Journal of Applied Multimedia and Networking (JAMN)
Vol.8, No.1, July 2024, pp. 01~08
e-ISSN: 2548-6853

Image Encryption Using Combination Of Chaotic System

Festy Winda Sari* , Ummi Aisha Ibrahim**
* Informatics Engineering, Batam State Polytechnic
** Cyber Security, Swansea University

Article Info

Article history:

Received May 12th, 2024
Revised Jun 20th, 2024
Accepted Jul 6th, 2024

Keyword:

Image Encryption
Chaos-based
Logistic Map
Lorenz System
Permutation
Substitution

ABSTRACT

These days, image encryption relies on chaos-based theory. Encrypting and decrypting images using random sequences is becoming increasingly popular. Accordingly, this study proposes a method of image encryption based on the Logistic Map and Lorenz System. The encryption and decryption process involves permutation and substitution steps. A permutation is performed using the Logistic Map, which is used for leading randomness of pixels through confusion, while the diffusion process is finished using the Lorenz System. Afterwards, the substitution is performed by bitwise-XORing the value. Throughout the permutation process, the value of the original image's red, green, and blue (RGB) channels will be swapped amongst each and then sent to the next stage, i.e., diffusion. The diffusion process involves changing the values of pixels of the original image. The disturbance in plain images will increase when pixel and bit levels are changed, usually called cypher images. A study will evaluate the effectiveness of chaos-based security and the time cost of key processes. Furthermore, we will investigate the relationship between contiguous pixels.

Corresponding Author:

Ummi Aisha Ibrahim
Cyber Security,
Swansea University
Singleton Park, Swansea, SA2 8PP, Wales, UK

1. INTRODUCTION

Data and information communications are an essential component of our daily existence and a significant asset to any individual or organisation in the current technological age. A growing amount of multimedia data is being exchanged over open networks and the internet, which calls for a secure and reliable way to ensure confidentiality and prevent unauthorized access to transferred files. Confidentiality can be achieved by encrypting the transformed image into a specific structure that only those with the key can interpret. On the other hand, a lack of security puts information at risk of being stolen. However, to solve the problem, chaos-based encryption has been researched massively to encounter the growing need for secure online media communication over the network.

Unlike text encryption, image encryption requires different cryptographic techniques to protect. Further, the inherent characteristics of images have led to their enormous size, volume, and redundancy of data, which make conventional block cyphers unsuitable for encrypting them. Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Shamir Adelman (RSA) are the conventional cryptographic techniques used for image encryption. In the encryption of digital images and high computational, the traditional encrypting mechanisms mentioned before are suffering from some shortcomings and weaknesses. The image size is enormous, and the redundancy and correlation between adjacent pixels are also very high [1]. That means it needs a high power to compute a vast image and takes a long time to store and process the encryption.

Furthermore, the encoding and decoding process needs much effort regarding the massive amount of data and converting image format is also tricky. Thus, the file header and control information should not be encrypted in image encryption [2]. Similarly, text-processing algorithms are usually very slow, making them unusable for real-time applications. Chaos-based systems are ideal when it comes to making encryption algorithms for images. Chaos-based random properties make them perfect for encrypting images. Thus, chaos-based schemes have proven superior to traditional encryption schemes in terms of performance and security due to utilising variable keys to enhance privacy and security. Specific chaos-based systems have essential properties, such as initial parameters, pseudorandom properties, and non-periodicity. As a result, the original image is transformed into a more complex form, making it complicated encryption to crack.

Chaos-based encryption process consists of two phases, i.e., confusion and diffusion [3]. In the first stage, the position of pixels will be randomly shuffled to disrupt the interconnection of contiguous pixels. The result is that the picture will not be able to identify as before. However, an attacker can still retrieve the picture, so the next phase is needed. Essentially, image encryption algorithms aim to boost pixel entropy and drop correspondence between them. The value of image entropy represents the randomness of pixels. Hence, an encrypted image needs a more significant matter of image entropy. Meanwhile, correlation coefficients show the similarity between adjacent pixels at various angles, which means that low correlation coefficients are preferred.

