

Original Article

# A More Secure Image Encryption Algorithm Using Dual 3-Dimensional Chaotic Maps for RGB Images

H. J. Yakubu<sup>1</sup>, E. G. Dada<sup>2</sup>

<sup>1,2</sup> Department of Mathematical Sciences, Faculty of Science, The University of Maiduguri, Maiduguri, Nigeria.

Received Date: 19 September 2020

Revised Date: 20 October 2020

Accepted Date: 22 October 2020

**Abstract** - The need for more secure image communications over the public network cannot be overemphasized due to the high increase in cyber-attacks. Cryptography is acknowledged as the best method of information protection and image security. An encryption algorithm's security must be entirely based on the secret key, also called the private key. The stronger the secret key, the more secured the encryption algorithm is. Studies have shown that 3-Dimensional continuous-time chaotic systems contain large chaotic structures and complex dynamical behaviour that are highly useful for secure communication systems. In this paper, we proposed a more secure image encryption algorithm using two 3-Dimensional chaotic maps (Rabinovich-Fabrikant Equations and Shimizu-Morioka System) for colour images. The proposed scheme adopts the general architecture of the chaotic image encryption algorithm of cryptography, ensuring both confusion and diffusion properties for a secure cypher. The confusion stage is achieved using the rich, chaotic properties of both the Rabinovich-Fabrikant equations and the Shimizu-Morioka system.

In contrast, the diffusion stage is achieved using the MOD and bitXOR operations on the pixels values of the confused image and the sequence of solutions generated from the two chaotic maps. The proposed scheme is an asymmetric key encryption scheme where both parties use the secret key (a set of 13 different numbers, which includes the control parameters and initial conditions for the two maps). A standard test image (Mandrill\_colour\_256.tif) was used in testing the proposed scheme. Security analysis, such as the statistical analysis, which includes Histogram Uniformity analysis and Correlation Coefficient analysis, as well as the differential analysis, which includes the Number of Pixels Change Rate (NPCR) and the Unified Averaged Changing Intensity (UACI), was carried out on the proposed scheme. Results obtained from the analysis show that the proposed scheme is highly effective and can resist any statistical, differential, or brute-force attacks.

**Keywords** - Private Key, Public key, Diffusion, Chaotic map, Brute-force attack, Differential attack, Cipher, Chaos.

## I. INTRODUCTION

Today, a huge amount of information (in the form of text, image, audio, or video) is transferred across the globe over the public network called the Internet. However, efficiency is highly insecure and therefore exposed to various threats [1]. The need to protect sensitive images from an unauthorized person wanting to have access to them becomes necessary. Image security is mostly handled using various cryptographic techniques that transform messages to be transmitted into an unreadable and unintelligent form by encryption process so that only authorized persons can correctly recover the information by decryption process and is generally acknowledged as the best method of information protection and image security [2], [3].

The traditional encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Rivest-Shamir-Adleman (RSA) algorithm, ElGamal algorithm are primarily designed for text and have been effective solutions to the information security problems [4], [5]. However, they are found not suitable for encrypting images due to the following three reasons: (i) Images are always very large in dimension, and therefore it takes more time to encrypt them with the traditional methods, (ii) A decrypted image needs not to be the same as the original image, since decrypted image with small distortion is usually acceptable to eyes due to human perception property and the high redundancy of image data, (iii) Digital image contents are strongly correlated, and this feature is not utilized by the traditional methods thereby affecting their encryption efficiency [4], [6], [7].

To improve the efficiency and security of image encryption methods, various image encryption and hiding schemes were proposed. Among these schemes, the chaos-based encryption schemes got the attention of many researchers because of their interesting properties, which include: sensitivity to initial condition and control parameters, deterministic and ergodicity [4], [6]. 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 scheme utilizing these properties will be strong against any attack [6], [12]. Encryption of digital images using chaotic maps started in 1997 by Fridrich, and since then, many researchers have applied chaos to different fields of image security [8]. Applying chaos to cryptography was a great contribution to improving the security of information and communications, in particular, image security.

Permutation (confusion) and substitution (diffusion) are the two basic components that constitute the general architecture of most chaotic image encryption algorithms [9]-[11]. The permutation is obtained by scrambling all the pixels values of the plain image using the properties of the chaotic map(s), while the diffusion is achieved by transforming all the pixels values to new values using different kinds of techniques.

In this paper, a more secure image encryption scheme using dual 3-Dimensional chaotic maps (Rabinovich-Fabrikant Equations and Shimizu-Morioka System) for colour images is proposed. The proposed scheme adopts the general architecture network in cryptography, which ensures both confusion and diffusion properties for a secure cypher. The confusion stage is achieved using the rich, chaotic properties of both the Rabinovich-Fabrikant equations and the Shimizu-Morioka system, and the diffusion stage is achieved using the MOD and bitXOR operations on the pixels values of the confused (scrambled) image and the sequence of solutions generated from both chaotic maps. The proposed scheme is a private key encryption scheme in which both the sender and the receiver have the same set of private keys, which must be established first using any of the public-key encryption schemes.

