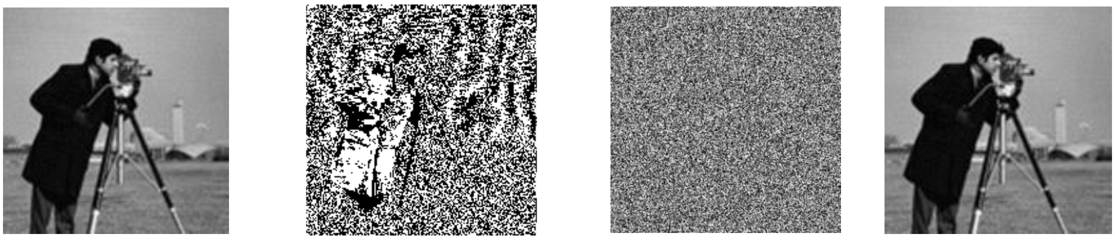

(a) Plain Image (b) Slightly Modified Key (c) Incorrect Key (d) Correct Key

Figure 6. Testing Phase

4. Conclusion

This study proposes a novel image encryption method that combines Elliptic Curve cryptography with the 3D Lorenz chaotic system to enhance security and efficiency. The encryption process involves pixel permutation, Elliptic Curve-based encryption, and diffusion using pseudo-random sequences generated by the 3D Lorenz system, while decryption reverses these steps to restore the original image. Performance evaluations on grayscale images, including MRI, Lena, Peppers, Cameraman, and Rice, demonstrate competitive results. For instance, the method achieves an MSE of 3032 and a PSNR of 8.8711 dB for the Rice image, with consistently high UACI (33.34%) and NPCR (99.64%) values, indicating strong resistance to pixel intensity changes and robustness against differential attacks. In further testing phases, this research confirms the algorithm's reliability, showing that only the correct key successfully restores the original image, while incorrect or modified keys fail, ensuring the encryption's integrity. Additionally, the uniform pixel distribution in encrypted images highlights its effectiveness in thwarting statistical attacks. The method's resilience to cryptographic attacks, coupled with its computational efficiency, underscores its practicality for real-world applications. Future research could explore extending this approach to color images, optimizing computational efficiency for larger datasets, and integrating additional chaotic systems to further enhance encryption strength. Such advancements would broaden the applicability of the proposed method in securing digital images across diverse domains.

Acknowledgement

The authors would like to express their sincere gratitude to Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Dian Nuswantoro (UDINUS) for providing financial support for this research through the Internal Research Scheme. This funding has been instrumental in facilitating the completion of this study through Grant Research No. 005/A.38-04/UDN-09/I/2025.

References

[1] K. N. Singh, O. P. Singh, and A. K. Singh, "ECiS: Encryption prior to compression for digital image security with reduced memory," *Comput Commun*, vol. 193, pp. 410–417, Sep. 2022. https://doi.org/10.1016/j.comcom.2022.07.049

[2] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," *Advance Sustainable Science, Engineering and Technology (ASSET)*, vol. 6, no. 1, 2024. https://doi.org/10.26877/asset.v6i1.17186

[3] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024. https://doi.org/10.1016/j.csa.2023.100031

[4] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," *Computers & Electrical Engineering*, vol. 85, p. 106685, Jul. 2020. https://doi.org/10.1016/j.compeleceng.2020.106685

[5] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," Nov. 01, 2022, *MDPI*. https://doi.org/10.3390/su142114226

[6] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahem, "Data Privacy Preservation and Security in Smart Metering Systems," Oct. 01, 2022, *MDPI*. https://doi.org/10.3390/en15197419

[7] E. R. Pramudya *et al.*, "Optimation of image encryption using fractal Tromino and polynomial Chebyshev based on chaotic matrix," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 22, no. 6, p. 1529, Aug. 2024. https://doi.org/10.12928/telkomnika.v22i6.26080

[8] M. Rohini, M. A. Srikanth, M. Prajwal, P. R. Kumar, M. Basavaraj, and M. U. Vinay, "Advanced Data Security Using Modulo Operator And LSB Method," *Journal of Scholastic Engineering Science and Management*, vol. 2023, no. 5, pp. 26–37, 2023.

