Current Journal of Applied Science and Technology

38(6): 1-14, 2019; Article no.CJAST.46191
ISSN: 2457-1024
*(Past name: British Journal of Applied Science & Technology, Past ISSN: 2231-0843,
NLM ID: 101664541)*

Chaos Based Image Encryption Scheme Using One Dimensional Exponential Logistic Map

Terlumun Gbaden[1*] and Blama Nachaba[2]

[1]Department of Mathematics, Statistics and Computer Science, University of Agriculture, Makurdi, Benue State, Nigeria.
[2]Department of Computer Science, University of Jos, Plateau State, Nigeria.

Authors' contributions

This work was carried out in collaboration between both authors. Author TG designed the study, performed the statistical analysis, wrote the protocol and wrote the first draft of the manuscript. Author BN managed the analyses of the study and the literature searches. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/CJAST/2019/v38i630451
Editor(s):
(1) Dr. Harry E. Ruda, Professor, Stan Meek Chair Professor in Nanotechnology, University of Toronto, Director, Centre for Advanced Nanotechnology, University of Toronto, Canada.
Reviewers:
(1) Ali Shakir Mahmood, Mustansiriyah University, Iraq.
(2) Zlatin Zlatev, Trakia University, Bulgaria.
(3) G. A. Sathish Kumar, Sri Venkateswara College of Engineering, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/46191

Original Research Article

Received 20 January 2019
Accepted 22 March 2019
Published 15 January 2020

ABSTRACT

The widespread use of images in various sectors of life makes its protection increasingly necessary and important. An improvement over encryption and decryption algorithm using exponential logistic chaotic map was proposed. In this work, we adopt an encryption/decryption strategy for colour images using the exponential logistic chaotic map. The proposed encryption/decryption algorithms are implemented in MATLAB for computer simulation. The experimental results indicate that the proposed algorithms can be used successfully to encrypt/decrypt images with secret keys. The performance analysis using histogram uniformity analysis and correlation coefficient show that the algorithms give larger space, quick speed and easy to realize. The encrypted images have good encryption effect and low correlation coefficient rendering it a good candidate for confidential and secure means of transmitting image information in untrusted networks.

Keywords: Encryption; decryption; chaos; cryptography and images.

**Corresponding author: E-mail: gbaden2014@gmail.com;*

1. INTRODUCTION

Images and other multimedia files are frequently transmitted via computer networks. The transmission of information across unsecured networks endangers the security of the information. For example, due to continuous attempts of hackers, images end up in the hands of illegal third parties during communication that might profit or amend them without the awareness of the appropriate receiver [1,2]. The security of information transmitted is a vital issue. Traditional encryption systems like Digital Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Rivest_Shamir_Adleman (RSA) are not very suitable for image encryption. The reason is that in these encryption schemes there exist high correlation among pixels, so it takes high computation time and power. While few researchers have applied the scatter and disorder characteristics of the chaotic system to encryption and security communication, a few have used these characteristics to the encryption of digital images. Even though the application of a one-dimension chaotic method for image encryption is convenient and quick, it is not competent to provide sufficient security. Therefore, a modification and use of a one dimension exponential chaotic system is approached in order to guarantee communication security.

2. RELATED WORKS

The search for alternative encryption techniques has led to different studies on cryptography in order to find effective encryption options. In this section, a number of image encryption reports have been considered.

2.1 Cryptography and Image Encryption

The security of digital images is given much attention nowadays and many image encryption algorithms have been proposed by many authors [3]. According to [4] chaotic cryptography pronounces the use of chaos theory in specific physical dynamical systems working in chaotic system as a measure of communication techniques and computational algorithms to accomplish different cryptographic tasks in a cryptographic system. Image encryption is the transformation of an image to a scrambled form so that it can be protected from unauthorized users [5,6]. Sneyers [7] and Kumar et al. [8] presents the idea that the scrambled input signal samples using a specific pattern, could only be recoverable by the intended receiver. Furthermore, [9] discovered that Chaos-based image cipher has been widely researched upon over the last decade or so to meet the growing demand for real-time secure image transmission over unprotected networks. Shah and Saxena [10] observed that an improved diffusion strategy could promote the efficiency of the most widely investigated permutation-diffusion type image cipher.

Aljazaery [11] developed a new method to encrypt the signals with one dimension and images (monochrome or color images) in a time more less than if these signals and images are encrypted with their original sizes. Discrete Wavelet transform (DWT) is used as a feature extraction because it is a powerful tool of signal processing for its multiresolutional possibilities [12].

