Journal of Modern Computing and Engineering Research

JMCER

Volume 2024, p. 9-19
https://jmcer.org

A Two-Layer For Image Encryption Using Lorenz and Rossler Chaotic Systems

Asmaa Y. Albakri[1] and Oğuz Karan [2]

[1,2] Altinbas University, Software Engineering, Information Technologies, Istanbul, Turkey
[1] Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

[1] 213721732@ogr.altinbas.edu.tr
[2] oguz.karan@altinbas.edu.tr

Received: November 18, 2023 *Revised: February 17, 2024* *Accepted: February 19, 2024*

Abstract

Unauthorized access to images in the digital age requires robust encryption techniques. This paper introduces a new two-layer colour image encryption algorithm that uses the chaotic dynamics of the Lorenz and Rossler systems. By processing XOR by deciding with chaotic random integers (CRINs) derived from these systems, the algorithm achieves a high level of protection for colour images. Each layer of randomness and inherent sensitivity to the initial conditions of chaotic systems makes encryption stronger for colour images. The decryption in the second party follows the same steps of encryption, ensuring efficient recovery of the original image from the encrypted image. The built-in encrypted layers form a highly secure image that is resistant to various types of attacks and other important advantages, such as enhanced security and computational efficiency, making it suitable for protecting images in diverse applications.

Keywords: *Image encryption, chaotic systems, Stream and block ciphering, PSNR, SSIM, MSE*

1 Introduction

In these late decades, very big technological revolutions have taken place, which have changed many people's lifestyles. This is evident in the progress of computing, wireless smart devices, the Internet and various 5G networks and the interaction between them. The emergence of these technologies has coincided with the boom in the multimedia industry, which sees millions of data transfers per second between computers, mobile phones and other smart devices. Consequently, scientists, mathematicians, and engineers face ongoing challenges to devise creative methods for securing data during its transmission between any two communication entities. This crucial security was formerly primarily supplied by several techniques. These included the triple DES algorithm (3DES), the Advanced Encryption Standard (AES), and the Data Encryption Standard (DES) (AES). Although they used to be good at securing data, they need to be more secure for photo encryption. This is because these techniques could be more efficient for picture encryption or be vulnerable to cryptanalysis. Images, in comparison to textual data, have a variety of characteristics that need the use of distinct encryption techniques. Data payloads for things like high-definition (HD) photographs are pretty large. In addition, there is a significant degree of repetition and connection between neighbouring image pixels (Alexan et al., 2021).

An analysis of the existing literature on picture encryption supports Shannon's theory, which states that the use of two distinct encryption stages—confusion and diffusion is required to provide a high level of image security (Anderson, 2008). Every bit of an encrypted picture is made to rely on various pieces of the key during the confusion stage, which obscures the relationship between the image and the key (Shannon C.E. & Shannon, 1949). A single bit in the plain image would cause a change in nearly half of all the bits in the encrypted image due to the avalanche effect created by the diffusion step. Diffusion in encryption eliminates any statistical association between an image's original and encrypted versions (H. A. Abdullah & Mohammed, 2022).

Chaotic functions have a role in the design of those two phases of encryption. Several features of chaotic processes make them useful in the context of communication security (H. N. Abdullah et al., 2022). These characteristics include sensitivity to initial values, ergodicity, pseudo-randomness, control parameters, and periodicity. (Hreshee et al., 2018). Chaotic functions are frequently divided into lower-dimensional (1D) and higher-dimensional (2D) categories (MD). When utilizing 1D or MD chaotic functions for picture encryption, there is always a trade-off between complexity and security. The Encryption of digital images using the signals of chaotic is separated into three parts: the first part involves changing the pixel's locations, the second part represents the changing the pixel's values, and the third part involves mixing the positions and values of pixels at the same time (Mansoor et al., 2021).

- The main contributions: In this study, two-layer image encryption using chaotic Lorenz and Rossler systems was proposed to generate chaotic random integers (CRINs), these CRINs are XORed by bits with image pixel values. Merging encrypted layers from both messy systems results in the encrypted image. Decryption reflects these processes, starting with Rossler and then Lorenz.
- Research Question: Can a two-layer image encryption algorithm utilizing the Lorenz and Rossler chaotic systems provide robust security for colour images, offering high resistance to attacks, computational efficiency, and suitability for real-time applications.
- Evaluation Methods: in this paper, the evaluation methods are divided into three types: (Security analysis) describes the metrics used to evaluate the security of the encrypted image, such as entropy, correlation coefficient, Peak Signal-to-Noise Ratio (PSNR), etc. (Performance analysis) explain how the computational efficiency of the encryption and decryption processes is measured, such as execution time. Finally (Comparison with other methods) describe how the proposed algorithm compares to existing image encryption methods in terms of security, performance, and other relevant aspects.
- Limitations: the chaotic systems depend on the careful selection of parameters and initial values. Choosing inappropriate values can cause the system's behavior to shift from chaotic to periodic or unknown, potentially impacting the algorithm's security and encryption efficiency. Additionally, despite the theoretical notion of an infinite number of encryption keys with chaotic systems, the practical sensitivity to initial conditions is finite.

