SEMARAK ILMU PUBLISHING

Semarak International Journal of Electronic System Engineering

Journal homepage:
https://semarakilmu.my/index.php/sijese/index
ISSN: 3030-5519

Color Image Encryption and Decryption using the Chaotic Lorenz Map and 3D Chaotic Chen System with Enhanced Performance

Nurul Asyiqin Bahari[1], Arif Mandangan[2,*], Che Haziqah Che Hussin[3], Babarinsa Olayiwola[4]

[1] Mathematics Computer Graphics, Faculty of Science and Natural Resources, Universiti Malaysia Sabah, Sabah, Malaysia
[2] Mathematics Visualization Research Group, Faculty of Science and Natural Resources, Universiti Malaysia Sabah, Sabah, Malaysia
[3] Preparatory Centre for Science and Technology, Universiti Malaysia Sabah, Sabah, Malaysia
[4] Department of Mathematics, Federal University Lokoja, P.M.B 1154, Kogi State, Nigeria

ARTICLE INFO

Article history:
Received 14 April 2025
Received in revised form 12 May 2025
Accepted 21 May 2025
Available online 30 June 2025

Keywords:
Image encryption; chaotic maps; chaotic cryptosystem; digital image; data compression

ABSTRACT

This paper aims to improve efficiency in terms of processing time of color image encryption and decryption using the chaotic Lorenz 3D and Chen 3D systems. Encrypting and decrypting high-resolution color images pose a challenge due to long execution times. To address this issue, we integrate the Huffman compression technique with the chaotic Lorenz 3D and Chen 3D systems. By compressing the image prior to the encryption process, the proposed scheme significantly reduces image size, leading to acceleration of the encryption and decryption running times. On top of that, Huffman compression also enhances security by generating more random patterns. Experimental results demonstrate that the proposed approach effectively reduces processing time, contributing to a more secure and efficient cryptographic system.

1. Introduction

In today's interconnected world, cryptography is essential for protecting sensitive data, including personal, financial, and governmental secrets. Notably, it plays a crucial role in securing personal information such as emails, online transactions, and financial records. Cryptography is a scientific discipline that can provide security goals such as confidentiality, integrity, authentication, non-repudiation, and data integrity. To provide confidentiality, the original information in its plain form is being transformed into an incomprehensible form through an encryption process. To recover the original information, a decryption process is required to invert the encryption process. Both encryption and decryption processes require public and private keys respectively, where both keys are mathematically related to each other. Only a correct private key could recover the original information from its encrypted form [1].

Digital data, including text, images, audio, and video, requires protection in terms of confidentiality. Image encryption has become particularly critical due to the vast amount of image

* *Corresponding author.*
E-mail address: arifman@ums.edu.my

https://doi.org/10.37934/sijese.6.1.112

data transmitted and stored digitally. For instance, Sprott B's hyperchaotic map is employed for greyscale image encryption in [2], while [3] utilizes Arnold's cat map and the Henon map for the encryption of color images. However, substantial execution time becomes a significant challenge in practice. This limitation hinders the feasibility of real-time image encryption in applications demanding rapid processing [4]. Despite the existence of various image encryption schemes, security received overwhelming attention compared to efficiency. Achieving both security and efficiency is crucial for better adoption in real-life applications.

In [5], a new approach to encrypting color images is introduced, utilizing the chaotic Lorenz map and the 3D chaotic Chen system, accompanied by sophisticated algorithms and appealing security attributes. Nonetheless, the method suffers from inefficiency, which limits its widespread application, particularly in devices with constrained environments. Evidently, a balance between security and efficiency is essential for the broader acceptance of any cryptographic algorithms, including those used for image encryption. To address the highlighted issue, we proposed an integration of Huffman compression technique in color image encryption and decryption processes using the chaotic Lorenz map and the chaotic 3-dimensional Chen system. The ultimate aim is to enhance the efficiency level in terms of processing time of the system by integrating a compression technique without compromising the security aspect of the proposed scheme.

2. Literature Review

2.1 Lorenz Map

The Lorenz map is a famous dynamic system that exhibits chaotic behavior [6]. In the study by Wang *et al.,* [7], an algorithm for color image encryption was proposed, which combines two complex chaotic systems, namely the complex Lorenz system and the complex Chen system. This method aims to enhance security and further expand the key space for color image encryption compared to existing methods. The encryption process is divided into three main steps. First, pixel scrambling involves scrambling the pixels of the original image through a process of two-dimensional and one-dimensional transformations in the RGB channels individually. This process helps to confuse the position of pixels in each channel. Second, the XOR operation is used to hide pixel information, where a sequence of pseudorandom numbers generated by a complex chaotic system is used to perform the XOR operation in each image channel. Finally, a process called "Chaotic Ponytail" involves mixing the RGB channels using a sequence of pseudorandom numbers generated by a complex chaotic system. This step breaks the boundaries between RGB channels, making it difficult to decrypt the image by starting with one channel and moving to another.