The proposed image encryption algorithm takes advantage of the Logistic Map and Lorenz System. Logistic Maps are often used to prove how complex the behaviour of chaotic maps is generated from simple nonlinear equations. The Logistic Map is parameterised by discrete time while the Lorenz System is continuous. Additionally, the encryption and decryption process involve permutation and substitution steps. The purpose of the permutation process is to destroy the mutual relationship of pixels from plain images by randomly spreading the pixels along the cypher image.

On the other side, the substitution process works through nonlinear functioning and a pseudorandom number generator (PRNG) to reduce the connection between the original image and the cypher image. PRNGs can be deliberated using chaotic systems or curve shapes [1]. In most cases, the encryption technique can be achieved the best security by performing both permutation and substitution stages. A permutation stage enhances the differential attack measures, and assists escalate the computational severity of attack that might be possible in the future, making the encryption scheme more wrinkled or not sensible to crack. A substitution stage is done to randomise the looks of the cypher image and exceed numerous evaluation criteria. Therefore, an encryption scheme that combines permutation and substitution will likely meet all the encryption evaluation standards and presumably can get through the NIST test [1].

A permutation is performed using Logistic Map, which is used for leading randomness of pixels through confusion while diffusion process is finished using Lorenz System, afterwards the substitution is performed by bitwise-XORing the value. Throughout the permutation process, the value of red, green, and blue (RGB) channels of the original image will be swapped amongst each and sent to the next stage, i.e., diffusion. The diffusion process involves changing the values of pixels of the plain picture. The amount of disturbance in original images will increase when pixel and bit levels are changed, usually called cypher images.

2. RESEARCH METHOD

2.1 CHAOTIC SYSTEMS

The chaotic system can be applied to change the grey values by rearranging the pixels and to randomise the pixel positions by generating pseudorandom sequences [13]. Images can be encoded to make them challenging to decrypt because the cypher text is randomly generated using a chaosbased system. Chaos-based encryption is an essential property of this recent digital era in protecting our data from unauthorised access and other attacks. In the case of an original image being transformed, this increases the difficulty of unauthorised encryption cracking. This section will explain the character of the Logistic Map and Lorenz System in terms of performing permutation and substitution in image encryption.

2.1.1 LOGISTIC MAP

Image data consist of adjacent pixels linked to each other. According to statistical analysis of large numbers of images, the pixels are connected to each other on every side, i.e., horizontal, vertical, and diagonal and they are associated with both natural and artificial images. In order to eliminate the correspondence, the Logistic Map is performed to swap the positions of the pixels in the plain image. Logistic Maps are commonly used to encrypt images for fast computations and to deliver the pseudorandom number—the Logistic Map analyses discrete time steps through a nonlinear difference equation. Mathematically, the equation is represented as Equation (1).

$$\boldsymbol{x(n+1) = rxn(1 - xn)} \qquad \textbf{Eq 1}$$

In the bifurcation process, r is a parameter known as a control parameter, which ranges between 0 and 4. The control parameter is considered in areas where the parameter is dependent on r, and Figure 1 shows that r is [1,4]. A sequence of the Logistic Map is greatly chaotic if the value of r is in the range 3.5-3.9999. Equation 1 generates the sequence by selecting appropriate initial and parameter values of X0 and r. The result is that each of the generated sequences appears to be random. In the process, the sequence generated from Logistic Map {Xn+1} = {X0, X1…...Xn} where length n=M×N, the initial value is X0 = [0,1], and the parameter value is r=3.9999 is chosen.