We strongly encourage authors to use this document for the preparation of the camera-ready. Please follow the instructions closely in order to make the volume look as uniform as possible (Moore and Lopes, 1999).

Please remember that all the papers must be in English and without orthographic errors.

Do not add any text to the headers (do not set running heads) and footers, not even page numbers, because text will be added electronically.

For a best viewing experience, the used font must be Times New Roman, on a Macintosh use the font named times, except on special occasions, such as program code (Section 2.3.7).

2 Chaotic Definition And Types

Chaotic, essentially nonlinear systems display behavior that appears random over a specific range of system parameter values. Nevertheless, the system's solutions or trajectories are still constrained inside the phase space. The parameter settings and the starting conditions significantly impact this unstable state (Mahdi, Jawad, and Hreshee 2016). There are two types of chaotic systems: those described by different equations, and maps, and those described by differential equations, or flows (Abdullah, Hreshee, and Jawad 2015). Two chaotic systems are used in this paper, the Lorenz and Rossler systems.

2.1 Lorenz System

A meteorologist and mathematician, Edward Lorenz was the first to examine the Lorenz system, a collection of ODEs (Ordinary Differential Equations). In 1963, a simpler mathematical model of atmospheric convection was developed. The model consists of three ordinary differential equations called Lorenz equations. (Abdullah, Hreshee, and Jawad 2015),(Ameer K. Jawad, Wa'il a. H. Hadi, and Hyayder F. Y. Husseain 2016).

$$\dot{\boldsymbol{x}} = \boldsymbol{\sigma}(\boldsymbol{y} - \boldsymbol{x}) \tag{1}$$

$$\dot{\boldsymbol{y}} = \boldsymbol{rx} - \boldsymbol{y} - \boldsymbol{xz} \tag{2}$$

$$\dot{\boldsymbol{z}} = \boldsymbol{xy} - \boldsymbol{bz} \tag{3}$$

Where the $\dot{x}, \dot{y}$ *and* $\dot{z}$ There are the vector of states for the Lorenz system, known as the Lorenz system. The Lorenz system parameters σ, r, and b are used to raise chaotic dynamics and should meet (Abdullah et al. 2022; Hussein, Khashan, and Jawad 2020):

$$\boldsymbol{\sigma}\ ,\boldsymbol{r}\ ,\boldsymbol{b}\ > \mathbf{0} \tag{4}$$

$$\boldsymbol{\sigma} > \boldsymbol{b} \tag{5}$$

$$\boldsymbol{r} > \frac{\boldsymbol{\sigma}(\boldsymbol{\sigma}+\boldsymbol{b}+\mathbf{3})}{(\boldsymbol{\sigma}-\boldsymbol{b}-\mathbf{1})} \tag{6}$$

To demonstrate this equation *Let b* = 8/3, and σ = 10, according to the previous equation because $\sigma > b$ to get chaotic state.

$$r > \frac{10(10+(8/3)+3)}{(10-(8/3)-1)} = 24.7386 \tag{7}$$

Since *r>24.7386*, then we choose $r = 28$. All state vectors are shown in Figure 1, and all cases of the strange attractors are shown in Figure 2.

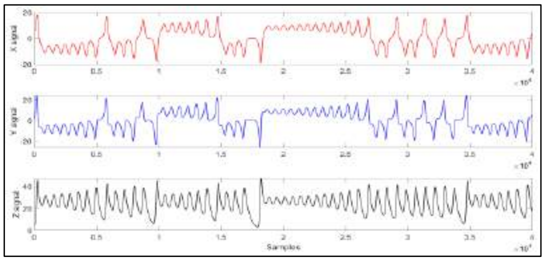

Figure 1: Time series state of Lorenz system X, Y, & Z respectively.

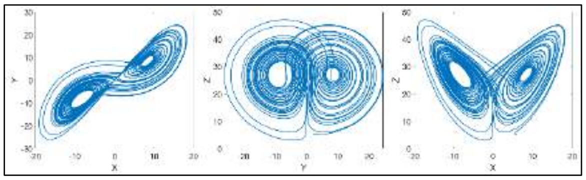

Figure 2: $(\boldsymbol{X}\ ,\boldsymbol{Y}), (\boldsymbol{Y}\ ,\boldsymbol{Z}), \boldsymbol{and}\ (\boldsymbol{X}\ ,\boldsymbol{Z})$ strange attractors for the Lorenz system.

2.2 Rossler System

Is one type of chaotic flow (continuous system) and a set of differential equations as flow (Hussein, Khashan, and Jawad 2020):

$$\dot{x} = -(\mathrm{y} + \mathrm{x}) \tag{8}$$

$$\dot{y} = \mathrm{ay} + \mathrm{x} \tag{9}$$

$$\dot{z} = \mathrm{b} - \mathrm{cz} + \mathrm{xz} \tag{10}$$

Where $\dot{x}, \dot{y}$ *and* $\dot{z}$ There are the state vectors, and a, b and c represent the constant parameters (Fig. 3 and 4).