Image applications have been increasing in recent years. According to [13] encryption is used to provide the security needed for image applications. [10] in their paper classified various image encryption schemes and analyzed them with respect to various parameters like tenability, visual degradation, compression friendliness, format compliance, encryption ratio, speed and cryptographic security. [14] observed that multimedia is one of the most popular data shared in the Web, and the protection of it via encryption techniques is of vast interest. [15] proposed a secure and computationally feasible algorithm called Optimized Multiple Huffman Tables (OMHT) technique. The effectiveness and robustness of this scheme was verified by measuring its security strength and comparing its computational cost against other techniques. The proposed technique guarantees security and fastness without noticeable increase in encoding image size [16].

The need of exchanging messages and secretly over unsecure networks promoted the creation of cryptosystems to enable receivers to interpret the exchanged information [17]. In the presentation of [18], a particular public key cryptosystem called the ElGamal Cryptosystem was considered with the help of MATLAB program used over images. This new modification made the cryptosystem of images more immune against some future attacks since breaking this cryptosystem depends on solving the discrete logarithm problem which is really impossible with large prime numbers [19,20].

Vector Quantization (VQ) is another efficient technique for image encryption [21]. Its basic idea is derived from Shannon's rate-distortion theory, which states that the better performance of an image compression is always achieved by coding image vectors instead of scalar [22]. There are two advantages of using VQ for image compression. One is that the required bit rate of VQ is small. Since VQ compresses the original image into a set of indices in the codebook, we can save a lot of storage. The other is that to encrypt the codebook. The set of indices on the codebook is transmitted in plaintext form [23].

Shannon proposed two basic techniques for obscuring the redundancies in plaintext message: diffusion and confusion involves many substitutions into the relationship between the plaintext and the ciphertext [24]. This makes difficult the attempts to study the ciphertext looking for redundancies and statistical patterns. [25] reported that the computational difficulty of computing discrete logarithms made this method a better encryption alternative. [26] noted that compression of encrypted data draws much attention in recent years due to the security concerns in a service-oriented environment such as cloud computing.

Some of these methods are criticized for weak keys, limited key space, vulnerability to cipher text attacks and other issues. In this paper, we use one dimensional exponential logistic map to develop an image encryption algorithm in order to provide effectiveness and robustness for various images of content and type transmitted over unsecured networks.

2.2 The One-dimensional Logistic Map

One of the most studied examples of a one-dimensional system capable of various dynamical regimes including chaos is the 1-D logistic map. It is a representation of an idealized population growth model and is defined by the equation

$$x_{n+1} = f(x_n) = rx_n(1 - x_n) \quad (1)$$

where $x_n \in [0,1]$ and represents the population at year *n*, and hence x_0 represents the initial population at year 0. Crucial to the behaviour of the map is the control parameter $r \in [0,4]$ whose dynamical behaviour is very complicated and it represents a combined rate for reproduction and starvation. Slight changes in the parameter, "*r*", of the map can cause the iterated map to change from stable and predictable behaviour to unpredictable behaviour which is called chaos. We begin the analysis of the logistic map by finding its periodic points and observe how orbits qualitatively change as the control parameter *r* is varied. This helps in illustrating the concepts of bifurcations and chaotic motions. To find the fixed points of the map (also called points of period one), it is necessary to solve the equation given by $f(x) = rx(1 - x) = x$ which gives the points that satisfy the condition$x_{n+1} = x_n$for all n. Two solutions were found: $x_{1,1} = 0$ and $x_{1,2} = 1 - \frac{1}{r}$.

2.3 Weaknesses of the One-dimensional Logistic Map

The one dimensional chaotic system's drawbacks include small key space and weak security. Logistic maps are faced with the problem of lack of robustness of their encryptions because of round off errors in real number quantization. This may lead to nonreversible functions for encryption and this makes decryption process impossible. The third defect reveals a high risk that initial values and parameters used in a chaotic system might be fully analyzed using existing tools and methods after a long term.

Increase in parameter space and key space were done to improve on the security of the one dimensional logistic map. The modification of the logistic chaotic map to one dimensional exponential logistic map is remarkable contribution to the cryptographic field in enhancing encryption process of digital images.

3. THE PROPOSED SYSTEM

In this section, the one dimensional exponential logistic map is presented (Fig. 1). The image encryption algorithm using the one dimensional exponential logistic map is also considered.