## II. RELATED WORK

A new hybrid chaotic map that is constructed by the composition of three classic chaotic maps: Logistic map, Henon map, and Ikeda map, which reveals remarkable sensitivity to the initial condition and control parameters, was proposed by [4]. Reference[5] proposed 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 chaotic hybrid map whose orbit disorder the pixel positions in the permutation process, while four skewed tent maps and one Arnold map were employed to yield two random grey value sequences to change the grey 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 keyspace, the statistical attack, and the differential attack. A chaotic image encryption algorithm with different modes of operation was proposed in [1]. The proposed encryption algorithm was achieved by implementing a two-dimensional chaotic Baker map for scrambling image pixels using three different modes of operation: cypher-block chaining (CBC), cypher feedback (CFB), and output feedback (OFB) to improve its security. Reference[26] proposed a new one-dimensional chaotic map suitable for real-time image encryption. Theoretical

analysis shows that the proposed map has a chaotic regime and proves its ergodicity for a large space of values of the control parameter. A novel approach for image encryption based on a 2-D Zaslavskii map and Pseudo Hadamard transform was proposed [14]. 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 backwards) 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. Reference [19]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 their value. At the diffusion step, the shuffled image is split into  $n$  sub-images. 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 the right candidate for real-time secure image transmission applications. A chaos-based image encryption scheme using an improved Quadratic chaotic map was proposed in [6]. The proposed image encryption scheme is based on two chaotic maps: the Chebyshev chaotic map that 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. Reference [25]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. In the diffusion stage, we performed MOD and bitXOR operations on the pixels values of the shuffled image and the sequence of solutions obtained from the system. Performance analysis of 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 statistical and differential attacks. A new image encryption scheme for RGB images using Rabinovich-Fabrikant Equations was proposed in [27]. First, new ranges of rich, complex, chaotic behaviour of the Rabinovich-Fabrikant Equations with no physical meaning sets of parameters values were discovered and used in building the proposed scheme. The proposed scheme adopts the classic framework of the permutation–substitution network of cryptographic architecture. A permutation is achieved using the rich, chaotic properties of the map.

In contrast, substitution is achieved using the MOD and bitXOR operations on the pixels values and chaotic sequence of the map. This ensures both confusion and diffusion properties for a secured cypher. Security Analysis of the proposed scheme reveals that the scheme is effective and can withstand any statistical, differential, or brute-force attacks.

### III. RABINOVICH-FABRIKANT EQUATIONS

The Rabinovich-Fabrikant equation is a chaotic dynamical system of three ordinary differential equations in three variables and two parameters given as

$$\begin{aligned} \dot{x} &= y(z - 1 + y^2) + ax, \\ \dot{y} &= x(3z + 1 - x^2) + ay, \\ \dot{z} &= -2z(b + xy). \end{aligned} \tag{1}$$

Where the parameters  $a, b$  are positive [22], this system (1) models the stochasticity arising from the modulation instability in a non-equilibrium dissipative medium. For  $a < b$ , the system (1) is characterized by the appearance of attractors in the phase space [13].

#### A. System Equilibrium Points

System (1) is equivariant with respect to the following symmetry:

$T: (x, y, z) \rightarrow (-x, y, z)$ , and has five equilibrium points:  $x_0^* = (0, 0, 0)$ ,

$$\begin{aligned} x_{1,2}^* &= \left( \pm \sqrt{\frac{bR_1 + 2b}{4b - 3a}}, \pm \sqrt{b \frac{4b - 3a}{R_1 + 2}}, \frac{aR_1 + R_2}{(4b - 3a)R_1 + 8b - 6a} \right) \\ x_{3,4}^* &= \left( \pm \sqrt{\frac{bR_1 - 2b}{3a - 4b}}, \pm \sqrt{b \frac{4b - 3a}{2 - R_1}}, \frac{aR_1 - R_2}{(4b - 3a)R_1 - 8b + 6a} \right). \end{aligned} \tag{2}$$

Where  $R_1 = \sqrt{3a^2 - 4ab + 4}$  and  $R_2 = 4ab^2 - 7a^2b + 3a^3 + 2a$ , which were obtained by hand-computing [13]. However, [13] used symbolic solvers for computational reasons to obtain the equilibrium points.

#### B. Stability Analysis of the Equilibrium Points

The behaviour of the system (1) depends sensibly on parameter  $b$  but not so much on  $a$ . Hence. One can fix  $a$  and let  $b$  be varied [16]. Because of the extreme sensitivity, numerical integration of the system (1) for  $b > 1.3$  and  $b < 0.13$  turns out to be very difficult, and therefore  $b$  is chosen in  $(b_{min}, b_{max}) = (0.13, 1.3)$ . Thus, for the region of interest defined by  $b \in (b_{min}, b_{max})$  and for fixed  $a$  say  $a = 0.1$ , the system (1) is dissipative [13]. The Jacobian matrix for system (1) is given by

$$J = \begin{pmatrix} 2xy + a & x^2 + z - 1 & y \\ -3x^2 + 3z + 1 & a & 3x \\ -2yz & -2xz & -2(xy + b) \end{pmatrix} \tag{3}$$

For equilibrium point  $x_0^*$  The associated characteristic equation is given by  $(\lambda^2 - 2a\lambda + a^2 + 1)(\lambda + 2b) = 0$ , with eigenvalues  $\lambda_{1,2} = a \pm i$  and  $\lambda_3 = -2b < 0$ . Therefore,  $x_0^*$  It is a repelling focus saddle [16]. The stability of the other four equilibrium points  $x_i^* i = 1, \dots, 4$ , cannot be evaluated in general by analytical means; therefore, a numerical approach with symbolic

computation was used to calculate and analyze the eigenvalues [16]. And because of the mentioned symmetry,  $x_{1,2}^*$  and  $x_{3,4}^*$  Have the same eigenvalues. They also found that the equilibriums  $x_{1,2}^*$  have a negative real eigenvalue  $\lambda_3$  for every  $b \in (b_{min}, b_{max})$ . On the other hand, there exists a tiny interval  $(b_1, b_2) = (1.05, 1.67)$  where the real parts of the complex roots  $\lambda_{1,2}$  are positive, while for  $b \in (b_{min}, b_1) \cup (b_2, b_{max})$  The  $Real(\lambda_{1,2}) < 0$ . Therefore,  $x_{1,2}^*$  is a stable focus node (sink) for  $b \in (b_{min}, b_1) \cup (b_2, b_{max})$  and is a repelling focus saddle for  $b \in (b_1, b_2)$ . Now for equilibriums  $x_{3,4}^*$ , because  $\lambda_3 > 0$  and  $Real(\lambda_{1,2}) < 0$  for all  $b \in (b_{min}, b_{max})$ ,  $x_{3,4}^*$  are attracting saddles for all  $b \in (b_{min}, b_{max})$ , so all orbits, starting from close neighbourhoods or attraction basins of  $x_{3,4}^*$ , will be attracted by  $x_{3,4}^*$  [16].