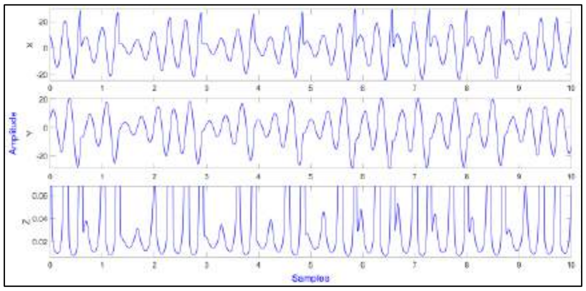

Figure 3: Time Series of Rossler System at a=0.2, b=0.3, c=16.

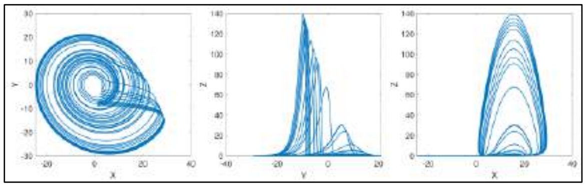

Figure 4: $(\boldsymbol{X}\ ,\boldsymbol{Y}), (\boldsymbol{Y}\ ,\boldsymbol{Z}), \boldsymbol{and}\ (\boldsymbol{X}\ ,\boldsymbol{Z})$ strange attractors for the Rossler system.

3 The Proposed Encryption Model

The proposed image encryption algorithm employs a two-layer encryption scheme, utilizing the Lorenz and Rossler chaotic systems to generate chaotic random integer numbers (CRINs). These CRINs are then XORed bitwise with the image pixel values to achieve effective scrambling, as shown in Fig. 5.

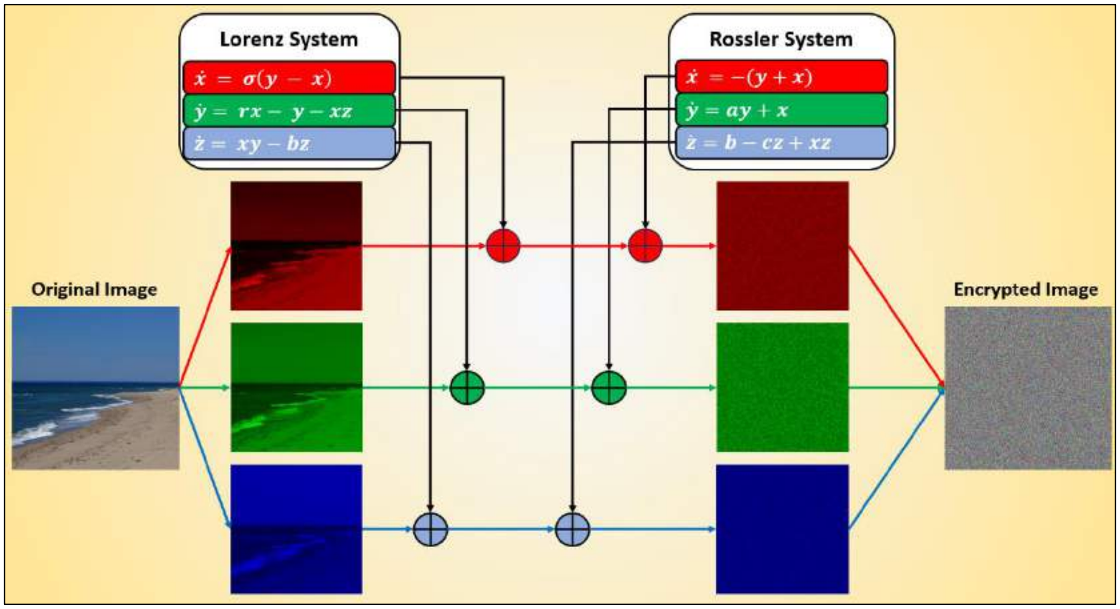

Figure 5: The proposed block diagram for colour image encryption.

The following steps of the proposed image encryption methodology:

1. The original colour image is decomposed into its three primary colour channels: red, green, and blue. This enables independent encryption of each colour component.
2. Using the Lorenz system, extremely sensitive to initial conditions are created. Random and unpredictable behaviour in these samples makes them well-suited for scrambling image data.
3. Converting the generated chaotic samples to CRINs, ranging between [0 – 255], by using the normalization equation as the following:

$$CRINs = round\big(Chaotic\ Samples(10^8)\big)\%255 \quad (11)$$

This ensures that the CRINs are compatible with the typical range of the pixel value in digital images and facilitate efficient bitwise operations.

4. The CRINs are XORed bitwise with the corresponding colour channels: CRIN(X) with the red channel, CRIN(Y) with the green channel, and CRIN(Z) with the blue channel.
5. To further enhance the encryption process, the Rossler system is employed additionally with the Lorenz system for generating CRINs. This introduces a second source of randomness, increasing the difficulty of decrypting the image without the correct keys.
6. The encrypted layers obtained from both the Lorenz and Rossler systems are combined to form the final encrypted colour image.
7. The process of decryption involves reversing the steps of the encryption process, starting with the Rosslare system and then moving to the Lorenz system. The corresponding CRINs are generated using the respective chaotic systems and XORed bitwise with the encrypted layers to recover the original colour channels.

