integrity Research Journals

Applied Journal of Physical Science
Volume 6(1), pages 13-23, February 2025
Article Number: 4832BAF02
ISSN: 2756-6684
https://doi.org/10.31248/AJPS2024.110
https://integrityresjournals.org/journal/AJPS

Full Length Research

Encryption algorithm for RGB images using Rossler chaotic system

Yakubu H. J.[1]*, Samuel K. A.[1] and Joseph S. B.[2]

[1]Department of Computer Science, Faculty of Physical Sciences, University of Maiduguri, Nigeria.
[2]Department of Computer Engineering, Faculty of Engineering, University of Maiduguri, Nigeria.

*Corresponding author. Email: yakubuhj@unimaid.edu.ng

Received 23rd November 2024; Accepted 16th January 2025

ABSTRACT: Providing privacy between two or more communicating parties on the Internet has been a major area of concern in our modern society due to the high cyber-attack rate. Some of this information is highly confidential and must be protected when it is stored in a computer and when it is in transit over the Internet. Cryptography has generally been acknowledged as the best method of information protection. Studies have shown that among the systems showing chaotic behaviour, 3-D continuous-time chaotic systems are found to contain abundant chaotic structures and complex dynamical behaviour which are highly useful in data security and hence, the need to explore the Rössler system. This paper proposed an image encryption algorithm for RGB images using the 3-D Rössler chaotic system. The proposed algorithm adopts the classic framework of the permutation substitution network in cryptography by using the rich chaotic properties of the Rössler system. This ensures both confusion and diffusion properties for a secure cipher. A standard test image namely Lena_colour_256.tif was used in testing the proposed scheme. Security analyses such as the Histogram Uniformity Analysis, Correlation Coefficient Analysis, Number of Pixels Change Rate (NPCR), and Unified Averaged Changing Intensity (UACI) were carried out on the proposed scheme. Results obtained from the analysis show that the proposed scheme is effective and strong against statistical, differential, and brute-force attacks.

Keywords: Asymmetric/symmetric-key, cipher image, encryption/decryption algorithm, fixed point, RGB Image, Rössler attractor.

INTRODUCTION

In today's world, a huge amount of information (text, image, audio, video and multimedia) is transferred. Though it is efficient, it is highly insecure and therefore exposed to various threats (Abd El-samie *et al*., 2014). Many different techniques for securing sensitive information that is either in transit or in storage have been developed, and still more techniques are being developed. Steganography and Cryptography are two of the most popular methods for securing sensitive information. Steganography is a method of hiding secret messages in a cover object while Cryptography is a technique that transforms information to be transmitted into an unreadable and unintelligent form so that only authorized persons can correctly recover the information by decryption process (Mishra *et al.,* 2012; Abd El-samie *et al*., 2014). However, of these two, cryptography is generally acknowledged as the best method for protecting information against both passive and active attacks (Denning, 1982; Mishkovski and Kocarev, 2011; Abraham and Daniel, 2013; Ramadan *et al*., 2016). The word "Cryptography" was derived from the Greek words kryptos, meaning hidden and graphikos, meaning writing (Hoffstein, 2008). It came in as a means to enable parties to communicate with each other even in the presence of an adversary that has access to the communication channels. Different authors defined cryptography in different ways. The science of keeping secrets secret is considered cryptography (Delfs and Knebl, 2007). While Goldreich (2004) defined crypto-graphy as the art of building encryption schemes that allow secret data

exchange over insecure channels. Providing confidentiality between two communicating parties using encryption methods is the fundamental and classical goal of cryptography. Furthermore, cryptography has now gone beyond secret communication. It can perform other functions such as message authentication, digital signatures, protocol for exchanging secret keys, etc. (Hoffstein *et al.,* 2008). Cryptography is further categorized into two: Symmetric-key cryptography and Asymmetric-key cryptography. The symmetric-key cryptography is where the sender and the receiver share a single secret key that are alike which are used both for encryption and decryption (i.e. $K_e = K_d$). The key must be transmitted between the sender and the receiver through a separate secret channel. While asymmetric-key cryptography (also called public-key cryptosystem) is where each party involved has a pair of different keys that are mathematically linked called the encryption key K_e, and the decryption key K_d. The encryption key K_e is made public, while the decryption K_d is kept secret (i.e. $K_e \neq K_d$). No additional secret channel is needed for key transfer (Delfs and Knebl, 2007). Symmetric key encryption scheme provides a secured communication channel to each pair of users after agreeing on a common secret key that is being shared between the communicating parties. It also provides confidentiality and data integrity. However, secured delivery of the secret key is observed to be its major setback. Other weaknesses observed are a lack of good methods for authentication and non-repudiation (Mishkovski and Kocarev, 2011).

The traditional encryption methods which include Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Rivest-Shimar-Adleman (RSA) algorithm and ElGamal algorithm have been effective solutions to the information security problems (Cao, 2013; Ye, 2013). They are, however, still being used heavily in different forms of information security. These traditional methods were primarily designed for text, and though can be used for images, are found not suitable due to the following three reasons: (**i**) Image size is always much greater than that of text, and therefore needs more time to directly encrypt/decrypt it with the traditional encryption schemes (**ii**) While the decrypted text must be exactly the same as the plain text, this strict requirement is not necessary for image data due to human perception and the high redundancy of image data. A decrypted image with small distortion is usually acceptable. (**iii**) Digital image contents are strongly correlated and this feature is not being utilized by the traditional methods thereby affecting their encryption efficiency (Cao, 2013; Ramadan *et al*., 2014; Abd El-samie *et al*., 2014).