#### C. Chaotic Attractors

System (1) has several different chaotic attractors with different shapes, as observed by [16]. Four chaotic attractors were obtained for  $b \in (b_{min}, b_{max})$  And  $a = 0.1$  and obtained another chaotic attractor for a non-physical meaning set of parameter values:  $a = -1$  and  $b = -0.1$  [16]. New ranges of chaotic attractors with non-physical meaning sets of parameters:  $a \in (-1.4, -1.1]$  and  $b = -0.9$ ;  $b \in (-1.0, -0.79)$  and  $a = -1.13$  were obtained, which are highly useful for secured communication systems [27].

#### D. Phase Portrait of the Rabinovich-Fabrikant Equations

The Rabinovich-Fabrikant chaotic equations with a non-physical meaning set of parameters values are described by

$$\begin{aligned} \dot{x} &= y(z - 1 + y^2) - 1.13x, \\ \dot{y} &= x(3z + 1 - x^2) - 1.13y, \\ \dot{z} &= -2z(xy - 0.9141). \end{aligned} \tag{4}$$

Where the  $x, y, z$  are the state variables, and the parameters are defined as  $a = -1.13$  and  $b = -0.9141$ .

Using a MATLAB/Simulink model version 7.10.0 (2010a), the phase portraits of the system (4) in the  $xy, xz, yz$  and  $xyz$  phase planes were also obtained as shown in Fig. 1 by (a), (b), (c), and (d) respectively and the time series of the system (4) in the  $x, y, z$  and  $xyz$  were also obtained as shown in Fig. 2 by (i), (ii), (iii), and (iv) respectively when initial conditions are chosen as  $x_0 = 1.0, y_0 = 0.0, \text{ and } z_0 = 0.5$ .

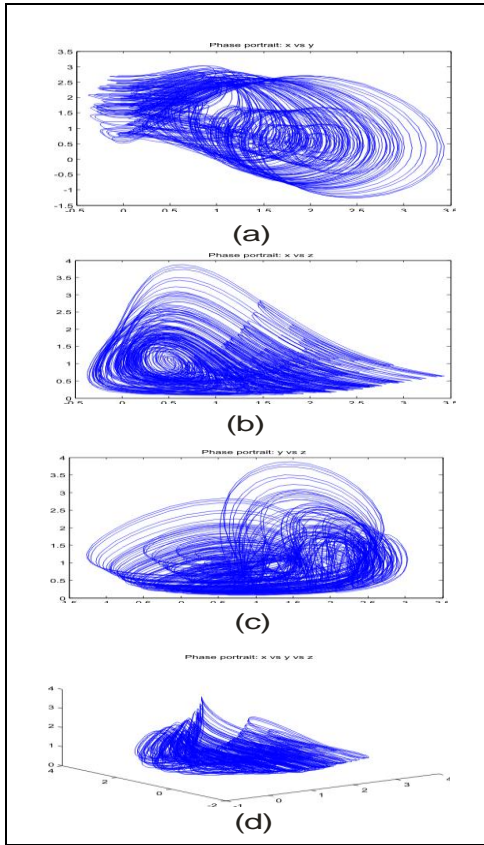


Fig. 1 Phase Portrait of System (4)

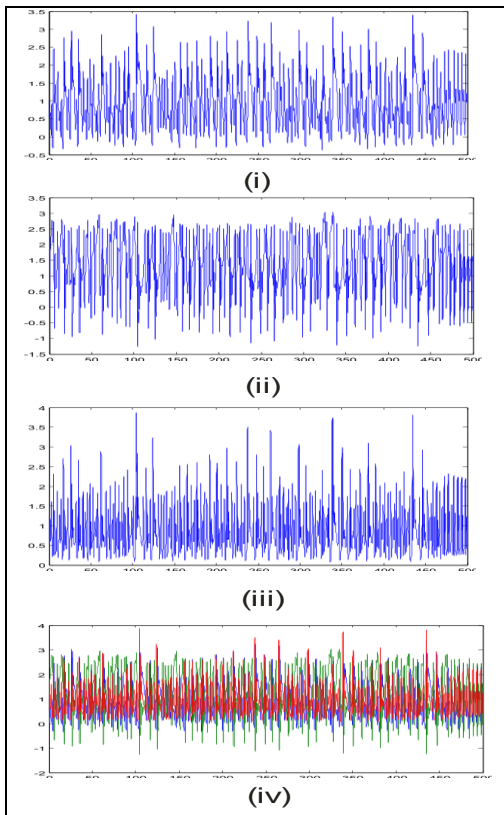


Fig. 2 Time Series of System (4)

#### IV. SHIMIZU-MORIOKA SYSTEM

The Shimizu-Morioka system is a classical three-dimensional chaotic system studied by Shimizu and Morioka in 1980 as a simplified model for studying the dynamics of the well-known Lorenz system for large Rayleigh numbers [18]. The following nonlinear equations define the Shimizu-Morioka chaotic system.

