Image Encryption Algorithm for Grayscale Images Using 3-D Chaotic System

[1]Yakubu H. J., [2]Malgwi Y. M., and [3]Emmanue P. M

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

[2]Department of Computer Science, Modibbo Adama University, Yola, Adamawa State, Nigeria.

[3]Department of Computer Science, Ramat Polytechnic Maiduguri. Borno State, Nigeria.

DOI: https://doi.org/10.51584/IJRIAS.2025.10020018

Received: 27 January 2025; Accepted: 01 February 2025; Published: 06 March 2025

ABSTRACT

Online attacks on sensitive information such as medical imaging, military imaging, architectural imaging, industrial imaging and many more of its kind is on the increase due to advancement in technology. Therefore, the search for a stronger method that can stand against these attacks either on transit or on storage is also on the increase. Studies have shown that 3-D continuous-time chaotic systems are found to contained in abundance chaotic structures and complex dynamical behaviour which could improve the quality and security of a cryptosystem and hence the need to explore the Rössler system. In this paper, a grayscale image encryption algorithm using 3-D Rössler chaotic system is proposed. The proposed algorithm used the rich chaotic properties of the Rössler system to ensured that both confusion and diffusion properties for a secure cipher is achieved. A standard test image namely "cameraman gray 256.tif" was used in testing the proposed scheme. Security analysis such as the Histogram Uniformity Analysis (HUA), Correlation Coefficient Analysis (CCA), Number of Pixels Change Rate (NPCR), and the Unified Averaged Changing Intensity (UACI) were carried out on the proposed scheme. Results obtained from the analysis revealed that the proposed scheme is very effective and can withstand any statistical, differential or brute-force attack.

Keywords: Confusion, Diffusion, Symmetric-Key, Grayscale image, Rössler attractor, Fixed point, Plain/cipher image, Encryption/Decryption algorithm.

INTRODUCTION

Images can be considered as one of the most widely used types of media being exchanged over the public network called the Internet, due to the fact that it is the fastest medium for conveying concepts. This Internet though efficient is exposed to various threats (Alkhonaini et al., 2024; Abd-Elsamie et al., 2014). Some of these images are highly confidential (sensitive) and need to be protected not only when they are on transit but also when on storage medium (Abd-Elsamie et al., 2014). Many different cryptographic techniques for securing sensitive information have been developed by many researchers over decades. Most of these techniques could not encrypt image data efficiently due to the fact that image data are large in size, have low entropy, strong pixel correlation and high redundancy (Hu et al., 2020). However, with the advent of chaotic cryptology (which is the study of mathematical chaos theory to the practice of cryptography, the study or techniques used to privately transmit information on the internet with the presence of adversary), the design of new cryptographic algorithms based on chaotic systems have become an attractive image encryption solution because of its interesting features such as high sensitivity to initial conditions and control parameters, random-like behavior and unpredictability yet reproducible (Hu et al., 2020; Zhang and Liu, 2023; Wikipedia, 2024). In order to use chaos theory efficiently in cryptography, the chaotic maps are implemented such that the entropy generated by the map can produce required Confusion and Diffusion (Wikipedia, 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

One of the most important concerns to cryptographic scheme researchers is the cryptanalyst who tried to deciphered an encrypted message as a whole or in part when the decryption key is not known. During cryptanalyzing a ciphering algorithm, the fundamental assumption is that the cryptanalyst knows exactly the design and working 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. Chaos-based cryptography is divided into two based on the type of key used: Symmetric and Asymmetric. 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 sender and the receiver via a separate secret channel while the 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 and is different from the decryption K_d that is kept secret (i.e. $K_e \neq K_d$). Here, no additional secret channel is needed for the key transfer (Delfs and Knebl, 2007). However, majority of these chaos-based encryption schemes are symmetric (Wikipedia, 2024).

Applying chaos to cryptography was a great contribution to improving the security of information and communications due to the adequate properties of chaotic sequences. With these, chaos has huge potential applications in several vital fields of cryptography and in recent days, chaos-based methods are used for encrypting images since it has proven to have higher resistance against different attacks when compared to the traditional methods and hence, it is a good tool for encrypting images (Wu et al., 2012; Ramahrishnan et al., 2014; Abd-Elsamie et al., 2014; Ye, 2013). Several chaos-based 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 is in line with the Kerkhoff's principle. Thus, there is still need to search for more secured and efficient encryption algorithms.