In order to adapt these unique characteristics of image data and to improve the efficiency and security of image encryption, numerous image encryption and hiding schemes were proposed. Among those schemes, the chaos-based encryption scheme was found to be most attractive to many researchers because of its interesting features such as high sensitivity to initial conditions and control parameters, random-like behaviour and unpredictability yet reproducible (Cao, 2013). The word chaos is derived from the Greek, which refers to unpredictability and is defined as the study of non-linear dynamical systems. Chaotic dynamic systems are dimensional nonlinear dynamic systems that are capable of complex and unpredictable behaviour. Chaos describes a system that is sensitive to initial conditions, generating apparently random-like behaviour while remaining completely deterministic. These properties of chaos have much potential for application in cryptography as it is hard to make long-term predictions on chaotic systems and that means the systems will be strong against *statistical*, *differential* and *brute-force attacks* (Wu *et al*., 2012; Ramadan *et al*., 2016; Abd El-samie *et al*., 2014).

Applying chaos to cryptography was a great contribution to improving the security of information and communications due to the adequate properties of chaotic sequences. Chaos has huge potential applications in several vital fields of cryptography. Fridrich was the first that start the application of chaos to the encryption of digital images in 1997 and since then, many researchers applied chaos to different fields of image security. Chaos-based encryption methods have proven to have higher resistance against different attacks than the traditional methods and hence, it is a good tool for encrypting images (Wu *et al.,* 2012; Ramahrishnan *et al*., 2014; Abd El-samie *et al.,* 2014; Ye, 2013).

Cryptanalysis, which is the art of deciphering an encrypted message as a whole or in part when the decryption key is not known, has been a source of concern to cryptographic scheme researchers. During cryptanalyzing a ciphering algorithm, the fundamental assumption is that the cryptanalyst knows exactly the design and workings of the cryptosystem under study except the secret key (Ye, 2013; Stinson 2006). This assumption was made by A. Kerkhoff in the 19th century and is usually referred to as Kerkhoff's Principle (Stinson, 2006; Delfs and Knebl, 2007). Thus, according to this principle, the security of a cryptosystem must be entirely based on the secret key. However, the possible attacks depend on the actual resources of the adversary: The most common attacks on cryptosystems are briefly explained as follows:

1. **Ciphertext-only attack**: The attacker has access to one or more encrypted messages.
2. **Known plaintext attack**: The attacker possesses some knowledge about the plaintext corresponding to the given ciphertext. This may help it determine the key or part of the key.
3. **Chosen plaintext attack**: The attacker can feed the chosen plaintext into the black box that contains the encryption algorithm and the encryption key that gives the corresponding ciphertext. The accumulated

knowledge about the pair of plaintext-ciphtertext may reveal the key or part of the key.

4. **Chosen ciphertext attack**: The attacker can feed the chosen ciphertext into the black box that contain the decryption algorithm and the decryption key which produces the corresponding plaintext. By analyzing the accumulated ciphertext-plaintext pairs, the attacker may obtain the secret key of part of the key.
5. **Brute-Force Attack**: A brute force attack is a method of breaking a cipher based on the exhaustive key search. It is the most expensive attack (Abd El-samie *et al*., 2014; Delfs and Knebl, 2007; Mishra and Mankar, 2011).

In addition to these five general attacks described above, there are some other specialized attacks, like, the differential and the linear attacks. The differential cryptanalysis is a kind of chosen-plaintext attack aimed at finding the secret key in a cipher, while the linear cryptanalysis is a type of known-plaintext attack, whose purpose is to construct a linear approximate expression of the cipher under study (Mishra and Mankar, 2011).

Several image encryption algorithms are already available in the literature; however, some of these algorithms suffered one form of attack or the other. The most serious among these attacks is the brute-force attack which adheres to Kerkhoff's principle. Thus, there is still a need to search for more secure and efficient encryption algorithms.

RELATED WORKS

A fast image encryption algorithm using Logistics-Sine-Cosine Mapping was proposed by Wang *et al*. (2022). First, the algorithm generates five sets of encrypted sequences from the logistics-sine-cosine mapping, then uses the order of the encryption sequence to scramble the image pixels and designs a new pixel diffusion network to further improve the key sensitivity and plain-image sensitivity of the encryption algorithm. The experimental results show that the fast image encryption algorithm based on logistics-sine-cosine mapping takes less time to encrypt, and the cipher image has good information entropy and diffusivity. Hence, it is a safe and effective fast image encryption algorithm. Cao (2013) proposed a new hybrid chaotic map that is constructed by composition of three classic chaotic maps which include the Logistic map, the Henon map and the Ikeda map. The results of the analysis reveal remarkable sensitivity to the initial condition and control parameters. A new chaos-based image encryption scheme with a permutation-diffusion mechanism, where six skewed tent maps and one six-dimensional Arnold map were utilized to generate one hybrid chaotic map was proposed by Ye (2013)**.** Here the orbit disorders the pixel positions in the permutation process, while four skewed tent maps and one Arnold map were employed to yield two random gray value sequences to change the gray values by a two-way diffusion process. The experimental results show that the proposed scheme is secure against the brute-force attack due to the large key space, the statistical attack and the differential attack. Alawida (2023) proposed a novel chaos-based permutation for image encryption that uses an enhanced chaotic map which was obtained by hybridizing backward and forward perturbation methods and offers high security and low time consumption. The two substitution operations involve an XORing operation for each pixel's block. The experimental findings show the superior performance of the proposed scheme and the ability to resist a diverse range of cyber-attacks. A chaotic image encryption algorithm with different modes of operation was proposed by Abd El-samie *et al*. (2014). The proposed encryption algorithm was achieved by implementing a two-dimensional chaotic Baker map for scrambling image pixels using three different modes of operation: cipher-block chaining (CBC), cipher feedback (CFB) and output feedback (OFB) with the aim of improving its security. Yakubu and Aboiyar (2018) proposed a chaos based image encryption scheme for RGB images using the Shimizu-Morioka system. The proposed scheme consists of two stages: the confusion stage and the diffusion stage. In the confusion stage, we utilized the rich chaotic properties of the Shimizu-Morioka chaotic system to scramble the plain image and in the diffusion stage, we performed MOD and bitXOR operations on the pixel values of the shuffled image and the sequence of solutions obtained from the system. Performance analysis on the proposed scheme such as the statistical analysis and the sensitivity analysis show that the proposed scheme is reliable and strong enough to withstand both the statistical and the differential attacks. A novel approach for image encryption based on a 2-D Zaslavskii map and Pseudo Hadmard transform was proposed by Hanchinamani and Kulakarni (2014). The encryption process is composed of two stages: permutation and diffusion. The permutation is achieved by scrambling rows and columns using chaotic values of the maps. Diffusion is achieved in two directions (forward and backward) with multiple additions and XOR operations. The proposed scheme achieves the required level of security with only one round of encryption operation. Hence the proposed method is computationally fast. Nkapkop *et al.* (2014) proposed a one-round chaos-based image encryption scheme based on the fast generation of large permutation and diffusion keys. In this scheme, at the permutation step, chaotic numbers are generated using a logistic map to shuffle the pixel positions without changing its value and at the diffusion step, the shuffled image is split into *n* sub-images and the combination of Piecewise Linear Chaotic Map (PWLCM) with solutions of Linear Diophantine Equation (LDE) is generated to mask the pixels in each sub-image. The experimental results indicate that the proposed algorithm has a satisfactory security level with low computational complexity, compared to the two-round encryption