$$\begin{aligned} \dot{x} &= y, \\ \dot{y} &= -xz + x - \beta y, \\ \dot{z} &= x^2 - \alpha z. \end{aligned} \quad (5)$$

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  $\alpha$  and  $\beta$  are positive constant parameters [12], [18],[21]. In this system, stable symmetric and asymmetric periodic motions, as well as stochastic behaviour of trajectories, were discovered by Shimizu and Morioka through a computer simulation [18], [20]. The following observations were made in [12]:

- (i). System (5) is invariant with respect to the substitution  $(x, y, z) \rightarrow (-x, -y, z)$  and
- (ii). System (5) has three equilibrium states:  $(0,0,0)$ ,  $(\sqrt{\alpha},0,1)$  and  $(-\sqrt{\alpha}, 0,1)$ .

##### A. Stability Analysis of the Equilibrium points of system (5)

The following observations were presented [21]:

- If  $\alpha \geq 0$ , then system (1) has three isolated equilibrium points:  $P_0(0,0,0)$ ,  $P_1(\sqrt{\alpha},0,1)$  and  $P_2(-\sqrt{\alpha}, 0,1)$  and for  $\alpha < 0$ , it has only one isolated equilibrium point  $P_0(0,0,0)$ .
- The equilibrium point  $P_0(0,0,0)$  is unstable for all  $\alpha \in \mathbb{R}$
- The equilibrium point  $P_1(\sqrt{\alpha},0,1)$  is asymptotically stable if and only if  $\alpha > \alpha_0 = \frac{2-\beta^2}{\beta}$  where  $\beta \in (0, \sqrt{2})$
- The equilibrium point  $P_1(\sqrt{\alpha},0,1)$  is unstable if and only if  $\alpha < \alpha_0 = \frac{2-\beta^2}{\beta}$  where  $\beta \in (0, \sqrt{2})$

##### B. Phase portrait of the Shimizu-Morioka chaotic equations

The Shimizu-Morioka chaotic equations are described by

$$\begin{aligned} \begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} &= \begin{bmatrix} 0 & 1 & 0 \\ 1-z & -\beta & 0 \\ x & 0 & -\alpha \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 & 0 \\ 1-0.87501 & -0.87501 & 0 \\ 0 & 0 & -0.36501 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \end{aligned} \quad (6)$$

where we defined our parameters value as  $\beta = 0.87501$  and  $\alpha = 0.36501$ . Using a MATLAB/Simulink model version 7.10.0 (2010a), the phase portraits of the system (6) in the  $xy, xz, yz$  and  $xyz$  phase planes were also obtained as

shown in Fig. 3 by (a), (b), (c), and (d) respectively and the time series of the system (6) in the  $x, y, z$  and  $xyz$  were also obtained as shown in Fig. 4 by (i), (ii), (iii), and (iv) respectively when initial conditions are chosen as  $x_0 = 0.1, y_0 = 0.1, \text{ and } z_0 = 0.1$ .

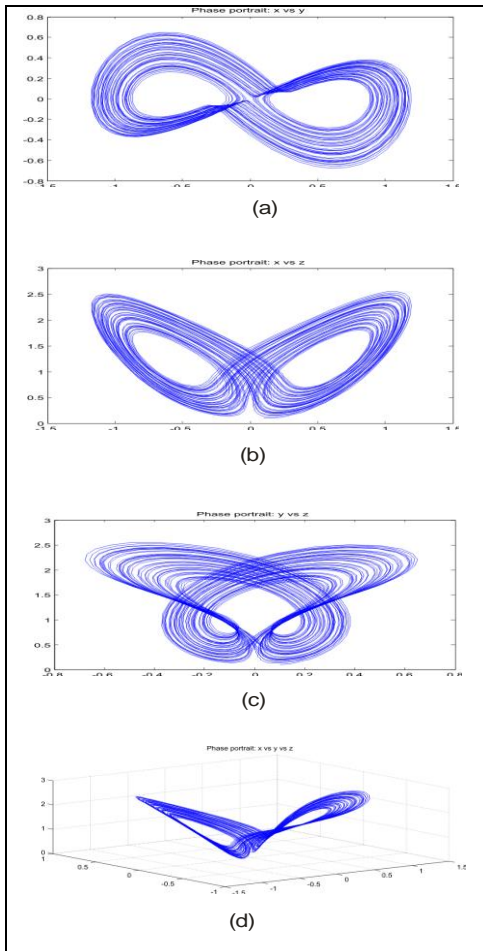


Fig. 3 Phase Portrait of System (6)

### V. PROPOSED ENCRYPTION ALGORITHM

This algorithm uses a private key for both encryption and decryption processes, which must be established first between the sender and the receiver through a public-key encryption scheme such as the RSA algorithm. The proposed scheme consists basically of two stages. The first stage is the *confusion* stage, also called the permutation or scrambling stage and the second stage is the *diffusion* stage. In the confusion stage, the pixels of the plain image is shuffled twice using the rich, chaotic properties of the Rabinovich-Fabrikant equations and the Shimizu-Morioka system using their initial conditions and control parameters as the key in order to break the strong correlation between the adjacent pixels. However, in the diffusion stage, the cypher image is obtained by performing the MOD and bitXOR operations on the shuffled image and the chaotic sequence generated from either the Rabinovich-Fabrikant equations or the Shimizu-Morioka system to redefine the pixels values of the shuffled image. The decrypted image is obtained by applying the same operations carried out in the encryption process using the same set of keys but in