[9] C. A. Sari, P. Purwanto, E. H. Rachmawanto, and A. Syukur, "An integration of quantum systems using BB84 for enhanced security in aeroponic smart farming," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 22, no. 6, p. 1491, Dec. 2024. https://doi.org/10.12928/telkomnika.v22i6.26450

[10] M. Abu-Faraj *et al.*, "Protecting Digital Images Using Keys Enhanced by 2D Chaotic Logistic Maps," *Cryptography*, vol. 7, no. 2, 2023. https://doi.org/10.3390/cryptography7020020

[11] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical Image Encryption: A Comprehensive Review," Aug. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. https://doi.org/10.3390/computers12080160

[12] M. Habek, Y. Genc, N. Aytas, A. Akkoc, E. Afacan, and E. Yazgan, "Digital image encryption using elliptic curve cryptography: A review," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, IEEE, 2022, pp. 1–8. https://doi.org/10.1109/HORA55278.2022.9800074

[13] V. Sathananthavathi, K. Ganesh Kumar, and M. Sathish Kumar, "Secure visual communication with advanced cryptographic and ımage processing techniques," *Multimed Tools Appl*, 2023. https://doi.org/10.1007/s11042-023-17224-6

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

[15] A. Banik, D. S. Laiphrakpam, A. Agrawal, and R. Patgiri, "Secret image encryption based on chaotic system and elliptic curve cryptography," *Digit Signal Process*, vol. 129, p. 103639, Sep. 2022. https://doi.org/10.1016/j.dsp.2022.103639

[16] C. A. Sari *et al.*, "A Chaotic Image Encryption Based on Random Noise and Arnold Cat Maps," in *2024 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2024, pp. 347–352. https://doi.org/10.1109/iSemantic63362.2024.10762216

[17] 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," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568–580, 2023. https://doi.org/10.22266/ijies2023.0831.46

[18] S. Yin, J. Liu, and L. Teng, "Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption.," *Int. J. Netw. Secur.*, vol. 22, no. 3, pp. 419–424, 2020. https://doi.org/10.6633/IJNS.202005_22(3).07

[19] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, "Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps," *IEEE Access*, vol. 9, pp. 76191–76204, 2021. https://doi.org/10.1109/ACCESS.2021.3072075

[20] G. Ye, M. Liu, and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Engineering Journal*, vol. 61, no. 9, pp. 6785–6795, Sep. 2022. https://doi.org/10.1016/j.aej.2021.12.023

[21] K. Wang, X. Wu, H. Wang, H. Kan, and J. Kurths, "New color image cryptosystem via SHA-512 and hybrid domain," *Multimed Tools Appl*, vol. 80, no. 12, pp. 18875–18899, 2021. https://doi.org/10.1007/s11042-021-10511-0

[22] S. Zhou, P. He, and N. Kasabov, "A dynamic DNA color image encryption method based on SHA-512," *Entropy*, vol. 22, no. 10, pp. 1–23, Oct. 2020. https://doi.org/10.3390/e22101091

[23] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher," *Mathematics*, vol. 10, no. 20, Oct. 2022. https://doi.org/10.3390/math10203878

[24] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput Sci Rev*, vol. 47, p. 100530, 2023. https://doi.org/10.1016/j.cosrev.2022.100530

[25] A. V. Lucca, G. A. M. Sborz, V. R. Q. Leithardt, M. Beko, C. A. Zeferino, and W. D. Parreira, "A review of techniques for implementing elliptic curve point multiplication on hardware," Mar. 01, 2021, *MDPI AG*. https://doi.org/10.3390/jsan10010003

[26] 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, Dec. 2022. https://doi.org/10.3390/sym14122559

[27] M. Naim, A. Ali Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem," *Advances in Space Research*, vol. 67, no. 7, pp. 2077–2103, Apr. 2021. https://doi.org/10.1016/j.asr.2021.01.018

[28] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal and Fractional*, vol. 7, no. 4, Apr. 2023. https://doi.org/10.3390/fractalfract7040287

[29] D. Chicco, M. J. Warrens, and G. Jurman, "The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation," *PeerJ Comput Sci*, vol. 7, p. e623, Jul. 2021. https://doi.org/10.7717/peerj-cs.623

[30] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019. https://doi.org/10.4236/jcc.2019.73002

[31] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," *Optik (Stuttg)*, vol. 261, p. 169122, 2022. https://doi.org/10.1016/j.ijleo.2022.169122