schemes, which renders it a good candidate for real-time secure image transmission applications. A chaos-based image encryption scheme using an improved Quadratic chaotic map was proposed by Ramadan *et al*. (2016). The proposed image encryption scheme is based on two chaotic maps: the Chebyshev chaotic map which is used for the permutation of image pixels and the improved Quadratic map used for the diffusion of the permuted image. Results show that the proposed scheme has a high-security level with low computational complexity, which makes it suitable for real-time applications. Yakubu and Aboiyar (2018) proposed a chaos-based image encryption scheme for RGB images using the Shimizu-Morioka system. The proposed scheme consists of two stages: the confusion stage and the diffusion stage. In the confusion stage, we utilized the rich chaotic properties of the Shimizu-Morioka chaotic system to scramble the plain image and in the diffusion stage, we performed MOD and bitXOR operations on the pixel values of the shuffled image and the sequence of solutions obtained from the system. Performance analysis on the proposed scheme such as the statistical analysis and the sensitivity analysis show that the proposed scheme is reliable and strong enough to withstand both the statistical and the differential attacks. A novel symmetric cryptosystem for the transmission of RGB colour images through open channels was proposed by Darani (2024). The proposed scheme is based on a suitable 3D hybrid chaotic system with a high exponent value. The encryption process incorporates reversible second-order cellular automata, which are applied to the shuffled image. Key generation is achieved through the utilization of irreversible cellular automata. The experimental results show that the proposed scheme proved its resilience against statistical and brute-force attacks.

THE RÖSSLER SYSTEM

The Rössler System was introduced in 1976 by Otto Rössler as a prototype of a simple autonomous differential system behaving chaotically for some values of parameters as shown in equation (1). It was originally conceived as a system for helping to understand the chaotic properties of some differential models of chemical reactions. These differential equations define a continuous-time dynamical system that exhibits chaotic dynamics associated with the fractal properties of the attractor. Some properties of the Rössler system can be deduced via linear methods such as eigenvectors, but the main features of the system require non-linear methods such as Poincare's maps and bifurcation diagrams. Since then, the chaotic behaviour of the Rossler system has been applied in many areas (Rössler, 2020; Wikipedia, 2023; Alsafasfeh and Al-Am, 2011).

$$\begin{aligned} \dot{x} &= -y - z; \\ \dot{y} &= x + ay; \\ \dot{z} &= bx - cz + xz: \end{aligned} \quad (1)$$

Where $(x, y, z) \in \mathbb{R}^3$ are state variables, the dot $(\cdot)$ on a variable indicates the derivative of the variable with respect to time t, while $a, b, and\ c$ are positive parameters

Fixed points

In order to find the fixed points, the three Rössler equations are set to zero and the (*x*, *y*, *z*) coordinates of each fixed point were determined by solving the resulting equations. This yields the general equations of each of the fixed-point coordinates (Rössler, 2023)

$$x = \frac{c \pm \sqrt{c^2 - 4ab}}{2a}, \qquad y = -\left(\frac{c \pm \sqrt{c^2 - 4ac}}{2a}\right), \quad \text{and} \quad z = \frac{c \pm \sqrt{c^2 - 4ab}}{2a} \quad (2)$$

which in turn can be used to show the actual fixed points for a given set of parameter values:

$$\left(\frac{c+\sqrt{c^2-4ab}}{2a}, \frac{-c-\sqrt{c^2-4ab}}{2a}, \frac{c+\sqrt{c^2-4ab}}{2a}\right)$$

$$\left(\frac{c-\sqrt{c^2-4ab}}{2a}, \frac{-c+\sqrt{c^2-4ab}}{2a}, \frac{c-\sqrt{c^2-4ab}}{2a}\right) \quad (3)$$

Stability analysis

The stability of each of these fixed points can be analyzed by determining their respective eigenvalues and eigenvectors. Beginning with the Jacobian (Rössler, 2023):

$$J = \begin{pmatrix} 0 & -1 & -1 \\ 1 & a & 0 \\ z & 0 & x - c \end{pmatrix} \quad (4)$$

The eigenvalues can be determined by solving the following cubic:

$$-\lambda^3 + \lambda^2(a + x - c) + \lambda(ac - ax - 1 - z) + x - c + az = 0 \quad (5)$$

For the centrally located fixed point, Rössler's original parameter values of *a* = 0.2, *b* = 0.2, and *c* = 5.7 yield eigenvalues of:

$\boldsymbol{\lambda_1} = 0.09710 + 0.9957i,\ \boldsymbol{\lambda_2} = 0.09710 - 0.9957i,\ \boldsymbol{\lambda_3} = -5.6872.$

