International Journal of communication and Computer Technologies, 6 (1) (2018) 7-11

International Journal of Communication & Computer Technologies

Website: www.ijccts.org
ISSN :2278-9723
Research Paper

A chaos based image encryption algorithm using Shimizu-Morioka system

Yakubu[1] H. J., Aboiyar[2] T.

[1]*Department of Mathematics/Statistics/Computer Science, University of Maiduguri, Maiduguri, Nigeria.*
[2]*Department of Mathematics/Statistics/Computer Science, University of Agriculture, Makurdi, Benue, Nigeria*
Email: thejoe_gdf@yahoo.com, hurcha65@gmail.com

Abstract

Recent research on image encryption schemes has focused on chaotic systems in order to meet the demand for real-time secure image transmission over the Internet. In this paper, we propose a new image encryption scheme based on Shimizu-Morioka chaotic system. The scheme consists of two stages: the confusion (mixing) stage and the diffusion stage. In the confusion stage, we utilized the rich chaotic properties of the Shimizu-Morioka chaotic system by solving the system N time's steps using Euler's method and scrambled the positions of the pixel values of the image using the randomness of the solutions obtained from the chaotic system. In the diffusion stage, we generate N (where N is the size of image per colour) random integer numbers that is non-periodic and performed MOD and bitXOR operations on the shuffled image using the random numbers to obtain encrypted (diffused) image. The proposed algorithm is tested on a standard RGB image that is of size 256x256 and is stored with TIFF file format. Performance analysis on the proposed scheme such as the statistical analysis and the sensitivity analysis show that the proposed encryption scheme is reliable and strong enough to withstand different attacks.

Keywords: *Chaos: Cryptosystem: Equilibrium Point: Image Encryption: Shimizu-Morioka System.*

1. Introduction

We are in an age where information is an asset that has value like any other asset. Information dissemination has continued to be much easier than before owing to the rapid advancement in communication technology. Today, huge amount of information (in form of text, image, audio or video) are transferred across the world over a public network called the Internet, though efficient is highly insecure, and therefore exposed to various threats [13]. The need to protect sensitive images from unauthorized person wanting to have access to them becomes necessary. Image security is based on cryptography, which is the technique that transforms information 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 [4, 5].

Traditional encryption methods which include Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Rivest-Shimar-Adleman (RSA) algorithm, ElGamal algorithm have been effective solutions to the information security problems [6, 14]. They are still being used heavily in different forms of information security. However, they are primarily designed for text and though can be used for image encryption, are usually found not suitable due to the following three reasons: **(i)** Image size is always very large and therefore needs more time to encrypt it with the traditional methods, **(ii)** A decrypted image need not be exactly the same as the original image, since decrypted image with small distortion is usually acceptable due to human perception property and the high redundancy of image data, **(iii)** Digital image contents are strongly correlated and this feature is not used by the traditional methods thereby affecting their encryption efficiency [1, 6, and 12].

To improve efficiency and security of image encryption, numerous image encryption and hiding schemes were proposed. Among these schemes, the chaos based encryption schemes turn out to be most attractive to many researchers because of its interesting properties which includes sensitivity to initial condition and control parameters, deterministicity and the ergodicity [1, 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 the statistical, the differential, and the brute-force attacks [13]. The application of chaos to encryption of digital images started in 1997 by Fridrich and since then, many researchers applied chaos to different fields of image security [2]. In this paper, a three-dimensional Shimizu-Morioka chaotic system is used in developing and implementing an image encryption scheme.

2. Shimizu-Morioka system

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

$$\begin{aligned} \dot{x} &= y, \\ \dot{y} &= -xz + x - \beta y, \\ \dot{z} &= x^2 - \alpha z, \end{aligned} \tag{1}$$

where $(x, y, z) \in \mathbb{R}^3$ are state variables, the dot (·) on a variable indicates the derivative of the variable with respect to time t, while α and β are positive parameters [9]. 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. The following observations were presented by [9]:

1. As in the Lorenz model, the Shimizu-Morioka system is invariant with respect to the substitution $(x, y, z) \rightarrow (-x, -y, z)$.
2. System (1) has three equilibrium states: (0,0,0), ($\sqrt{\alpha}$,0,1) and ($\sqrt{\alpha}$, 0,1).

