A Desktop-Based Digital Image Encryption System Using The Lorenz Chaotic Map

Makmun

Department Informatic Technic, Faculty of Industry Technology, Gunadarma University, Indonesia
* Corresponding Author:
Email: makmun@staff.gunadarma.ac.id

Abstract.

The increasing use of digital images in communication, healthcare, and information systems has raised the need for effective image security mechanisms. Conventional encryption methods are often less suitable for image data because of its large size and high correlation among adjacent pixels. Therefore, chaos-based cryptography has gained attention due to its sensitivity to initial conditions and ability to generate highly random sequences. This study aims to develop and evaluate a desktop-based digital image encryption application using the Lorenz System Chaotic Map to ensure image confidentiality and accurate reconstruction. This study employed a quantitative experimental approach in the form of a computational experiment. Data were collected through direct testing using RGB and grayscale images with different dimensions and formats, including .jpg, .png, and .bmp. The system was implemented in a desktop environment and evaluated using processing time, histogram analysis, Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and key sensitivity analysis. The results show that the proposed system successfully transformed original images into visually unrecognizable encrypted images and reconstructed them perfectly during decryption. The encrypted images exhibited more uniform histogram distributions and low PSNR values, while the decrypted images showed zero MSE and infinite PSNR, indicating lossless recovery. The system also demonstrated high sensitivity to small key changes. These findings imply that the proposed method is effective for digital image protection in practical applications. The originality of this study lies in integrating a Lorenz-based encryption algorithm into a user-oriented desktop application equipped with built-in evaluation features.

Keywords: *Image Encryption; Lorenz Chaotic System; Digital Image Security; PSNR and MSE.*

I. INTRODUCTION

The rapid advancement of digital technology has significantly increased the use of digital images across various domains, including healthcare, security, communication, and multimedia systems. In modern digital environments, images are no longer merely visual representations but also carriers of sensitive and critical information [1]. In healthcare systems, for example, medical images such as radiological scans and diagnostic records must be securely stored and transmitted to prevent unauthorized access and data breaches. Recent studies indicate that the increasing interconnectivity of digital health systems has amplified cybersecurity risks, exposing sensitive patient data to potential threats and vulnerabilities [2]. Furthermore, data breaches involving healthcare information have become a major concern, as they may compromise patient privacy, institutional integrity, and regulatory compliance [3]. These conditions highlight the urgent need for robust security mechanisms, particularly for digital image data [4].Beyond healthcare, the security of digital images is equally critical in broader digital communication systems [5]. Unlike textual data, digital images possess unique characteristics such as large data size, high redundancy, and strong correlations among adjacent pixels, making them unsuitable for traditional encryption methods designed for text. Recent surveys emphasize that conventional encryption techniques may not efficiently address these characteristics, thereby necessitating specialized image encryption approaches [6,7].

Moreover, chaos-based image encryption has emerged as a promising solution due to its inherent properties [8, 9], including high sensitivity to initial conditions, nonlinearity, and pseudo-random behavior, which are well-suited for securing image data [10, 11]. These findings demonstrate that developing efficient and secure image encryption systems remains a critical research challenge.Previous studies in this field can be categorized into three main groups. The first category focuses on survey-based and analytical studies that examine the development, evaluation metrics, and application domains of chaos-based image encryption. These studies highlight that modern image encryption schemes must be evaluated not only based on visual randomness but also on security robustness, computational efficiency, and resistance to cryptanalytic attacks [6, 7, 10, 11]. This category provides a comprehensive foundation for understanding how image encryption

systems should be assessed in real-world applications.The second category emphasizes the development of encryption techniques and architectures based on chaotic systems. Various approaches have been proposed, including hybrid chaotic maps, hyperchaotic systems, permutation–diffusion structures, and Lorenz-based models. For instance, hybrid chaotic encryption schemes and lightweight cryptographic approaches have been introduced to enhance both security and computational efficiency [12, 13].