3.1 The One-Dimensional Exponential Logistic Map

The proposed one dimensional exponential logistic map is defined by

$$x_{n+1} = f(x_n) = rx_n(1 - x_n)e^{x_n}, \quad (2)$$

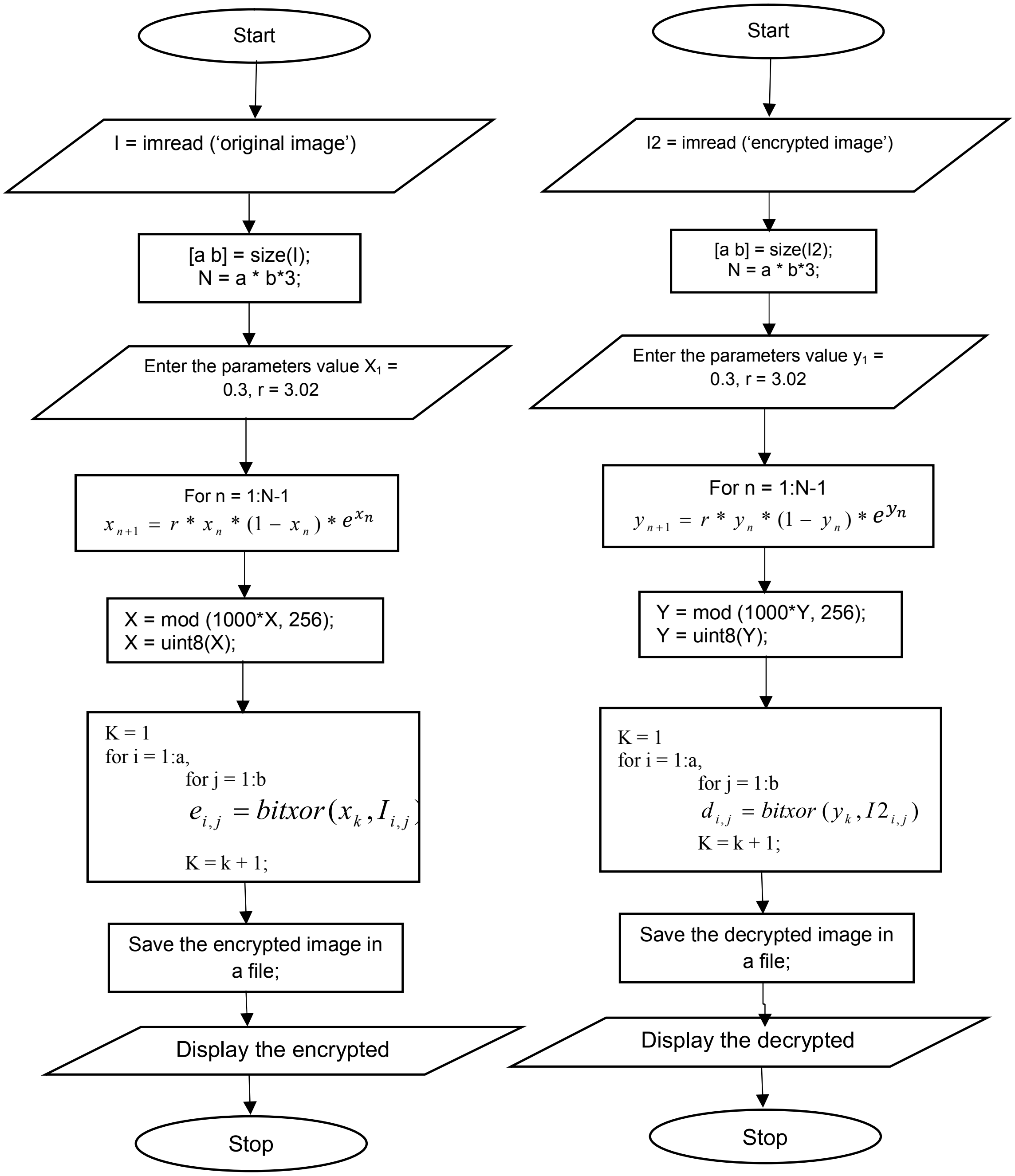
Start
I = imread ('original image')
[a b] = size(I);
N = a * b*3;
Enter the parameters value X_1 = 0.3, r = 3.02
For n = 1:N-1
$x_{n+1} = r * x_n * (1 - x_n) * e^{x_n}$
X = mod (1000*X, 256);
X = uint8(X);
K = 1
for i = 1:a,
for j = 1:b
$e_{i,j} = bitxor(x_k, I_{i,j}$
K = k + 1;
Save the encrypted image in a file;
Display the encrypted
Stop
Start
I2 = imread ('encrypted image')
[a b] = size(I2);
N = a * b*3;
Enter the parameters value y_1 = 0.3, r = 3.02
For n = 1:N-1
$y_{n+1} = r * y_n * (1 - y_n) * e^{y_n}$
Y = mod (1000*Y, 256);
Y = uint8(Y);
K = 1
for i = 1:a,
for j = 1:b
$d_{i,j} = bitxor(y_k, I2_{i,j})$
K = k + 1;
Save the decrypted image in a file;
Display the decrypted
Stop

Fig. 1. Gives the flow diagram for image encryption and decryption using the exponential logistic map

where $x_n \in [0,1]$ and where $r \in [0, 2.25]$ is the control parameter. Slight changes in the values of the parameter, "r", of the map can cause the iterated map to change from stable and predictable behaviour to unpredictable behaviour which is called chaos.

3.2 Image Encryption Algorithm using the Exponential Logistic Map

In this section, we present the detail algorithm for encryption/decryption of gray scale images using modified 1-D logistic map.