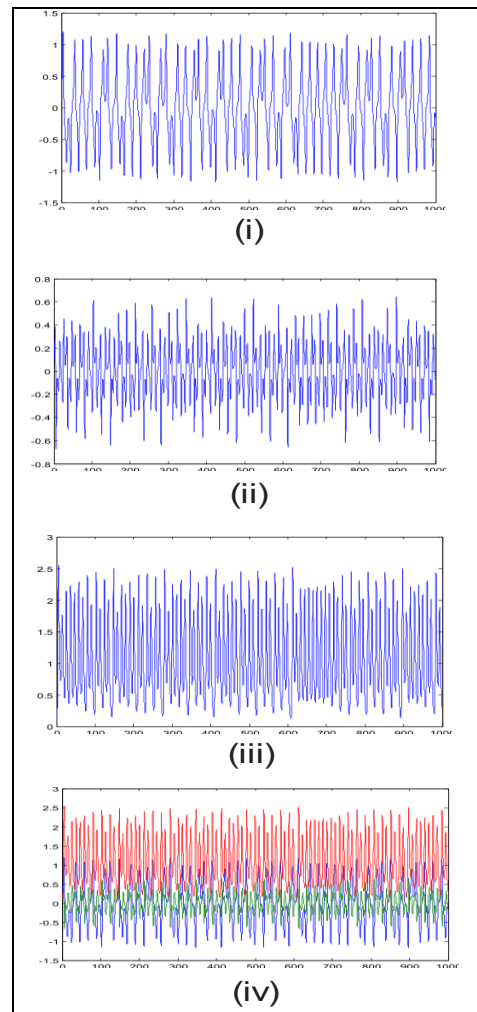


Fig. 4 Time Series of System (6)

Reverse order. The detailed algorithms for encryption and decryption processes are presented below.

#### A. Encryption Algorithm

- Read an RGB image into a file I,
- Obtain the image dimension  $p \times q \times 3$ ,
- Compute the number of pixels per colour ( $N = p \times q$ ),
- Enter the private key - set of numbers that comprised control parameters, initial conditions, and other necessary values for obtaining solutions for the two systems,
- Obtain solutions of the two systems in vector form using Euler's method with N time's steps, Say  $(x, y, z)$  and  $(X, Y, Z)$  for Rabinovich-Fabrikant equations and Shimizu-Morioka system respectively),
- Add confusion to the solutions using the round function,
- Sort the solution vectors  $(x, y, z)$  and  $(X, Y, Z)$  with their list of indices as  $l_x, l_y \text{ and } l_z$  and  $k_x, k_y \text{ and } k_z$  respectively,



- Define A, B, and C to be matrices for red, green, and blue intensities, respectively, of the plain image.
- Reshape A, B, and C into row vectors (1-Dimension) as A1, B1, and C1.
- Use the indices  $l_x, l_y$  and  $l_z$  obtained in (vii) to scramble the row vectors A1, B1, and C1 and obtain row vectors A2, B2, and C2 (first scrambled image),
- Use the indices  $k_x, k_y$  and  $k_z$  obtained in (vii) to scramble the row vectors A2, B2, and C2 and obtain A3, B3, and C3 (second scrambled image),
- Perform MOD and bitXOR operations on A3, B3, C3, and the sequence of solutions generated from the Rabinovich-Fabrikant equations to obtain another row vectors as A4, B4, and C4
- Perform MOD and bitXOR operations on A4, B4, C4, and the sequence of solutions generated from the Shimizu-Morioka system to obtain other row vectors as A5, B5, and C5
- Reshape A5, B5, and C5 into m x n matrices (2-dimension) to obtain A6, B6, and C6.
- Form the encrypted image as I1 by merging the intensities in A6, B6, and C6.
- Display the encrypted image I1.
- Save the encrypted image I1.

**B. Decryption Algorithm**

- Read the encrypted image I1,
- Define A6, B6, and C6 to be matrices for the red, green, and blue intensities, respectively, for I1.
- Reshape A6, B6, and C6 into row vectors to obtain A7, B7, and C7,
- Perform MOD and bitXOR operations on A7, B7, C7, and the sequence of solutions generated from the Shimizu-Morioka system to obtain row vectors as A8, B8, and C8
- Perform MOD and bitXOR operations on A8, B8, C8, and the sequence of solutions generated from the Rabinovich-Fabrikant Equations to obtain row vectors as A9, B8, and C8 (Recovered second scrambled image).
- Reposition the entries in A9, B9, and C9 with the indices  $k_x, k_y$  and  $k_z$  to obtain row vectors as A10, B10, and C10 (Recovered first scrambled image).
- Reposition the entries in A10, B10, and C10 with indices  $l_x, l_y$  and  $l_z$  and obtain row vectors as A11, B11, and C11 ( Recovered plain image),
- Reshape A11, B11, and C11 into square matrices to obtain A12, B12, and C12,
- Merge A12, B12, and C12 to obtain the decrypted image as I2,
- Display the decrypted image I2.
- Save the decrypted image I2 in a file.

**VI. RESULTS AND DISCUSSION**

**A. Implementation**

The proposed encryption algorithm was experimented on a standard test digital colour image of size 256x256 and stored with TIF file format (Mandrill\_colour\_256.tif) as our input data, as shown in Fig. 5. The code for the proposed scheme was implemented in MATLAB version 7.10.0 (R2010a) to simulate the proposed encryption algorithm.