More recent works have explored advanced models such as four-dimensional hyperchaotic systems, block permutation with weighted diffusion, and improved Lorenz chaotic systems for image encryption [14-16]. Additionally, the integration of chaos with deep learning techniques, such as autoencoders, has been proposed to further improve encryption performance and robustness [17]. Overall, this category demonstrates the continuous evolution of chaos-based encryption techniques in addressing complex security requirements.The third category addresses the limitations and challenges of existing image encryption methods. Despite significant advancements, several studies report that many encryption schemes still face issues related to security robustness, efficiency, and practical implementation. For example, survey studies reveal that cryptanalysis remains a crucial aspect in evaluating chaos-based encryption systems, as some methods may still exhibit vulnerabilities under certain attack models [7]. Other studies emphasize that challenges such as computational overhead, usability, and adaptability to different image formats and sizes remain unresolved [11]. Furthermore, recent research indicates that some Lorenz-based systems may suffer from weak chaotic characteristics or insufficient diffusion strength, leading to potential reconstruction risks [11, 14]. These findings suggest that there is still a research gap in developing image encryption systems that are not only secure but also flexible, efficient, and practical for real-world applications.

Based on these research gaps, this study aims to develop a desktop-based digital image encryption application using the Lorenz System Chaotic Map. The study focuses on designing and implementing an encryption–decryption algorithm, developing a user-friendly graphical user interface (GUI), and evaluating the system using various image types, including RGB and grayscale images in .jpg, .png, and .bmp formats, as well as both square and non-square dimensions. In addition, the system performance is evaluated using multiple metrics, including encryption and decryption processing time, histogram analysis, Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and key sensitivity analysis.Based on these objectives, this study argues that the Lorenz System Chaotic Map can provide a secure, flexible, and practical solution for digital image encryption. The effectiveness of the encryption process is demonstrated through significant visual and statistical differences between the original and encrypted images, as indicated by uniform histogram distribution, high MSE values, and low PSNR values. Meanwhile, the reliability of the system is confirmed by the ability of the decryption process to perfectly reconstruct the original image, indicated by zero MSE and infinite PSNR values. Furthermore, the high sensitivity of the system to slight changes in initial conditions and parameters ensures strong resistance against brute-force and key-related attacks. Therefore, integrating the Lorenz chaotic system into a desktop-based application is expected to provide both strong security performance and practical usability for digital image protection.

II. METHODS

The unit of analysis in this study was a desktop-based digital image cryptography application developed using the Lorenz System Chaotic Map, along with the digital images processed by the system. Accordingly, the study did not involve human participants, institutions, or social groups, but focused on the behavior and performance of the encryption–decryption system when applied to digital image data. The test objects consisted of both RGB and grayscale images with different dimensions, resolutions, and file formats, including *.jpg, .png, and .bmp.* These image variations were intentionally selected to evaluate whether the proposed application could process both square and non-square images while maintaining consistent encryption and decryption performance.This study employed a quantitative experimental design, specifically a computational experiment, because the main objective was to design, implement, and evaluate an image encryption system in a measurable and objective manner. A quantitative approach was considered appropriate because the proposed method had to be assessed using numerical indicators reflecting system effectiveness, reconstruction accuracy, and computational performance.

Through this design, the study examined whether the Lorenz-based method was capable of generating a secure chaotic keystream, producing highly randomized encrypted images, reconstructing the original images correctly during decryption, and operating efficiently in a desktop environment. Therefore, the selected research design was aligned with the algorithmic, technical, and evaluative nature of the study.The sources of data and information in this study consisted of digital image files and outputs generated by the developed application. The primary data were image files used as experimental inputs, including color and grayscale images with different sizes and file formats. Additional data were obtained from the application outputs, such as encrypted images, decrypted images, processing time records, histogram distributions, and quantitative image quality values. The system was developed using Python 3.12.0 in Visual Studio Code, with Tkinter used for the graphical user interface, Pillow (PIL) and OpenCV for image manipulation, NumPy for numerical processing, and Matplotlib for data visualization.

In the proposed system, the cryptographic key was generated from six Lorenz parameters, namely the initial values x_0, y_0, and z_0, and the system parameters σ, ρ, and β.The data collection technique was carried out through direct computational testing of the developed application. First, the researcher prepared a set of test images with varying characteristics in terms of size, type, and format. Second, each image was loaded into the application through the graphical interface, and the user entered the required Lorenz key parameters. Third, the chaotic Lorenz system generated a numerical sequence, which was discretized and mapped into the byte range of 0–255 to form the keystream. This keystream was then applied to the image pixels through a bitwise XOR operation during the encryption process. For decryption, the same parameters were re-entered so that the system could regenerate an identical keystream and restore the encrypted image to its original form. The randomness characteristics of the generated keystream are illustrated in Figure 1.