The magnitude of a negative eigenvalue characterizes the level of attraction along the corresponding eigenvector. Similarly, the magnitude of a positive eigenvalue characterizes the level of repulsion along the corresponding eigenvector. The eigenvectors corresponding to these eigenvalues were found to be (Wikipedia, 2023):

$$v_1 = \begin{pmatrix} 0.7073 \\ -0.07278 - 0.7032i \\ 0.0042 - 0.0007i \end{pmatrix},\ v_2 = \begin{pmatrix} 0.7073 \\ -0.07278 + 0.7032i \\ 0.0042 + 0.0007i \end{pmatrix},$$
$$v_3 = \begin{pmatrix} 0.1682 \\ -0.0286 \\ 0.09856 \end{pmatrix}$$

Phase portrait of the Rössler chaotic system

The Rössler chaotic system is given by

$$\begin{aligned} \dot{x} &= -y - z; \\ \dot{y} &= x + 0.20101y; \\ \dot{z} &= 0.20101x - 5.69999z + xz: \end{aligned} \quad (6)$$

Where the parameters are defined as $a = b = 0.20101$ and c= 5.69999. Using a MATLAB /Simulink model version 7.10.0 (2010a), the phase portraits of system (6) in the $xy, xz, yz\ and\ xyz$ phase planes were obtained as shown in Figure 1 by (a), (b), (c), and (d) respectively when initial conditions are chosen as $x_0 = 0.1,\ y_0 = 0.1,\ and\ z_0 = 0.1$.

THE PROPOSED ALGORITHM

The proposed algorithm is a symmetric-key encryption scheme where a private key is used for both encryption and decryption processes which must be established first between the communicating parties (the sender and the receiver) through a public-key encryption scheme. The proposed scheme uses two stages. The first stage is the *confusion* (mixing) stage which breaks the correlation between adjacent pixels and the second stage is the *diffusion* stage where the pixel values are transformed into new values. To achieve the confusion stage, the rich chaotic properties of the Rössler system is used in shuffling the plain image using initial conditions and control parameters as the key and in the diffusion stage, the cipher image is obtained by performing the MOD and bitXOR operations on the shuffled image using the chaotic sequence generated from the Rössler system. The decrypted image is obtained by applying the same operations carried out in the encryption process using the same set of keys but in reverse order. The detailed algorithms for encryption and decryption processes are presented below.

Encryption algorithm

1. Read RGB image I from a file as your plain image,
2. Obtain the image dimension of I as m x n x 3,
3. Compute the number of pixels per colour for I (N= p*q),
4. Enter the value of the parameter for $\alpha, \beta, x_0, y_0, z_0\ h$ (h is the step size) as your key
5. Solve the Rössler chaotic system N time's steps using the Euler's method to obtain solutions in vector form as x, y, z,
6. Add confusion to the solution using the round function to obtain X, Y, and Z,
7. Sort the vectors X, Y, and Z to obtain X1, Y1, and Z1 with their list of indices as $l_x,\ l_y\ and\ l_z$.
8. Define A, B, and C to be matrices (m x n) for red, green and blue intensities respectively of the plain image I.
9. Reshape A1, B1, and C1 into row vectors (1-D) as A2, B2, and C2.
10. Use the indices of the sorted solution of the Rössler chaotic system to scramble A2, B2, and C2 and obtain new row vectors as A3, B3, and C3,
11. Perform MOD and bitXOR operations on A3, B3, and C3 using the chaotic sequence generated from the Rössler chaotic system to generate an encrypted image for each intensity as A4, B4, and C4.
12. Reshape A4, B4, and C4 into m x n matrices (2-dimension) to obtained A5, B5 and C5.
13. Merge the intensities A5, B5 and C5 to obtain the encrypted image as I1.
14. Display the encrypted image I1.
15. Save the encrypted image I1.

Decryption algorithm

1. Read the encrypted image I1,
2. Define A6, B6, and C6 to be matrices for the red, green and blue intensities respectively for I1.
3. Reshape A6, B6, and C6 into row vectors to obtain A7, B7, and C7,
4. Perform MOD and bitXOR operations on A7, B7, and C7 using the chaotic sequence generated from the Rössler chaotic system to obtain scrambled images as A8, B8, and C8.
5. Reposition the entries in A8, B8, and C8 with the indices $l_x,\ l_y\ and\ l_z$ to obtain in row vectors unconfused intensities as A9, B9, and C9.
6. Reshape A9, B9, and C9 into square matrices to obtain A10, B10, and C10.
7. Form the decrypted image as I2 by merging the intensities A10, B10, and C10.
8. Display the decrypted image I2.
9. Save the decrypted image I2 in a file.

RESULTS AND DISCUSSION

Implementation

The practical aspect of this work was carried out using a standard test digital colour image of size 256x256, stored with TIF file format (Lena_colour.tif) as input data to test the proposed encryption scheme as shown in Figure 2. The code for the proposed scheme was implemented in MATLAB version 7.10.0 (R2010a) to simulate the proposed encryption algorithm.

