SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

International Journal of Advanced Research in Computational Thinking and Data Science

Journal homepage:
https://semarakilmu.com.my/journals/index.php/ctds/index
ISSN: 3030-5225

SEMARAK ILMU
International Journal of
ADVANCED RESEARCH IN COMPUTATIONAL THINKING AND DATA SCIENCE
ISSN 3030 5225

Chaotic Encryption Scheme for Colour Image using 3D Lorenz Chaotic Map and 3D Chen System

Irene Lim Jin Ying[1], Arif Mandangan[1,*]

[1] Mathematics Visualization Research Group, Faculty of Science and Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia

ARTICLE INFO

Article history:
Received 29 February 2024
Received in revised form 20 March 2024
Accepted 25 March 2024
Available online 15 April 2024

Keywords:
Chaos; Image encryption; permutation; diffusion; security

ABSTRACT

Chaos-based image encryption system is an encryption method that uses chaotic systems in encrypting digital images for the purpose of enhancing security. Chaos theory exhibits some distinctive characteristics, which include butterfly-like patterns, unpredictable behavior, and sensitive dependence to initial conditions. . In the past few decades, image encryption based on a single chaotic map has been a common technique in encrypting images. However, there are still unauthorized interceptors who illegally access and obtain the private information of the image. With that being the case, an encryption method that applies more than one chaotic system will contribute to creating a more complex relationship between the original and encrypted images, making it challenging for unauthorized individuals to decipher or extract the original content of the image without the appropriate decryption key. In this study, two chaotic maps, 3D Lorenz Map and 3D Chen system, are applied to generate random cryptographic keys for encrypting color images using permutation and diffusion mechanisms. The proposed algorithm that employs two chaotic maps is proven to be an effective system that achieves excellent results in security.

1. Introduction

In this digital era, where the world is revolving around the advancement of technologies and people are transmitting information over the network boundlessly, cryptography has become an indispensable element in protecting online users' privacy and securing the confidentiality of their information. The choice of proper encryption and decryption theme can save more amount of time and is invulnerable both to noise-based attacks and hacking instances [1]. The role of cryptography becomes more crucial recently for providing robust security including in IoT devices [2]. Cryptography is used to secure the confidentiality and authenticity of data during communication by converting original readable text into secret text that can only be recognized by authorized and intended receivers. Not only do text messages and banking information need to be encrypted, but digital

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

images that are also very important to be kept safe from unauthorized users who want to discover the original image without the owner's consent [3].

Chaos theory is a mathematical theory that was officially discovered and founded by Edward Lorenz in the 1960s, despite the term "chaos" being given by the mathematician named James Yorke in 1975 [4]. Lorenz discovered the phenomenon of "sensitive dependence on initial conditions" or can be also known as the "butterfly effect" when he found out that small changes in behaviour could cause catastrophic impacts in the resulting weather output that was exhibited in the computer weather system.

In general, chaos theory can be defined as a stochastic phenomenon of a deterministic dynamical system that develops randomness, nonlinearity, and unpredictability of events that could be sensitive to initial conditions. Chaotic dynamics has sparked a lot of interest in mixing equipment and other process equipment both experimentally and numerically. In chaos theory, chaotic mixing is a process by which flow tracers develop into complex fractals under the action of a fluid flow [5]. Chaos theory is advantageous in image encryption due to its main properties such as ergodicity, pseudo randomness, control parameter, dynamic and deterministic nature, bifurcation complexity, and also its sensitivity to initial starting conditions [6]. By using a chaotic map in an encryption scheme, it would be much more challenging for the third party without the secret key to crack the code and decrypt the cipher image due to the high randomness and unpredictability properties in the chaos theory.

In the past few decades, image encryption based on a single chaotic map with a small key space, for instance, a one-dimensional chaotic map, has been a common technique in encrypting images. However, there are still unauthorized interceptors who illegally access and obtain the private information of the image. This certainly tells us that the proposed image encryption algorithms by using chaotic systems with lower dimensionality are not sufficient to provide high security in securing the privacy and secrecy of image data, despite its implementation being much simpler and uncomplicated.

In this paper aims to propose a newly chaos-based encryption algorithm which is developed based on the combination of the three-dimensional Lorenz and Chen chaotic maps for encrypting colour digital images. By combining both chaotic maps, the proposed method demonstrates notable enhancement specifically on the level of security of colour image information. Our experimental outputs showed significant increment in randomness and irregularity using multiple three-dimensional chaotic maps.

1.1 Lorenz Map

The Lorenz chaotic map that acts as one of the high-dimensional chaotic maps exhibits more complex chaotic dynamics and generates a higher number of chaotic sequences as compared to chaotic systems with lower dimensions. The system was first introduced by Edward Lorenz in the 1960s as stated in the study [7].

Fu *et al.,* [8] suggested a symmetric image encryption algorithm on grayscale images based on a chaotic baker map and Lorenz chaotic system. The authors applied the discretized baker map and conventional three-dimensional Lorenz system for confusion and diffusion phases to reduce the correlation among image pixels. The Lorenz system showed a significant encryption effect as it has complex dynamical properties and more state variables compared to other one-dimensional chaotic maps. The proposed system with higher randomness and larger key space proved that the encryption algorithm could provide high security for the image encryption system.