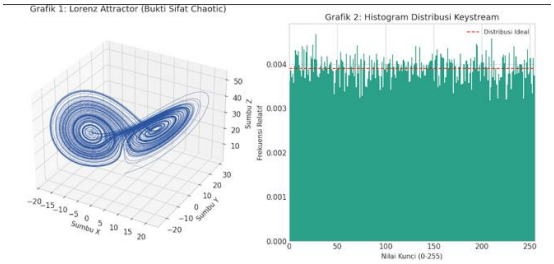


Fig 1. Keystream generation test using the Lorenz chaotic system.

For the encryption stage, the generated keystream was combined with the image pixels using a bitwise XOR operation to transform the original image into an unreadable cipher image. The logical sequence of this procedure is illustrated in Figure 2. For the decryption stage, the same Lorenz parameters were re-entered so that the system could regenerate an identical keystream and restore the encrypted image to its original form. The logical sequence of the decryption procedure is shown in Figure 3.

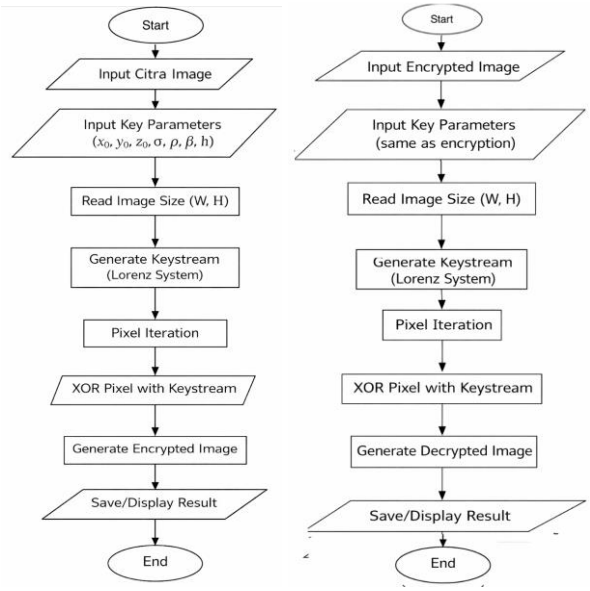


Fig 2. (Left) Flowchart of the encryption process, (right) Flowchart of the decryption process.

The data analysis was conducted using quantitative performance analysis. First, the generated keystream was examined graphically to observe its chaotic behavior and distribution pattern. Second, the encrypted and decrypted images were compared to determine whether the system successfully transformed the original image into an unreadable cipher image and accurately reconstructed it after decryption. Third, processing time analysis was performed to measure the duration required for encryption and decryption for each test image. Fourth, histogram analysis was used to compare the pixel intensity distributions of the original, encrypted, and decrypted images as an indicator of randomness and restoration quality. Fifth, Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) were calculated to quantify image distortion and reconstruction accuracy. Finally, key sensitivity analysis was conducted by introducing very small changes to the initial conditions and Lorenz parameters in order to observe whether minimal key variations produced significantly different decryption results. Through these stages, the study evaluated the effectiveness, reliability, and security performance of the proposed Lorenz-based digital image cryptography system.

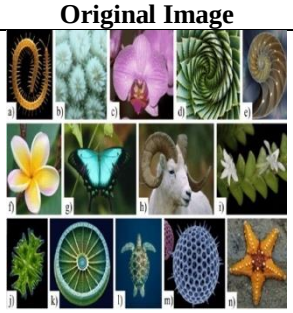
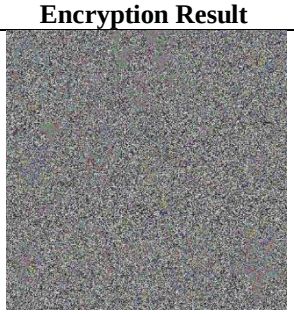
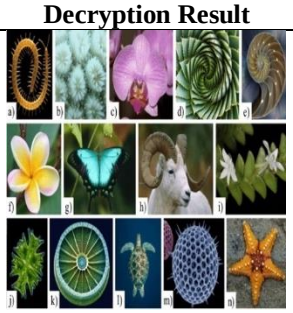
III. RESULT AND DISCUSSION

