Chaos-Based Image Encryption Algorithm for RGB Images Using Rucklidge Chaotic System

JOSEPH H. YAKUBU[1], MUSA ASHIRU[2], EMMANUEL P. MUSA[3]
[1]*Department of Computer Science, Faculty of Physical Sciences, University of Maiduguri, Nigeria*
[2]*Department of Mathematics and Computer Science, Borno State University, Maiduguri, Nigeria*
[3]*Department of Computer Science, Ramat Polytechnic, Maiduguri, Borno State, Nigeria*

Abstract-The advent of chaos theory has brought significant advancement in the field of cryptography. In recent years, chaos-based cryptosystems have been an active area of research. This is due to the fact that properties of chaotic systems and cryptographic primitives share unique characteristics that allow for the chaotic systems to be applied to cryptography. A chaos-based cryptosystem that utilizes a chaotic system that contained chaotic structures and complex dynamical behavior makes it next to impossible for the adversary to gain access to the message either on transit or on storage without any knowledge of the key. Studies have shown that 3-D continuous-time chaotic systems are found to contained in abundance chaotic structures and complex dynamical behavior which could improve the quality and security of a cryptosystem and hence the need to explore the Rucklidge chaotic system. This paper proposed image encryption algorithm for RGB images using the Rucklidge chaotic system. The proposed algorithm adopted the classic framework of the permutation substitution network in cryptography by using the rich chaotic properties of the Rucklidge system which produced required confusion and diffusion properties for a secure cipher. A standard test image namely mandrill_colour_200.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 show that the proposed scheme is effective and strong against the statistical, differential and brute-force attacks.

Indexed Terms-Asymmetric/Symmetric-Key, RGB Image, Plain/Cipher image, Encryption/Decryption algorithm, Rucklidge system

I. INTRODUCTION

Network security and Data security have always remained issues of significant importance when it comes to sharing confidential information on public domain such as the Internet though efficient is exposed to various threats. Advancement in technology has made multimedia information to be shared and stored over the Internet mostly in form of images some of which are highly sensitive. Confidentiality and authenticity of digital images are ensured by using different image hiding techniques [23]. Steganography and Cryptography are two 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 into an unreadable and unintelligent form so that only authorized person can recover the information by decryption processes. However, of these two, cryptography is generally acknowledged as the best method of information protection against both passive and active attacks [10] & [11].

One of the fundamental and classical goals of cryptography is Providing confidentiality between two communicating parties using encryption methods. However, cryptography has now gone beyond secret communication. It can perform other functions such as message authentication, digital signatures, protocol for exchanging secret keys, etc. [6]. 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 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 [5] & [14].

The advent of chaos theory, has made the study of chaotic systems become an important topic in the field of nonlinear dynamics because of their complex and high dynamic nature characterized by sensitivity to initial conditions and control parameters, random-like behavior and unpredictability yet reproducible that make it difficult to predict and control the systems [8], [23] & [21]. Chaotic systems have wide range of applications in many fields. For instance, in finance, chaotic systems are used in modeling the behavior of financial markets and develop trading strategies, in biology, chaotic systems are used in studying population dynamics and behavior of biological systems, while in neural networks, chaotic systems are used in modeling behavior of neurons and develop new algorithms for machine learning and artificial intelligence, and in data communications, chaotic systems are used in developing secured communication systems through encryption techniques that is now referred to as chaotic cryptography which is the application of mathematical chaos theory to the practice of cryptography, [21]. In recent years, many researchers have shifted their research interest to chaotic cryptography which include discrete chaotic maps and continuous chaotic systems [16] & [21].

Studies have shown that properties in chaotic systems and cryptographic primitives share unique characteristics that allow for the chaotic systems to be applied to cryptography. However, in order to use chaos theory efficiently in cryptography, the chaotic maps are implemented such that the entropy generated by the maps can produce required confusion and diffusion [21]. 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 statistical and differential attacks when compared to the traditional methods like Data Encryption Standard (DES), Advance Encryption standard (AES), International Data Encryption Algorithm (IDEA), etc. and hence, it is a good tool for encrypting images [1], [12], [18], & [20].