In the previous study conducted by Zhang [9], a grayscale image encryption that involved the application of a two-dimensional discretized Arnold cat map for the permutation stage and the hyperchaotic Lorenz system for the diffusion stage is proposed. In the diffusion stage, the key streams from each iteration in the system were rearranged following the previous plain pixel. This resulted in high security against powerful plaintext attacks as the quantified key streams were related to the plain image other than the secret keys.

Zhou and Li [10] presented a quantum image encryption algorithm on grayscale images based on Lorenz hyperchaotic system. There were two main parts in the encryption process where the first part used a pseudo-random sequence generated from the Lorenz hyper-chaotic system to scramble the image position information, while the second part of the encryption involved using hyperchaotic sequences to diffuse and confuse image pixels for colour information replacement.

1.2 Rössler Map

The Rössler system is a three-dimensional chaotic system that was introduced by Otto Rössler in the 1970s. Hamza and Omer [11] proposed a grayscale image encryption system based on symmetric stream cipher Rivest Cipher 4 (RC4) and the Rössler chaotic system. The algorithm started with an image encryption process using RC4 where the original grayscale image was encrypted using the encryption key. The encryption key was also used to generate initial conditions for Rössler attractor where the encrypted image was then used as an input for the Rössler chaotic system to create a two-dimensional array of random values. The proposed method proved to be a good encryption method that was sufficient to resist some known attacks such as differential attacks, statistical attacks, and brute-force attacks.

In the paper proposed by Abundiz-Pérez *et al.,* [12] a highly secure fingerprint encryption scheme using the hyperchaotic Rössler map was proposed to protect the secrecy of the biometric system. The pseudorandom sequences generated from the hyperchaotic Rössler were used to diffuse and permute the image pixels for the encryption process, and to inverse diffuse and inverse permute to obtain deciphered images. The proposed scheme resulted in high security especially when the authors conducted an experiment by omitting the permutation stage to find out if the plain image can still be encrypted. Besides, the authors also stated the pros of using this algorithm which include there is a low correlation of pixels, uniform distribution histograms, and high speed of encryption with high security.

1.3 Chen System

The Chen attractor that exhibits complex chaotic behaviours like other high-dimensional chaotic systems was proposed by Chen in 1999 [13]. Xu *et al.,* [14] presented a colour image encryption scheme based on the bit plane and Chen chaotic system that gives the benefit of reducing computational complexity while providing a better encryption effect. In this approach, the logistic chaotic sequences that were generated from the combination of the logistic chaos system and the Chen chaos system shuffled and scrambled the bit plane of the image internally to reduce the computational complexity of the image encryption process. The pixel bit-plane internal scrambling method allowed the encryption of higher four-bit planes and lower four-bit planes, making the encryption scheme more resistant to attacks. The overall algorithm is said to have proven a good encryption scheme that gives high-security properties with a low computational complexity of encryption.

In the previous study [15], the researchers proposed grayscale image encryption that involved the use of hyperchaotic multi-attractors Chen system with time delay (HCMACS-TD). In contrast with the ordinary Chen system, HCMACS-TD had higher sensitivity key space and a larger chaotic parameter range. In this approach, the chaotic sequences generated from HCMAS-TD were used for the confusion stage for the pixels scrambling process and multi-shift cipher function to complete the encryption of the shuffled image. The paper also stated that the use of HCMACS-TD in the algorithm gave the key space potentially unlimited dimensions. The large key space of the system contributed to an excellent performance in the system in resisting burst attacks such as differential attacks, noise attacks, and statistical attacks.

1.4 Chua's Circuit

The double-scroll system, also known as Chua's circuit, is also one of the high-dimensional chaotic maps that exhibit complex chaotic behaviours with sufficient number of parameters. Arpacı *et al.*, [16] suggested a new colour image encryption and decryption algorithm by using a modified Chua's circuit (MCC) that exhibits a hyperchaotic character due to its double frequency feature to generate pseudorandom numbers for the encryption process. The researchers carried out several experimental tests to test the security level of the algorithm such as speed analysis, correlation analysis, differential analysis, and information entropy analysis. The results proved that the algorithm was an effective encryption method that provided sufficient security and secrecy to the system with speedy execution.

Luo *et al.*, [17] proposed a robust image compression-encryption scheme on grayscale images that utilized Chua's circuit and logistic map together with the threshold processing of local binary patterns (LBP) to generate pseudorandom sequences for diffusion process. Besides reducing the amount of data during transmission process, the proposed algorithm also proved to be a secure chaos-based algorithm that has high robustness against all kinds of attacks, such as differential attacks, statistical attacks, or even shear and noise attacks.

Al-Musawi *et al.*, [18] studied an image encryption system using masking technique based on Chua chaotic system that acts as a chaotic noise generator in the proposed scheme. The algorithm was tested by using a field programmable gate array (FPGA) device with the help of the Xilinx System Generator (XSG) tool. The proposed algorithm served as an effective chaos-based grayscale and color image encryption method for secure communication as it exhibited chaotic behaviours that yield unpredictability and randomness, thus improving the security of the system.