4 Image Testing Quality

In this section, we will run seven different statistical tests with three different image sizes to determine how safe the proposed cryptographic method is and how well the system works. The Histogram graph, Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), Correlation (Corr), and Entropy, are some of the tests that may be performed—finally, the time of the encryption process (delay per second).

4.1 Histogram Plots

An image's histogram is a bar graph that illustrates the dispersion of pixel values. To thwart an adversary's attempt to deduce significant information from the histogram of a streaming encrypted picture, an ideal encrypted image must possess an even distribution and be completely unique from the plain image. (Witwit and Al-Sultan 2023).

4.2 Structural Similarity Index Measure (SSIM)

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \qquad (11)$$

μ_x , μ_y are the average of x and y respectively.

σ_x^2, σ_y^2 the variance of x and y , σ_{xy} The covariance of x and y.

$c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ two variables to stabilize the division with a weak denominator.

L the dynamic range of the pixel values (typically is $2^{bits\ per\ pixel} - 1$).

$k_1 = 0.01$, $k_2 = 0.03$ by default.

Predicting the perceived quality of digital images and videos is the purpose of SSIM. By using a comprehensive reference metric and an initial picture that is neither compressed nor distorted, it assesses the similarity between the two images. The SSIM index is computed over several picture windows, with dimensions ranging from one to two windows of the typical N*M format (Bakurov et al. 2022).

4.3 Mean Square Error (MSE)

$$MSE = \frac{1}{MN}\sum_{n=0}^{M}\sum_{m=1}^{N}[O(n,m) - E(n,m)]^2 \qquad (12)$$

In this equation, O and E represent the unencrypted and encrypted versions of the picture, respectively. When MSE equal 0, the encryption fails to obscure the original image's features (Al-Musawi, Al-Ibadi, and Wali 2023).

4.4 Peak Signal-to-Noise Ratio (PSNR)

$$PSNR(dB) = 10 * log_{10}\left[\frac{255^2}{MSE}\right] \qquad (13)$$

The lower the PSNR value, the higher and better the encryption (Satish et al. 2023; Witwit and Al-Sultan 2023).

4.5 The Correlation Coefficient

$$Corr. = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}((x_i - E(x)))^2}\sqrt{\sum_{i=1}^{N}((y_i - E(y)))^2}} \qquad (14)$$

Where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x(i)$, x and y are the pixel values of the original and encrypted images, respectively. When it's 0, the images are different (the original and the encrypted images). If it's 1, the encryption fails to obscure the original image's features (Ameen and Hreshee 2022; Rahman et al. 2023; Witwit and Al-Sultan 2023).

4.6 Entropy

$$E = \sum_{i=0}^{2^n-1}\left[p(i) * log_2\left(\frac{1}{p(i)}\right)\right] \qquad (15)$$

Where p(i) is the bit-valued I probability, for images with 256 grey levels (0 to 255), the maximum Entropy equals 8, and it's considered optimum randomness. Practical image entropy is lower than maximal image entropy (Halboos and Albakry 2023).

5 Simulation Results and System Performance

5.1 The Residual Unintelligibility of Encrypted Image

In this sub-section, we test images and display the original, encrypted, decrypted images and histogram figures. And then determine the Correlation, PSNR, and Entropy for encrypted and decrypted images, as shown in the figures and tables.

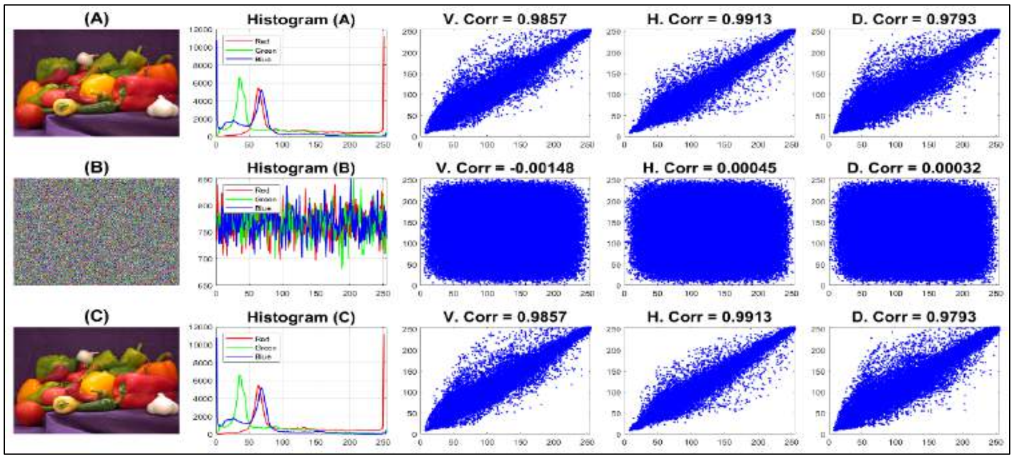

Figure 6: The histogram, and correlation plots and results for the O. peppers, E., and D. Images.