Fu *et al.,* [8] proposed an encryption method for color images involves symmetric cipher images with a diffusion scrambling architecture. This method aims to enhance the security of image encryption against known or chosen plaintext attacks by using a key stream generation mechanism related to the plaintext. The encryption process begins with image scrambling (permutation) using a discrete Baker map to scramble the image, which helps eliminate strong correlations between adjacent pixels. This step rearranges the pixel positions to obscure the relationship between the original image and the ciphered image. Next, the regular text diffusion where the Lorenz system, with its more complex dynamic properties and multiple variables, is used at this stage. The variables of the Lorenz system are selected according to the original pixels, or it can be said that the flow keys used in the diffusion are not only determined by the keys but also by the original image itself.

2.2 Rössler Map

The Rössler system is a 3-dimensional nonlinear system first introduced by Otto Rössler in 1976. It is a continuous-time dynamic system that exhibits chaotic behavior for certain parameter values [9]. Cao and Fu [10] proposed an encryption scheme based on the Rössler chaotic system to enhance the security and performance of image encryption compared to methods based on conventional simple chaotic systems. The most important aspects of the proposed method include the analysis of the balance properties and time sequence correlation generated by the Rössler system, the introduction of a preprocessing scheme to further enhance the statistical properties of the key stream, the combination of three initial parameters of the Rössler system as a single key to increase the key space under limited precision conditions, and the implementation of position permutation and gray scale substitution to a single pixel in a single iteration operation which subsequently increases encryption speed and creates a system resistant to adaptive parameter alignment attacks caused by complex 3D structures.

In [11], Hamza *et al.,* further enhance the security of image encryption by combining the RC4 algorithm with the Rössler chaotic system. This method focuses on enhancing resistance against various attacks. For example, statistical attacks while improving the difficulty of the decrypted image and minimizing encryption and decryption time. By influencing the chaotic dynamics of the Rössler system to generate pseudorandom values for encryption, this approach aims to enhance security and ensure high resistance against attacks.

2.3 Chen System

The Chen system is a chaotic dynamic system introduced to study the behavior of nonlinear systems [12]. The Chen system is also one of the Lorenz-style systems, meaning it shares some equations with the famous Lorenz system but also has unique characteristics that make it a special subject of study in the field of chaotic theory. Fu *et al.,* [13] proposed a new fast color image encryption scheme using the chaotic Chen system to generate key streams for permutation and substitution to encrypt color images. This method aims to enhance computational efficiency and security by integrating both processes and reducing the number of iterations required.

2.4 Chua's Circuit

The Chua system is a nonlinear circuit that exhibits chaotic behavior. It is the first chaotic circuit to be physically constructed and proven through laboratory experiments, computer simulations, and rigorous mathematical proofs [9]. Arpacı *et al.,* [14] proposed a new encryption and decryption method to enhance the security of color images using a modified Chua's circuit. This process involves a combination of diffusion and permutation stages, with key generation using the SHA-256 algorithm and a regular image. The security of this algorithm is enhanced by its resistance to plaintext attacks and its ability to reduce correlation through the mixing of the three-color components of the image. Ye *et al.,* [15] proposed an encryption algorithm based on the multi-scroll Chua chaotic system, which offers greater complexity compared to classical discrete systems. The method by Ye *et al.,* includes three steps, namely Arnold Cat transformation for pixel scrambling, zigzag transformation for further scrambling, and a random diffusion algorithm based on the multi-scroll chaotic system to determine pixel values. This approach aims to minimize the correlation between adjacent pixels and enhance the algorithm's resistance to decryption.

2.5 Lossless Compression

Lossless compression techniques consist of Huffman coding, run-length encoding (RLC), and Shannon-Fano coding [16]. Not only that, Arithmetic coding, bit-plane coding, and dictionary techniques are also examples of lossless compression techniques [17,18]. Pai *et al.,* [19] proposed that the compression technique using two lossless coding technologies, Huffman and Lempel-Ziv-Welch (LZW), for image compression. The image is compressed using Huffman coding in the first stage, which generates a Huffman tree and produces Huffman code words.

The study conducted by Sharma [20] focused on data transmission and multimedia compression and considered this issue as compression encoding and transmission to generate a model transmission with a low bit rate, which relies on the Huffman coding algorithm. The proposed technique balances 0 and 1 bits by measuring the probability of discrepancies present in the traditional Huffman tree. Furthermore, the proposed method is also adapted with a transitional tree at the same compression ratio. Jassim and Qassim in [21] presented an ideal technique for image compression known as the five-module method (FMM). In that technique, each pixel value in the 8x8 block is multiplied by five for each RGB array. After that, the values are divided by five to obtain a new bit length value for each pixel, which is approximately less in storage space compared to the actual value of 8 bits. Their results also show that the efficiency of the image compression method depends on FMM. The advantage of their technique is that it allows for a high Peak-Signal-to-Noise-Ratio (PSNR) even with a low compression ratio. This technique is suitable for bit levels such as black and white medical images, where the pixels in the image are represented by one byte (8 bits).