1.5 Summary

The chaos system is widely used in image encryption schemes due to its random-like nature, making it harder to break without a correct encryption key. From the studies of each conventional three-dimensional chaotic map, the Lorenz map and Chen system are mostly applied in the proposed encryption scheme. This is simply because the Lorenz system and Chen system that give complicated chaotic properties are more preferrable over Rössler model that has less complex dynamic behaviour. In addition to that, the implementation of Chua's circuit mostly depends on the hardware, which is not compatible with the proposed encryption scheme. Hence, only Lorenz and Chen systems will be considered in the encryption algorithm. With the increasing complexity and randomness in the system, the algorithm is believed to achieve an excellent performance in terms of security.

2. Methodology

2.1 Generation of Lorenz Chaotic Sequences

The first stage involves generating secret keys and chaotic sequences by using two high-dimensional chaotic maps, which include the 3D Lorenz chaotic system and 3D Chen chaotic system. Chaotic maps would generate a sequence of values that exhibit complex, inconstant, and unpredictable behaviours. The sequence of values generated is often referred to as a chaotic sequence or a chaotic signal. Since there are two different chaotic systems that are of three dimensions that will be used in the proposed encryption and decryption scheme, there will be six different chaotic sequences, as of six different parameters will be generated in the system.

From the Lorenz system, we consider x, y and z as the state variables that evolve with the time, and we assume that x_0, y_0 and z_0 are the initial conditions, whereas α, β, $\sigma \in \mathbb{R}$ are the control parameters in the chaotic system.

The control parameters give specific values to achieve the Lorenz attractor, where $\alpha = 10$, $\beta = \frac{8}{3}$, and $\sigma = 28$ [19]. The defining equations of the 3D Lorenz chaotic system that will be implemented are described as follows:

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

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

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

2.2 Generation of Chen Chaotic Sequences

Similar to the Lorenz system, the Chen system also consists of the state variables $x, y, z \in \mathbb{R}$ as well as the parameters $\alpha, \beta, \gamma \in \mathbb{R}$ that causes the system to develop a chaotic-like behavior. In order to obtain the secret keys, we consider the initial conditions that need to be determined as $x_0, y_0, z_0 \in \mathbb{R}$. As mentioned in the paper [20], the control parameters in a chaotic case give some fixed values, where $\alpha = 35$, $\beta = 3$, and $\gamma = 28$. The differential equations of the three-dimensional Chen chaotic system are described as follows:

$$\frac{dx}{dt} = 35y - 35x, \tag{4}$$

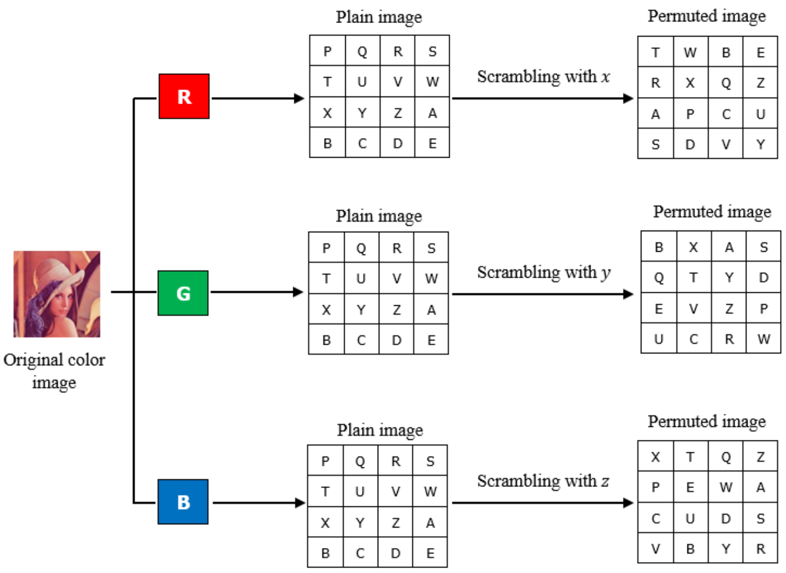
$$\frac{dy}{dt} = -7x + 28y - xz, \tag{5}$$

$$\frac{dz}{dt} = xy - 3z. \tag{6}$$

2.3 Pixel Permutation

The second stage is the permutation process. During the permutation process, the positions of image pixels are scrambled and shuffled based on the chaotic sequences derived from the Lorenz chaotic map. The original image undergoes permutation operation to produce permuted image. The permuted image will then be carried to the next stage to complete the encryption process.

Fig. 1 shows the illustration of how permutation process is performed on colour images by shuffling the positions of image pixels with separate chaotic sequences x, y, and z. From the figure, it is shown that an original color image is split into three different color channels (R, G, and B channels) for separate permutation process implemented at pixel-level. During the permutation process, each image pixel is assigned a corresponding index value from the chaotic sequence. The locations of pixels of each color component are shuffled using separate chaotic sequences generated from Chen system. Then, the permuted images with new positions for each colour channel are obtained.