II. RELATED WORKS

[4] proposed a novel symmetric cryptosystem for the transmission of RGB colour images through open channels. 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 its resilience against statistical and brute-force attacks. A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata was proposed by [3]. 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. [2] 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 [19]. 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. [22] 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 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. [8] proposed a colour image encryption algorithm based on dynamic chaos and matrix convolution. The algorithm combines the cloud model with the generalized Fibonacci, creating a new complex chaotic system that realizes the dynamic random variation of chaotic sequences which is used to scramble the pixel coordinates of the plain image. The chaotic sequence value is used as a matrix convolution cloud algorithm that alternately updates the input value of the matrix convolution operation and the pixel value to obtain the permutation transformation of the original pixel value. Finally, the pixel values of the replacement and cloud model Fibonacci chaotic sequence and the pixel values of the front adjacent pixel points are subjected to a two-way exclusive XOR operation. Results from the experiment show that the algorithm can resist attack such as differential attack, plain text attack and brute force attack.

1)

2)

3)

4)

III. THE RUCKLIDGE SYSTEM

The Rucklidge system is a 3-D nonlinear model of a double convection process in which motion is limited to long thin coils that models the convection in an applied vertical magnetic field and a smoothly rotating fluid layer. The Rucklidge chaotic system is defined by the following equations

$$\begin{aligned} \dot{x} &= -ax + by - yz \\ \dot{y} &= x \\ \dot{z} &= -z + y^2 \end{aligned} \quad (1)$$

where a and b, are unfolding real parameters of the system and where $x, y, z \in \boldsymbol{R}^3$ are the state variables and the dot (·) on a variable indicates the derivative of the variable with respect to time t. The system described by equation (1) was derived from partial differential equations with the help of Galekin finite element method [7].

A. Dynamical Properties of Rucklidge System

Nonlinearity: The Rucklidge system has three first order ordinary differential equation with two nonlinear terms yz and y^2 [7].

Symmetry: The Lorenz System is invariant under the symmetry [7] & [13]:

$$\begin{aligned} &(x, y, z) \to (-x, -y, z), \text{ since} \\ &-\dot{x} = -a(-x) + b(-y) - (-y)z \Longrightarrow \\ &\dot{\dot{x}} = -ax + by - yz \\ &-\dot{y} = -x \Longrightarrow \dot{y} = x \\ &\dot{z} = -z + (-y)^2 \Longrightarrow \dot{z} = -z + y^2 \end{aligned} \quad (2)$$

Equilibrium Points of the Rucklidge System: The equilibrium point of system (1) were obtained and presented as follows:

$$\text{If} \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ and } F = \begin{pmatrix} -ax + by - yz \\ x \\ -z + y^2 \end{pmatrix} \quad (3)$$

then the equilibrium points of F are found by solving $F = 0$ and the following equilibrium points were obtained [7] & [13]: $C_0 = (0, 0, 0)$ for all values of a, b and $C^{\pm} = (0, \pm\sqrt{b}, b)$ for values of $b \geq 0$.

Eigenvalues: The real eigenvalues of system (1) with parameters a = 2, b = 6.7 were found to be $\lambda_1 = 1.7749,\ \lambda_2 = -3.7749,\ \lambda_3 = -1.$ Where $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}^3$ such that the absolute values satisfy

this inequality $-\lambda_2 > \lambda_1 > -\lambda_3 > 0$. Thus system (1) is a generalized Lorenz-like system [7] & [9].

B. Phase Portrait of the Rucklidge Chaotic System

The Rucklidge chaotic system is obtained from system (1) by defining the control parameters as follows: $a = 2.120$ and $b = 6.191$. Using a MATLAB /Simulink model version 7.10.0 (2010a), the phase portraits of system (5) 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 $x_0 = 0.0\ \ y_0 = 0.1,\ \ and\ z_0 = 0.5$.