2.1. Stability analysis of the equilibrium points

The following observations and their proofs were presented by [10]:

1. 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 $P_0(0,0,0)$.
2. The equilibrium point $P_0(0,0,0)$ is unstable for all $\alpha \in \mathbb{R}$
3. 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 $\beta \in (0, \sqrt{2})$.
4. The equilibrium point $P_1(\sqrt{\alpha},0,1)$ is unstable if and only if $\alpha < \alpha_0 = \frac{2-\beta^2}{\beta}$ where $\beta \in (0, \sqrt{2})$.

2.2. Phase portrait of the Shimizu-Morioka chaotic system

The Shimizu-Morioka chaotic system is described by

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1-z & -\beta & 0 \\ x & 0 & -\alpha \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1-z & -0.91 & 0 \\ x & 0 & -0.365 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \tag{2}$$

where we defined our control parameters value as β = 0.91 and α = 0.365. Using a MATLAB/Simulink model, version 7.10.0 (R2010a) the phase portraits of the Shimizu-Morioka chaotic system in the *xy, xz, yz*, and *xyz* phase space 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 $z_0 = 0.1$

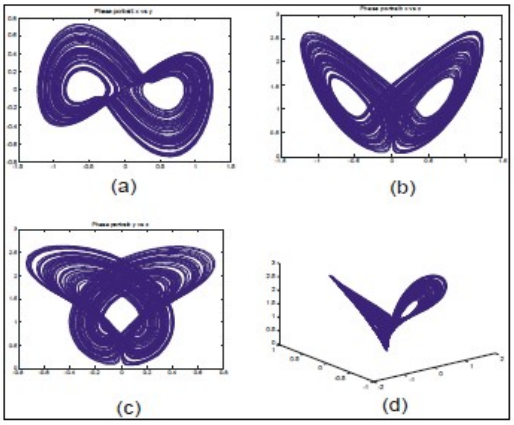

Fig. 1: Phase portrait of the Shimizu-Morioka chaotic system in the (a) *xy*, (b) *xz*, (c) *yz*, (d) *xyz* phase space.

3. Proposed cryptosystem

The proposed encryption scheme consists basically, of two stages. The first stage is the *confusion* (mixing) stage and the second stage is the *diffusion* stage. In the confusion stage, we utilized the rich chaotic properties of the Shimizu-Morioka chaotic system to shuffle the image using initial conditions and control parameters as the key. In the diffusion stage, we generated a set of N (size of image per colour) random integer numbers that has irregularity and non-periodicity properties and performed MOD and bitXOR operations on the shuffled image using the random numbers in order to change the pixel values of the confused image. The resulting image is the cipher (encrypted) image. The decrypted image is obtained by applying the same operations carried out in the encryption process using the same initial conditions and control parameters but in the reverse order. The detail algorithm for encryption and decryption processes is presented below.

3.1. Encryption algorithm

1. Read RGB image from a file as I,
2. Obtain the image dimension m x n x 3,
3. Compute number of pixels per colour (N= m*n),
4. Enter the parameters value for α, β, x_0, y_0, z_0, h (h is the step size),
5. Solve the Shimizu-Morioka chaotic system N times steps using the Euler's method to obtain solutions in vector form as X, Y, Z,
6. Add confusion to the solution using round function,
7. Sort the vectors X, Y, and Z to obtain X1, Y1, and Z1 with their list of indices l_x, l_y, and l_z.
8. Define A, B, and C to be matrices for red, green and blue intensities respectively.
9. Convert the A, B and C matrices to double to obtain A1, B1, and C1.
10. Reshape A1, B1, and C1 into row vectors as A2, B2, and C2.
11. Use the indices of the sorted solution of the Shimizu-Morioka chaotic system to scramble the row vectors A2, B2, and C2 and obtain new row vectors as A3, B3, and C3,
12. Generate a set of N random integer numbers that has irregularity and non-periodicity properties.
13. Perform MOD and bitXOR operations on A3, B3, and C3 and the random numbers to obtain our encrypted image as A4, B4, and C4.
14. Reshape A4, B4, and C4 into m x n matrices to obtained A5, B5 and C5.
15. Form the encrypted image as I1 by merging A5, B5 and C5.
16. Convert the image I1 to uint8.
17. Display the scrambled image I1.
18. Save the encrypted image I1.