3.2.1 Encryption algorithm

i. Read the original image I.
ii. Obtained the image dimension as axbx3 for RGB images or a x b for gray scale images.
iii. Compute the number of Pixels in I as N= axbx3 or a x b.
iv. Read the parameters value for the x_1 and r.
v. Evaluate the logistic map up to N-1 times to generate vector X.
vi. Add confusion to the vector X with mod function.
vii. Convert the vector X to uint8.
viii. Perform the encryption using bit XOR operation.
ix. Save the encrypted image in the file named I2.
x. Display the encrypted image from file I2.

3.2.2 Decryption algorithm

i. Read the encrypted image file I2.
ii. Obtain the image dimension as a x b x 3.
iii. Compute number of pixels in I2 as N=axbx3.
iv. Enter your parameters value for $y_1$and r.
v. Evaluate the logistic map up to N-1 times to generate vector Y.
vi. Confuse the vector Y with mod function.
vii. Convert vector Y to uint8.
viii. Perform the decryption process using bit XOR operation.
ix. Save the decrypted image as I3.
x. Display the decrypted image I3.

4. RESULTS

4.1 Simulation Results

We conducted this experiment using Hp 250 G5 computer with a processing speed of 1.6GHZ and a RAM size of 2048MB. The language of implementation is MATLAB R200 7b. Two images were used to test the proposed one-dimensional exponential logistic encryption algorithm; Lena_gray_256.tif and peppers_gray_256.tif.

Below are the results of the simulations of the digital image encryption algorithm using 1-Dimensional exponential logistic map.

4.2 Performance Analysis Results

The performance of the proposed encryption algorithms was measured using two metrices. The metrices used includes histogram uniformity analysis and the correlation coefficients analysis. The results of the performance amalysis for the proposed encryption algorithms are presented below:

4.2.1 Histogram uniformity analysis results

(a) Histogram analysis of the modified one-dimensional exponential logistic chaotic map encryption algorithm on gray image of Lena is shown in Fig. 2.

Table 1. Correlation coefficient analysis results of some chaotic methods in the literature and our proposed chaotic methods on a 256x256 image for the purpose of comparison

Method	Plain image			Cipher image		
	Row	Column	Diagonal	Row	Column	Diagonal
1-D exponential logistic scheme-Lena-Gray	0.9302	0.9614	0.8814	0.0263	0.0124	0.0949
1-D exponential logistic scheme-Peppers-Gray	0.9941	0.9949	0.9637	0.0662	0.0040	0.0736
encryption algorithm-Mandril	0.8943	0.8674	0.8640	0.0316	0.0022	0.0169
Fu *et al.* 2012 –Lena	0.9404	0.9299	0.9257	0.0088	-0.0087	-0.0060
Amber (2015) –Lena	0.9703	0.9425	0.9188	-0.0013	-0.0274	-0.0199
Yakubu and Aboiyar (2017)-Lena	0.9594	0.9735	0.9333	-0.0043	0.0061	-0.0018