P	Q	R	S
T	U	V	W
X	Y	Z	A
B	C	D	E

T	W	B	E
R	X	Q	Z
A	P	C	U
S	D	V	Y

P	Q	R	S
T	U	V	W
X	Y	Z	A
B	C	D	E

B	X	A	S
Q	T	Y	D
E	V	Z	P
U	C	R	W

P	Q	R	S
T	U	V	W
X	Y	Z	A
B	C	D	E

X	T	Q	Z
P	E	W	A
C	U	D	S
V	B	Y	R

Fig. 1. Permutation process on different colour channels

2.4 Diffusion

The third stage of the encryption scheme is the diffusion operation. The diffusion operation refers to spreading the individual grayscale pixel values across the colour channel of the image, resulting in lower correlation between pixels and increase complexity of the image data. By employing a diffusion method using the pseudorandom sequences, the system introduces a higher level of randomness and security.

In this stage, the diffusion process is conducted on the permuted images by using the chaotic sequences generated from the Chen system. An exclusive-OR (XOR) operation is performed between the values of image pixels and values of chaotic sequences, where the operation can be denoted as (the symbol ⊕ represents XOR):

$$pixel\_value \oplus chaotic\_sequence \ = diffused\_pixel\_value \tag{7}$$

After performing diffusion process on the permuted images that the positions of pixels have been shuffled, the encrypted images will surely exhibit an even more random and chaotic behaviour. It is said that the image contents have been shuffled and confused multiple times, hence, not only does it prove that a higher security level can be achieved, but it also highlights the importance of permutation and diffusion processes in an encryption scheme.

2.5 Encryption Algorithm Design

The three stages which are generation of chaotic sequences, permutation, and diffusion, are performed in encryption process for encrypting images.

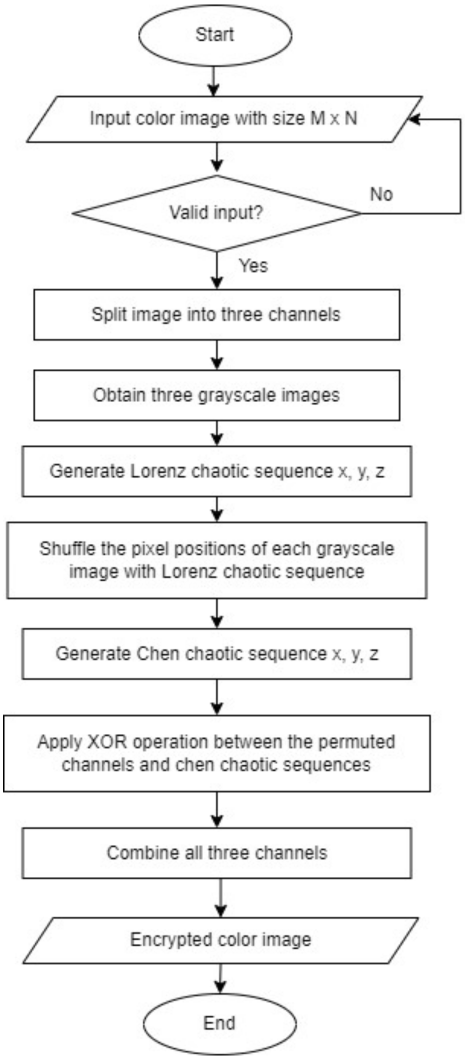

Start
Input color image with size M x N
Valid input?
No
Yes
Split image into three channels
Obtain three grayscale images
Generate Lorenz chaotic sequence x, y, z
Shuffle the pixel positions of each grayscale image with Lorenz chaotic sequence
Generate Chen chaotic sequence x, y, z
Apply XOR operation between the permuted channels and chen chaotic sequences
Combine all three channels
Encrypted color image
End

Fig. 2. Flowchart of the proposed encryption scheme

As described in Figure 2, the input of the system is an original colour image while the output is a scrambled colour image. The image will first be split into three different colour channels and three grayscale images will be obtained. After that, chaotic sequences x, y and z of both Lorenz and Chen chaotic systems are generated for permutation and diffusion stages afterwards. It can be seen that the permutation and diffusion operations are performed for each color channel and iterated by row and column. The final encrypted image will be obtained by combining three different grayscale images back together.

2.6 Decryption Algorithm Design

The decryption process is the inverse of the encryption process. Both processes are mutually inverse processes. In decryption scheme, the input image read by the system needs to be a cipher image instead of plaintext image. The input encrypted image will also be split into three different colour channels inverse permutation and inverse diffusion purposes.