3.2. Decryption algorithm

1. Read the encrypted image I1,
2. Convert the image to double,
3. Define A6, B6, and C6 to be matrices for the red, green and blue respectively for I1.
4. Convert A6, B6, and C6 to double as A7, B7, and C7.
5. Reshape A7, B7, and C7 into row vectors to obtain A8, B8, and C8,
6. Perform MOD and bitXOR operations using the set of N random integer numbers on A8, B8, and C8 to obtain the scrambled image as A9, B9, and C9.
7. Reposition the entries in A9, B9, and C9 with the indices l_x, l_y, and l_z to obtain new row vectors A10, B10, and C10,
8. Reshape A10, B10, and C10 into square matrices to obtain A11, B11, and C11.
9. Form the decrypted image as I2 by merging the A11, B11, and C11.
10. Convert the image I2 to uint8.
11. Display the decrypted image I2.
12. Save the decrypted image I2 in a file

4. Results and discussion

4.1. Implementation

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

4.2. Results Obtained

After applying the proposed algorithm to the plain image in Figure 2 using initial conditions and control parameters as the key, the following results were obtained during the encryption processes as shown in Figures 3 and 4 below:

Fig. 2: Original-image (Plain-image)

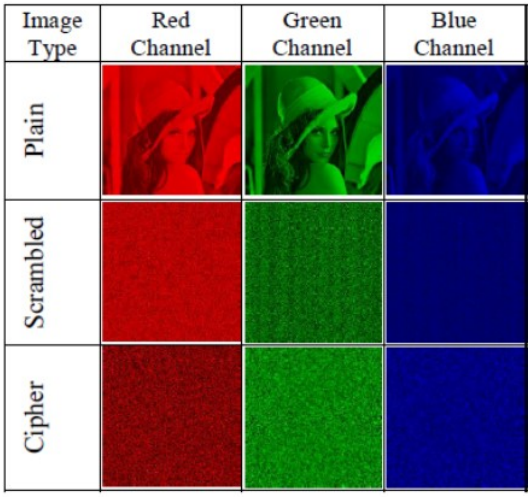

Fig. 3: Red, green and blue channel of the plain, scrambled and cipher image.

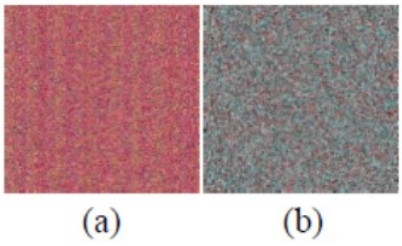

Fig. 4: (a) Scrambled (Confused) image, (b) Cipher image

The decryption processes began with the cipher image (Figure 4b as input data. The cipher image is first split into red, green and blue channels as shown in Figure 3. We then performed the bitXOR and MOD operations using same set of random integer numbers to obtained undiffused image along the red, green and blue channel as shown in Figure 5. These Undiffused channels are then scrambled using the solutions obtained from the Shimizu-Morioka chaotic system with same initial conditions and control parameters that were used as encryption key during the encryption process are used as decryption key. Figure 6 shows the unconfused image in the red, green and blue channel. Merging these channels resulted in a decrypted image as shown in Figure 7.

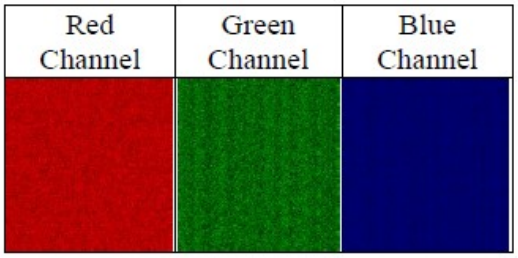

Fig. 5: Red, green and blue channels of the undiffused image.