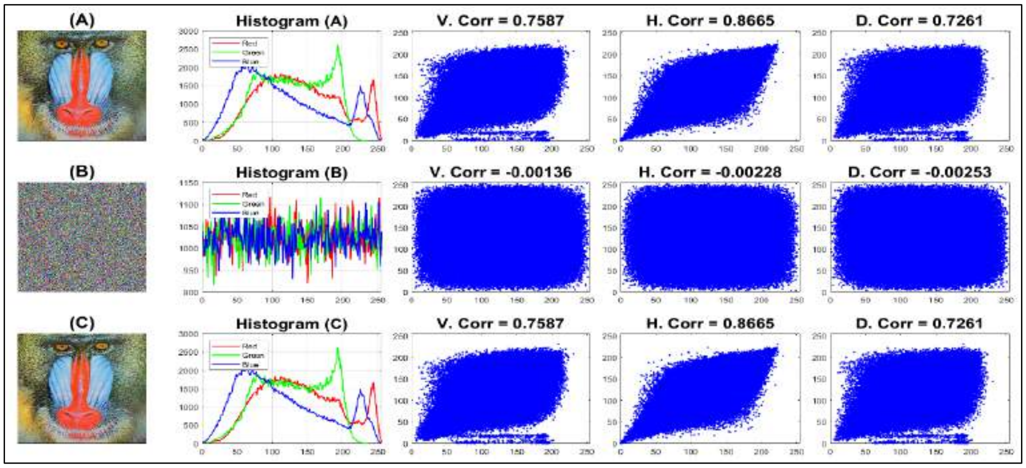

Figure 7: The histogram, and correlation plots and results for the O. baboon, E., and D. Images.

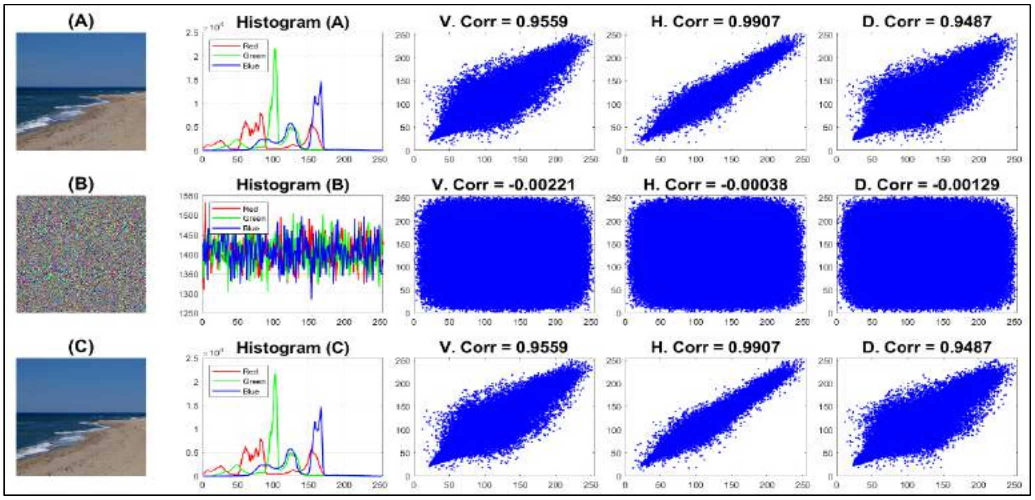

Figure 8: The histogram, and correlation plots and results for the O. Seaside, E., and D. images.

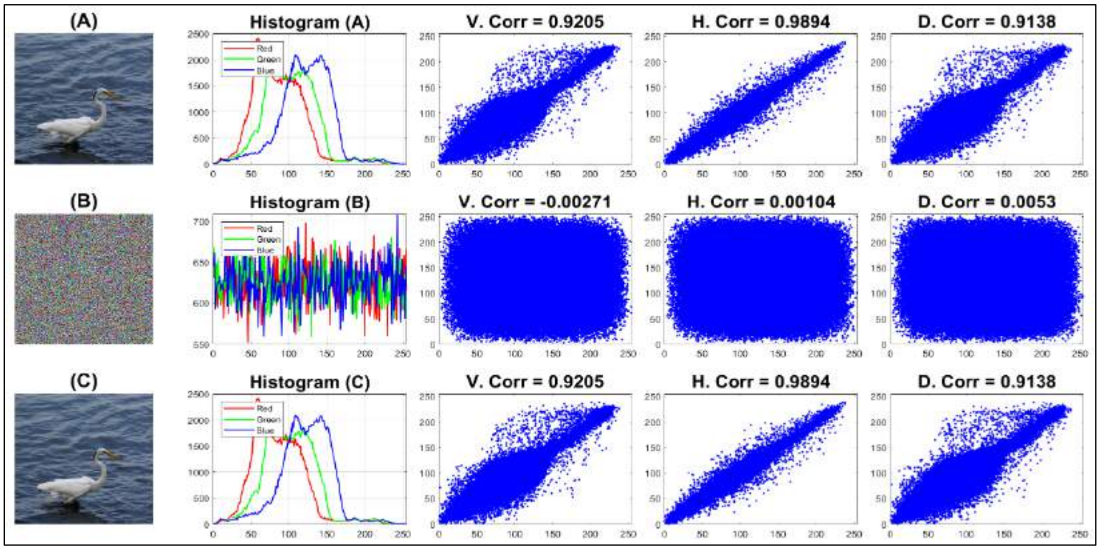

Figure 9: The histogram, and correlation plots and results for the O. Goose Bird, E., and D. images.