RELATED WORKS

Alkhonaini et al., (2024) proposed a new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata. The proposed method combines two-way chaotic maps and reversible cellular automata (RCA). The two-way chaotic model called spatiotemporal chaos is for image confusion while the RCA is utilized for image diffusion. The method performance in encrypting grayscale images was evaluated using various analysis methods. Results show that the proposed method is a compelling image encryption algorithm with high robustness against brute force, statistical, and 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 3-D hybrid chaotic system with 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 prove it's resilience against statistical and brute-force attacks. **Alawadi, (2023)** proposed a novel chaos-based permutation for image encryption that uses 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 a XORing operation for each pixel's block. The experimental findings show the superior performance of the proposed scheme and have the ability to resist a diverse range of cyber-attacks. RGB Image Encryption Algorithm Using RSA Algorithm and 3D Chaotic System was proposed by **Yakubu et al., (2023)**. The proposed scheme adopted the confusion-diffusion technique where the RSA algorithm was used for image diffusion and a 3-D chaotic system called Shimizu-Morioka System was used for image confusion. A standard test image (Mandrill colour 200.tif) was used for testing the proposed algorithm using three different sets of keys. Results from the analyses show that the proposed scheme is highly effective and can withstand any statistical and brute-force attacks. **Zhou et al. (2023)** proposed a novel multiple-image encryption algorithm based on a two-dimensional hyperchaotic modular model. First, two-dimensional chaotic model that generate multiple types of chaotic system was proposed. Secondly, multiple images were fused and used SHA-512 to generate a secret key that increased resistance to the plain image attacks. Finally, a simultaneous permutation and diffusion was proposed to improve security and efficiency. The experimental simulations and security analysis show that the proposed algorithm can encrypt multiple images of different

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

sizes and types with good attack resistance and encryption efficiency. 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 safe and effective fast image encryption algorithm. **Yakubu and Dada, (2020)** proposed a more secured image encryption algorithm using dual 3-dimensional chaotic maps for RGB images. The proposed scheme was achieved using the chaotic sequences generated from the two 3D systems and bitXOR operations to encrypt and decrypt images. Results from the analysis revealed that the scheme is effective and can resist any statistical, differential or brute force attack. Development and analysis of a novel grayscale image encryption algorithm using a modified 1D Logistic map was proposed by **Yakubu and Zirra, (2019)**. The proposed scheme used the chaotic properties of the modified logistic map as well as MOD and bitXOR operations to obtain the cipher image and the decrypted image. The results of the analysis show that the scheme is highly effective and strong against the 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 reaction. 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 behavior of the Rossler system has been applied in many areas (Rössler, 2020; Wikipedia, 2023).

$$\dot{x} = -y - z;\ \dot{y} = x + ay;\ \ \dot{z} = bx - cz + xz: \qquad (1)$$

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

3.1 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 (Wikipedia, 2023).

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

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

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

(3)

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

3.2 Stability Analysis

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

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

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

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:

$$\boldsymbol{\lambda_1} = 0.09710 + 0.9957i, \quad \boldsymbol{\lambda_2} = 0.09710 - 0.9957i, \quad \boldsymbol{\lambda_3} = -5.6872. \quad (6)$$

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).

$$v_1 = \begin{pmatrix} 0.7073 \\ -0.07278 - 0.7032i \\ 0.0042 - 0.0007i \end{pmatrix}, v_2 = \begin{pmatrix} 0.7073 \\ -0.07278 + 0.7032i \\ 0.0042 + 0.0007i \end{pmatrix}, \ \& \ v_3 = \begin{pmatrix} 0.1682 \\ -0.0286 \\ 0.09856 \end{pmatrix} \quad (7)$$