Fig. 6: Red, green and blue channels of the unconfused image

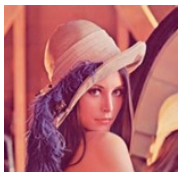

Fig. 7: Decrypted image

5. Security analysis

With the application of an encryption algorithm to an image, it is expected that its pixel 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 original and the encrypted images. Also, to obtain a good encrypted image, it must be composed of totally random patterns that do not reveal any of the features of the original image [13]. To test the robustness of the proposed scheme, 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) was performed.

5.1. Histogram uniformity analysis

For image encryption algorithm to be considered worthy of use, the histogram of the encrypted image should satisfy these two properties [13]:

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

Looking at Figures 8 and 9, one can see that the plain and the scrambled image have the same histogram. However, the histogram of the encrypted (cipher) image (see Fig. 10) is completely different from that of the plain image and also it is uniformly distributed thus; the proposed scheme has satisfied both the two conditions of histogram uniformity analysis which indicates that the attacker cannot obtain any hint about the plain image from the cipher image.

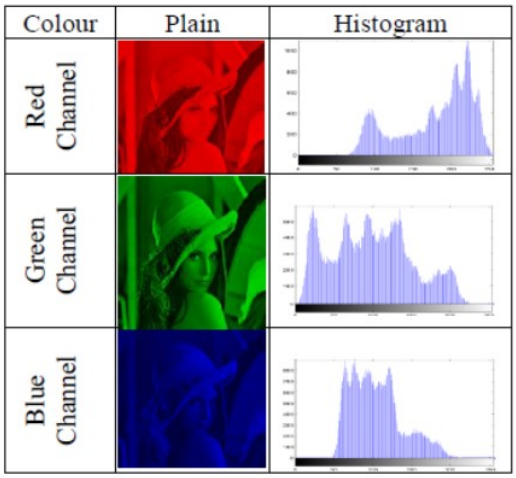

Fig. 8: Histogram for red, green and blue channel of the plain image

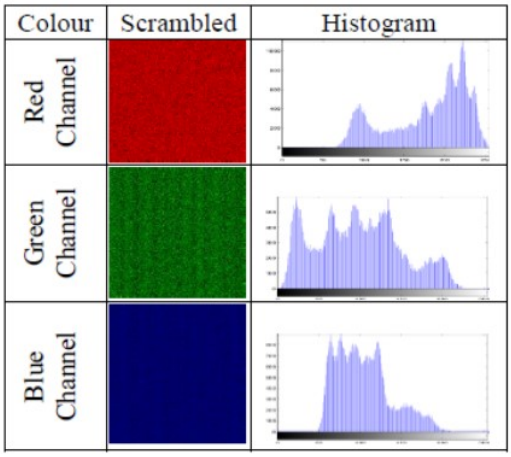

Fig. 9: Histogram for red, green and blue channel of the scrambled (confused) image

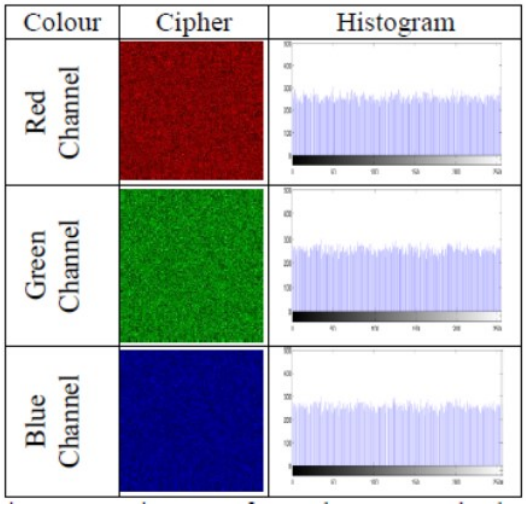

Fig. 10: Histogram for red, green and blue channel of the encrypted (diffused) image.