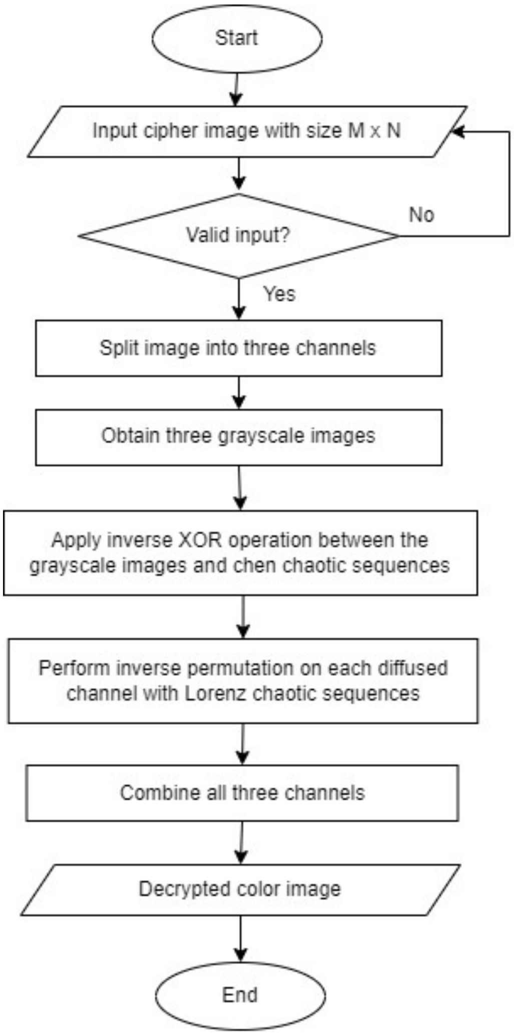

Start
Input cipher image with size M x N
Valid input?
No
Yes
Split image into three channels
Obtain three grayscale images
Apply inverse XOR operation between the grayscale images and chen chaotic sequences
Perform inverse permutation on each diffused channel with Lorenz chaotic sequences
Combine all three channels
Decrypted color image
End

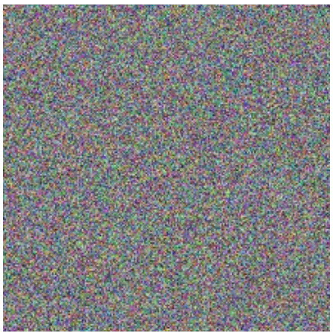
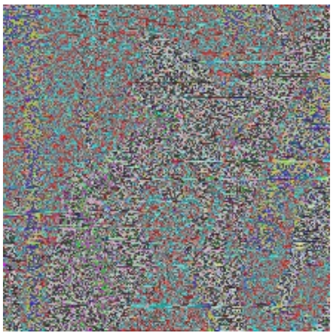
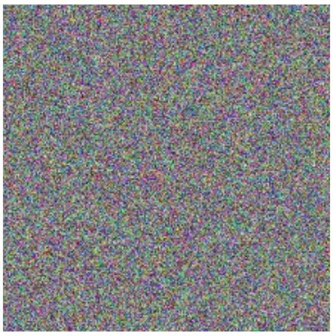
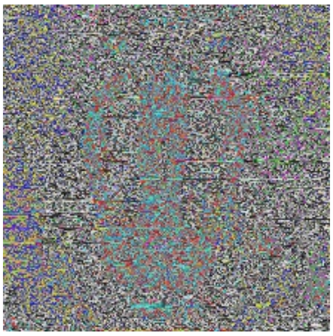
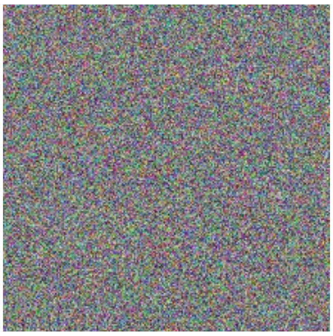
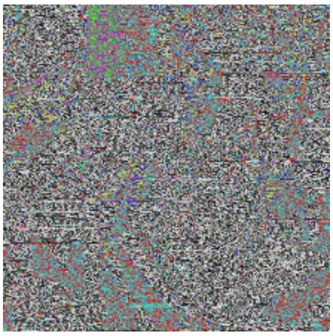
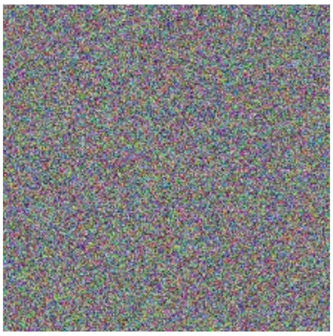
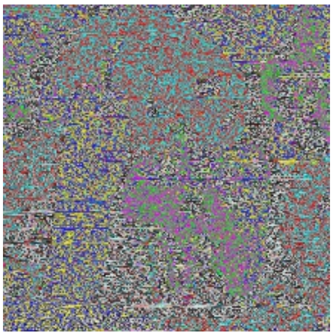
Fig. 3. Flowchart of the proposed decryption scheme