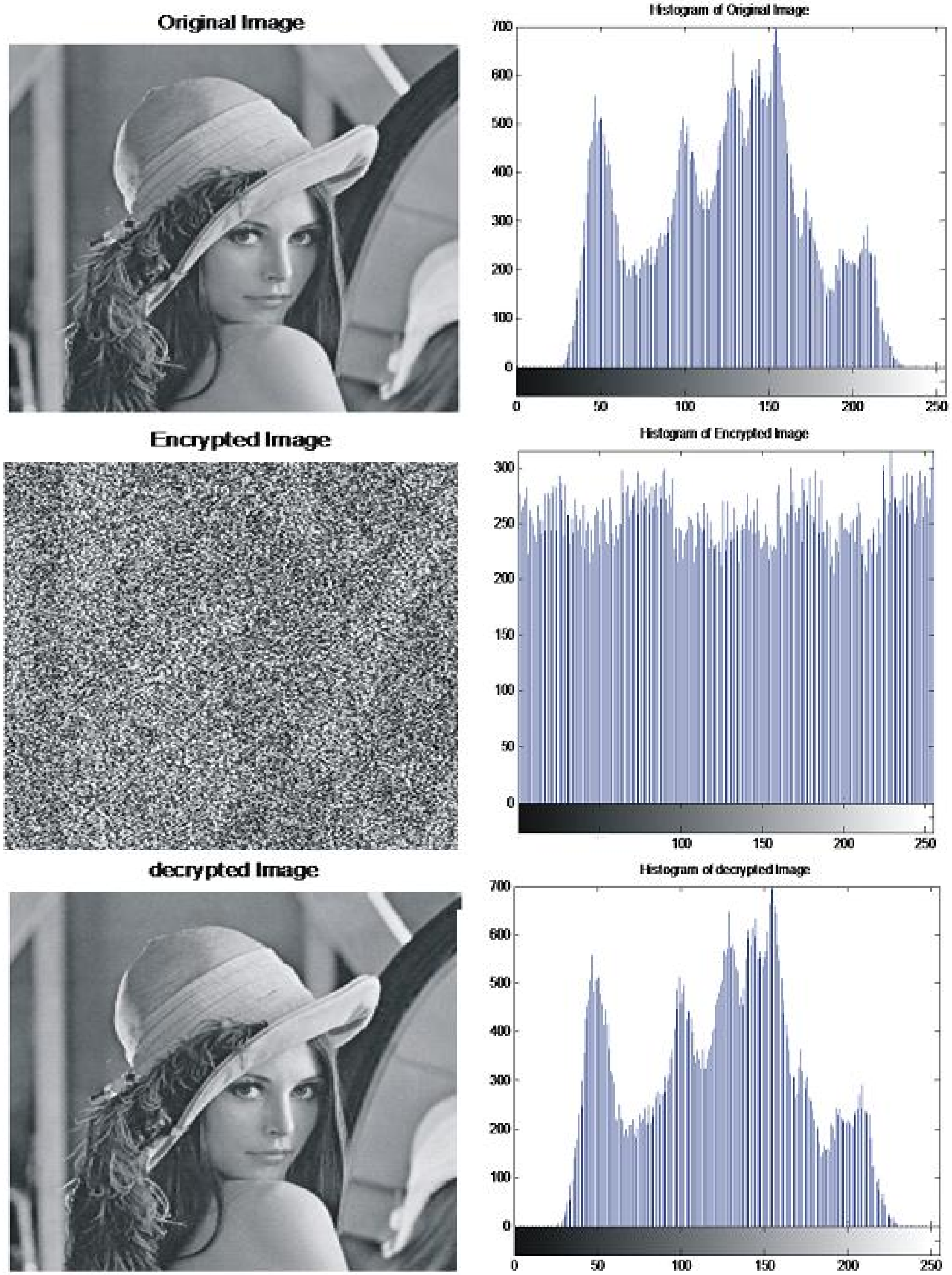

Fig. 2. Original, encrypted and decrypted gray lena images with their histograms using I-dimensional exponential logistic map image encryption algorithm