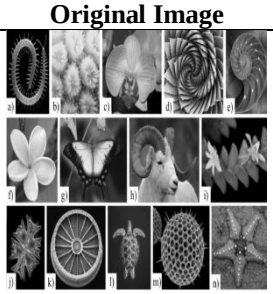
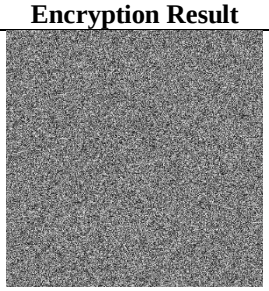
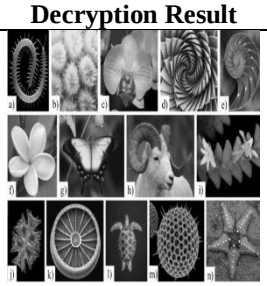
The application was tested on a computer equipped with an Intel Core i5-7200U processor running at 2.7 GHz and 8 GB of RAM. The system was successfully implemented using Python 3.12.0 together with the supporting libraries required for the graphical interface, image processing, numerical computation, and data visualization. Functional and performance testing was conducted using 10 test images with different formats, dimensions, and color types, including both RGB and grayscale images. This variation was intended to evaluate whether the developed application could operate consistently across different image characteristics.

3.1 Functional Results of the Encryption and Decryption Processes

The first finding of this study shows that the developed application was able to perform both encryption and decryption successfully on all test images. During the encryption stage, the original images were transformed into visually unrecognizable outputs that appeared as random noise-like patterns, indicating that the visual information had been effectively obscured. During the decryption stage, the encrypted images were restored to their original form using the same key parameters, demonstrating that the proposed method was able to reconstruct the original image without visible distortion.To illustrate this result, the output of the encryption–decryption process for representative RGB and grayscale images is presented in Table 1. The table shows the original image, the encrypted image, and the decrypted image, together with their dimensions, file sizes, and file formats. Although the encrypted images preserved the same spatial dimensions as the original ones, their visual appearance changed completely, whereas the decrypted images returned to the same visual form as the original images.

Table 1. Functional results of image encryption and decryption.

Data Test	Original Image	Encryption Result	Decryption Result
1	 Dimension: 512 x 512 Size: 469 KB Format: PNG	 Dimension: 512 x 512 Size: 767 KB Format: PNG	 Dimension: 512 x 512 Size: 469 KB Format: PNG

Data Test	Original Image	Encryption Result	Decryption Result
2	 Dimension: 512 x 512 Size: 151 KB Format: PNG	 Dimension: 512 x 512 Size: 653 KB Format: PNG	 Dimension: 512 x 512 Size: 261 KB Format: PNG

The data indicate several consistent tendencies. First, the application worked successfully for both RGB and grayscale images. Second, the method was able to handle both square and non-square image dimensions. Third, the encrypted images did not preserve any visually identifiable structure from the original image, which is an important characteristic of a secure image encryption system. Fourth, the decrypted images showed perfect visual recovery, indicating that the XOR-based process combined with the Lorenz-generated keystream remained reversible as long as the correct key parameters were used. These findings demonstrate that the proposed application is not only functional in computational terms but also reliable in preserving image integrity after decryption.

3.2 Computational Performance of the Proposed System

The second result concerns the computational performance of the application, particularly the time required for encryption and decryption. The processing time was measured for each test image in order to assess how image characteristics affected computational speed. The results show that the main factor influencing the duration of the process was the image dimension, or the total number of pixels, rather than the file size in kilobytes.For example, images with dimensions of 532 × 532 pixels required an average processing time of approximately 0.35 seconds, whereas images with dimensions of 266 × 266 pixels required only about 0.08 seconds. In addition, the processing times for encryption and decryption of the same image were nearly identical, which indicates that both processes impose a balanced computational load on the system.

Table 2. Encryption and decryption processing time for test images.

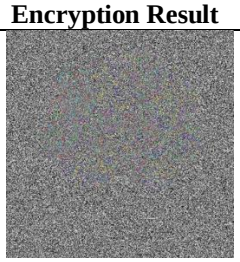
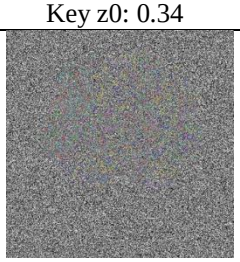
Data Test	Image Name	Dimension (Piksel)	Size (KB)	Average Encryption Time (second)	Average Decryption Time (second)
1	Animal and Plants_512.png	512 x 512	469	0.3376	0.3217
2	Animal and Plants _GS_512.png	512 x 512	151	0.3326	0.3301
3	Animal and Plants _266.png	266 x 266	140	0.0857	0.0838
4	Animal and Plants _GS_266.png	266 x 266	44,5	0.0837	0.0834
5	Plants.png	512 x 266	290	0.1686	0.1755
6	Plants_GS.png	512 x 266	92,3	0.1626	0.1638
7	Tree_532.jpg	532 x 532	80,7	0.3589	0.3565
8	Tree_GS_532.jpg	532 x 532	80,7	0.3595	0.3556
9	Plants.bmp	640 x 350	653	0.2917	0.2762
10	Plants_GS.bmp	640 x 350	314	0.2864	0.2844