3.3 Phase Portrait of the Rössler Chaotic System

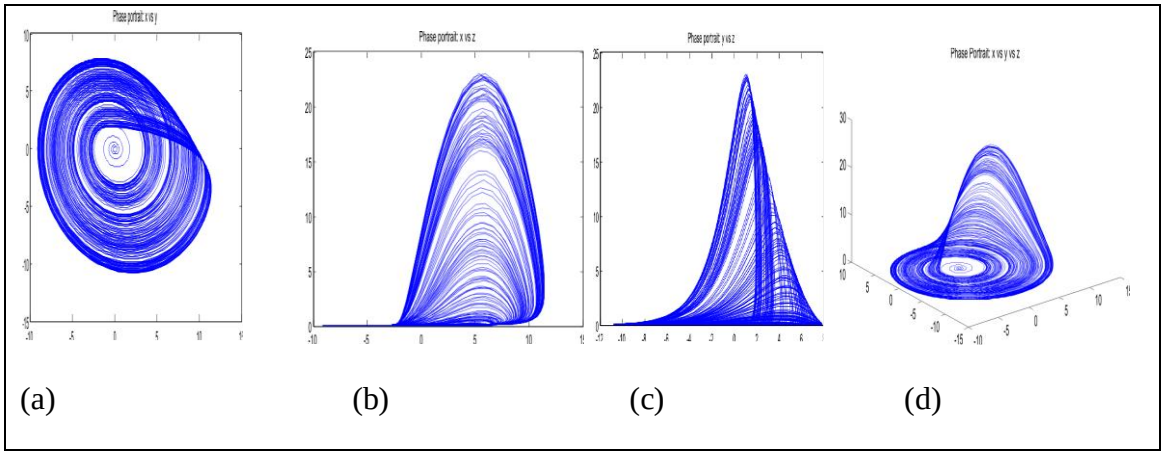
The Rössler chaotic system is given by

$$\dot{x} = -y - z;$$

$$\dot{y} = x + 0.201011y; \quad (8)$$

$$\dot{z} = 0.201011x - 5.699001z + xz:$$

where the parameters are defined as $a = b = 0.201011$ and c= 5.699001. 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 $x_0 = 0.1, \ y_0 = 0.1, \ and \ z_0 = 0.1$.



(a) (b) (c) (d)

Figure 1: Phase Portrait of the Rössler Chaotic System

THE PROPOSED ALGORITHM

This 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). The proposed scheme uses two stages. The first stage is the *confusion* (permutation) stage that breaks the correlation between adjacent pixels and the second stage is the *diffusion* stage where the pixels values are

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

transform to new values. To achieve the first 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 bit XOR operations on the scrambled image using the chaotic sequence generated from the solution of the Rössler chaotic 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 details algorithm for encryption and decryption processes are presented below

4.1 Encryption Algorithm

i. Read the gray image from a file I as your plain image,

ii. Obtain the image dimension of I as p, q,

iii. Compute the number of pixels in I (N= p*q),

iv. Enter the parameters value for $\alpha, \beta, x_0, y_0, z_0\ h$ (h is the step size) as your key

v. Solve the Rössler chaotic system N time's steps using the Euler's method to obtain solutions in vector form as x, y, z,

vi. Add confusion to the solution using round function to obtained x, y, and z,

vii. Sort the vectors x, y, and z and obtain their list of indices as $l_x,\ l_y\ and\ l_z$.

viii. Reshape the image I in to a row vector (1D) to obtain A1

ix. Use the index l_x of the sorted solution of the Rössler chaotic system to scramble the image A1 to obtain Scrambled image A2,

x. repeat step ix with the indices l_y and l_z on A2 to obtain scrambled image B2 and on B2 to obtain scrambled image C2 respectively,

xi. Reshape the scrambled image into a 2D image (p x q)

xii. Perform MOD operations on the vector solutions x, y, and z of the Rössler chaotic system and convert them into uint8 data type and 2D vector solution,

xiii. Perform bit XOR operation on the vector solution x obtained in (xii) and the pixels values of the final scrambled image C2 to obtain the first diffused image E,

xiv. Perform bit XOR operation on vector solution y obtained in (xii) and the pixels values of the image E to obtain the second diffused image F,

xv. Perform bit XOR operation on vector solution z obtained in (xii) and the pixels values of the image F to obtain the Third diffused image G as the encrypted image

xvi. Display the encrypted image G,

xvii. Save G in a file I1.

4.2 Decryption Algorithm

i. Read the encrypted image I1,

ii. Perform bitXOR operation on the encrypted image and the vector solution z obtained in (xii) to obtain image R1,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

iii. Repeat step (ii) with the vector solution y obtained in (xii) and the image R1 to obtain image R2,

iv. Repeat step (ii) again with the vector solution x obtained in (xii) and the image R2 to obtain image R3,

v. Reshape the image R3 into 1D to obtain image R4

vi. Reposition the entries in R4 with the indices l_z first then l_y and finally l_x to obtain image R5 as our decrypted image,

vii. Reshape R5 into square matrix (p x p) to obtain image R6.

viii. Display the decrypted image R6.

ix. Save R6 in a file I2.