Table 1: Encryption Results Based on The Proposed System.

Images	MSE	PSNR(dB)	SSIM	Entropy	Delay (Sec)
Peppers	11262	7.6148	-3e-5	9.9997	0.0402
Baboon	8610	8.7806	0.0015	7.9997	0.0520
Seaside	7337	9.475	-3e-5	7.9998	0.0471
Goose Bird	7448	9.4099	3.3e-4	7.9996	0.0253

The results presented in the table illustrate the efficacy of the XOR operation applied to the combination of the CRIN and image pixels. The encrypted image exhibits notable dissimilarities compared to the original image, as shown by the decreased PSNR, SSIM, and correlation values indicating a lack of significant correlation between the encrypted images and their corresponding original images. The high values of Mean Squared Error (MSE), and Entropy, the encryption algorithms exhibit high efficiency, as evidenced by the shallow delay values. The data presented in the table demonstrates that the algorithm for encrypting images is secure and efficient.

Table 2: Decryption Results Based on the Proposed System.

Image	MSE	PSNR (dB)	SSIM	Entropy	Delay (Sec)
Peppers	0	Inf	1	7.3785	0.0036
Baboon	0	Inf	1	7.7629	0.0727
Seaside	0	Inf	1	7.1103	0.0627
Goose Bird	0	Inf	1	7.2046	0.0963

The effectiveness of the decryption process is enhanced as MSE decreases. Decryption quality improves as the PSNR increases. The effectiveness of the decryption process is directly proportional to the proximity of the SSIM to a value of 1. The rate at which decryption occurs is directly proportional to the reduction in delay. The Table displays the MSE, values for all four images, which indicate that the decryption method effectively restores the original image, as all values are zero.

5.2 Brute-Force Attack for The Proposed System

A brute force attack involves an attacker trying all possible combinations of keys until they find the correct one. In the proposed method, the attacker would try all possible combinations of the Lorenz system and Rossler parameters to encrypt the secret image. To ensure a secure system, the key space should be large enough to prevent brute-force attacks. Increasing the keyspace exponentially increases the time it takes for attackers to execute such attacks (Alexan et al. 2023; Mahalingam et al. 2023; Mfungo et al. 2023).

5.2.1 Key Sensitivity

The encryption is based on the proposed method; the Lorenz system has three initial conditions and three parameters; and the Rossler system also has three initial conditions and three parameters. Any slight change in the value of any initial state or parameter creates a new trajectory. From this sensitivity, a unique chaotic random number is generated, and these numbers do not allow the original image to be recovered, as shown in the following figures.

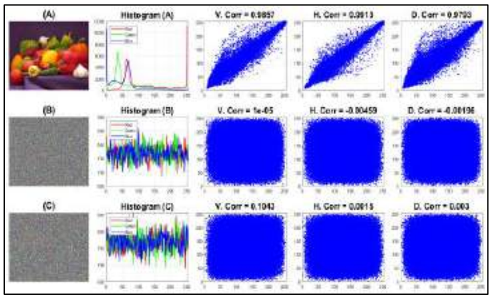

Figure 10: Decrypted Image 1 by Changing Y (1) of the Lorenz System by 10e-15.

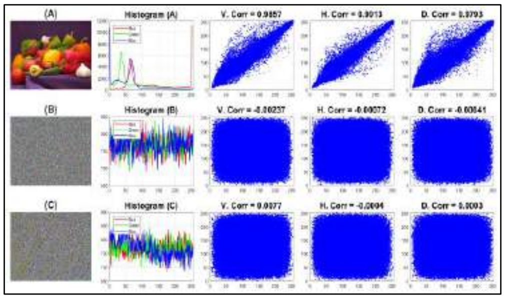

Figure 11: Decrypted Image 1 by Changing the C-Parameter of the Rossler System by 10e-10.

The simulation results in MATLAB showed that if any parameter or initial value is changed, the decryption process will be interrupted. And revealed that the Lorenz or Rossler systems are affected by (10^{-15}) by any parameter or initial value.

5.2.2 Keyspace Calculation

The exact number in chaotic systems cannot calculate the number of keys, but it can be calculated approximately and is largely correct, as shown in the following equation:

$$Keyspace\ for\ 1D = \frac{1}{S} * R(i) \tag{16}$$

Where: d: Number of Parameters and Initial Values for chaotic system.

S: Key Sensitivity for a chaotic system.

R: The range between the most significant and most minor value for any parameter or initial value that the system remains within the limits of chaos. To facilitate the solution, we assume that the R is 1, although it is much more than 1 in most cases. In this case, the real number of keys will be greater than the calculated number.

$$Keyspace\ for\ 1\ D \approx \frac{1}{10^{-15}} * 1 \approx 10^{15} \quad \approx 2^{50} \tag{17}$$

$$All\ Keyspace = \prod_{i=1}^{d} (Keyspace\ 1\ D) \tag{18}$$

Where d equal 12 for two chaotic systems. The Lorenz system has 6d (3 initial values and 3 parameters), and also 6d for the Rosslar system (3 initial values and 3 parameters), and also 6d for the Rosslar system.

$$All\ Keyspace = \prod_{i=1}^{12} (2^{50}) = (2^{50})^{12} = 2^{600} \tag{19}$$

5.3 Comparison of The Proposed System with Other Research

Here, we will look at simulation results from the proposed system that uses modulo addition and multiplication to encrypt images. We will compare them to prior research that employed the XOR operation between the key and the original image to produce the encrypted image, as shown in **Error! Reference source not found.**.