These results can be restated more simply as follows: the larger the image resolution, the longer the encryption and decryption process takes. However, the system still completed all operations in less than one second for the tested images, which suggests that the application is sufficiently efficient for practical desktop-based use. Another important pattern is that the file size itself was not the dominant factor in processing speed; instead, the total number of pixels was more influential. This means that computational effort is more strongly related to image dimension than to storage size. Overall, the findings indicate that the proposed system performs efficiently and consistently across various image types and sizes.

3.3 Security Evaluation of the Encryption Algorithm

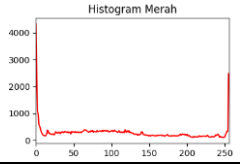
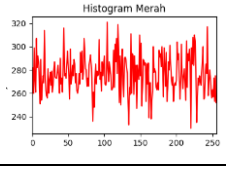
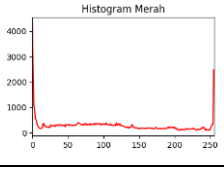
The third result concerns the security performance of the proposed encryption algorithm. Security was evaluated using three main analyses, namely key sensitivity analysis**,** histogram analysis**,** and PSNR–MSE analysis. These analyses were used to determine whether the algorithm could effectively conceal image information, resist incorrect-key decryption, and preserve the original image during the reconstruction stage. The key sensitivity test showed that the system was highly sensitive to slight changes in key parameters. Even a very small modification in one of the six key parameters, such as adding $10^{-15}$to z_0, resulted in total decryption failure. In such cases, the output image remained completely scrambled and did not resemble the original image. This confirms the strong dependence of the system on the exact initial values and Lorenz parameters. To further verify the security strength of the proposed method, a key sensitivity test was conducted by introducing very small changes to the Lorenz initial parameters during the decryption process. The purpose of this test was to determine whether minimal key variations would produce significantly different outputs and prevent successful image reconstruction. The results of this experiment are presented in Table 3.

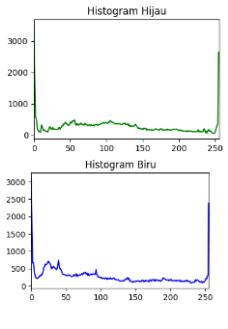
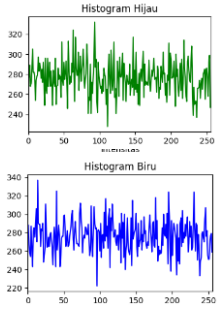
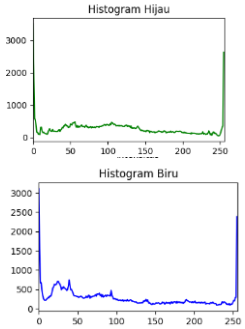
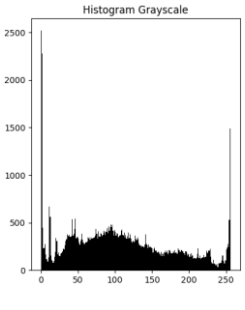
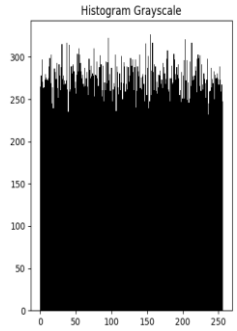
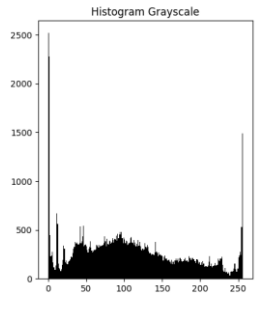
Table 3. Key sensitivity test results.