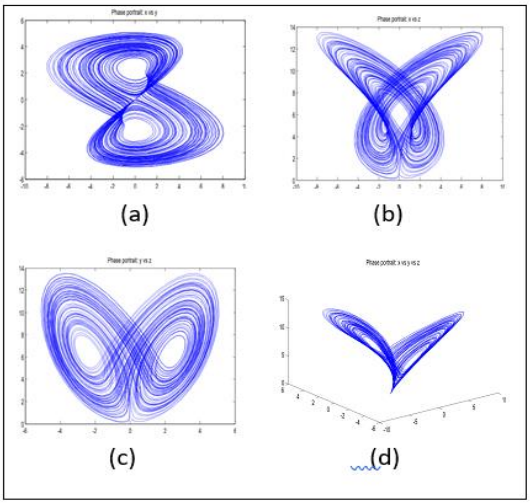


Figure 1: Phase Portrait of the Rucklidge Chaotic System

IV. THE PROPOSED ALGORITHM

The proposed algorithm is a symmetric-key encryption algorithm where a private key is shared by both communicating parties, the sender and the receiver for encryption and decryption processes respectively. To encrypt a plain image, the proposed scheme uses two stages: first is the *confusion* (mixing) stage that breaks the correlation between adjacent pixels of the plain image and second is the *diffusion* stage where pixels values are transform into new values. These two stages are achieved using the rich chaotic properties of the Rucklidge system. The solutions (x, y, z) of the Rucklidge chaotic system are obtained with Euler's method N-time's step as chaotic sequences which are used in shuffling the pixels of the plain image using initial conditions and control parameters as the key to obtain the scrambled image also called confused image. This is followed by performing the bitXOR operations on the pixels values of the shuffled image and the chaotic sequences obtained from the solutions of the Rucklidge chaotic system to obtained the cipher image also called the diffused image. To recover the plain image called the decrypted image, The decryption algorithm is applied to the cipher image with the same set of keys and using the same processes used in the encryption processes but in reverse order. The detail algorithms for encryption and decryption processes are presented below

A. Encryption Algorithm

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

B. 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 bitXOR operations on A7, B7, and C7 and the chaotic sequence obtained from the solutions of the Rucklidge chaotic system to obtain vectors A8, B8, and C8.
5) Reposition the entries in A8, B8, and C8 with the indices l_x, l_y *and* l_z respectively to obtain 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 A10, B10, and C10.
8) Display the decrypted image I2.
9) Save the decrypted image I2 in a file

V. RESULTS AND DISCUSSION

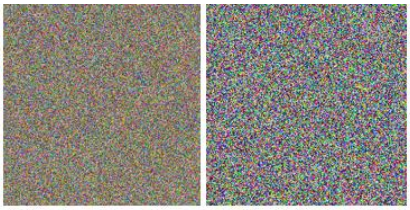
A. Implementation

The code for the proposed scheme was implemented in MATLAB version 7.10.0 (R2010a) to simulate the proposed encryption algorithm. The experimental aspect of this work was carried out on a standard test digital colour image of size 200x200, stored with TIF file format namely mandrill_colour_200.tif as an input data shown in Figure 2 to test the proposed encryption scheme.

Figure 2: Plain Image

B. 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 intensities which were then scrambled using the chaotic properties of the Rucklidge 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 then merged to obtain the cipher (encrypted) image as shown in Figure 3b.



(a) (b)

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

The plain image was recovered when 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 separated 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 reposition to their original positions and merged them to recover the plain image also called the decrypted image as shown in Figure 4.

Figure 4: Decrypted image

VI. SECURITY 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 [1]. To test the strength of the proposed algorithm, security analysis such as Histogram Uniformity Analysis (HUA), Correlation Coefficient Analysis (CCA), Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) were carried out.

A. Histogram Uniformity Analysis

In this analysis, the histograms of both the plain image and the cipher image were obtained as shown in Figures 5 and 6 respectively for the purpose of comparison. For an encryption algorithm to withstand any statistical attack, the histogram of the cipher image must be totally different from the histogram of the plain image and must have a uniform distribution, which means that the probability of occurrence of any gray scale value in the cipher image is more or less the same [1]. On comparing the histogram of the cipher image (see Figure 6) and that of the plain image (see Figure 5), the proposed scheme satisfied both conditions of histogram uniformity analysis indicating that the attacker cannot find any useful information about the plain image from the cipher image. Thus, the proposed algorithm is effective.