2.6 Efficiency of Image Encryption Scheme

In addition to ensuring security, an encryption scheme must also demonstrate adequate efficiency regarding computational and storage capacity costs. High-quality image processing often incurs significant expenses due to the large file sizes of the images. Consequently, there has been considerable attention in literature focused on enhancing the efficiency of image encryption algorithms. Studies in [22] and [23] present analytical tools for evaluating both the efficiency and security of image encryption schemes. In [24], the authors adopt a hardware-based approach to enhance an image encryption algorithm by implementing a parallel computing system. Following the same methodology, a new hardware-oriented contrast enhancement algorithm suitable for effective hardware design is introduced in [25]. Additionally, [26] details the proposal of an image encryption/decryption algorithm along with its VLSI architecture. Improving efficiency of the image encryption scheme is another aspect of research that requires the same level of attention as security improvement research. In addition to the hardware approach, alternative methods can be explored to achieve varying effects. One promising innovative approach involves incorporating a data compression algorithm into the image encryption scheme, as suggested in this study.

3. Methodology

3.1 Lorenz Map Differential Equation

The differential equations for the chaotic Lorenz map that will be implemented are as follows:

$$\frac{dx}{dt} = 10(y - x) \tag{1}$$

$$\frac{dx}{dt} = 28x - y - xz \tag{2}$$

$$\frac{dx}{dt} = xy - \frac{8}{3}z \tag{3}$$

where $x, y, z \in \mathbb{R}$ are variables, while $\sigma, \rho, \beta \in \mathbb{R}$ are constants, specifically σ = 10, ρ = 28, and β = 8/3, which determine the specific behaviour of the system, and dt represents an infinitesimal change in time [18].

3.2 Chen System Differential Equation

The differential equation of the chaotic 3-dimensional Chen system is described as follows:

$$\frac{dx}{dt} = a(y - x) \tag{4}$$

$$\frac{dx}{dt} = -xz - (c - a)x + cy \tag{5}$$

$$\frac{dx}{dt} = xy - bz \tag{6}$$

where $x, y, z \in \mathbb{R}$ represent the state variables of the system while $a, b, c \in \mathbb{R}$ are the system's fixed positive parameters, namely a = 35, b = 3, and c = 28 [19].

3.3 Huffman Compression Algorithm

The Huffman compression technique serves as the first layer before the chaotic Lorenz and chaotic Chen encryption methods. Efficiency can be improved by reducing the size of the image data, thereby making the encryption process faster. This technique can also enhance security. With an additional complex layer on the data, the compressed data is more difficult to analyse.

As can be seen in Figure 1, the compression process in encoding starts by calculating the frequency of each pixel value in the flattened image data into a 1D form. The frequency is used to build the min-heap structure. Next, the node with the lowest frequency will be combined to form the Huffman tree. From the Huffman tree, a unique Huffman code will be assigned to each pixel value. The pixel data of the image will then be converted into binary code using Huffman coding. Additional bits are added so that the length of the data is a multiple of 8, then the binary data is converted to byte format. Finally, the compressed data is produced and stored, and the Huffman tree is also stored for the decompression process.