Original Image	Encryption Result	Decryption Result
		
Animal and Plants_266.png	Key x0: 0.12 Key y0: 0.23 Key z0: 0.34	Kunci x0: 0.12 Kunci y0: 0.23 Kunci z0: 0.34 + 10^{-15}
		
Animal and Plants_266.png	Key x0: 0.12 Key y0: 0.23 Key z0: 0.34	Key x0: 0.12 Key y0: 0.23 Key z0: 0.34 + 10^{-16}

The histogram analysis further supports the security of the proposed algorithm. The histogram of the original image generally showed uneven pixel intensity distributions with distinct peaks corresponding to dominant image structures. After encryption, the histogram became much flatter and more uniformly distributed, indicating that the statistical characteristics of the original image had been concealed. After decryption, the histogram returned to the same distribution as the original image, confirming that the image information was perfectly restored. To further examine the statistical effect of the encryption process, histogram analysis was performed on the original, encrypted, and decrypted images. This analysis was intended to observe changes in pixel intensity distribution before and after encryption, as well as to confirm whether the decrypted image recovered the same distribution as the original image. The comparative histogram results are presented in Table 4.

Table 4. Histogram comparison of original, encrypted, and decrypted images

Data Test	Original Image	Histogram Original Image	Histogram Encrypted Image	Histogram Decrypted Image
1	Animal and Plants_266.png			

Data Test	Original Image	Histogram Original Image	Histogram Encrypted Image	Histogram Decrypted Image
				
2	Animal and Plants_GS_266.png			

The quantitative quality analysis using PSNR and MSE also confirmed this pattern. For the comparison between the original and encrypted images, the MSE values were very high and the PSNR values were very low, generally below 10 dB. This indicates that the encrypted image differed greatly from the original image, meaning that the visual information had been successfully disrupted. In contrast, for the comparison between the original and decrypted images, the MSE value was 0 and the PSNR value was infinite, demonstrating that the decryption process was completely lossless. In addition to visual and histogram-based evaluation, quantitative image quality analysis was conducted using Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). These metrics were used to measure the degree of distortion between the original and encrypted images, as well as the reconstruction accuracy between the original and decrypted images. The results of this quantitative evaluation are presented in Table 5.

Table 5. PSNR and MSE analysis results.

Data Image	Image Test	Comparison	MSE	PSNR (dB)	Notes
1	Animal and Plants_512.png	Original vs Encrypted Original vs Decrypted	12198.4404 0	7.27 inf dB	Extremely High Difference
2	Animal and Plants _266.png	Original vs Encrypted Original vs Decrypted	11958.2494 0	7.35 inf dB	Extremely High Difference
3	Tree_532.jpg	Original vs Encrypted Original vs Decrypted	15255.8089 0	6.30 inf dB	Extremely High Difference
4	Plants.bmp	Original vs Encrypted Original vs Decrypted	11488.1834 0	7.53 inf dB	Extremely High Difference

Taken together, these results reveal several important trends. First, the system produces encrypted images with strong visual distortion and statistically flattened histograms, which supports confidentiality. Second, the original image can be reconstructed perfectly when the correct key is used, showing high reliability. Third, the algorithm is extremely sensitive to minimal key variation, which strengthens resistance against incorrect-key attacks. Fourth, the combination of visual, statistical, and quantitative evidence consistently indicates that the proposed Lorenz-based encryption system performs effectively as a secure image cryptography method.

3.4 Discussion

The results of this study demonstrate that the proposed desktop-based digital image cryptography application using the Lorenz System Chaotic Map was able to perform encryption and decryption reliably while maintaining strong security characteristics. Three major findings emerged from the experiment. First, the application successfully transformed original images into unreadable encrypted forms and reconstructed

them perfectly during decryption. Second, the computational performance of the system remained efficient across different image dimensions and formats. Third, the security evaluation showed high key sensitivity, a more uniform histogram distribution after encryption, and clear quantitative separation between original and encrypted images as indicated by the PSNR and MSE results.These findings can be explained by the inherent behavior of the Lorenz chaotic system. Because the Lorenz system is highly sensitive to its initial conditions, even a very small modification in x_0, y_0, z_0, σ, ρ, or βproduces a significantly different chaotic sequence. When this sequence is converted into a keystream and applied through a pixel-wise XOR operation, the encryption output becomes highly dependent on the exact key values. This explains why the encrypted images appeared random and why decryption failed when the parameters were altered even slightly.