Fig. 5 Plain image (Original image)

**B. Results Obtained**

After applying the proposed algorithm to the plain image shown in Fig. 5 using the private key, which comprises the initial conditions and control parameters. First, the plain image was shuffled using the chaotic sequence of solutions generated from the Rabinovich-Fabrikant Equations, and the result is shown in Fig. 6a. The shuffled image was again shuffled using the chaotic sequence of solutions generated from the Shimizu-Morioka system and obtained the second scrambled image, as shown in Fig. 6b. This second scrambled image was then encrypted using MOD and bitXOR operations on it, and the chaotic sequence of solutions generated from the Rabinovich-Fabrikant equations and the Shimizu-Morioka system where we obtained the encrypted image, also called the cypher image, as shown in Fig. 6c.

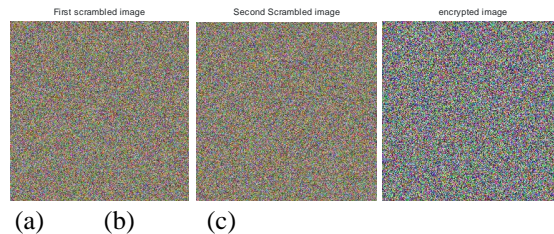


Fig. 6(a) First Scrambled Image, (b) Second Scrambled Image, (c) Encrypted (Cipher) Image

In order to recover the plain image, the decryption algorithm was applied to the cypher image using the same set of private keys. The decryption processes began with the cypher image being separated into red, green, and blue intensities, which were then transformed into undiffused but confusing images using MOD and bitXOR operations on the cypher image and the sequence of solutions obtained from the chaotic maps to obtain the second scrambled image when the intensities were merged as shown in Fig. 7a. The pixels' values of this second scrambled image were then repositioned to their original positions in their respective intensities using the indices  $k_x, k_y$  and  $k_z$  And then merged to obtain the first scrambled image, as shown in Fig. 7b. The pixels' values

of the first scrambled image were also repositioned to their original positions in their respective intensities using the indices  $l_x$ ,  $l_y$  and  $l_z$ . And were merged to obtain the decrypted image, as shown in Fig. 7c.

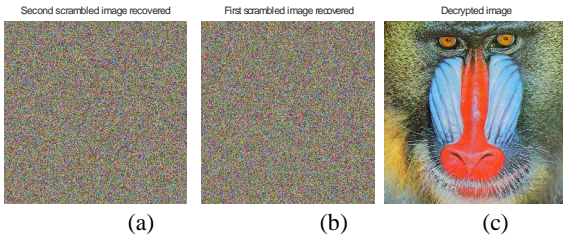


Fig. 7 (a) Second Scrambled Image, (b) First Scrambled Image, (c) Decrypted image

### VII. 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. These changes must be in an irregular manner that maximizes the difference in pixel values between the original and the encrypted image for the encryption algorithm to be considered good enough. Also, a good encrypted image must be composed of totally random patterns that do not reveal any of the features of the original image [1]. To test the robustness of the proposed scheme, security analyses such as Histogram Uniformity analysis, Correlation Coefficient analysis, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI) were performed on the results of the proposed scheme.

#### A. Histogram Uniformity Analysis

For an image encryption algorithm to be considered worthy of use, the histogram of the encrypted image should satisfy these two properties [1]:

- It must be different from the histogram of the original image.
- It must have a uniform distribution, which means that the probability of occurrence of any grayscale value is the same.

Fig. 8 shows the histogram of the plain image in the Red, Green, and Blue intensities, and Fig. 9 shows the histogram of the encrypted (cypher) image also in Red, Green, and Blue intensities. On comparing the two, it is very clear that the histogram of the cypher image in all three intensities is completely different from that of the plain image. Also, the histogram of the cypher image in all three intensities are uniformly distributed. Thus, the proposed scheme satisfies the two conditions of histogram uniformity analysis, indicating that the attacker cannot obtain any hint about the plain image from the cypher image.

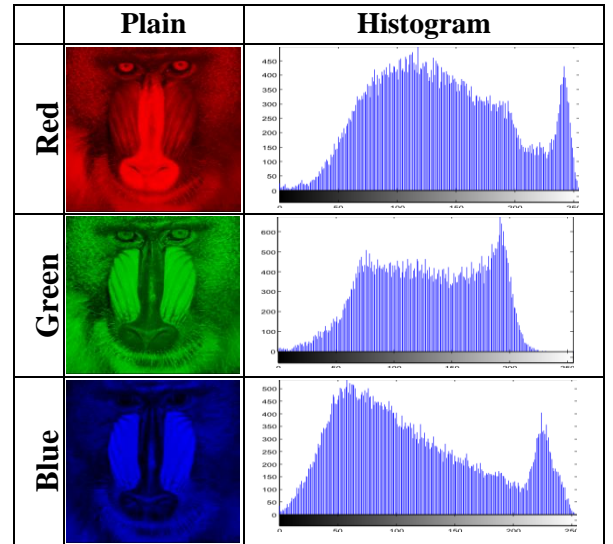


Fig. 8 Histogram of the Plain Image

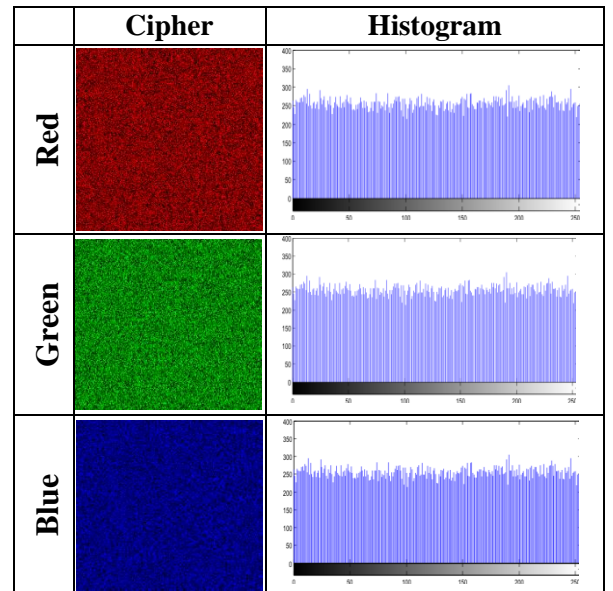


Fig. 9 Histogram of the Cipher Image

#### B. Correlation Coefficient Analysis

One useful metric for assessing the quality of any image encryption algorithm is the correlation coefficient between adjacent pixels of the cypher image. Out of the 65536 pixels of the image used, only the first 5000 pixels were used in the analyses for determining the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in the cypher-image as well as the plain image for comparison purposes. This metric is calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (7)$$