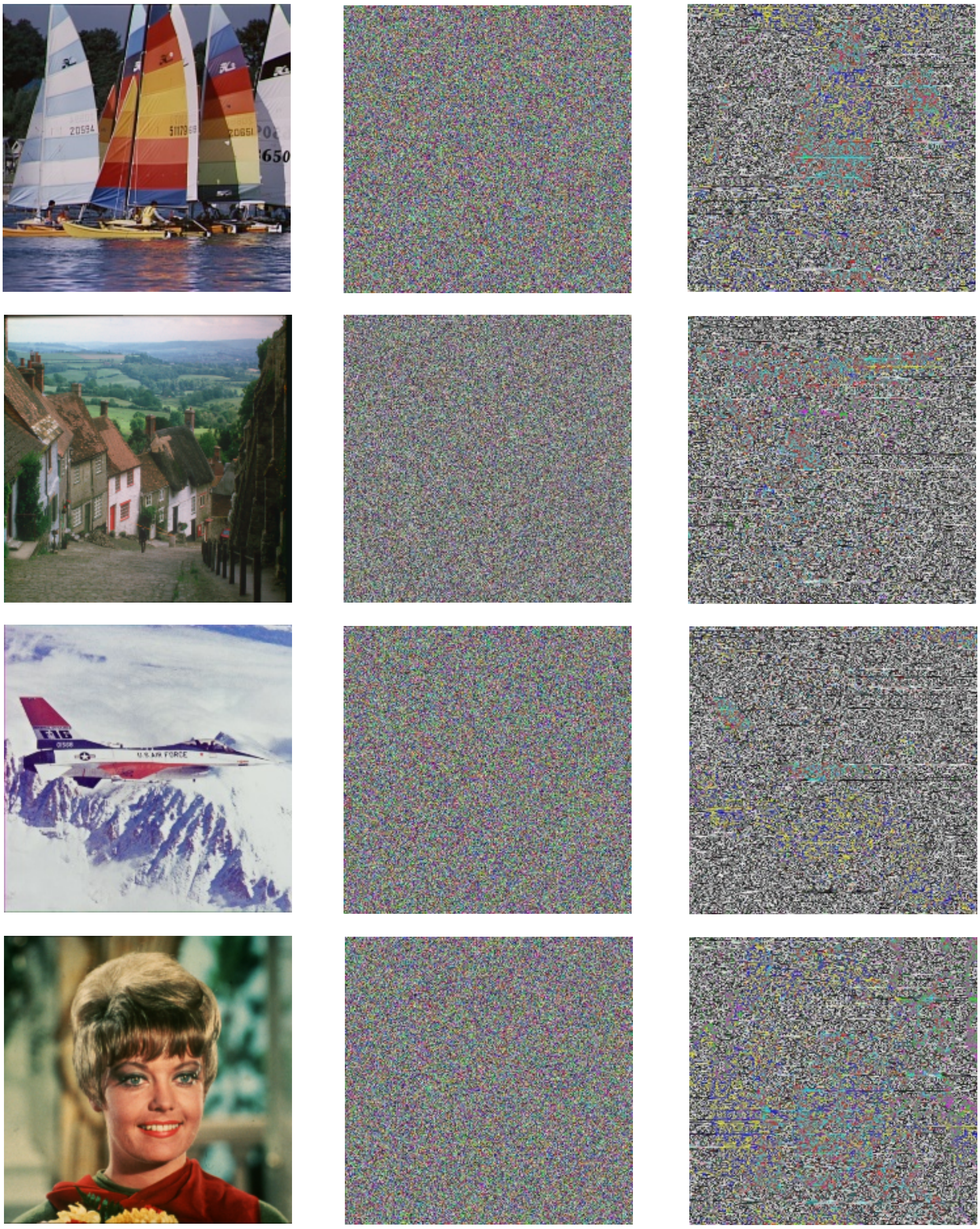
As described in Figure 3, the input of the system is an encrypted colour image while the output is a readable original colour image. Likewise, the encrypted image of size $M \times N$ will first be split into three different color channels and three grayscale images will be obtained. After that, inverse XOR operation will be performed followed by inverse permutation to relocate all the pixels back to the original positions. The final decrypted image will be obtained by combining three different grayscale images back together.

3. Results

This section discusses how the test results are evaluated and analyzed. The selected images are colour images that are of standard and same file types and dimensions which are PNG file format and dimension of 512 x 512 respectively. Table 1 shows the original, encrypted images obtained from the proposed system and existing method.

Table 1
Output cipher images of selected input images for proposed system and existing system

Original image	Encrypted image (proposed method)	Encrypted image (existing method)
		
		
		
		



3.1 Differential Attack Analysis

Number of Pixels Change Rate (NPCR) is used for defining the changing rate of the number of pixels of the encrypted image while calculating the percentage difference in pixel numbers of the encrypted image. Unified Average Changing Intensity (UACI) is used to compare the pixel values between the encrypted images and calculate the average difference in intensity. Both metrics help to assess the security of image encryption and evaluate the strength of the encryption scheme. The calculation formulas are described as follows [21]:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{8}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%. \tag{9}$$

where Eq. (8) expresses the formula of NPCR while Eq. (9) represents the formula of UACI. In both equations, the character $M, N \in \mathbb{N}$ represent the dimensions of the images, with M denotes the number of rows in the image and N denotes the number of columns in the image. The character i and j represent the positions of pixels in the image. $D(i,j)$ is the total number of differing pixels between the original image and encrypted image while $C_1(i,j)$ and $C_2(i,j)$ represent the intensity values of pixel (i,j) of the plain image and cipher image respectively. There are two conditions where: if $D(i,j) = 0$, then $C_1(i,j) = C_2(i,j)$; whereas if $D(i,j) = 1$, then $C_1(i,j) \neq C_2(i,j)$.

Table 2
NPCR analysis results

Image	NPCR (%)	
	Proposed method	Existing method
Lenna	99.6070	99.6059
Baboon	99.6042	99.6087
Barbara	99.6081	99.6067
Pepper	99.6168	99.5958
Yacht	99.6187	99.6138
Goldhill	99.6094	99.6077
Airplane	99.6231	99.6156
Zelda	99.6221	99.6052
Average	99.6137	99.6074

From Table 2, it can be seen that the obtained average NPCR values for both encryption methods are greater than 99.5% which implies that a larger percentage of pixel changes between the input image and output image, where the position of pixels has been randomly changed and shuffled.