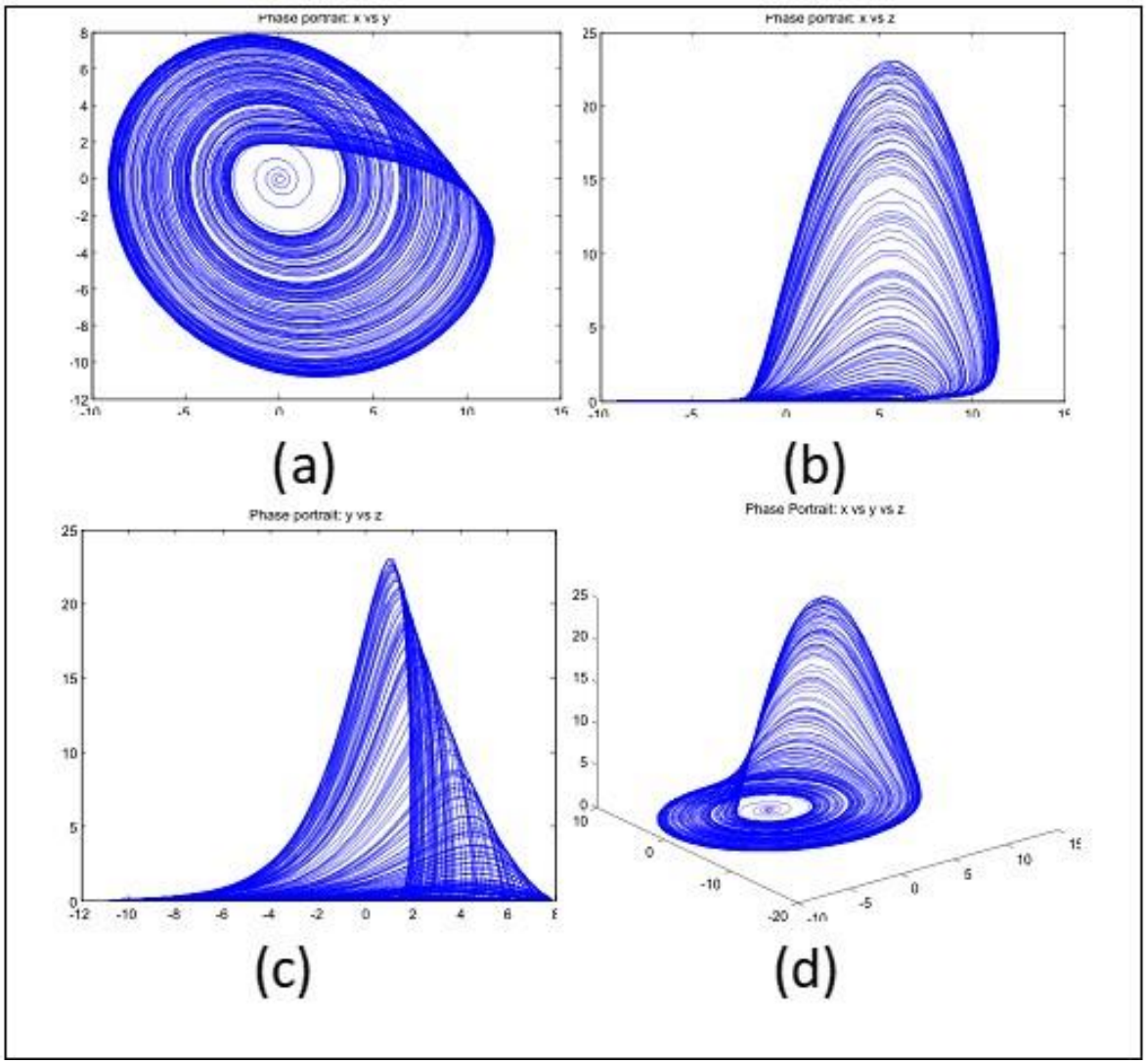

Figure 1. Phase portrait of the Rössler system.

Figure 2. Plain image.

Results obtained

When the proposed algorithm was applied to the plain image using initial conditions and control parameters as the key, the scrambled image was obtained first by separating the plain image into the red, green and blue channels which were then scrambled using the chaotic properties of the Rössler system in their respective intensities before being merged to obtain the scrambled image as shown in Figure 3a. The scrambled images in their separate intensities were encrypted, and their respective diffused images were merged to obtain the cipher (encrypted) image as shown in Figure 3b.

The plain image was recovered when the decryption algorithm was applied to the cipher image using the same set of initial conditions and control parameters that were used in the encryption stage as the key. The decryption processes began with the cipher image being separated

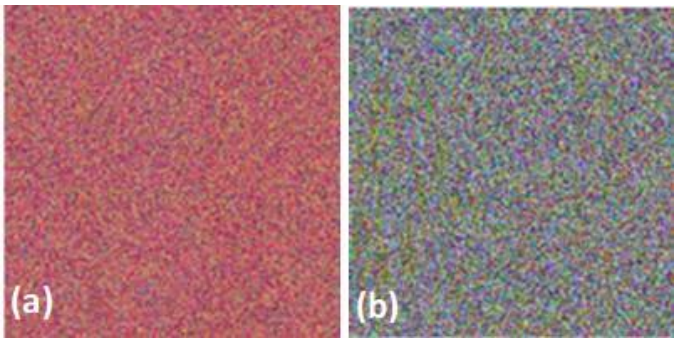

Figure 3. (a) Scrambled Image, (b) Encrypted image.

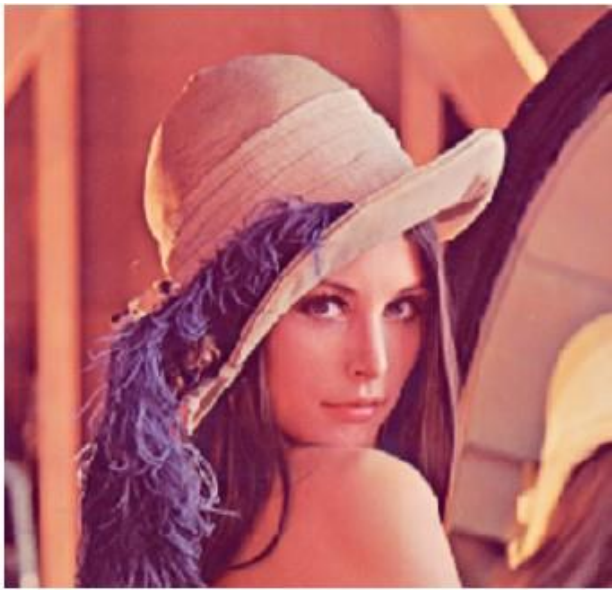

Figure 4. Decrypted image.

into red, green and blue intensities which were then transformed into undiffused but confused images that were then merged to obtain the scrambled image. The pixels' values of the scrambled image in their respective intensities were then repositioned to their original positions and merged to obtain the plain image as shown in Figure 4.

PERFORMANCE ANALYSIS

When an encryption algorithm is applied to an image, it is expected that its pixels' values change when compared with the original image. A good encryption algorithm must make these changes in an irregular manner and maximize the difference in pixel values between the plain image and the cipher image. Also, a good cipher image must be composed of totally random patterns that do not reveal any of the features of the plain image (Abd El-samie *et al*., 2014). To test the strength of the proposed algorithm, security analysis such as the statistical analysis (which includes histogram uniformity analysis and the correlation coefficient analysis) and the differential analysis (which includes the Number of Pixel Change Rate-NPCR and Unified Average Changing Intensity-UACI) were carried out as presented below.