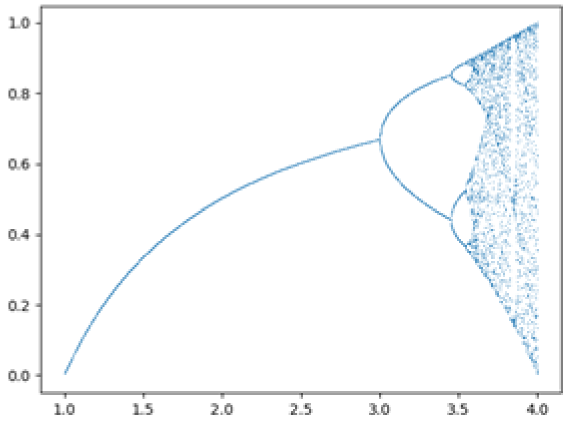


Figure 1. Bifurcation diagram of the Logistic Map

In the permutation process, the map is projected for NxN iterations for each size block. Assembling the permutation matrix for this block requires sorting the output in ascending order. A Logistic Map has one parameter exists i.e., r, X0 is used as an initial value.

In this step, the algorithm of the Logistic Map will reorder each pixel in the image. The result is expected to complicate the correlation amongst the adjacent pixel, so the image is unrecognizable.

2.1.2 LORENZ SYSTEM

The Lorenz System has complicated dynamic properties and multiple state variables that make it the best to use in the encryption process. However, encryption based on the Lorenz System has stronger unpredictability and larger keyspace, providing excellent random sequences suitable for information encryption [11]. A Lorenz equation represents the thermally induced convection of fluid in the atmosphere. The method was first submitted and published by E.N Lorenz in 1963 [14]. Lorenz System is speculated as a classically chaotic system and as the source of the butterfly effect in many scientific studies from the consequences of the fact that the attractor has two wings like butterflies [15]. This has led to widespread research into chaos theory, modelling the system dynamic, chaos control, and synchronization.

The pixel values are modified sequentially in the diffusion stage to prevent the plain image from unauthorized access and attack. In the Lorenz System, the initial parameters and conditions determine whether there are chaotic solutions to ordinary differential equations. However, the Lorenz attractor is a chaotic physical system if optimal initial conditions are not fully known (even the slight disturbance of air caused by a butterfly flapping its wings). There will always be a failure to predict its future course.

$$\frac{dx}{dt} = \alpha(y - z)$$

$$\frac{dy}{dt} = x(\delta - z) - y$$

$$\frac{dz}{dt} = xy - \beta z$$

Eq 2

In Equation (2), α, β, δ are Lorenz System parameters control the attractor and bifurcation of the system. Default values for system parameters are 10, 28 and $\frac{8}{3}$ respectively.

2.2 ENCRYPTION METHOD

Image encryption using permutation and substitution steps generally shows safe and has an optimal security [17]. A substitution stage works to bring the cypher image unrecognisable and get through every evaluation criterion, while a permutation stage can increase the differential attack fortress. Another benefit of permutation is that it makes the encryption scheme more intricated, which helps increase the complexity of defending against attacks. Hence, permutation and substitution phase are good to improve all the assessment specification related to encryption. In this study, the encryption process involves permutation and substitution steps to get the best security, as mentioned above. The detailed image encryption is described in Figure 2.

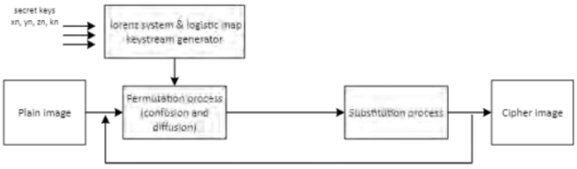

secret keys
xn, yn, zn, kn
lorenz system & logistic map keystream generator
Plain image
Permutation process (confusion and diffusion)
Substitution process
Cipher image

Figure 2. Encryption approach

In the permutation phase, the confusion and diffusion processes are repeated R times to break the correlated adjacent pixel to generate a cypher image. In the earlier stage, a Lorenz System is used in the mixing process aims to get a low-quality image before the permutation process. The original image is masked with a randomly generated mixing process. Afterwards, the permutation process is repeated using a Logistic Map algorithm until the maximum-security level is achieved. The composite image will be converted to a binary sequence size of MxNx8. Figure 2 shows xn, yn, zn, and kn are the secret keys that will be used for the permutation step.