Table 3
UACI analysis results

Image	NPCR (%)	
	Proposed method	Existing method
Lenna	33.1496	30.3764
Baboon	29.5224	29.2634
Barbara	29.1948	29.8163
Pepper	29.0281	31.2784
Yacht	32.5116	30.9835
Goldhill	31.4649	30.6821
Airplane	31.9946	30.5892
Zelda	30.4355	30.6251
Average	30.9127	30.4518

As shown in Table 3, the UACI values are within an acceptable range, which is between 29% to 33%. This suggests that the encrypted image has larger average intensity change compared to the original image, suggesting that the encrypted image has more visible differences from the original image.

3.2 Information Entropy Analysis

Image information entropy analysis is used to measure the randomness of the distribution of data in the image, hence commonly used to measure the security level of the encryption scheme. The image information entropy value is calculated from the aspect of the average number of bits required to represent each symbol in the data. Consider that an image contains N different values with i represents the pixel position within the image, the mathematical formula of the entropy, $H(s)$ can be expressed as follows [21]:

$$H(s) = -\sum_{i=0}^{N-1} p(s_i)\log_2[p(s_i)]. \tag{10}$$

where the set of values are represented by s_i. Besides that, $p(s_i)$ represents the probability of s_i occurring in the distribution of image s.

Table 4
Information entropy analysis results

Image	Entropy value		
	Original image	Cipher image (proposed method)	Cipher image (existing method)
Lenna	6.9684	7.9993	7.9993
Baboon	7.6662	7.9992	7.9992
Barbara	7.5141	7.9994	7.9993
Pepper	7.05838	7.9994	7.9994
Yacht	7.6312	7.9992	7.9993
Goldhill	6.2138	7.9993	7.9993
Airplane	7.5267	7.9992	7.9992
Zelda	7.8141	7.9993	7.9993
Average		7.9993	7.9993

As shown in Table 4, the information entropy value of the cipher images for both proposed encryption scheme and existing encryption scheme locate between 7.9992, 7.9993, and 7.9994, with an average value of 7.9993. As the obtained entropy value is high and is close to the theoretical value, it indicates that the output encrypted images appear to be random, complex, and unpredictable. Hence, it can be deduced that both systems have high performance in terms of security as the cipher images produced by both schemes are less predictable and contain more information.

3.3 Correlation Coefficient Analysis

Correlation coefficient analysis is used to measure the correlation of two adjacent pixels between the input original image and the output encrypted image. To evaluate the correlation coefficients, the following mathematical calculations can be applied [21]:

$$\rho_{xy} = \frac{conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{11}$$

where,

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{12}$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i, \tag{13}$$

$$conv(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}), \tag{14}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2, \tag{15}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2\ . \tag{16}$$

with $x, y \in \mathbb{Z}$ are the two adjacent pixels in the image while N is the total number of pixels chosen from the image. From all the equations listed, Eq. (11) is the correlation between the adjacent pixels with the symbol $\rho_{x,y}$ represents the correlation coefficient. Eq. (12) represents the calculation of convolution between the pixels x and y. Besides that, Eq. (13) and Eq. (14) denote the means of x and y respectively, whereas Eq. (15) and Eq. (16) represent the standard deviations of x and y respectively.

Table 5 shows the correlation coefficient between original images and encrypted images for both proposed and existing systems.

Table 5
Correlation coefficient analysis results

Image	Correlation coefficient	
	Proposed method	Existing method
Lenna	-0.002252	0.003338
Baboon	-0.003854	0.000050
Barbara	-0.001908	-0.002094
Pepper	-0.000473	-0.003825
Yacht	-0.003714	-0.005481
Goldhill	-0.001001	-0.006317
Airplane	0.000591	-0.002759
Zelda	-0.002560	-0.004772

As can be seen from the experimental results, the correlation coefficients for both encryption schemes are close to 0, indicating low linear relationships between the original image and the encrypted image, making it difficult for an observer to tell the exact information about the original image from the encrypted one.

Nevertheless, when we compare the correlation coefficients between two different encryption methods, it can also be seen that the correlation coefficients of the proposed system are closer to 0 compared to the correlation coefficients of the existing system. The difference between the encryption algorithms suggests that the system with lower correlation coefficients is more resistant and robust against visual analysis and attacks.

4. Conclusions

On a final note, the proposed chaotic-based encryption and decryption algorithm which joint the Lorenz chaotic map and Chen chaotic map is demonstrated to be an effective system for encrypting and decrypting colour images. The proposed scheme is also proven to have satisfied all the security tests and analysis, thus resulting in a system that gives high performance in security and robustness against cryptanalysis attacks. When the proposed scheme is compared to the existing method that uses only a single chaotic map for encryption, the proposed method can be seen to produce encrypted images that exhibit more random and complex behaviours. This shows that the proposed system that uses more than one chaotic system for encryption is more of a better option as compared to the encryption scheme that uses only one chaotic map as it is more secure and resistant to different kinds of attacks.

Acknowledgement

All authors would like to thank anonymous reviewers for all their constructive comments and recommendations for the betterment of this paper. This study is financially supported by Universiti Malaysia Sabah through the Research Grant SBK0508-2021.