Histogram uniformity analysis

In this analysis, the histogram of both the plain image and the cipher image must be obtained and compared. For an encryption algorithm to be considered worthy of use, the histogram of the cipher image must satisfy the following two properties (Abd El-samie et al., 2014):

1. It must be totally different from the histogram of the original image.
2. It must have a uniform distribution, which means that the probability of occurrence of any gray scale value is the same.

On comparing the histogram of the encrypted image (see Figure 6) and that of the plain image (see Figure 5), the proposed scheme satisfied the two conditions of histogram uniformity analysis indicating that the attacker cannot find any hint about the plain image from the cipher image.

Correlation coefficient analysis

This metric is for assessing the encryption quality of any image encryption scheme. The correlation coefficient between adjacent pixels of the cipher-image obtained from the proposed scheme is used for the quality test. Out of the 65,536 pixels of the plain image used, only the first 5,000 pixels were used in the analyses for determining the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels of the cipher-image as well as that of the plain-image for comparison purposes. This correlation coefficient denoted by r_{xy} is calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (3)$$

Where *x* and *y* are the values of two adjacent pixels in the cipher-image. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{L}\sum_{i-1}^{L} x_i, \qquad D(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))^2, \quad \text{and}$$
$$cov(x,y) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y)) \quad (4)$$

where *L* is the number of pixels involved in the calculations. The closer the value of r_{xy} to zero, the better the quality of the encryption algorithm is (Wu *et al*., 2012; Abd El-samie *et al.,* 2014).

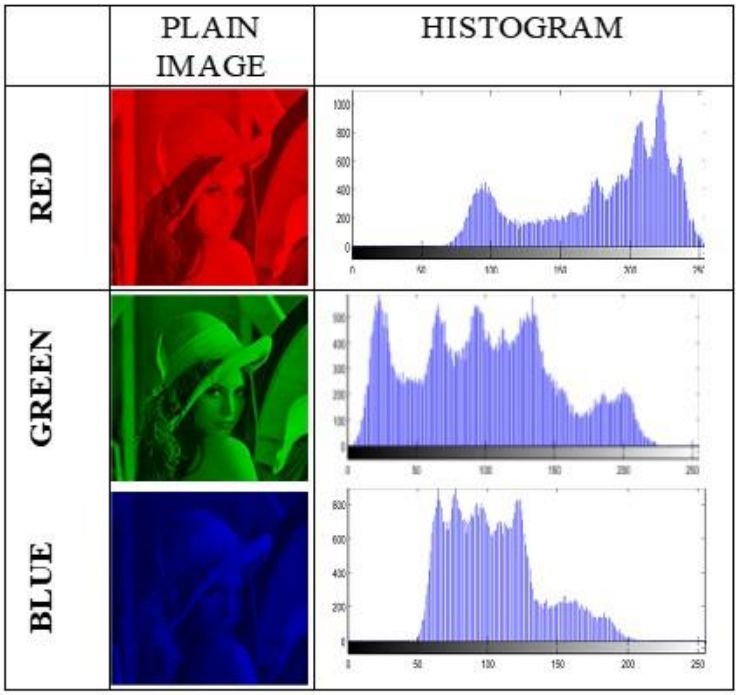

Figure 5. Histogram of the plain image.

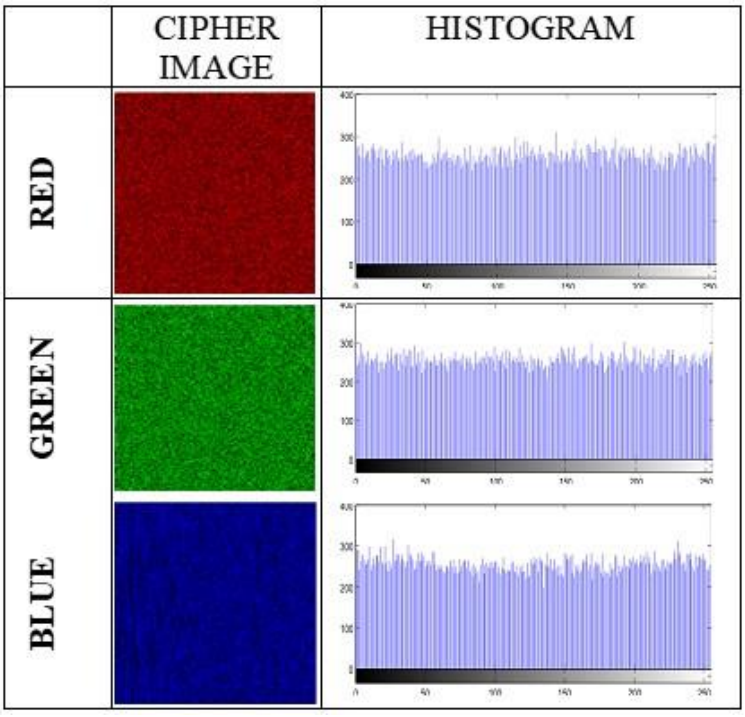

Figure 6. Histogram of the cipher image.