5.2. Correlation coefficient analysis

A useful metric to assess the encryption quality of any image encryption algorithm is the correlation coefficient between adjacent pixels of the cipher-image. Correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in the cipher-image were analyzed. The same correlation coefficients analysis was also obtained in the plain-image for comparison purposes. This metric is calculated as follows:

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

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

$$E(x) = \frac{1}{L}\sum_{l=1}^{L} x_l, \quad D(x) = \frac{1}{L}\sum_{l=1}^{L} (x_l - E(x))^2, \quad (4)$$

$$Cov(x, y) = \frac{1}{L}\sum_{l=1}^{L} (x_l - E(x))(y_l - E(y)) \quad (5)$$

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 will be [11, 13, and 14].

The correlation coefficient analysis in the plain and cipher image of Lena are shown in Figures 11 and 12 respectively. From Figure 11, we can see that the plain image is strongly correlated with an average of about 0.94 while in Figure 12, we see that there is almost no correlation among the adjacent pixels in the cipher images as these can be seen clearly from their respective correlation values which is almost zero in all the three directions. This indicates that the attacker cannot obtain any information regarding the plain image from the cipher image.

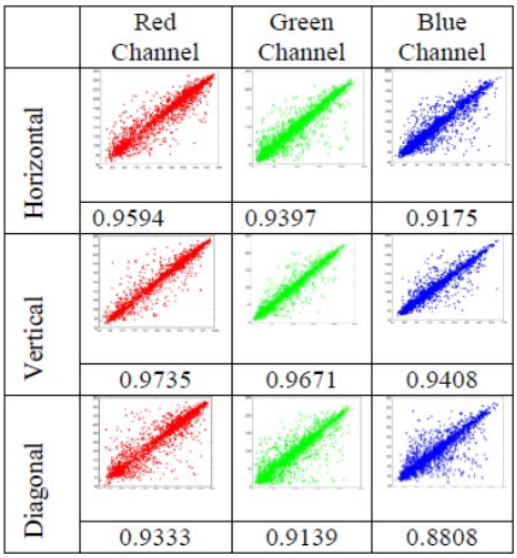

Fig. 11: Correlation coefficient analysis of the Shimizu-Morioka chaotic image encryption scheme on plain image.

5.3. Sensitivity 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 cipher image. To test the influence of only one-pixel change in the plain-image over the whole cipher-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 differ-

ent 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. The formula for evaluating NPCR and UACI are as follows:

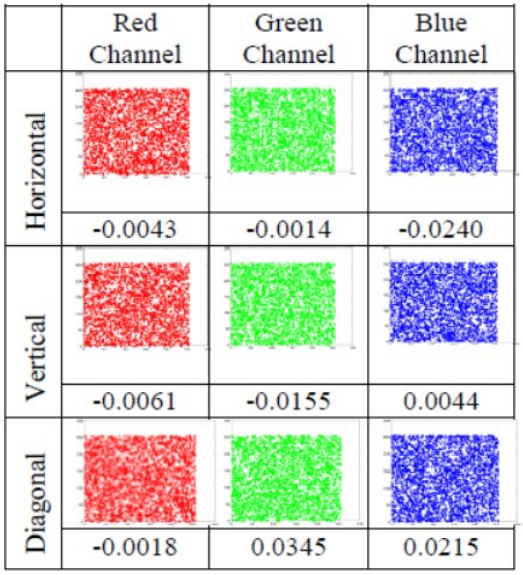

Fig. 12: Correlation coefficient analysis of the Shimizu-Morioka chaotic image encryption scheme on cipher image.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{WxH} x100 \quad \% \qquad (6)$$

$$UACI = \frac{1}{WxH}\left[\sum_{i,j} \frac{[C_1(i,j) - C_2(i,j)]}{255}\right] x100 \quad \% \qquad (7)$$

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 [1, 2, 7, and 15].