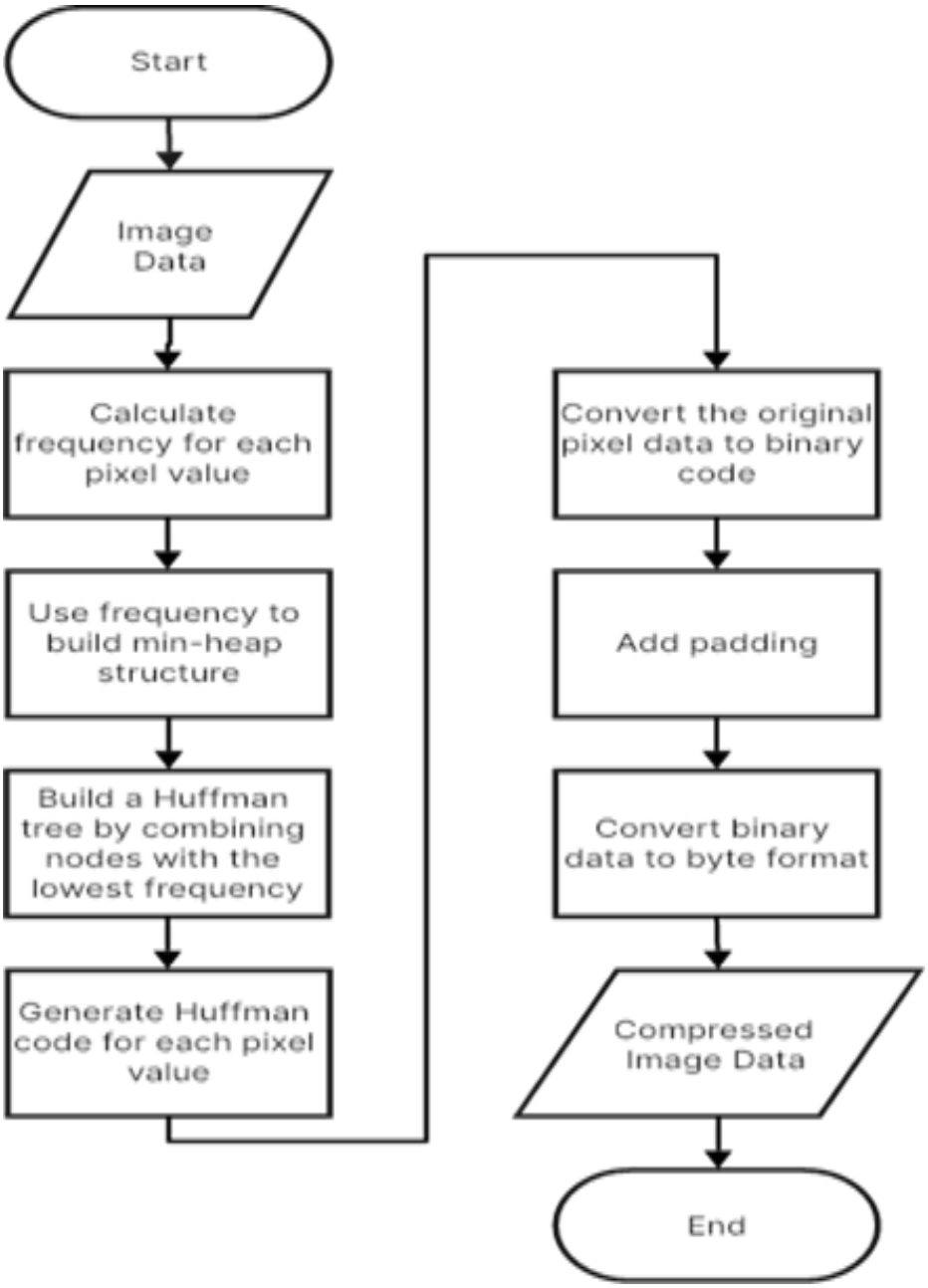
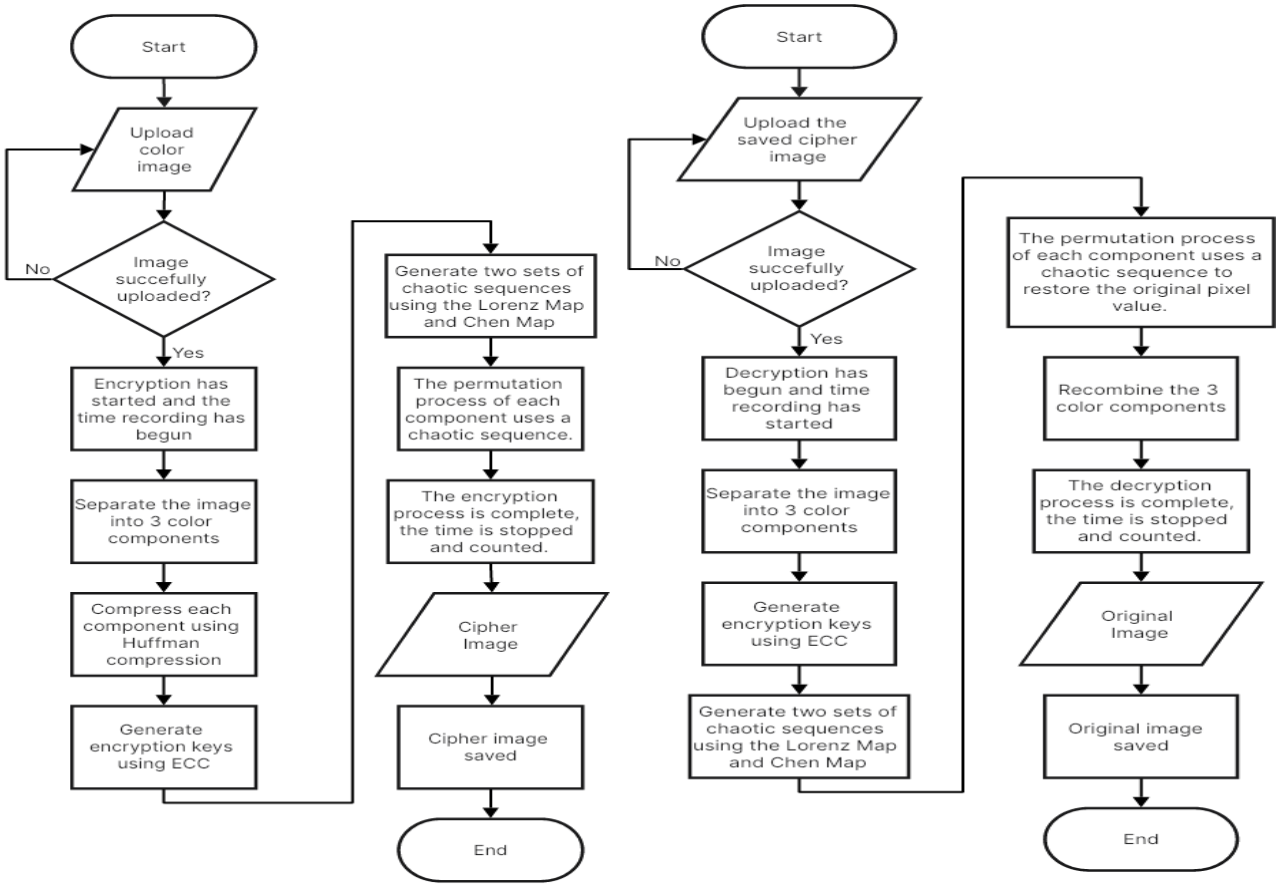