At the same time, the involutive property of XOR made perfect reconstruction possible when the exact same parameters were re-entered. In this sense, the effectiveness of the proposed system lies in the combination of chaotic sensitivity and reversible binary operation, which together support both confidentiality and reconstruction accuracy.Compared with previous studies, the present work offers several practical advantages. Recent reviews have shown that chaos-based image encryption remains a widely used approach because it can provide strong randomness, flexibility, and image-oriented protection, particularly for digital images that are less efficiently handled by conventional text-based encryption schemes [6, 7, 11]. At the same time, these studies also note that many existing methods focus mainly on algorithm design, mathematical modeling, or simulation-based evaluation rather than on practical implementation in user-oriented software [7, 11]. In contrast, the present study implemented the Lorenz-based method in a desktop application with a graphical user interface, allowing the encryption method to be applied directly rather than remaining only at the conceptual or simulation level. This comparison suggests that the novelty of the present study is not merely algorithmic, but also applicative and usability-oriented. The present findings are also consistent with recent developments in Lorenz-based and chaos-enhanced image encryption.

For example, Wen proposed a chaos-based block permutation and weighted bit-plane chain diffusion method to address insufficient security in earlier image encryption systems [14], while Zhang developed an improved Lorenz chaotic system combined with Galois field diffusion to enhance encryption performance [16]. These studies emphasize strengthening diffusion complexity and resistance to cryptanalytic attacks through more elaborate mathematical structures. In comparison, the present study did not primarily seek to build a mathematically more complex chaotic model, but rather to demonstrate that a Lorenz-based XOR encryption system can be implemented in a practical desktop environment with integrated analysis features such as histogram analysis, processing time measurement, and PSNR–MSE evaluation. Therefore, the contribution of this study is positioned more strongly in the area of practical implementation and functional integration than in the development of a new chaotic variant. From an interpretive perspective, the results of this study support the broader view that effective image cryptography should not be assessed from only one dimension, such as visual distortion or numerical randomness alone. Instead, a robust image encryption system should combine several properties at once: strong visual concealment, high sensitivity to the key, reliable reconstruction under correct parameters, and acceptable computational efficiency. Recent surveys on image encryption likewise emphasize that practical evaluation should include not only security indicators but also implementation-oriented measures such as efficiency, flexibility, and resistance to attack [6, 7].

In this regard, the present study contributes by showing that these properties can coexist in a desktop-based application that is operationally simple yet functionally effective. The findings also have broader implications for digital image protection. The ability to transform original images into visually meaningless outputs while preserving exact reconstruction capability is highly relevant for domains such as medical image transmission, confidential image storage, and protected digital communication. Previous studies have noted that digital image encryption is particularly important in image-intensive and security-sensitive environments, where confidentiality must be balanced with accurate restoration of the visual data [2, 15]. At the same time, the strong dependence on precise key parameters highlights both a strength and a limitation of the proposed system. It is a strength because it increases resistance to unauthorized decryption, but it is also a limitation because any key management error by the legitimate user may prevent successful image recovery. This means that practical implementation should be accompanied by careful key storage and

parameter management procedures. Overall, this study confirms that the Lorenz-based image cryptography approach is effective, practical, and suitable for further development. Nevertheless, several limitations remain. The present system was tested in a desktop environment using a limited number of image samples and did not yet incorporate hybrid encryption mechanisms, cloud deployment, or real-time transmission scenarios. Future studies may extend this work by combining the Lorenz chaotic map with additional cryptographic layers, optimizing the method for larger image datasets, or integrating it into real-time secure communication systems. Such improvements would strengthen both the scientific contribution and the practical applicability of the proposed method.

IV. CONCLUSION

The findings of this study show that the proposed desktop-based digital image cryptography application using the Lorenz System Chaotic Map is capable of performing encryption and decryption effectively and reliably. The system successfully transformed original images into visually unrecognizable encrypted images and reconstructed them perfectly during the decryption process. This result was supported by several performance indicators, including high key sensitivity, more uniform histogram distribution after encryption, and clear quantitative differences between original and encrypted images as reflected in the PSNR and MSE values. These results confirm that the proposed method is able to provide both image confidentiality and reconstruction accuracy.From a scientific perspective, this study contributes by demonstrating the practical implementation of chaos-based image encryption in the form of a desktop application with a graphical user interface.