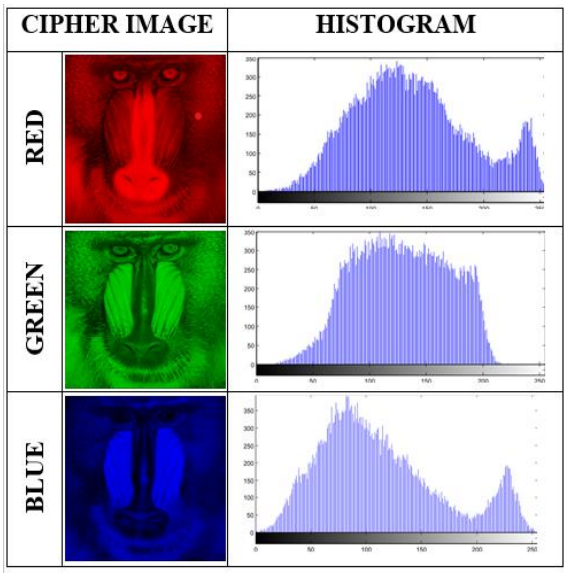


Figure 5: Histogram of the Plain Image

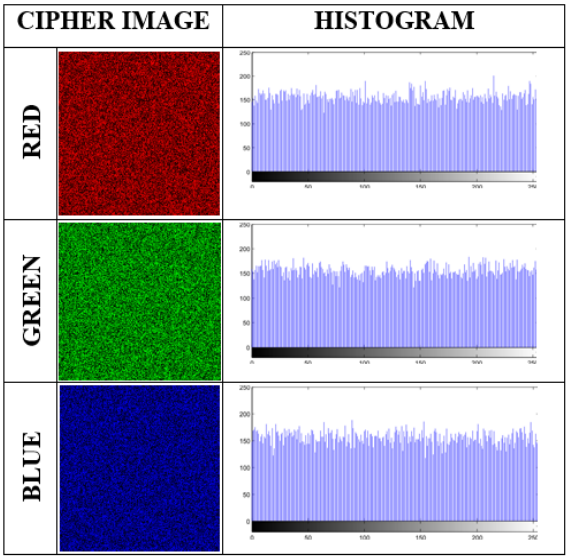


Figure 6: Histogram of the Cipher Image

B. Correlation Coefficient Analysis

This metric is for assessing the quality of any image encryption algorithm against the statistical attack. To determine this metric, only the first 5,000 pixels out of the 40,000 pixels that make up the plain/cipher image were used in the analyses. Correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels of the cipher image as well as the plain image were obtained for comparison purposes. This correlation coefficient denoted by r_{xy} is calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \quad (5)$$

where *x* and *y* are the values of two adjacent pixels in either the cipher image or the plain image. In numerical computations, the following discrete $E(x) = \frac{1}{L}\sum_{i-1}^{L} x_i$; $D(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))^2$ and $cov(x, y) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y))$ (6) where L is the number of pixels involved in the calculations [1], [3], & [23]. The closer the value of r_{xy} to zero, the better the quality of encryption algorithm is [1].

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 the three directions of the plain image in the three intensities are very strong as indicated by the correlation coefficients obtained with a minimum correlation coefficient of 0.8249 on the diagonal direction of the green channel and a maximum correlation coefficient of 0.9322 in the blue channel of the horizontal direction. However, Figure 8, presents a complete opposite of Figure 7. From the figure, one can see clearly that correlation between adjacent pixels in all the three directions on the cipher image of the three intensities are very weak as indicated by the correlation coefficients obtained with a minimum correlation coefficient of −0.0011 on the vertical direction of the red channel and a maximum correlation coefficient of 0.0085 in the green channel on the vertical direction which are almost zero, indicating that the proposed scheme is effective and can withstand any statistical attack.