Table 3: Compare the proposed encryption results with the other research.

Ref.	Image	MSE	PSNR (dB)	Corr	Entropy	Delay (Sec)
(Alexan et al. 2023)	Peppers	10034	8.1622	0.00175	7.9968	2.637
(Wang and Su 2020)	Peppers	-	-	0.0035	7.9959	-
(Alsaabri and Hreshee 2021)	Peppers	-	8.6261	0.4917	7.9997	-
(Long and Tan 2010)	Peppers	-	-	0.0017	7.9976	-
(Yasser et al. 2020)	Peppers	8413	8.8818	-	7.9994	-
(Kari and Ghomian 2023)	Baboon	-	-	-	7.9996	0.090
	Peppers	-	-	-	7.9985	-
(Shakir, Mehdi, and Hattab 2023)	Baboon	-	-	-	-	1.3652
(Wen and Lin 2023)	Baboon	-	-	-	-	2.7526
(Mahalingam et al. 2023)	Peppers	9255	8.4667	-	0.0090	-
Proposed System	Peppers	11262	7.6148	-3.4e-5	9.9997	0.0402

From the simulation results in **Error! Reference source not found.**, it is clear that the results of the proposed system are equal to or better than the results of previous studies. Also, the encryption time in the fun system is much better than the encryption time in Ref. (Alexan et al. 2023), Ref. (Shakir, Mehdi, and Hattab 2023), and Ref. (Wen and Lin 2023).

Error! Reference source not found. shows the number of keys in previous articles and their comparison with the number of keys in the proposed system.

Table 4: The keyspace in the proposed system is compressed with the other articles.

References	Key Space
(Jawad, Abdullah, and Hreshee 2018)	2e266
(Hussein, Khashan, and Jawad 2020)	2e319
(Alexan et al. 2023)	2e478
(Alsaabri and Hreshee 2021)	10e144 = 2e479
(Hamood and Ibrahem 2018)	Case1=2e128 Case2=2e192
(Fetteha et al. 2023)	2e208
(Kari and Ghomian 2023)	2e558
Proposed System	2e600

6 Conclusions

The Lorenz and Rossler chaotic systems, which power the suggested image encryption algorithm, set a new standard for picture security by offering a safe and effective way to prevent unauthorized access to colour images. The technique is an essential tool for guaranteeing image confidentiality in a variety of applications due to its two-layer encryption scheme, unwavering sensitivity to beginning conditions, and persistent resistance to statistical attacks. In this paper, we proposed an efficient method for digital image encryption using chaotic systems and modified algebraic processes.

The results of the simulation demonstrated that the image encryption and keyspace results from the first and second levels were satisfactory. Combining the two encryption levels resulted in a doubling of the number of keys while maintaining the level of encryption. Due to the short processing times for encryption and decryption, the system can be used instantly (in fractions of a second).

7 Future Works

1. Investigate secure key management and distribution protocols.
2. Explore the applicability in other domains (medical image encryption, data security, multimedia content protection).
3. Analyze the impact of parameter selection on security and performance.
4. Investigate new chaotic systems and their potential for encryption.
5. Explore quantum-resistant encryption techniques. And develop new methods for secure key management and distribution.

8 References

Abdullah, Hikmat N, Saad S Hreshee, and Ameer K Jawad. 2015. “Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals.” *Journal of American Science* 11(7): 49–55.

Abdullah, Hikmat N, Saad S Hreshee, Gholamreza Karimi, and Ameer K Jawad. 2022. “Performance Improvement of Chaotic Masking System Using Power Control Method.” In *International Middle Eastern Simulation and Modelling Conference 2022, MESM 2022*, , 19–23.

Al-Musawi, Wisal Adnan, Mohammed Abd Ali Al-Ibadi, and Wasan A. Wali. 2023. “Artificial Intelligence Techniques for Encrypt Images Based on the Chaotic System Implemented on Field-Programmable Gate Array.” *IAES International Journal of Artificial Intelligence* 12(1): 347–56.

Alexan, Wassim et al. 2023. “Color Image Encryption Through Chaos and KAA Map.” *IEEE Access* PP: 1.

Alsaabri, Huda H., and Saad S. Hreshee. 2021. “Robust Image Encryption Based on Double Hyper Chaotic Rabinovich System.” *7th International Conference on Contemporary Information Technology and Mathematics, ICCITM 2021*: 146–52.

Ameen, Mohammed Jabbar Mohammed, and Saad Saffah Hasson Hreshee. 2022. “Hyperchaotic Modulo Operator Encryption Technique for Massive Multiple Input Multiple Output Generalized Frequency Division Multiplexing System.” *International Journal on Electrical Engineering and Informatics* 14(2): 311–29.