The contribution of this research lies not only in applying the Lorenz chaotic system as a keystream generator for digital image cryptography, but also in integrating encryption–decryption functions with evaluation tools such as processing time analysis, histogram analysis, and PSNR–MSE measurement within one system. In this way, the study offers an applied contribution that connects theoretical chaos-based cryptography with a functional and user-oriented software environment. However, this study also has several limitations. The application was tested only in a desktop environment and used a limited number of image samples with specific formats and dimensions. In addition, the study did not yet incorporate hybrid encryption mechanisms, larger-scale image datasets, or real-time transmission scenarios. Therefore, future research is recommended to develop hybrid chaos-based cryptographic models, improve computational scalability for larger image datasets, and extend the system into cloud-based or real-time secure image communication applications. Such developments would strengthen both the robustness and the practical applicability of the proposed method.

REFERENCES

[1] W. H. O. WHO, "Global Strategy on Digital Health," 2024.

[2] P. Ewoh and T. Vartiainen, "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review," ***Journal of Medical Internet Research***, vol. 26, p. e46904, 2024, doi: 10.2196/46904.

[3] M. Sajitha and S. Mathew, "A Review of Chaos-Based Image Encryption Techniques," *Multimedia Tools and Applications*, vol. 81, pp. 16827-16867, 2022, doi: 10.1007/s11042-021-11468-2.

[4] J. Pool, S. Akhlaghpour, F. Fatehi, and A. Burton-Jones, "A systematic analysis of failures in protecting personal health data: A scoping review," ***International Journal of Information Management,*** vol. 74, p. 102719, 2024, doi: 10.1016/j.ijinfomgt.2023.102719.

[5] A. S. Ahmad and K. H. Santoso, "The Urgency of Establishing AI Regulations to Ensure Legal Certainty and AI Ethics in Responding to Challenges Digitalization in Indonesia," ***International Journal of Science and Environment (IJSE),*** vol. 6, no. 1, pp. 366-371, 2026, doi: 10.51601/ijse.v6i1.353.

[6] Y. Alghamdi and A. Munir, "Image encryption algorithms: A survey of design and evaluation metrics," ***Journal of Cybersecurity and Privacy,*** vol. 4, no. 1, pp. 126-152, 2024, doi: 10.3390/jcp4010007.

[7] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," ***International Journal of Information Security,*** vol. 21, no. 4, pp. 917-935, 2022, doi: 10.1007/s10207-022-00588-5.

[8] Y. Zhang, X. Wang, L. Liu, and Z. Zhang, "A Chaotic Image Encryption Algorithm Based on Permutation-Diffusion Structure," *Nonlinear Dynamics*, vol. 78, pp. 2021-2032, 2014, doi: 10.1007/s11071-014-1563-3.

[9] Y. Zhou, L. Bao, and C. L. P. Chen, "A New 1D Chaotic System for Image Encryption," *Signal Processing*, vol. 97, pp. 172-182, 2014, doi: 10.1016/j.sigpro.2013.11.008.

[10] A. Dinu and M. Frunzete, "Image encryption using chaotic maps: Development, application, and analysis," *Mathematics*, vol. 13, no. 16, p. 2588, 2025, doi: 10.3390/math13162588.

[11] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2585, 2023, doi: 10.3390/math11112585.

[12] F. Masood *et al.*, "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1405-1432, 2022, doi: 10.1007/s11277-021-08584-z.

[13] I. Yasser, F. Khalifa, M. A. Mohamed, and B. B. Samir, "A new image encryption scheme based on hybrid chaotic maps," *Complexity*, vol. 2020, p. 9597619, 2020, doi: 10.1155/2020/9597619.

[14] H. Wen, Y. Lin, S. Kang, X. Zhang, and K. Zou, "Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion," *iScience*, vol. 27, p. 108610, 2024, doi: 10.1016/j.isci.2023.108610.

[15] N. Yang, S. Zhang, M. Bai, and S. Li, "Medical image encryption based on Josephus traversing and hyperchaotic Lorenz system," ***Journal of Shanghai Jiaotong University (Science),*** vol. 29, pp. 91-108, 2024, doi: 10.1007/s12204-022-2555-x.

[16] X. Zhang, G. Man, R. Gao, C. Dai, and Q. Meng, "An image encryption method based on improved Lorenz chaotic system and Galois field," *Applied Mathematics and Computation*, vol. 472, p. 128623, 2024, doi: 10.1016/j.amc.2024.128623.

[17] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognition Letters*, vol. 153, pp. 59-66, 2022, doi: 10.1016/j.patrec.2021.11.025.