From Figure 2, a detail of the encryption process is described as follows:

Step 1: Secret key is generated from Eq 1 and Eq 2. Afterwards, perform the mixing process to generate an integer sequence.

Step 2: The original image pixels are converted into integer sequences.

Step 3: Convert the generated image from the mixing process into a binary image to start the permutation process by shifting the bits of mixed images.

Step 4: Random binary sequences spread permuted image pixel bits across the pixels.

Step 5: Substitute the permuted image to create a cipher image.

2.3 DECRYPTION METHOD

The encryption process will be inverted to get the original image from the encrypted image. The secret keys will be shifted through a closed channel between the end-users.

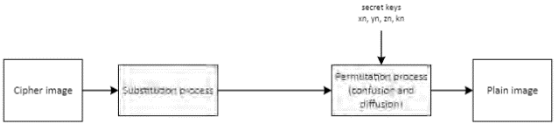


Figure 3. Decryption process

As shown in Figure 3, cipher image will encounter the substitution process first and then confusion and diffusion process thereupon. Secret keys will be used to validate the process amongst the image to get the original image.

3. RESULTS AND ANALYSIS

All the technical step about the research will be given in this section. It consists of user interface and result evaluation. The encryption and decryption methods, however, is already given in the previous chapter. To support analysis in this study, seven pictures were given to be tested. Five images were taken from common test image website, while other two were taken from author’s device.

3.1 Correlation Coefficient

In order to reduce this kind of correlation as much as possible, good image encryption should reduce this correlation significantly. Table 2 shows the correlation coefficient from the proposed scheme for original and encrypted image.

Table 1. Correlation coefficient results

Test Image	Original Image	Encrypted Image
Baboon (500 x 480)	0.923	-0.0194
Cameraman (256 x 256)	0.852	0.0685
Flower (512 x 480)	0.986	0.0488
Lena (512 x 512)	0.973	-0.0066
Pepper (512 x 512)	0.988	-0.0802
Draw (612 x 427)	0.971	-0.0105
Newyear (612 x 427)	0.875	-0.0022

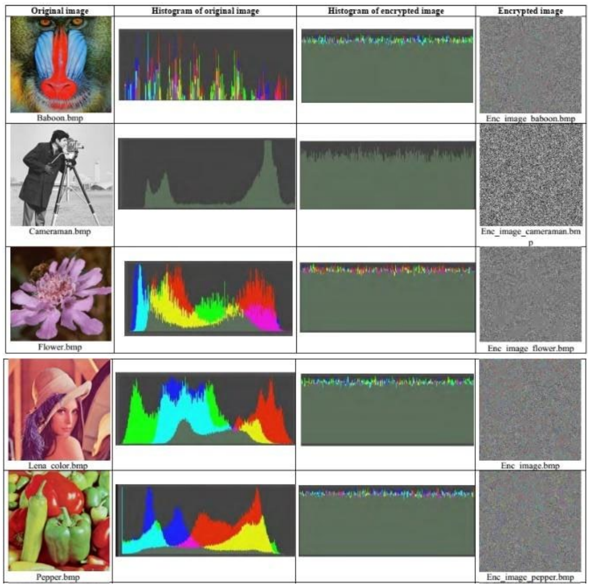
As shown in the table 1, at first, the number shows very nearly one (1). That indicates the distribution of the adjacent pixels in the original image stipulates a high connection between each pixel. In contrast, the encrypted image shows that the relationship between each pixel on all sides is displayed remarkably down, all the results are there about equal to zero, which means the connection is low.