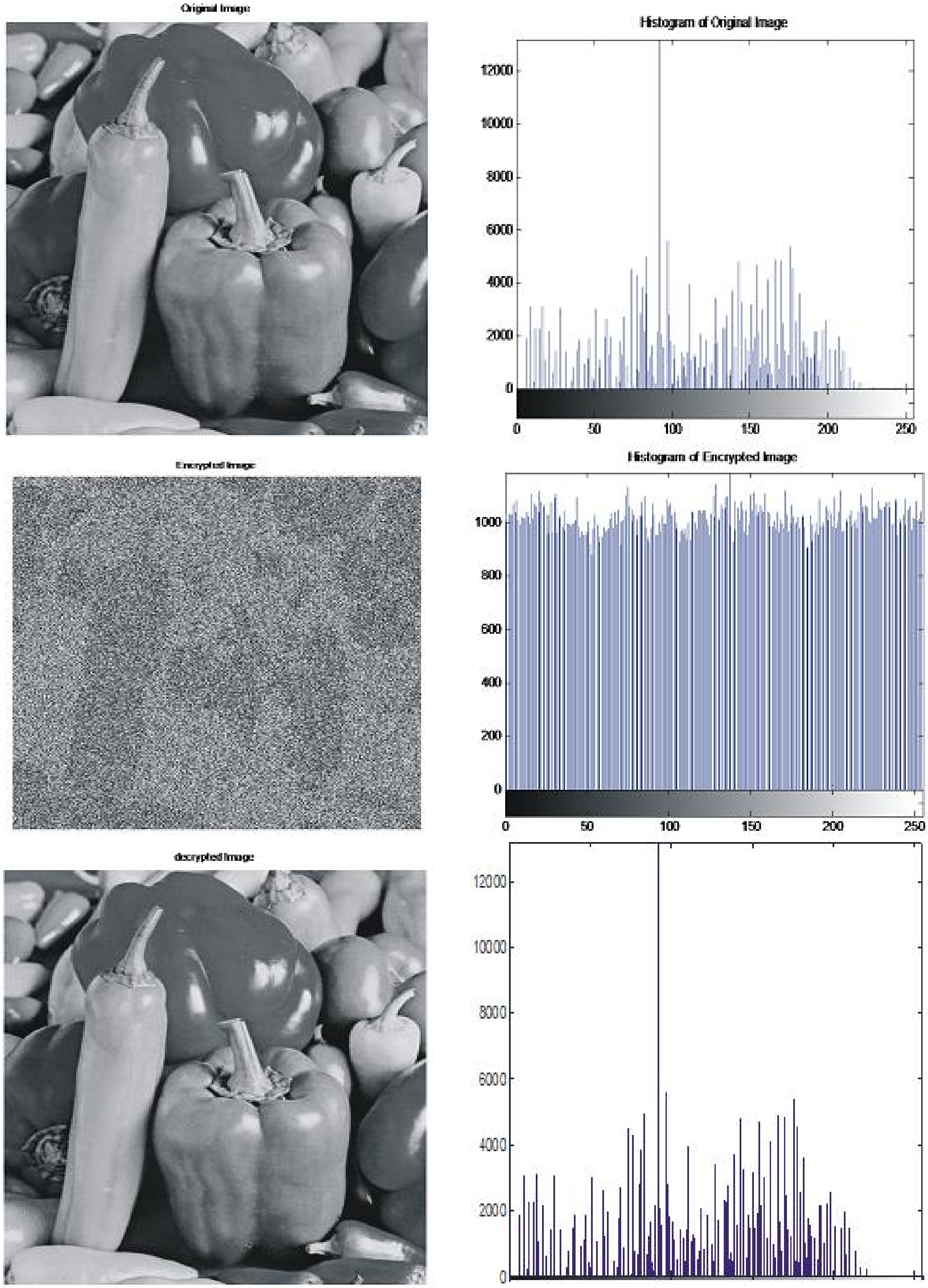

Fig. 3. Original, encrypted and decrypted gray peppers images with their histograms using I-dimensional exponential logistic map image encryption algorithm

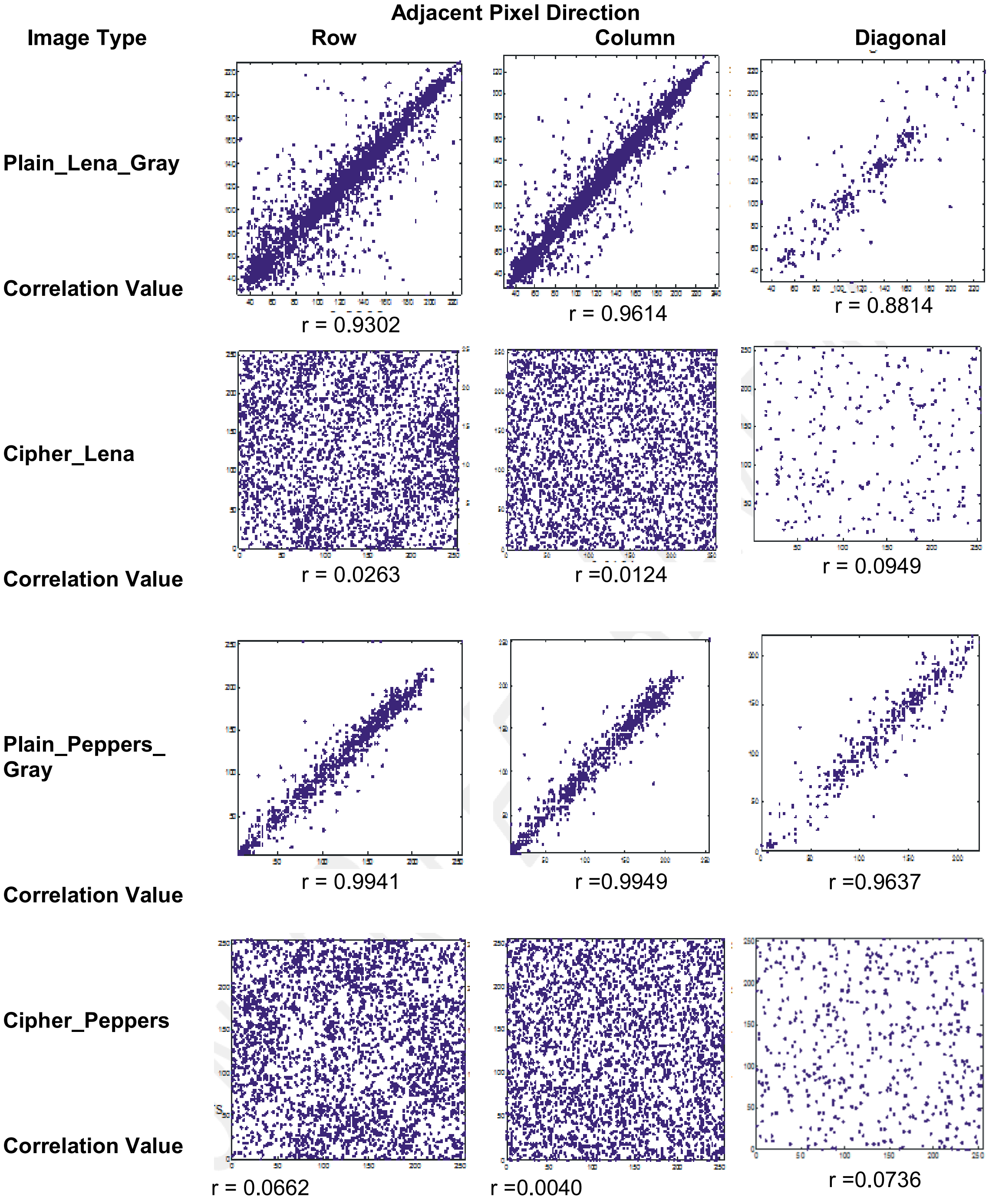

Fig. 4. Correlation coefficient between adjacent pixels of plain and cipher gray images of Lena and peppers using exponential logistic encryption algorithm

(b) Histogram analysis of the modified one-dimensional exponential logistic chaotic map encryption algorithm on gray image of Peppers is shown in Fig. 3.