Ameer K. Jawad, Wa’il a. H. Hadi, and Hyayder F. Y. Husseain. 2016. *Enhancement of Image Transmission Using Chaotic Interleaver over Wireless Sensor Network*. www.ijntr.org.

Bakurov, Illya et al. 2022. “Structural Similarity Index (SSIM) Revisited: A Data-Driven Approach.” *Expert Systems with Applications* 189: 116087.

Fetteha, Marwan A., Wafaa S. Sayed, Lobna A. Said, and Ahmed G. Radwan. 2023. “Chaos-Based Image Encryption Using DNA Manipulation and a Modified Arnold Transform.” *(including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 13761 LNAI(December): 3–15. http://dx.doi.org/10.1007/978-3-031-21595-7_1.

Halboos, Estabraq Hussein Jasim, and Abbas M. Albakry. 2023. “Improve Steganography System Using Agents Software Based on Statistical and Classification Technique.” *Bulletin of Electrical Engineering and Informatics* 12(3): 1595–1606.

Hamood, Laith Abdulhussien, and Mahmood Khalel Ibrahem. 2018. “Video Encryption Based on Chaotic System and Stream Cipher.” *Iraqi Journal of Information & Communications Technology* 1(2): 33–40.

Hussein, E.A.R. Ehab AbdulRazzaq E.A.R., M.K. Murtadha K. Khashan, and A.K. Ameer K. Jawad. 2020. “A High Security and Noise Immunity of Speech Based on Double Chaotic Masking.” *International Journal of Electrical and Computer Engineering* 10(4): 4270–78.

Jawad, A.K., H.N. Abdullah, and S.S. Hreshee. 2018. “Secure Speech Communication System Based on Scrambling and Masking by Chaotic Maps.” In *IEEE, International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, , 7–12.

Kari, Ahmad Pourjabbar, and Taher Ghomian. 2023.

"An e Cient Image Cryptosystem Based on the Residue Number System and Hybrid Chaotic Maps." *research square*: 0–22.

Long, Min, and Li Tan. 2010. "A Chaos-Based Data Encryption Algorithm for Image/Video." *2010 International Conference on MultiMedia and Information Technology, MMIT 2010* 1(5): 172–75.

Mahalingam, Hemalatha et al. 2023. "Dual-Domain Image Encryption in Unsecure Medium—A Secure Communication Perspective." *Mathematics* 11(2): 1–25.

Mahdi, Amina, Ameer K Jawad, and Saad S Hreshee. 2016. "Digital Chaotic Scrambling of Voice Based on Duffing Map." *International Journal of Information and Communication Sciences* 1(2): 16–21.

Mfungo, Dani Elias, Xianping Fu, Yongjin Xian, and Xingyuan Wang. 2023. "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information." *Applied Sciences* 13(12): 1–25.

Rahman, Shahid et al. 2023. "A Huffman Code LSB Based Image Steganography Technique Using Multi-Level Encryption and Achromatic Component of an Image." *Scientific Reports* 13(1): 1–20. https://doi.org/10.1038/s41598-023-41303-1.

Satish, E G et al. 2023. "Multimedia Multilevel Security by Integrating Steganography and Cryptography Techniques." 01012: 1–13.

Shakir, Huda R., Sadiq A. Mehdi, and Anwar A. Hattab. 2023. "A New Four-Dimensional Hyper-Chaotic System for Image Encryption." *International Journal of Electrical and Computer Engineering* 13(2): 1744–56.

Wang, Xingyuan, and Yining Su. 2020. "Color Image Encryption Based on Chaotic Compressed Sensing and Two-Dimensional Fractional Fourier Transform." *Scientific Reports* 10(1).

Wen, Heping, and Yiting Lin. 2023. "Cryptanalyzing an Image Cipher Using Multiple Chaos and DNA Operations." *Journal of King Saud University - Computer and Information Sciences* 35(7): 1–9. https://doi.org/10.1016/j.jksuci.2023.101612.

Witwit, Noor Haider, and Ali Yakoob Al-Sultan. 2023. "A High-Security Image Utilizing Triple Generators for the Rabinovitch System." *International Journal of Intelligent Engineering & Systems* 16(4).

Yasser, Ibrahim, Mohamed A. Mohamed, Ahmed S. Samra, and Fahmi Khalifa. 2020. "A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications." *Entropy* 22(11): 1–23.

Biography

Asmaa Y. Albakri: She is an assistant programmer with a M.Sc. degree in software engineering at Altinbaş University - Turkey - Istanbul. She now works as a lecturer in the laboratories of the Computer Science Department/ College of Computer Science and Mathematics / University of Mosul. She also completed a higher diploma in the Department of Computer Science/University of Mosul. I completed my B.Sc. degree in the Department of Computer Science, University of Mosul.

Oğuz Karan: He is an assistant prof. with a PH.D. degree from the Turkish Forces Command/ Air Force Academy / Institute of Aviation and Space Technologies / Computer Engineering Department. teaching in the Department of Software Engineering at Alinbas University - Turkey - Istanbul. he has a M.SC. degree in software engineering from Haliç University.