3.2 HISTOGRAM ANALYSIS

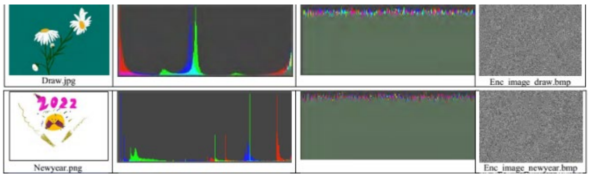
The histogram contains the statistical characteristics of a certain image. Attackers might use it to extract image information since it exhibits the distribution of the concentration level of the grey pixel. A histogram depicts the allocation of color values over an entire image, where certain colors appear to have curves and peaks. It is expected that this distribution will be flat for images that are strongly encrypted.

Table 2 below shows the comparison of the original and encrypted images, and notice how the histograms are relatively uniform.

Table 2. Histogram analysis of original and encrypted image



Original image	Histogram of original image	Histogram of encrypted image	Encrypted image
Baboon.bmp			Enc_image_baboon.bmp
Cameraman.bmp			Enc_image_cameraman.bmp
Flower.bmp			Enc_image_flower.bmp
Lena_color.bmp			Enc_image.bmp
Pepper.bmp			Enc_image_pepper.bmp



3.3 Differential Attack

The encryption scheme is sensitive even to minuscule changes in plain images (by a single bit), which makes it effective in protecting sensitive information. In addition, even a one-bit change on the original image can head to a completely distinct encrypted image. It implies that the proposed encryption scheme can stand firm against differential attacks. There are two common criteria to measure vulnerability of the differential attacks, i.e., the number of pixels changes rate (NPCR) and the unified average changing intensity (UACI) [12].

NPCR and UACI can be mathematically determined by Equation 7 and 9 [19]:

$$NPCR(C1,C2) = \sum_{i,j} \frac{D(i,j)}{H \times W} \times 100\%$$

Eq 3

Where,

$$D(i,j) = \begin{cases} 1, & if\ C1 \neq C2 \\ 0, & if\ C1 = C2 \end{cases}$$

$$UACI(C1,C2) = \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255 \times H \times W} \times 100\%$$

Eq 4

When carrying out differential attacks, NPCR focuses on the absolute number of pixels that change the value, whereas UACI is concerned with the average difference between two paired ciphertext images. The ideal number for UACI is ≥33%, while the ideal number for NPCR is ≥99%.

Table 3. NPCR & UACI value of tested image

Images	**NPCR (%)**	**UACI (%)**
Baboon (500 x 480)	96,1	48,5
Flower (512 x 480)	79,6	33,7
Lena (512 x 512)	205,4	91,3
Pepper (512 x 512)	109,5	37,6
Draw (612 x 427)	113,1	82,3
Newyear (612 x 427)	49,1	5,8

Table 3. illustrates the values of NPCR and UACI of the proposed method. From seven colour images that has been tested, there are three images which give unexpected result less than 99%; Baboon (500 x 480), Flower (512 x 512), and Newyear (612 x 427). However, more than 50% of the images give outstanding results of the NPCR ideal value of 99%, which means the algorithm works in some cases. There are several factors that could lead the three images have low NPCR values, such as the distribution of RGB colour is uneven, one colour has dominantly appeared, and other things. Thus, further research is needed to identify the reason.

On the other side, almost all UACI values fall within the acceptable range. Only one picture has given the very low value, i.e., Newyear (612 x 427). The results demonstrate that the encrypted image scheme obtained is highly random. Thus, the proposed technique is proven superior to be referred in this study.

Furthermore, UACI values are also within a reasonable range and can be used in other schemes. In conclusion, the scheme is capable of countering differential attacks.