Although these two tests are compactly defined and are easy to calculate, test scores are difficult to interpret in the sense of whether the performance is good enough. In [15], some findings on the acceptable NPCR and UACI scores for an image encryption scheme to be considered secured were made Theoretical values of NPCR and UACI scores of binary and gray images were evaluated at 0.05-level, 0.01-level and 0.001-level. Their results show that the type and size of image used have significant influence on the NPCR and UACI scores. An NPCR score is acceptable if the experimental score is equals to or greater than the theoretical NPCR score. Also, for UACI score, the experimental UACI score should be on or within the theoretical UACI critical scores.

Table 1 below present our experimental 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 [15]. Looking at our experimental NPCR scores in Table 1, which is the average score for the red, green and blue component, (each colour is equivalent to a gray component), and it therefore shows that the proposed scheme has satisfied the requirement. 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 [15]. Also, the experimental UACI score in Table 1 has passed the requirement. Thus, the proposed scheme can withstand any differential attack.

Table 1: The NPCR and the UACI Scores for the Proposed Scheme on Lena.

NPCR (%)	UACI (%)
99.57	33.43

6. Conclusion

To improve the security of image transmission, we proposed in this paper, a new confusion-diffusion cryptosystem which we achieved by utilizing the rich chaotic properties of the 3-D Shimizu-Morioka chaotic system to shuffled the image. The encrypted image is obtained by performing bitX-OR and MOD operations on the shuffled image using a set of generated random integer numbers that is non-periodic. The proposed scheme is tested on a standard test colour image- Lena.Tif. We also performed security analysis such as the histogram uniformity analysis, the correlation coefficient analysis, the NPCR and the UACI on the proposed scheme. From the experimental results obtained, the proposed scheme is highly secured and strong against the statistical, differential and brute-force attacks.

References

[1] Ramadan, N., Ahmed, H. H., Elkhamy, S. E., Abd Abd El-Samie, F. E., "Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map", *American Journal of Signal Processing,* Vol. 6, No. 1, (2016), pp.: 1-13.

[2] Wu, Y., Yang, G., Jin, H., and Noonan, J. P., "Image Encryption Using the Two-dimensional Logistics Chaotic Map", *Journal of Electronic Imaging*, Vol. 21, No.1, (2012), 28pp.

[3] Denning, D. E., Cryptography and Data Security, Addison-Wesley Publishing Company Inc. USA, (1982), pp.: 1-116.

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

[5] Abraham, L., and Daniel, N., "Secure Image Encryption Algorithms: A Review", *International Journal of Scientific and Technology Research*, Vol. 2, No. 4, (2013), pp.: 186 – 189.

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

[7] Ramahrishnan, S., Elakkiya, B., Geetha, R., and Vasuki, P., "Image Encryption Using Chaotic Maps in Hybrid Domain", *International Journal of Communication and Computer Technologies*, Vol. 2, No. 5, (2014), pp.: 44 – 48.

[8] Shil'nikov, A. L., "Bifurcation and Chaos in the Shimizu-Morioka System". *Selecta Mathematica Sovietica*, vol. 10, No. 2, (1991), pp.: 105-117.

[9] Köse, E. 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,* Vol. 4, No. 6, (2015), pp.: 895-902.

[10] Salih, H. R., "The Stability Analysis of the Shimizu-Morioka System with Hopf Bifurcation", *Journal of Kirkuk University-Scientific Studies*, Vol. 6, No. 2, (2011), pp.: 184-200.

[11] Sathishkumar,G. A., Bagan, K. B., and Sriraam, N., "Image Encryption Based on Diffusion and Multiple Chaotic Maps", *International Journal of Network Security and its Applications*, Vol. 3, No. 2, (2011), pp.: 181 – 194.

[12] Mishra, M., Mishra, P., Adhikary, M. C. and Kumar, S., "Image Encryption Using Fibonacci-Lucas Transformation", *International Journal on Cryptography and Information Security*, vol. 2, No. 3, (2012), pp.: 131-141.

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

[14] Ye, R., "A Highly Secure Image Encryption Scheme Using Compound Chaotic Maps". *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 4, No. 6, (2013), pp.: 532 – 544.

[15] Wu, Y., Noonan, J. P., and Agaian, S., "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.