RESULTS AND DICUSSION

5.1 Implementation

The practical aspect of this work was carried out using a standard test digital grayscale image of size 256x256, stored with TIF file format (cameraman_gray_256.tif) as an 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.

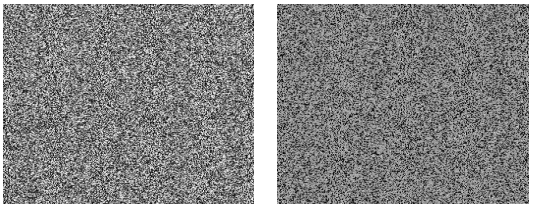
Original image

Figure 2: Plain Image

5.2 Results and Discussion

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 using the chaotic properties of the solutions vector x, y, and z obtained from the Rössler system (first scrambled with x then with y and finally with z) in order to break the correlations between adjacent pixels of the plain image. as shown in Figure 3a. The encrypted (diffused) image also called cipher image was obtained using XOR operation on the solution vectors x, y, and z obtained from the Rössler chaotic system (First with x then y and finally z) and the pixels values of the scrambled image as shown in Figure 3b.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025



(a) (b)

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

To recover the plain image, the decryption algorithm was applied to the cipher image using 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 deciphered by applying the XOR operation solution vectors and the cipher image but in reversed order (vector z first, then vector y and finally vector x) to obtain scrambled image. Next, the pixels values of the scrambled image obtained were then reposition to their original position using the sorted list l_x, l_y and l_z but in reverse order (first with l_z, then with l_y and finally with l_x). Finally, reshape the image vector into a square matrix to obtain our original image called the plain image or decrypted image as shown in Figure 4.

Decrypted image

Figure 4: Decrypted (Cipher) image

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-Elsamie et al., 2014). To test the strength of the proposed algorithm, security analysis such as the statistical analysis (which include histogram uniformity analysis and the correlation coefficient analysis) and the differential analysis (which include the Number of Pixel Change Rate-NPCR and Unified Average Changing Intensity-UACI) were carried out as presented below.

6.1 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-Elsamie et al., 2014):

a. It must be totally different from the histogram of the original image.

b. It must have a uniform distribution, which means that the probability of occurrence of any grayscale value is the same.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