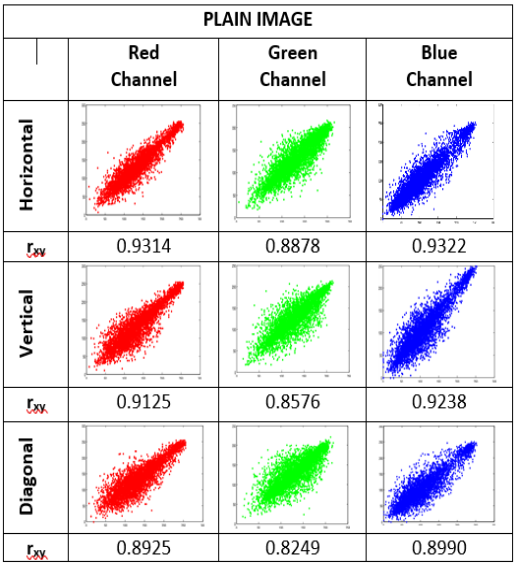


Figure 7: Correlation between adjacent pixels of the Plain Image

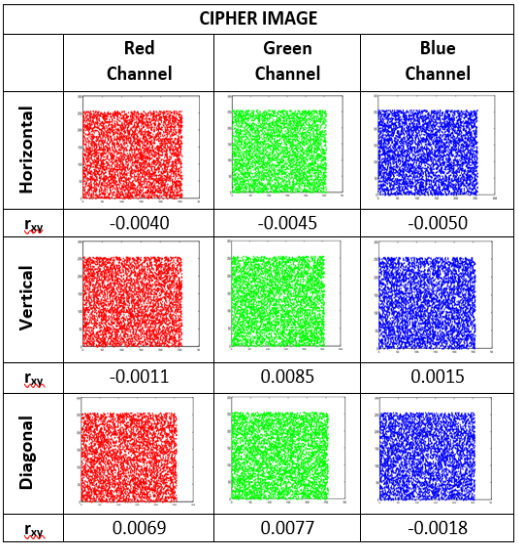


Figure 8: Correlation between adjacent pixels of the Cipher Image

C. 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:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (7)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{I,J} \frac{[C_1(i,j) - C_2(i,j)]}{255}\right] \times 100\% \quad (8)$$

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 [2], [8], & [21].

Study by [17] shows 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 [17].

Table 1 presents the experimental NPCR and UACI scores of the proposed scheme on 200x200 image in the three channels: red, green and blue components (where 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.

TABLE 1: THE NPCR AND UACI VALUES FOR THE PROPOSED SCHEME

Intensities	NPCR (%)	UACI (%)
Red	99.5731	33.3104
Green	99.5475	33.2970
Blue	99.5843	33.4355

CONCLUSION

This paper proposed image encryption algorithm for RGB images using the Rucklidge chaotic system. The proposed algorithm adopted the classic framework of the permutation substitution network in cryptographic techniques by using the rich chaotic properties of the Rucklidge system and this ensures both confusion and diffusion properties for a secured cipher. A standard test image (mandrill_colour_200.tif) was used for testing the proposed scheme. Security analyses such as the statistical and differential analysis were carried out on the proposed scheme and the results obtained show that the proposed scheme is highly effective and strong against the statistical, differential and brute-force attacks.

REFERENCES

[1] E. F. Abd El-Samie, H. E. H. Ahmed, F. I. Elashry, H. M. Shahieen, S. O. Faragallah, M. E. El-Rabaie, & A. S. Alshebeili, Image Encryption- A Communication Perspective. CRC Press, London, 1st Edition. (2014) Pp: 1-86.

[2] M. Alawadi, A Noval Chaos-based Permutation for Image Encryption. Journal of King Saud University-Computer and Information Sciences. (2023). 35(6): 101593.

[3] M. A. Alkhonaini, E. Gemeay, F. M. Z. Mahmood, M. Ayari, F. A. Alenizi, & S. Lee, A New Encryption Algorithm for Image Data Based on Two-way Chaotic Maps and Iterative Cellular Automata. Scientific Reports,14(2024):16701.