(c) Histogram analysis of the one-dimensional exponential logistic chaotic map encryption algorithm on colour image of Mandril is shown in Fig. 5

(d) Histogram analysis of the one-dimensional exponential logistic chaotic map encryption algorithm on colour image of Lena is shown in Fig. 6.

(e) Histogram analysis of decrypted colour images of Lena and Mandril using one-dimensional exponential logistic chaotic map encryption algorithm is shown in Fig. 7.

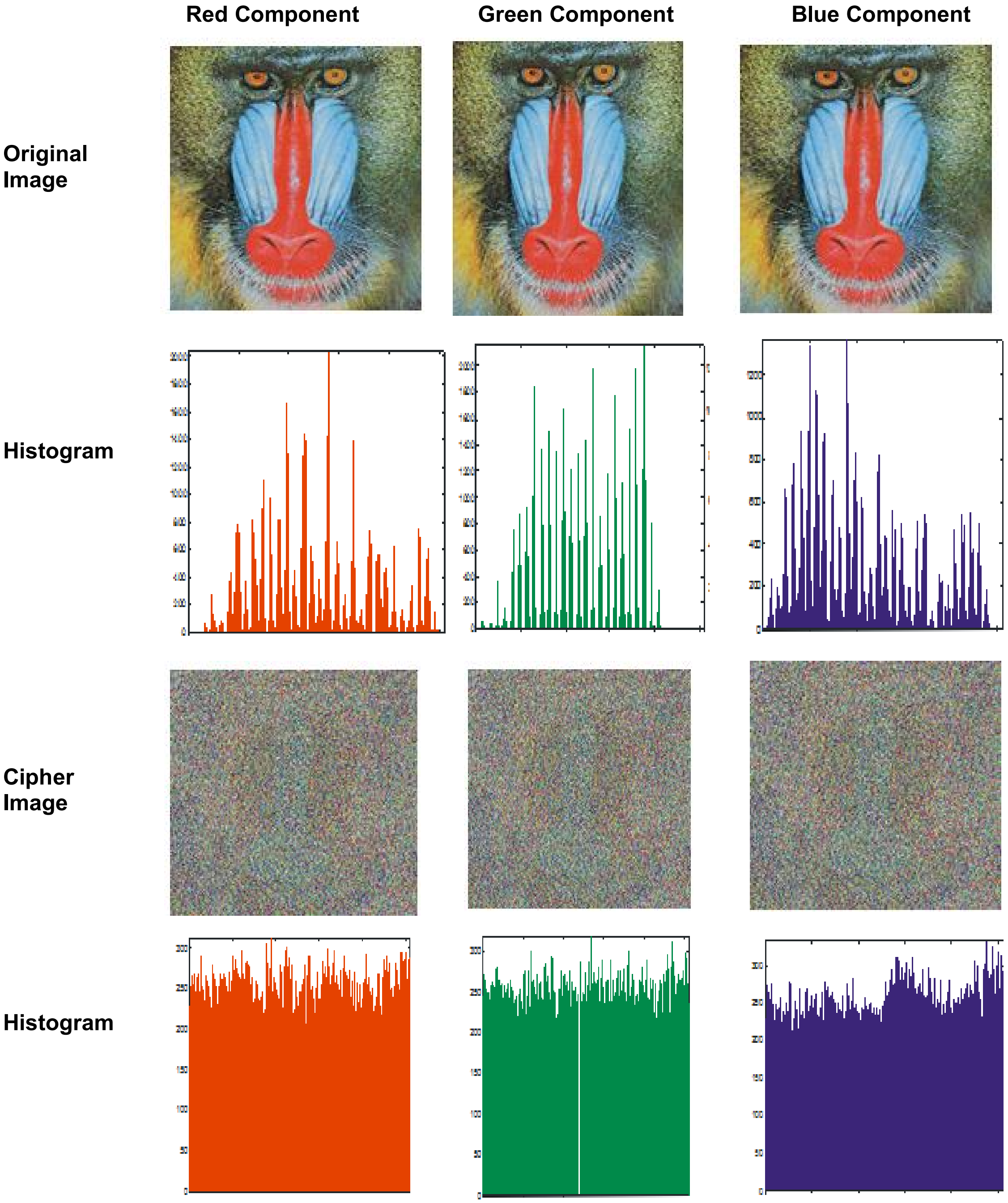

Fig. 5. Histogram of original and encrypted RGBMandril image using 1-dimensional exponential logistic chaotic map encryption scheme