Fig. 1. Huffman compression process

3.4 Encryption Algorithm Design

The process of image encryption is the process of transforming the original image into an encrypted image to prevent it from being understood by third parties. As can be seen in Figure 2(a), the method of color image encryption begins with uploading a color image and separating it into three color components. Next, the Huffman compression process will be performed on each color component to reduce the data size. After that, the encryption keys are generated using ECC and two sets of chaotic sequences are generated from the Lorenz map and Chen map using the specified initial parameters. The permutation process is carried out on the compressed image using the chaotic sequence as the image encryption step. After the encryption process is complete, the encrypted image is stored.



(a) Image encryption process (b) Image decryption process

Fig. 2. The proposed image encryption and decryption processes

3.5 Decryption Algorithm Design

The process of image decryption is the process of transforming an encrypted image back into its original image using the appropriate key. As can be seen in Figure 2(b), the process of decrypting a color image begins with uploading the encrypted image stored during the encryption process, then each RGB component is aligned using the same chaotic sequence used during encryption, but this time for the decryption process. Next, the decryption key generated through ECC is used to obtain the required chaotic sequence. After that, the aligned image is permuted again using the corresponding chaotic sequence to restore the original pixel values in each color component. The restored image is saved in its original uncompressed state.

4. Results and Discussions

This section will discuss the results and discussion of the improved system, consisting of output images, time comparison analysis using existing scheme and the methods of this study, and PSNR analysis. The images used in this study consist of PNG and JPG file format, with the same dimensions of 512 x 512. Figure 3 shows the list of colored sample images used throughout this study.

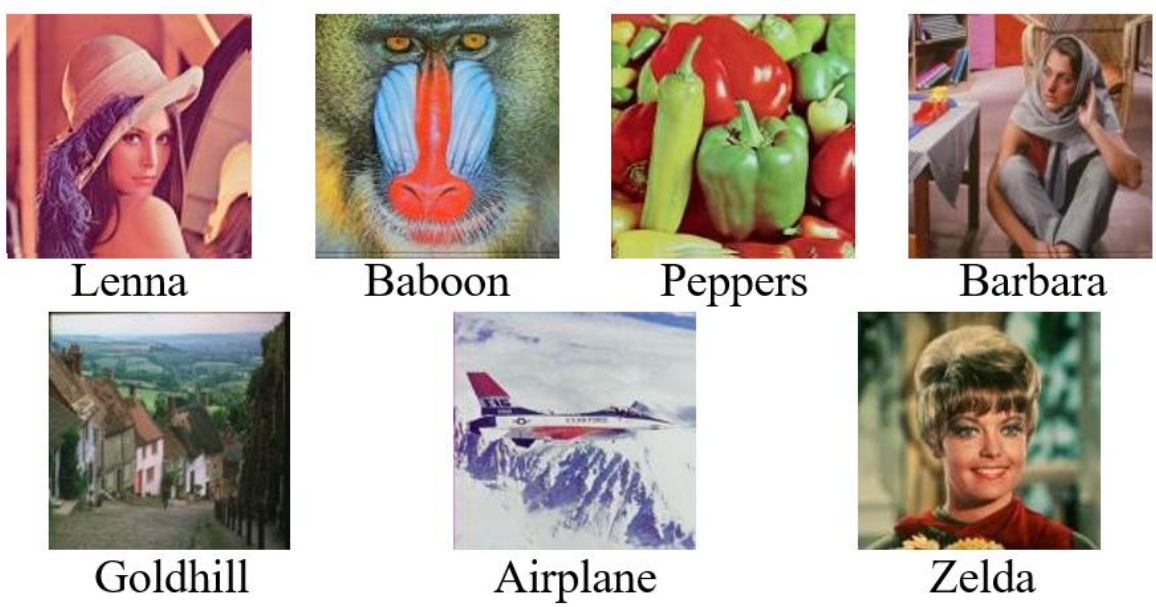


Fig. 3. Sample images for experimental purposes

After encryption is performed, the original image will become an unreadable cipher image to third parties. The image produced during the decryption process will also remain in the dimensions of 512 x 512. The purpose of the cipher image is to maintain the confidentiality of a message to be sent only to certain parties. Figure 4 shows the cipher image produced for each sample images.

Fig. 4. Plain color images with the corresponding cipher images

4.1 Time Comparison Analysis

During encryption and decryption, the time will be recorded to test the efficiency of the proposed algorithms, namely the Lorenz chaotic map and the Chen chaotic map. The efficiency of the algorithm can be proven when the time taken for the encryption and decryption processes is shorter compared to existing algorithms. This section will discuss the comparison of efficiency levels in terms of execution time between the existing method and the method proposed in this study to achieve efficient time. Both methods are techniques that use the 3D Lorenz chaotic map and the 3D Chen chaotic system for the encryption and decryption process of colored images. However, what distinguishes the two methods is that the Huffman compression technique has already been integrated into the proposed method, which aims to test the efficiency level in terms of execution time. Table 1 shows the difference in execution time between the existing method and the proposed method in the encryption and decryption processes and Figure 5 shows the comparison charts between encryption and decryption performances of the existing scheme and the proposed scheme respectively. Obviously, the execution times for both processes have been significantly reduced.