References

[1] Gopalakrishnan, Rajasree, and Retnaswami Mathusoothana Satheesh Kumar. "Cloud Security System for ECG Transmission and Monitoring Based on Chaotic Logistic Maps." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 39, no. 2 (2024): 1-18. https://doi.org/10.37934/araset.39.2.118

[2] Aung, Pyi Phyo, Nordinah Ismail, Chia Yee Ooi, Koichiro Mashiko, Hau Sim Choo, and Takanori Matsuzaki. "Data Remanence Based Approach towards Stable Key Generation from Physically Unclonable Function Response of Embedded SRAMs using Binary Search." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 35, no. 2 (2024): 114-131. https://doi.org/10.37934/araset.32.3.178189

[3] Younes, Mohammad Ali Bani. "A Survey of The Most Current Image Encryption and Decryption Techniques." *International Journal of Advanced Research in Computer Science* 10, no. 1 (2019). https://doi.org/10.26483/ijarcs.v10i1.6350

[4] Bütz, Michael R. "Chaos theory, philosophically old, scientifically new." *Counseling and Values* 39, no. 2 (1995): 84-98. https://doi.org/10.1002/j.2161-007X.1995.tb01012.x

[5] Thanki, Rohit, Surekha Borra, Rohit Thanki, and Surekha Borra. "Technical Information." *Medical Imaging and its Security in Telemedicine Applications* (2019): 11-21. https://doi.org/10.1007/978-3-319-93311-5

[6] Kaur, Mandeep, Surender Singh, and Manjit Kaur. "Computational image encryption techniques: a comprehensive review." *Mathematical Problems in Engineering* 2021 (2021): 1-17. https://doi.org/10.1155/2021/5012496

[7] Lorenz, Edward N. "Computational chaos-a prelude to computational instability." *Physica D: Nonlinear Phenomena* 35, no. 3 (1989): 299-317. https://doi.org/10.1016/0167-2789(89)90072-9

[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] Zhang, Jian. "An image encryption scheme based on cat map and hyperchaotic lorenz system." In *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, pp. 78-82. IEEE, 2015. https://doi.org/10.1109/CICT.2015.134

[10] Zhou, Ri-Gui, and Ying-Bin Li. "Quantum image encryption based on Lorenz hyper-chaotic system." *International Journal of Quantum Information* 18, no. 05 (2020): 2050022. https://doi.org/10.1142/S0219749920500227

[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.v10n2a916

[12] Abundiz-Pérez, F., C. Cruz-Hernández, M. A. Murillo-Escobar, R. M. López-Gutiérrez, and A. Arellano-Delgado. "A fingerprint image encryption scheme based on hyperchaotic Rössler map." *Mathematical Problems in Engineering* 2016 (2016). https://doi.org/10.1155/2016/2670494

[13] Guanrong, Chen, Mao Yaobin, and Charles K. Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos, Solitons and Fractals* 21 (2004). https://doi.org/10.1016/j.chaos.2003.12.022

[14] 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

[15] Zhao, Chaofeng, Tingzhong Wang, Haoyu Wang, Qinghui Du, and Chengwei Yin. "A novel image encryption algorithm by delay induced hyper-chaotic chen system." *J. Imaging Sci. Technol* 10501 (2023): 1. https://doi.org/10.2352/J.ImagingSci.Technol.2023.67.1.010501

[16] Arpacı, Batuhan, Erol Kurt, Kayhan Çelik, and Bünyamin Ciylan. "Colored image encryption and decryption with a new algorithm and a hyperchaotic electrical circuit." *Journal of Electrical Engineering & Technology* 15 (2020): 1413-1429. https://doi.org/10.1007/s42835-020-00393-x

[17] Luo, Yuling, Jia Lin, Junxiu Liu, Duqu Wei, Lvchen Cao, Ronglong Zhou, Yi Cao, and Xuemei Ding. "A robust image encryption algorithm based on Chua's circuit and compressive sensing." *Signal Processing* 161 (2019): 227-247. https://doi.org/10.1016/j.sigpro.2019.03.022

[18] Al-Musawi, Wisal Adnan, Wasan A. Wali, and Mohammed Abd Ali Al-Ibadi. "Field-programmable gate array design of image encryption and decryption using Chua's chaotic masking." *International Journal of Electrical and Computer Engineering* 12, no. 3 (2022): 2414. https://doi.org/10.11591/ijece.v12i3.pp2414-2424

[19] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps," *Math Comput Simul*, vol. 178, pp. 646–666, Dec. 2020, doi: 10.1016/j.matcom.2020.07.007. https://doi.org/10.11591/ijece.v12i3.pp2414-2424

[20] Alhawarat, Mohammad, Waleed Nazih, and Mohammad Eldesouki. "Studying a chaotic spiking neural model." *arXiv preprint arXiv:1310.7115* (2013). https://doi.org/10.5121/ijaia.2013.4508

[21] Ge, Bin, and Hai-Bo Luo. "Image encryption application of chaotic sequences incorporating quantum keys." *International Journal of Automation and Computing* 17, no. 1 (2020): 123-138. https://doi.org/10.1007/s11633-019-1173-z