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

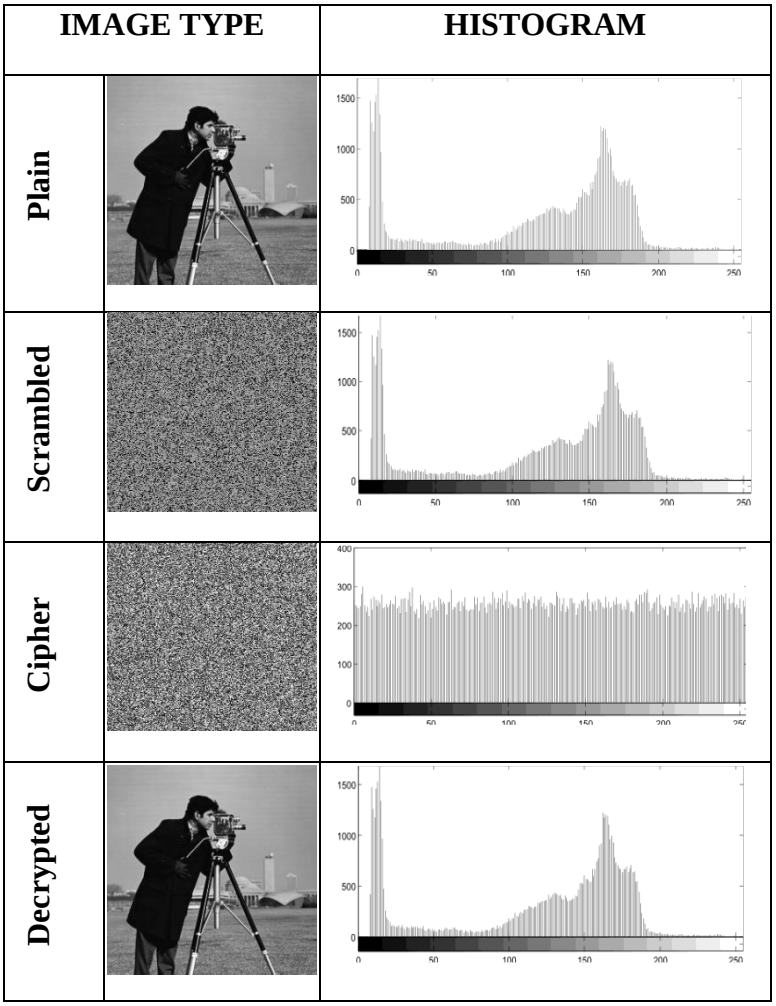


Figure 5: Histogram of the Plain, Scrambled, Cipher and Decrypted Image

6.2 Correlation Coefficient Analysis

This metric is for assessing the encryption quality of any image encryption scheme. 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. The correlation coefficient denoted by r_{xy} is calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

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:

$$E(x) = \frac{1}{L}\sum_{i-1}^{L} x_i,\ D(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))^2, \text{ and } cov(x,y) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y)) \tag{10}$$

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** (Abd-Elsamie et al., 2014; Zia et al., 2022).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

Figure 6 and Figure 7 present the correlation between adjacent pixels of the plain image and the cipher image respectively. From Figure 6, one can see that the correlation between adjacent pixels in all the three directions of the plain image are very strong as indicated by the correlation coefficients obtained (with a minimum correlation coefficient of 0.9352 on the horizontal direction and a maximum correlation coefficient of 0.9601 on the vertical direction). Also, looking at Figure 7, we can see is a completely opposite result of Figure 6. From the figure, one can see clearly that the correlation between adjacent pixels in all the three directions of the cipher image are very weak as indicated by the correlation coefficients obtained (with a maximum correlation coefficient of 0.0036 on the horizontal direction and a minimum correlation coefficient of -0.0018 along the diagonal direction) that are almost zero, indicating the proposed scheme is of good quality and therefore can withstand any statistical attack.

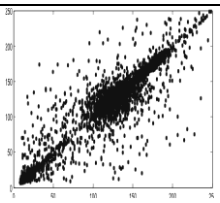
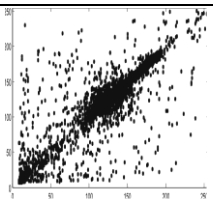
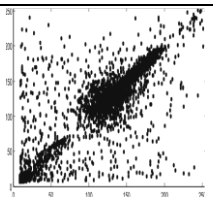
PLAIN IMAGE		
Vertical	**Horizontal**	**Diagonal**
		
r_{xy} = 0.9601	r_{xy} = 0.9352	r_{xy} = 0.9504

Figure 6: Correlation between adjacent pixels of the Plain Image

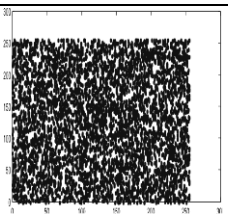
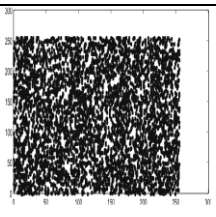
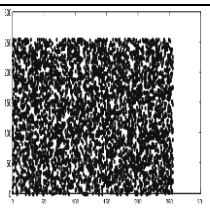
CIPHER IMAGE		
Vertical	**Horizontal**	**Diagonal**
		
r_{xy} = 0.0032	r_{xy} =- 0.0036	r_{xy} = -0.0018

Figure 7: Correlation between adjacent pixels of the Cipher Image

6.3. Differential/Sensitivity Analysis

For an image encryption scheme to be able to resist the differential attack efficiently, the scheme must be sensitive to small change in the plain image that gives 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-image. NPCR and UACI values of an encryption scheme are evaluated using the following formulas:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (11)$$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue II February 2025

$$UACI = \frac{1}{W \times H}\left[\sum_{I,J} \frac{[C_1(i,j) - C_2(i,j)]}{255}\right] \times 100\% \quad (12)$$

where C_1 and C_2 denote the two ciphered images whose corresponding plain-images have only 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., 2011; Wu et al., 2012; Ramadan et al., 2016; Zia et al., 2022).

Study 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 varies depending on the image type and size used. The theoretical NPCR scores for gray images with 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 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. An encryption algorithm is considered worthy of use if the experimental NPCR score is equals 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 presents the experimental NPCR and UACI scores of the proposed scheme on three different grayscale images of size 256x256 namely: cameraman_gray_256.Tif, Lena_gray_256.Tif, and Baboon_gray_256.Tif. The results obtained have satisfied both the NPCR and UACI requirements, which shows that the proposed scheme is effective and can withstand any differential attack.