Table 1
Comparison of encryption and decryption processes time between the existing scheme and the proposed scheme

Sample Image	Encryption process time (seconds)		Decryption process time (seconds)	
	Existing scheme	Proposed scheme	Existing scheme	Proposed scheme
Lenna	4.5313	1.8839	3.7659	1.9349
Baboon	4.5200	1.7492	3.7994	1.9793
Peppers	4.4366	1.6355	3.7661	1.7741
Barbara	4.4570	1.7363	3.8622	1.7488
Goldhill	4.4562	1.7060	3.8425	1.7456
Airplane	4.7694	1.6093	3.9078	1.7620
Zelda	4.4347	1.5862	3.7379	1.7586

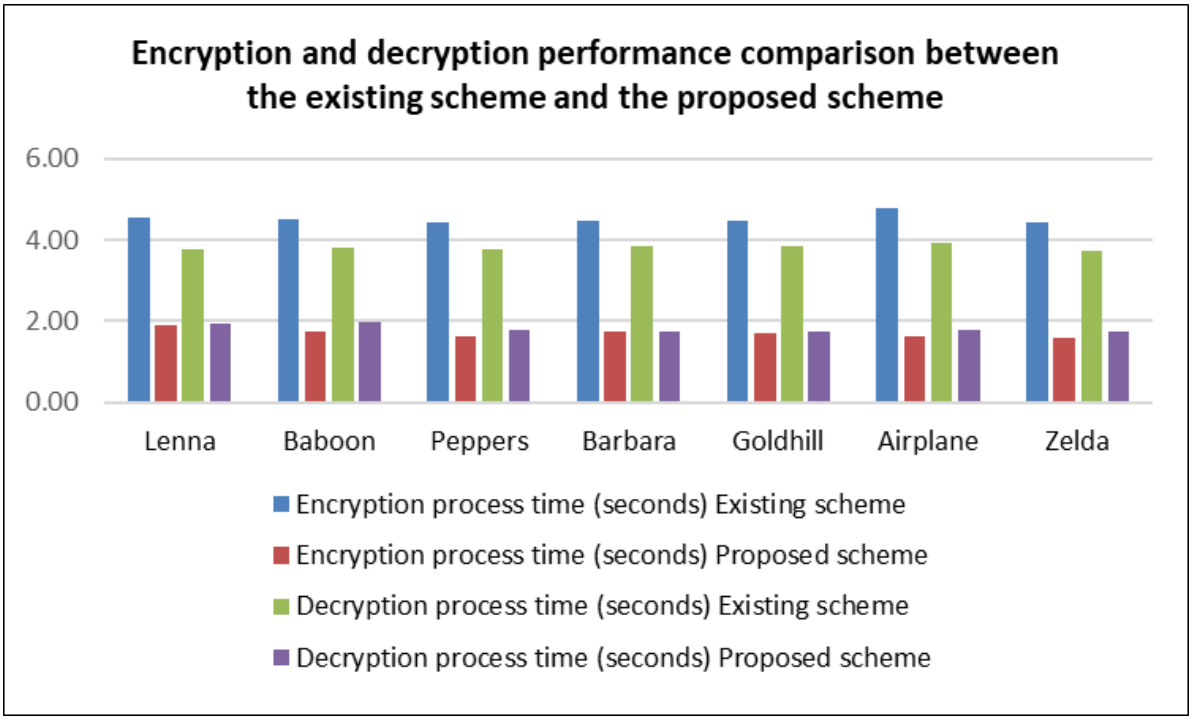


Fig. 5. Comparison charts between encryption and decryption performances of the existing scheme and the proposed scheme respectively

4.2 Peak-Signal to Noise-Ratio Analysis

Peak-Signal to Noise-Ratio Analysis (PSNR) is an important metric used to assess the quality of image recovery in the process of encoding and decoding color images. It quantitatively measures how well the decrypted image retains detail and quality compared to the original image. PSNR is important in assessing the accuracy of the decrypted image compared to the original value. A higher PSNR value indicates minimal loss of information and a closer resemblance to the original image, reflecting better image recovery. This metric is sensitive to any degradation or loss of detail that may occur during the encryption and decryption process. In the context of color images, PSNR is calculated with the average PSNR value involving the calculation of Mean Squared Error (MSE) between the corresponding pixels of the original image (I) and the decrypted image (K), followed by logarithmic scaling to emphasize differences in higher signal levels:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n=1}\big(I(i,j) - K(i,j)\big)^2 \quad (7)$$

where $m, n \in \mathbb{Z}^+$ are the dimensions of the image, and $I(i,j)$ and $K(i,j)$ represent the intensity values of the original image and the decrypted image. The PSNR value is calculated using the formula:

$$PSNR = 20 \cdot \log\left(\frac{255}{MSE}\right) \quad (8)$$

Table 2 shows the PSNR values for the cipher image and the decrypted image. During the encryption process, the pixel values of the cipher image will be compared with the pixel values of the encrypted image. This is to test the effectiveness of the process. Next, in the decryption process, the pixel values of the image to be compared are between the decrypted image and the cipher image. The goal is to test the accuracy of the decrypted image recovery. The PSNR value is measured to ensure that the image recovery process is running well by minimizing information loss.