Figures 7 and 8 present the correlation between adjacent pixels of the plain image and the cipher image respectively. From Figure 7, one can see that the correlation between adjacent pixels in all three directions of the plain image in the three intensities have very strong correlations as indicated by the correlation coefficients obtained with a

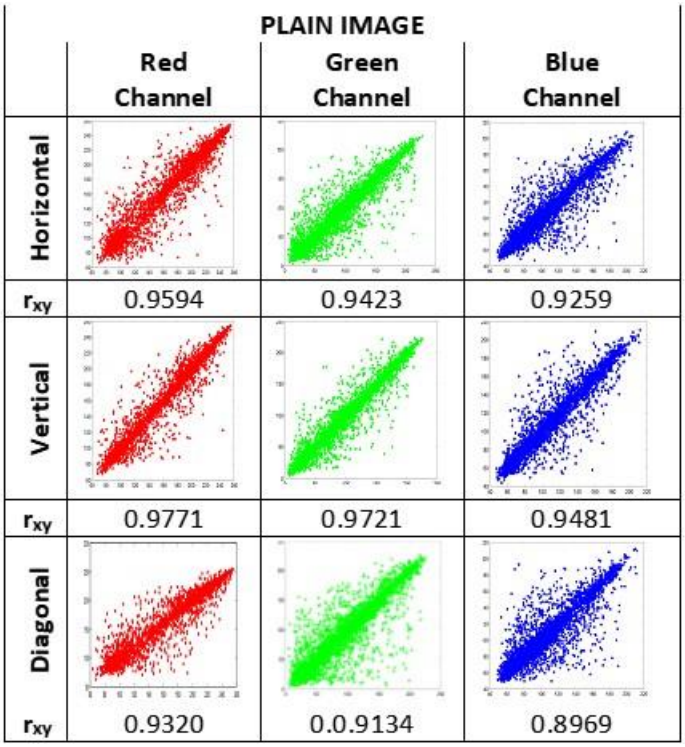

Figure 7. Correlation between adjacent pixels of the plain image.

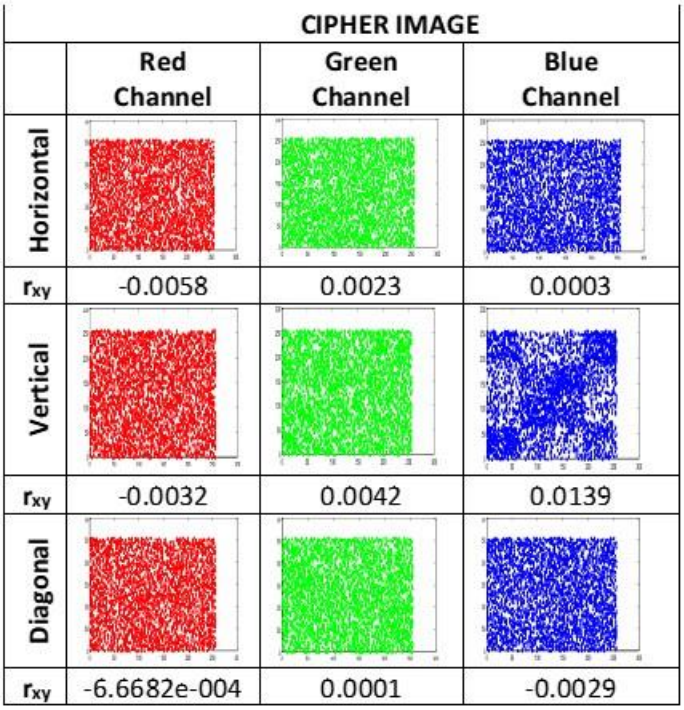

Figure 8. Correlation between adjacent pixels of the cipher image.

minimum correlation coefficient of 0.8969 on the diagonal direction in the blue channel and a maximum correlation coefficient of 0.9771 in the red channel on the vertical direction. However, looking at Figure 8, it is the complete opposite of Figure 7. From the figure, one can see clearly that the correlation between adjacent pixels in all three

directions of the cipher image in the three intensities indicates a very weak correlation as indicated by the correlation coefficients obtained with a maximum correlation coefficient of 0.0139 on the vertical direction in the blue channel and a minimum correlation coefficient of -6.6682e-004 in the red channel on the diagonal direction which is very close to zero, indicating that the proposed scheme is of good quality and therefore can withstand any statistical attack.

Differential/sensitivity analysis

For an image encryption scheme to be able to resist the differential attack efficiently, the scheme must be sensitive to a small change in the plain image that gives a significant change in the cipher image. To test the influence of only one-pixel change in the plain image over the whole cipher-image, two common measures were used: The Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). The NPCR measures the percentage of different pixels' numbers between the two cipher-images whose plain-images only have one-pixel difference, whereas, the UACI measures the average intensity of differences between the two cipher-images. They indicate the sensitivity of the cipher-images to the minor change of plain-images. NPCR and UACI values of an encryption scheme are evaluated using the following formulas:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (5)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{I,J} \frac{[C_1(i,j) - C_2(i,j)]}{255}\right] \times 100\% \quad (6)$$

where C_1 and C_2 denote the two ciphered images whose corresponding plain-images have only a one-pixel difference, the $C_1(i,j)$ and $C_2(i,j)$ represent the gray scale values of the pixels at grid (i,j) in the C_1 and C_2 respectively, the D(i,j) is a binary matrix with the same size as the images C_1 and C_2 whose entries is determined from $C_1(i,j)$ and $C_2(i,j)$ by the following: if $C_1(i,j) = C_2(i,j)$, then D(i,j) = 0, otherwise, D(i,j) = 1. The W and H are the width and height of the image (Wu *et al.,* 2012; Ramahrishnan *et al.,* 2014; Ramadan *et al*., 2016; Wu *et al*., 2011).

Studies have shown that the theoretical values of NPCR and UACI scores of images evaluated at 0.05-level, 0.01-level and 0.001 level vary depending on the image type and size used. The theoretical NPCR scores for gray images with the size 256 x 256 at 0.05-level; 0.01-level and 0.001-level are 99.5693%, 99.5527% and 99.5341%, respectively while the theoretical UACI critical values for gray images with the size 256 x 256 at 0.05-level, 0.01-level, and 0.001-level are 33.2824% - 33.6447%, 33.2255% - 33.7016%, and 33.1594% - 33.7677% respectively **(**Wu *et al.,* 2011). An encryption algorithm is considered worthy of use if the experimental NPCR score is equal to or greater than the theoretical NPCR score but must be less than 100% and also the experimental UACI score should be on or within the theoretical UACI critical scores **(**Wu *et al.,* 2011)**.**

Table 1. The NPCR and UACI values for the proposed scheme.