where  $x$  and  $y$  are the values of two adjacent pixels in the cypher image. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{L} \sum_{i=1}^L x_i, \quad (8)$$

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

$$cov(x, y) = \frac{1}{L} \sum_{i=1}^L (x_i - E(x))(y_i - E(y))$$

Where  $L$  is the number of pixels involved in the calculations, the closer the value of  $pro_{xy}$  to zero, the better the quality of the encryption algorithm is [1], [5], [17].

The correlation coefficient analysis of the plain and cypher image are shown in Figs—10 and 11, respectively. Looking at 10, one can see that the correlation between adjacent pixels in all three directions of the plain image in the three intensities are strongly correlated with a minimum correlation coefficient of 0.6140 in the green channel and a maximum correlation coefficient of 0.8695 in the red channel. However, the story is different from the cypher image in Fig. 11. There is no correlation between the adjacent pixels in all three intensities and all the three directions, as these can be seen clearly from their respective correlation coefficient values, which are almost zero.

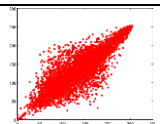
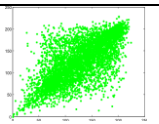
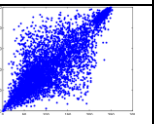
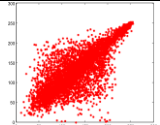
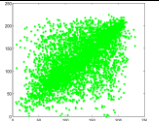
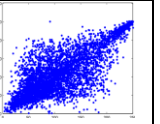
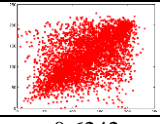
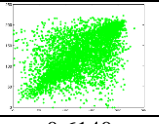
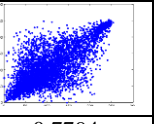
	Red	Green	Blue
Horizontal			
$r_{xy}$	0.8695	0.7264	0.8224
Vertical			
$r_{xy}$	0.8196	0.6421	0.8125
Diagonal			
$r_{xy}$	0.6242	0.6140	0.7794

Fig. 10 Correlation between adjacent pixels of the Plain Image

This indicates that the attacker cannot obtain any information regarding the plain image from the cipher image. Hence, the scheme is effective.

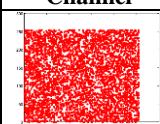

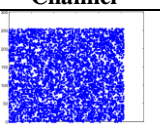
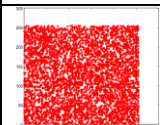
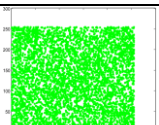
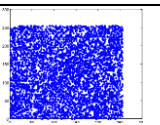
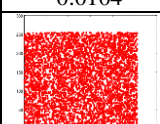
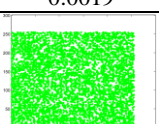
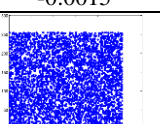
	Red Channel	Green Channel	Blue Channel
Horizontal			
$r_{xy}$	-0.0052	-0.0021	0.0011
Vertical			
$r_{xy}$	0.0104	0.0019	-0.0015
Diagonal			
$r_{xy}$	0.0057	0.0011	0.0034

Fig. 11 Correlation between adjacent pixels of the Cipher Image

### A. Sensitivity (Differential) Analysis

For an image encryption scheme to be able to resist the differential attack efficiently, it must be sensitive to small changes in the original image. That is, one small change in the plain image must cause a significant change in the cypher image. To test the influence of only one-pixel change in the plain-image over the whole cypher-image, we used two common measures: 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 cypher-images whose plain-images only have one-pixel difference. In contrast, the UACI measures the average intensity of differences between the two cypher-images. They indicate the sensitivity of the cypher-images to the minor change of plain-image. The formula for evaluating NPCR and UACI are as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (9)$$

$$UACI = \frac{1}{W \times H} \left[ \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \quad (10)$$

Where  $C_1$  and  $C_2$  denote the two ciphered images whose corresponding plain-images have the only one-pixel difference, the  $C_1(i,j)$  and  $C_2(i,j)$  represent the grayscale 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 [6], [8], [15], [23].

These two tests defined by (9) and (10) are easy to calculate, but the test scores are difficult to interpret with regard to the performance of an encryption scheme. The theoretical values of NPCR and UACI scores of binary and grey images were evaluated at 0.05-level, 0.01-level, and 0.001-level for different image sizes [23]. Their results show that image type and size used have a significant influence on the NPCR and UACI scores. 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 and 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 [23]. An encryption algorithm is considered worthy of use if the experimental NPCR score 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 [23].