Table **1:** The Npcr And Uaci Values From The Proposed Scheme

IMAGE	NPCR (%)	UACI (%)
Cameraman gray 256	99.6315	33.2107
Lena gray 256	99.6023	33.3412
Baboon gray 256	99.6195	33.2951

CONCLUSION

This paper proposed image encryption algorithm for grayscale 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 cameraman_gray_256.tif was used in testing the proposed scheme. Security analysis such as statistical and differential analyses were carried out on the proposed scheme and the results obtained from these analyses show that the proposed scheme is highly effective and very strong against the statistical, the differential and the brute-force attack.

REFERENCES

1. 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. CRC Press, London. 1st Edition. Pp: 1-86.
2. Alawadi M. (2023). A Noval Chaos-based Permutation for Image Encryption. Journal of King Saud University-Computer and Information Sciences, 35(2023):101595.
3. Alkhonaini M. A., Gemeay E., Mahmood F. M. Z., Ayari M., Alenizi F. A., & Lee S. (2024). A New Encryption Algorithm for Image Data Based on Two-way Chaotic Maps and Iterative Cellular Automata. Scientific Reports,14(2024):16701

4. Darani A. Y., Yengejeh Y. K., Pakmanesh H., & Navarro G. (2024). Image Encryption Algorithm based on New 3D Chaotic System Using Cellular automata. Chaos, Soliton and Fractals, 179(2024), 114396.
5. Delfs, H., & Knebl, H. (2007). Introduction to Cryptography-Principles and Applications. Springer Berlin Heidelberg, New York, USA. 2nd Edition. Pp: 1-65.
6. Denning, D. E. (1982). Cryptography and Data Security. Addison-Wesley Publishing Company Inc., USA. Pp. 1-116.
7. Hu X., Wei L., Chen W., Chen Q., & Guo Y. (2020). Color Image Encryption Algorithm Based on Dynamic Chaos and Matrix Convolution. IEEE Access, 8(2020):12452-12466.
8. Ramadan, N., Ahmed, H. H., Elkhamy, S. E., & 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.
9. 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.
10. Rössler O. E. (2020). On the Rössler Attractor. Chaos Theory and Applications, 2(1): 1-2.
11. Stinson, D. R. (2006). Cryptography Theory and Practice. Chapman & Hall/CRC, New York. 3rd Edition. Pp: 1-186.
12. Wang P., Wang Y., Xiang J., & Xiao X. (2022). Fast Image Encryption Algorithm using Logistics-Sine-Cosine Mapping. Sensing and Imaging, 22(24): 9929, https://doi.org/10.3390/s22249929.
13. Wikipedia (2023). Rössler Attractor. https://en.wikipedia.org/wiki/R%C3%B6ssler attractor, 12p.
14. Wikipedia (2024). Chaotic Cryptology. https://wikipedia.org/wiki/Chaotic cryptology, 5p.
15. 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. Pp: 31-38.
16. 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): 28pp.www.nature.com/scientificreports
17. Yakubu H. J. & Dada E. G. (**2020**). A More Secured Image Encryption Algorithm using Dual 3-Dimensional Chaotic Maps for RGB Images. International Journal of Computer Trends and Technology, 68(10): 35-43.
18. Yakubu H. J. & Zirra P.B. (2019). Development and Analysis of a Novel Grayscale Image Encryption Algorithm using a Modified 1D Logistic Map. Research Journal of Science, 19(1): 39-51.
19. Yakubu H. J., Joseph S. B. & Yahi N. M. **(2023)**. RGB Image Encryption Algorithm Using RSA Algorithm and 3D Chaotic System. Arid Zone Journal of Basic and Applied Research, 2(2): 151-167.
20. 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.
21. Zhang B. & Liu L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics, 11(2023):2585, https://doi.org/10.3390/math11112585
22. Zhou, Z., Xu, X., Yao Y., Jiang Z., & Sun K. (2023). Novel Multiple-Image Encryption Algorithm Based on a Two-dimensional Hyperchaotic Modular Model. Chaos, Solitons & Fractals, 173(2023):113630.
23. Zia U., McCartney M., Scotney B., Martinez J., Abutair M., Memon J., & Sajjad A. (2022). Survey on Image Encryption Techniques Using Chaotic Maps in Spatial Transform and Spatiotemporal Domains. International Journal of Information Security, 21(2022):917-935.