[4] A. Y. Darani, Y. K. Yengejeh, H. Packmanesh, & G. Navarro, Image Encryption Algorithm based on New 3D Chaotic System Using Cellular automata. Chaos, Soliton and Fractals, 179(2024):114396.

[5] H. Delfs, & H. Knebl, Introduction to Cryptography-Principles and Applications.

Springer Berlin Heidelberg, New York, USA. 2nd Edition. 2007. Pp: 1-65.

[6] J. Hoffstein, J. Pipher, & J. H. Silverman, An Introduction to Mathematical Cryptography. Springer Science + Business Media, New York, USA. 1st Edition. 2008. Pp: 10-65.

[7] MD. Z. Hosen, MD. Nurujjaman, S. Tahura, &, P. Ahmed. Controlliog Of Chaotic Rucklidge System with Dynamical Behaviors. The Seybold Report, 18(5). 2023. Pp:849-865.

[8] X. Hu, L. Wei, W. Chen, Q. Chen, & Y. Guo, Color Image Encryption Algorithm Based on Dynamic Chaos and Matrix Convolution. IEEE Access, 8(2020). Pp:12452-12466.

[9] Z. Keles, G. Sonugur, & M. Alcin, The Modeling of Rucklidge Chaotic System with Artificial Neural Networks. Chaos Theory and Application, 5(2). 2023. Pp: 59-64.

[10] I. Mishkovski, & L. Kocarev, Chaos-Based Public-key Cryptography, Springer-Verlag Berlin Heidelberg, SCI 354. 2011. Pp: 27-65.

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

[12] S. Ramahrishnan, B. Elakkiya, R. Geetha, & P. Vasuki, Image Encryption Using Chaotic Maps in Hybrid Domain. International Journal of Communication and Computer Technologies, 2(5). 2014. Pp: 44 – 48.

[13] V. Rusyn, Modeling, Analysis and Control of Chaotic Rucklidge System. Journal of Telecommunication, Electronic and Computer Engineering, 11(1). 2019. Pp:43-47.

[14] D. R. Stinson, Cryptography Theory and Practice, 3rd Edition, Chapman & Hall/CRC, New York. 2006. Pp.: 1-186.

[15] P. Wang, Y. Wang, J. Xiang, & X. Xiao, Fast Image Encryption Algorithm using Logistics-Sine-Cosine Mapping. Sensing and Imaging, 22(24). 2022. Pp:9929, https://doi.org/10.3390/s22249929.

[16] Wikipedia (2025). Chaotic Cryptology. https://wikipedia.org/wiki/Chaotic_cryptology, 5p.

[17] Y. Wu, J. P. Noonan, & S. Agaian, NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications. 2011. Pp: 31-38.

[18] Y. Wu, G. Yang, H. Jin, & J. P. Noonan, Image Encryption Using the Two-dimensional Logistics Chaotic Map. Journal of Electronic Imaging, 21(1). 2012. 28pp.

[19] H. J. Yakubu, S. B. Joseph & N. M. Yahi, RGB Image Encryption Algorithm Using RSA Algorithm and 3D Chaotic System. Arid Zone Journal of Basic and Applied Research, 2(2). 2023. Pp: 151-167.

[20] R. Ye, A Highly Secure Image Encryption Scheme Using Compound Chaotic Maps. Journal of Emerging Trends in Computing and Information Sciences. 4(6). 2013.Pp: 532 – 544.

[21] B. Zhang & L. Liu, Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics, 11(2585). 2023.39p. https://doi.org/10.3390/math11112585

[22] Z. Zhou, X. Xu, Y. Yao, Z. Jiang, & K. Sun, Novel Multiple-Image Encryption Algorithm Based on a Two-dimensional Hyperchaotic Modular Model. Chaos, Solitons & Fractals, 173(2023):113630.

[23] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. Abutair, J. Memon, & A. Sajjad. Survey on Image Encryption Techniques Using Chaotic Maps in Spatial Transform and Spatiotemporal Domains. International Journal of Information Security, 21(2022). Pp: 917-935.