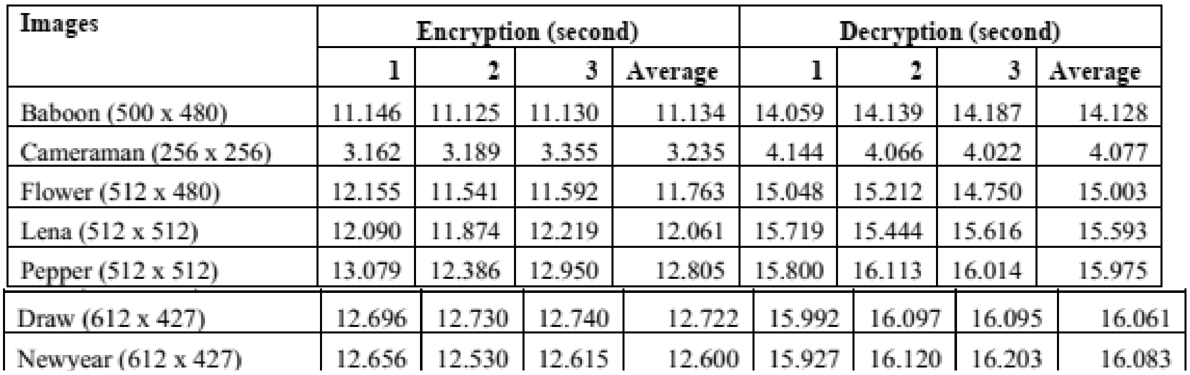
3.4 TIME COST

Several conditions have been considered for calculating the encryption and decryption process time, such as hardware specification and software running in the background.
The hardware specifications used in the encryption and decryption process are:

Brand	: Dell
Processor	: Intel(R) Core (TM) i5-8265U CPU @ 1.60GHz (8 CPUs)
Memory	: 16 GB RAM

While executing the encryption and decryption process, some software is running at the same time; Chrome, Spotify, and Microsoft One Drive. Thus, this software affects the processor in carrying out the proposed process. Time of encryption and decryption process is shown in Table 4. below.

Table 4. Time Analysis of encryption and decryption process



Images	Encryption (second)				Decryption (second)			
	1	2	3	Average	1	2	3	Average
Baboon (500 x 480)	11.146	11.125	11.130	11.134	14.059	14.139	14.187	14.128
Cameraman (256 x 256)	3.162	3.189	3.355	3.235	4.144	4.066	4.022	4.077
Flower (512 x 480)	12.155	11.541	11.592	11.763	15.048	15.212	14.750	15.003
Lena (512 x 512)	12.090	11.874	12.219	12.061	15.719	15.444	15.616	15.593
Pepper (512 x 512)	13.079	12.386	12.950	12.805	15.800	16.113	16.014	15.975
Draw (612 x 427)	12.696	12.730	12.740	12.722	15.992	16.097	16.095	16.061
Newyear (612 x 427)	12.656	12.530	12.615	12.600	15.927	16.120	16.203	16.083

As shown in the Table 4, the encryption process was carried out three times. The average time is taken to determine the encryption and decryption time. A final check is made on the time complexity of the proposed method. This scheme is applied to a few images of various sizes, and their different sizes are taken into consideration.
Amongst all images that have been tested, they give almost the same result for encryption an decryption time cost except for Cameraman (256 x 256). While the others provide around 11-13 seconds, those two smallest images offer only 3 and 0.9 seconds, respectively, regarding its size and the colour complexity.

4. CONCLUSION

The purpose of this study is to present a combination of chaotic systems in digital image encryption techniques, specifically, Logistic Map and Lorenz System, as a means of encrypting digital images. The initial conditions for both the Logistic Map and Lorenz System are given regarding generating the keys used in the permutation and substitution process. The encryption method involves permutation pixels, spreading their locations, diffusing pixel values, and substituting the pixel values by bitwise-XOR of the equation.

Several analysis techniques are performed due to support the study, which includes histogram analysis, correlation coefficient calculation, NPCR and UACI measurements, and time cost analysis. Several attacks are also given to the research to find the robustness of the algorithm against miscellaneous things in the future; salt-and-pepper and speckle noise are two methods used in attack trials.

According to the theoretical analysis and experiments, the proposed algorithm achieves a more excellent chaotic range and uniform distribution of chaotic sequences than a single chaotic map. A security analysis has shown that the algorithm is successfully restrain differential attacks. Even though some cases give unexpected results in NPCR and UACI values, the proposed algorithm generally works well and can be used to transmit the image safely. As well as the time cost, encryption and decryption processing time are expected be able to compete with similar algorithms.