Table 2
PSNR values of the encryption and decryption processes

Sample Image	PSNR values (dB)	
	Encryption	Decryption
Lenna	8.6387	41.5473
Baboon	9.0031	35.0463
Peppers	8.1462	42.1787
Barbara	8.8868	39.7603
Goldhill	8.2842	41.8449
Airplane	8.0144	39.7960
Zelda	8.6084	44.7505

The higher the PSNR value, the more accurately the decrypted image matches the original image. Based on the table above, the PSNR value during the encryption process shows a value of less than 10dB, indicating poor image quality and significant degradation compared to the original image. Therefore, the encrypted image cannot be understood by third parties. However, during the decryption process, the PSNR value shows a higher value of 35-40 dB and above. The value of 30-40 dB proves that the quality of the restored image is good, where the decrypted image is almost identical to the original image with minimal distortion. Meanwhile, a PSNR value exceeding 40dB indicates very good image recovery where the decrypted image is very similar, and any distortion is not visible to the naked eye.

4.3 Security Analysis

In this study, we aim to enhance the performance of the color image encryption scheme that employs the chaotic Lorenz map and the 3D chaotic Chen system, as presented in [5]. This improvement is accomplished by incorporating the Huffman compression technique into the scheme without significantly modifying its algorithm. Consequently, the security of the scheme can be preserved while adding performance benefits introduced through this study. A comprehensive security analysis of the scheme can be found in [5]. These include differential attack analysis, information entropy analysis, and correlation coefficient analysis.

5. Conclusions

This study has successfully achieved the goal of improving the efficiency of the encryption and decryption processes of color images using the Chaotic Lorenz 3D and Chaotic Chen 3D systems. Through the integration of Huffman compression techniques, this study demonstrates a significant reduction in execution time, where the encryption process becomes faster without compromising the quality of the encrypted image. High PSNR values prove that the decrypted images maintain good visual quality. Additionally, the enhancement of security through random patterns in the encryption process provides extra protection against potential threats. Thus, the results of this study indicate that a chaotic- based approach, combined with compression techniques, is a potential solution for enhancing efficiency and security in image cryptography.

References

[1] Mandangan, Arif, Nazreen Syazwina Nazaruddin, Muhammad Asyraf Asbullah, Hailiza Kamarulhaili, Che Haziqah Che Hussin, and Babarinsa Olayiwola. 2024. "A New Countermeasure to Combat the Embedding-Based Attacks on the Goldreich-Goldwasser-Halevi Lattice-Based Cryptosystem". *Journal of Advanced Research Design* 122 (1):173-83. https://doi.org/10.37934/ard.122.1.173183

[2] Ramlee, Syahidatul Shafiqah, and Arif Mandangan. 2024. "Chaotic Encryption Scheme for Double Grayscale Images Using Sprott B Hyperchaotic Map". *International Journal of Advanced Research in Computational Thinking and Data Science* 1 (1):25-40. https://doi.org/10.37934/ctds.1.1.2540a

[3] Mohammad, Siti Nurul Hatikah, and Arif Mandangan. "Colour Image Encryption and Decryption using Arnold's Cat Map and Henon Map." *International Journal of Advanced Research in Computational Thinking and Data Science* 1, no. 1 (2024): 41-52. https://doi.org/10.37934/ctds.1.1.4152a

[4] Sarosh, Parsa, Shabir A. Parah, and G. Mohiuddin Bhat. "An efficient image encryption scheme for healthcare applications." *Multimedia Tools and Applications* 81, no. 5 (2022): 7253-7270. https://doi.org/10.1007/s11042-021-11812-0

[5] Lim Jin Ying, Irene, and Arif Mandangan. 2024. "Chaotic Encryption Scheme for Colour Image Using 3D Lorenz Chaotic Map and 3D Chen System". *International Journal of Advanced Research in Computational Thinking and Data Science* 1 (1):10-24. https://doi.org/10.37934/ctds.1.1.1024a

[6] Al-Hazaimeh, Obaida M., Mohammad F. Al-Jamal, Nouh Alhindawi, and Abedalkareem Omari. "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys." *Neural Computing and Applications* 31 (2019): 2395-2405. https://doi.org/10.1007/s00521-017-3195-1

[7] Wang, Leyuan, Hongjun Song, and Ping Liu. "A novel hybrid color image encryption algorithm using two complex chaotic systems." *Optics and Lasers in Engineering* 77 (2016): 118-125. https://doi.org/10.1016/j.optlaseng.2015.07.015