Intensities	NPCR (%)	UACI (%)
Red	99.6123	33.5104
Green	99.5401	33.3932
Blue	99.5952	33.2109

Table 1 presents the experimental NPCR and UACI scores for the proposed scheme on 256 x 256 images in the three channels: red, green and blue components (each colour is equivalent to a gray component). The results have satisfied both the NPCR and UACI requirements, which shows that the proposed scheme is effective and can withstand any differential attack.

Conclusion

The search for a more secure communication between two communicating parties is on the increase. This paper proposed image encryption algorithm for RGB images using the 3-D Rossler chaotic system. The proposed algorithm adopts the classic framework of the permutation substitution network in cryptographic techniques by using the rich chaotic properties of the Rossler system and this ensures both confusion and diffusion properties for a secure cipher. A standard test image namely Lena_colour_256.tif was used in testing the proposed scheme. Security analyses were carried out on the proposed scheme and the results obtained from the analysis show that the proposed scheme is effective and strong against the statistical attack, differential attack and brute-force attack.

Recommendation

This paper recommends that further study be carried out on other 3-D chaotic maps such as Mikhail Anatoly Chaotic Attractor, Sakarya Chaotic attractor and Burke-Show chaotic attractor which contain abundant chaotic structures that are useful in the area of securing sensitive information.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

Abd El-Samie, E. F., Ahmed, H. E. H., Elashry, F. I, Shahieen, H. M., Faragallah, S. O., El-Rabaie, M. E., & Alshebeili, A. S. (2014). *Image encryption- A communication perspective* (1st Edition). CRC Press, London. Pp. 1-86.

Abraham, L., & Daniel, N. (2013). Secure image encryption algorithms: A review. *International Journal of Scientific and Technology Research*, *2*(4),186-189.

Alawida, M. (2023). A novel chaos-based permutation for image encryption. *Journal of King Saud University-Computer and Information Sciences*, *35*(6), 101595.

Alsafasfeh, Q. H., & Al-Arni, M. S. (2011). A new chaotic behaviour from Lorenz and Rossler systems and its electronic circuit implementation. *Circuits and Systems, 2*(2), 101-105.

Cao, Y. (2013). A new hybrid chaotic map and its application on image encryption and hiding. *Mathematical Problems in Engineering*, *2013*(1), 728375.

Darani, A. Y., Yengejeh, Y. K., Pakmanesh, H., & Navarro, G. (2024). Image encryption algorithm based on a new 3D chaotic system using cellular automata. *Chaos, Solitons & Fractals*, *179*, 114396.

Delfs, H., & Knebl, H. (2007). Introduction to cryptography-principles and applications. Springer Berlin Heidelberg, New York, USA. 2nd Edition. Pp.1-65.

Denning, D. E. (1982). *Cryptography and data security*. Addison-Wesley Publishing Company Inc. USA. Pp. 1-116.

Goldreich, O. (2004). *Foundations of cryptography-basic techniques* (2nd edition). Cambridge University Press, UK. Pp. 1-63.

Hanchinamani, G., & Kulakarni, L. (2014). Image encryption based on 2-D Zaslavskii chaotic map and pseudo hadmard transform. *International Journal of Hybrid Information Technology, 7*(4), 185-200.

Hoffstein, J., Pipher, J. & Silverman, J. H. (2008). An introduction to mathematical cryptography (1st edition). Springer Science + Business Media, New York, USA. Pp.10-65.

Mishkovski, I., & Kocarev, L. (2011). Chaos-based public-key cryptography. In *Chaos-Based Cryptography: Theory, Algorithms and Applications* (pp. 27-65). Berlin, Heidelberg: Springer Berlin Heidelberg.

Mishra, M., & Mankar, V. H. (2011). Chaotic Encryption Scheme Using 1-D Chaotic Map. *International Journal of Communications, Network and System Sciences*, *4*(10), 452-455.

Mishra, M., Mishra, P., Adhikary, M. C., & Kumar, S. (2012). Image encryption using Fibonacci-Lucas Transformation. *International Journal on Cryptography and Information Security*, *2*(3), 131-141.

Nkapkop, D. J., Effa, Y. J., Fouda, E. A. J., Alidou, M., Bitjoka, L., & Borda, M. (2014). A fast image encryption algorithm based on chaotic maps and the linear diophantine equation. *Computer Science and Applications*, *1*(4), 232-243.

Ramadan, N., Ahmed, H. H., Elkhamy, S. E., & Abd Abd El-Samie, F. E. (2016). Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map. *American Journal of Signal Processing,* 6(1), 1-13.

Ramahrishnan, S., Elakkiya, B., Geetha, R., & Vasuki, P. (2014). Image encryption using chaotic maps in Hybrid Domain. *International Journal of Communication and Computer Technologies*, *2*(5), 44-48.

Rössler, O. E. (2020). On the Rössler Attractor. *Chaos Theory and Applications*, 2(1), 1-2.

Stinson, D. R., (2006). *Cryptography theory and practice* (3rd edition). Chapman & Hall/CRC, New York, Pp. 1-186.

Wang, P., Wang, Y., Xiang, J., & Xiao, X. (2022). Fast image encryption algorithm using logistics-sine-cosine mapping. *Sensing and Imaging*, 22(24), 9929.

Wikipedia (2023). Rossler Attractor. Retrieved from https://en.wikipedia.org/w/index.php?title=Rössler_attractor&oldid=1155904881

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications*, *1*(2), 31-38.

Wu, Y., Yang, G., Jin, H., & Noonan, J. P. (2012). Image encryption using the two-dimensional logistics chaotic map. *Journal of Electronic Imaging*, 21(1), 28p.

Yakubu, H. J., & Aboiyar, T. (2018). A chaos-based image encryption algorithm using Shimizu-Morioka System. *International Journal of Communication and Computer Technologies*, *6*(1), 07-11.

Ye, R. (2013). A highly secure image encryption scheme using compound chaotic maps. *Journal of Emerging Trends in Computing and Information Sciences*, *4(*6), 532-544.