REFERENCES

[1] J. Zhang, "An image encryption scheme based on cat map and hyperchaotic Lorenz System," in Proceedings - 2015 IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2015, Apr. 2015, pp. 78–82. doi: 10.1109/CICT.2015.134.

[2] J. Zhang, D. Fang, and H. Ren, “Image encryption algorithm based on DNA encoding and chaotic maps,” Math Probl Eng, vol. 2014, Dec. 2014, doi: 10.1155/2014/917147.

[3] N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic Logistic Map,” Image Vis Comput, vol. 24, no. 9, pp. 926–934, Sep. 2006, doi: 10.1016/j.imavis.2006.02.021.

[4] A. A. Abdallah and A. K. Farhan, “A New Image Encryption Algorithm Based on Multi Chaotic System,” Iraqi Journal of Science, pp. 324–337, Jan. 2022, doi: 10.24996/ijs.2022.63.1.31

[5] V. Kumar and A. Girdhar, “A 2D Logistic Map and Lorenz-Rossler chaotic system based RGB image encryption approach,” Multimed Tools Appl, vol. 80, no. 3, pp. 3749–3773, Jan. 2021, doi: 10.1007/s11042-020-09854-x.

[6] J. Wang and L. Liu, “A Novel Chaos-Based Image Encryption Using Magic Square Scrambling and Octree Diffusing,” Mathematics, vol. 10, no. 3, p. 457, Jan. 2022, doi: 10.3390/math10030457.

[7] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, “Medical image encryption algorithm based on Latin square and memristive chaotic system,” Multimed Tools Appl, vol. 78, no. 24, pp. 35419–35453, Dec. 2019, doi: 10.1007/s11042-019-08168-x.

[8] A. G. Radwan, S. K. Abd-El-Hafiz, and S. H. Abdelhaleem, “Image encryption in the fractional-order domain,” 2012. doi: 10.1109/ICEngTechnol.2012.6396148.

[9] A. Girdhar and V. Kumar, “A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences,” Multimed Tools Appl, vol. 77, no. 20, pp. 27017–27039, Oct. 2018, doi: 10.1007/s11042-018-5902-z.

[10] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review,” Journal of Advanced Research, vol. 7, no. 2. Elsevier, pp. 193–208, Mar. 01, 2016. doi: 10.1016/j.jare.2015.07.002.

[11] E. Hato and D. Shihab, “Lorenz and Rossler Chaotic System for Speech Signal Encryption,” 2015.

[12] W. Zhou, X. Wang, M. Wang, and D. Li, “A new combination chaotic system and its application in a new Bit-level image encryption scheme,” Opt Lasers Eng, vol. 149, Feb. 2022, doi: 10.1016/j.optlaseng.2021.106782.

[13] K. Celik and E. Kurt, “A new image encryption algorithm based on Lorenz System,” Feb. 2017. doi: 10.1109/ECAI.2016.7861097.

[14] W. Song and J. Liang, “Difference equation of Lorenz System,” International Journal of Pure and Applied Mathematics, vol. 83, no. 1, pp. 101–110, 2013, doi: 10.12732/ijpam.v83i1.9.

[15] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez, “Encryption and decryption of images with chaotic map lattices,” Chaos, vol. 16, no. 3, 2006, doi: 10.1063/1.2242052.

[16] M. A. Zidan, A. G. Radwan, and K. N. Salama, “The effect of numerical techniques on differential equation based chaotic generators,” 2011. doi: 10.1109/ICM.2011.6177395.

[17] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review,” Journal of Advanced Research, vol. 7, no. 2. Elsevier, pp. 193–208, Mar. 01, 2016. doi: 10.1016/j.jare.2015.07.002.

[18] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI Randomness Tests for Image Encryption,” Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011.