[8] Fu, Chong, Wen-Jing Li, Zhao-yu Meng, Tao Wang, and Pei-xuan Li. "A symmetric image encryption scheme using chaotic baker map and Lorenz system." In *2013 Ninth International Conference on Computational Intelligence and Security*, pp. 724-728. IEEE, 2013. https://doi.org/10.1109/CIS.2013.158

[9] Abdulaali, Ryam Salam, Raied K. Jamal, and Salam K. Mousa. "Generating a new chaotic system using two chaotic Rossler-Chua coupling systems." *Optical and Quantum Electronics* 53 (2021): 1-10. https://doi.org/10.1007/s11082-021-03341-9

[10] Cao, Ying-yu, and Chong Fu. "An image encryption scheme based on high dimension chaos system." In *2008 International Conference on Intelligent Computation Technology and Automation (ICICTA)*, vol. 2, pp. 104-108. IEEE, 2008. https://doi.org/10.1109/ICICTA.2008.397

[11] Hamza, Yasir Ahmed, and Marwan Dahar Omer. "An Efficient Method of Image Encryption Using Rossler Chaotic System." *Academic Journal of Nawroz University* 10, no. 2 (2021): 11-22. https://doi.org/10.25007/ajnu.v10n1a916

[12] Xu, Jiangjian, Bing Zhao, and Zeming Wu. "Research on color image encryption algorithm based on bit-plane and Chen Chaotic System." *Entropy* 24, no. 2 (2022): 186. https://doi.org/10.3390/e24020186

[13] Fu, Chong, Zhou-Feng Chen, Wei Zhao, and Hui-yan Jiang. "A new fast color image encryption scheme using chen chaotic system." In *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 121-126. IEEE, 2017. https://doi.org/10.1109/SNPD.2017.8022710

[14] Arpacı, Batuhan, Erol Kurt, and Kayhan Celik. "A new algorithm for the colored image encryption via the modified Chua's circuit." *Engineering Science and Technology, an International Journal* 23, no. 3 (2020): 595-604. https://doi.org/10.1016/j.jestch.2019.09.001

[15] Ye, Xiaolin, Xingyuan Wang, Suo Gao, Jun Mou, and Zhisen Wang. "A new random diffusion algorithm based on the multi-scroll Chua's chaotic circuit system." *Optics and Lasers in Engineering* 127 (2020): 105905. https://doi.org/10.1016/j.optlaseng.2019.105905

[16] Clunie, David A. "Lossless compression of grayscale medical images: effectiveness of traditional and state-of-the-art approaches." *Medical Imaging 2000: PACS Design and Evaluation: Engineering and Clinical Issues* 3980 (2000): 74-84. https://doi.org/10.1117/12.386389

[17] Kim, Jungrae, Michael Sullivan, Esha Choukse, and Mattan Erez. "Bit-plane compression: Transforming data for better compression in many-core architectures." *ACM SIGARCH Computer Architecture News* 44, no. 3 (2016): 329-340. https://doi.org/10.1145/3007787.3001172

[18] Skibiński, Przemysław, Szymon Grabowski, and Sebastian Deorowicz. "Revisiting dictionary-based compression." *Software: Practice and Experience* 35, no. 15 (2005): 1455-1476. https://doi.org/10.1002/spe.678

[19] Pai, Yu-Ting, Fan-Chieh Cheng, Shu-Ping Lu, and Shanq-Jang Ruan. "Sub-trees modification of Huffman coding for stuffing bits reduction and efficient NRZI data transmission." *IEEE transactions on broadcasting* 58, no. 2 (2012): 221-227. https://doi.org/10.1109/TBC.2012.2189610

[20] Sharma, Mamta. "Compression using Huffman coding." *IJCSNS International Journal of Computer Science and Network Security* 10, no. 5 (2010): 133-141.

[21] Jassim, Firas A., and Hind E. Qassim. "Five modulus method for image compression." *arXiv preprint arXiv:1211.4591* (2012). https://doi.org/10.48550/arXiv.1211.4591

[22] Ahmad, Jawad, and Fawad Ahmed. "Efficiency analysis and security evaluation of image encryption schemes." *computing* 23, no. 4 (2010): 25.

[23] Mahendiran, N., and C. Deepa. "A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics." *SN Computer Science* 2, no. 1 (2021): 29. https://doi.org/10.1007/s42979-020-00397-4

[24] Wang, Xingyuan, Le Feng, and Hongyu Zhao. "Fast image encryption algorithm based on parallel computing system." *Information sciences* 486 (2019): 340-358. https://doi.org/10.1016/j.ins.2019.02.049

[25] Guo, Jiun-In. "A new chaotic key-based design for image encryption and decryption." In *2000 IEEE international symposium on circuits and systems (ISCAS)*, vol. 4, pp. 49-52. IEEE, 2000. https://doi.org/10.1109/ISCAS.2000.858685

[26] Yen, Jui-Cheng, and Jiun-In Guo. "A new image encryption algorithm and its VLSI architecture." In *1999 IEEE Workshop on Signal Processing Systems. SiPS 99. Design and Implementation (Cat. No. 99TH8461)*, pp. 430-437. IEEE, 1999. https://doi.org/10.1109/SIPS.1999.822348