Table 1 presents the experimental NPCR and UACI scores for the proposed scheme on a 256x256 image in the three channels: red, green, and blue components (each colour is equivalent to a grey component). The results have satisfied both the NPCR and UACI requirements,



indicating 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 (%)	UCI (%)
Red	99.6921	33.4189
Green	99.7011	33.3932
Blue	99.6852	33.4019

**VIII. CONCLUSION**

To have a more secure image transmission, a new cryptosystem was developed and analyzed. The new scheme was achieved by utilizing the rich, chaotic properties of two 3-D chaotic maps (Rabinovich-Fabrikant equations and the Shimizu-Morioka system). The scheme was tested on one of the standard test colour images: Mandrill\_colour\_256.Tif. Security analysis such as the histogram uniformity analysis, the correlation coefficient analysis, the number of pixel change rates (NPCR), and the unified average changing intensity (UACI) was performed on the proposed scheme. Results obtained from the analysis show that the proposed scheme is effective and can resist any statistical, differential, and brute-force attacks.

**REFERENCES**

[1] E. F. Abd El-Samie, H. E. H. Ahmed, F. I. Flash, H. M. Shaheen, S.O. Faragallah, M. E. El-Rabie, and A. S. Alshebeili, *Image Encryption- A Communication Perspective*. 1st Ed., CRC Press, London, (2014) 1-86.

[2] I. Mishkovski, and L.Kocarev, *Chaos-Based Public-key Cryptography*, Springer-Verlag Berlin Heidelberg, SCI 354 (2011), 27-65,

[3] L. Abraham and N. Daniel, *Secure Image Encryption Algorithms: A Review*, *International Journal of Scientific and Technology Research*, 2(4)(2013) 186 – 189.

[4] Y. Cao, *A New Hybrid Chaotic Map and its Application on Image Encryption and Hiding*, *Mathematical Problems in Engineering*,728375, 13(2013).

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

[6] 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) 1-13.

[7] M. Mishra, P. Mishra, M. C.Adhikary and S. Kumar, *Image Encryption UsingFibonacci-Lucas Transformation*, *International Journal on Cryptography and Information Security*, 2(3)(2012) 131-141.

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

[9] A. A. Abd El-Latif, L. Li, T. Zhang, N. Wang, X. Song and X. Niu, *Digital image encryption scheme based on multiple chaotic systems*, *Sensing and Imaging*, An international Journal on continuing subsurface sensing technologies and applications, Springer, 56(2)(2012) 67-88.

[10] S. Sam, P. Devaraj, and R. S. Bhuvaneshwaran, *A novel image cypher based on mixed transformed logistic maps*, *Multimedia tools and applications*, An International Journal, Springer, 56(2) (2012)315-330.

[11] J. Won Yoon and H. Kim, *An image encryption scheme with a pseudorandom permutation based on chaotic maps*, *Communications in nonlinear science and numerical simulations*, Elsevier., 15(12)(2010). 3998-4006.

[12] A. L. Shil'nikov, *Bifurcation and Chaos in the Shimizu-Morioka System*, *Selecta Mathematica Sovietica*, 10(2)(1991) 105-117.

[13] M-F. Danca and G. Chen, *Bifurcation and Chaos in a Complex Model of Dissipative Medium*, *International Journal of Bifurcation and Chaos*, 14(1)(2004) 3409-3447.

[14] G. Hanchinamani. and L. Kulkarni, *Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform*. *International Journal of Hybrid Information Technology*, 7(4) (2014)185-200.

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

[16] M-F. Danca, M. Feckan, N. Kuznetsov, and G. Chen, *Looking More Closely to the Rabinovich-Fabrikant System*, *ArXiv:1509.09206v2 [nlin.CD]* 1 (23)(2015).

[17] G. A. Sathishkumar, K. B. Bagan, and N. Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps, *International Journal of Network Security and its Applications*, 3 (2)(2011)181 – 194.

[18] T. Shimizu and N. Morioka, *on the Bifurcation of a Symmetric Limit Cycle to an Asymmetric one in a Simple Model*, *Physics Letters A*, 76(1980) 201-204,

[19] D. J. Nkpkop, Y. J. Effa, E. A. J. Fouda, M. Alidou, L. Bitjoka, and M. Borda, *A Fast Image Encryption Algorithm Based on Chaotic Maps and the Linear Diophantine Equation*, *Computer Science and Applications*, 1(4)(2014) 232-243.

[20] E. Köse, *Controller Design by Using Sliding Mode and Passive Control Methods for Continuous-Time Non-linear Shimizu-Morioka Chaotic System*, *International Journal of Engineering Innovation and Research*, 4(6)(2015) 895-902

[21] H. R. Salih, *The Stability Analysis of the Shimizu-Morioka System with Hopf Bifurcation*, *Journal of Kirkuk University-Scientific Studies*, 6(2)(2011) 184-200.

[22] M. I. Rabinovich, and A. I. Fabrikant, *Stochastic self-modulation of waves in non-equilibrium media*, *J. Exp. Theor. Phys.*, 77(1979)617-629.

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

[24] I. Mishkovski, and L. Kocarev, *Chaos-Based Public-key Cryptography*, Springer-Verlag, Berlin Heidelberg. SCI 354, (2011)27-65.

[25] H. J. Yakubu and T. Aboiyar, *A Chaos Based Image Encryption Algorithm using Shimizu-Morioka System*, *International Journal of Communication and Computer Technologies*, 6(1)(2018)07-11.

[26] E. R. Borgia, A. C.Dascalescu, and A. Diaconu, *A New One-Dimensional Chaotic Map and its use in a Novel Real-Time Image Encryption Scheme*, *Advances in Multimedia*, 2(1) (2014) 1-15.

[27] H. J. Yakubu, E. G. Dada, S. B. Joseph, and A. K. Anukem, *A New Chaotic Image Encryption Algorithm for Digital Colour Images Using Rabinovich-Fabrikant Equations*, *International Journal of Computer Science and Information Security*, 17(1)(2019)15-23.