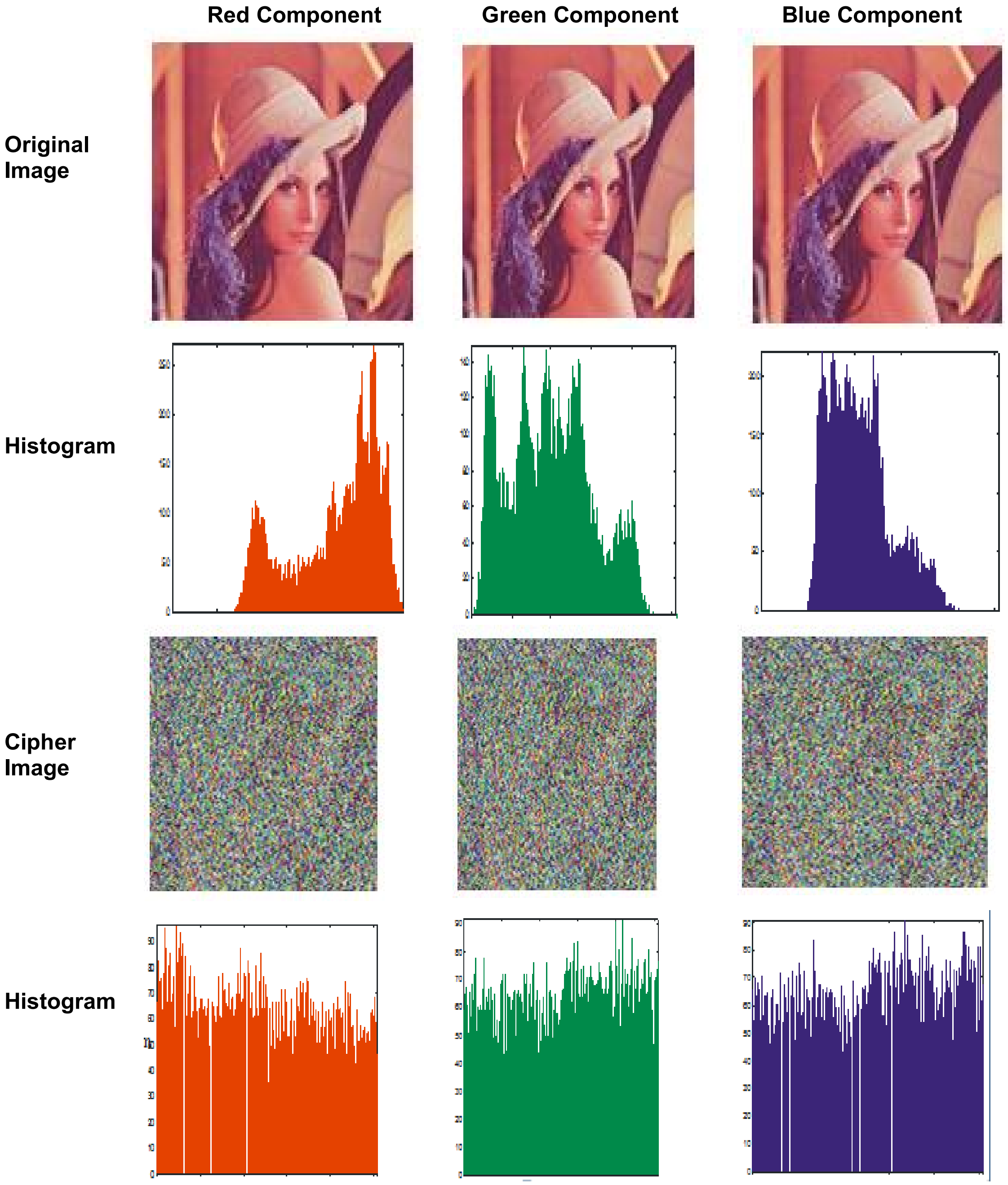

Fig. 6. Histogram of original and encrypted RGBlena image using 1-dimensional exponential logistic chaotic map encryption scheme

4.2.2 Correlation coefficient analysis results

(a) Correlation between two adjacent pixels (row, column and diagonal) of plain and cipher gray images of Lena and Peppers using one-dimensional exponential logistic chaotic map encryption algorithm are shown in Fig. 4.

5. DISCUSSION

Two different image encryption algorithms were proposed. Two images, Lena_gray.tif and Peppers_gray.tif were tested on the one-dimensional exponential logistic chaotic map algorithm. The experimental results obtained from the application of the proposed algorithm

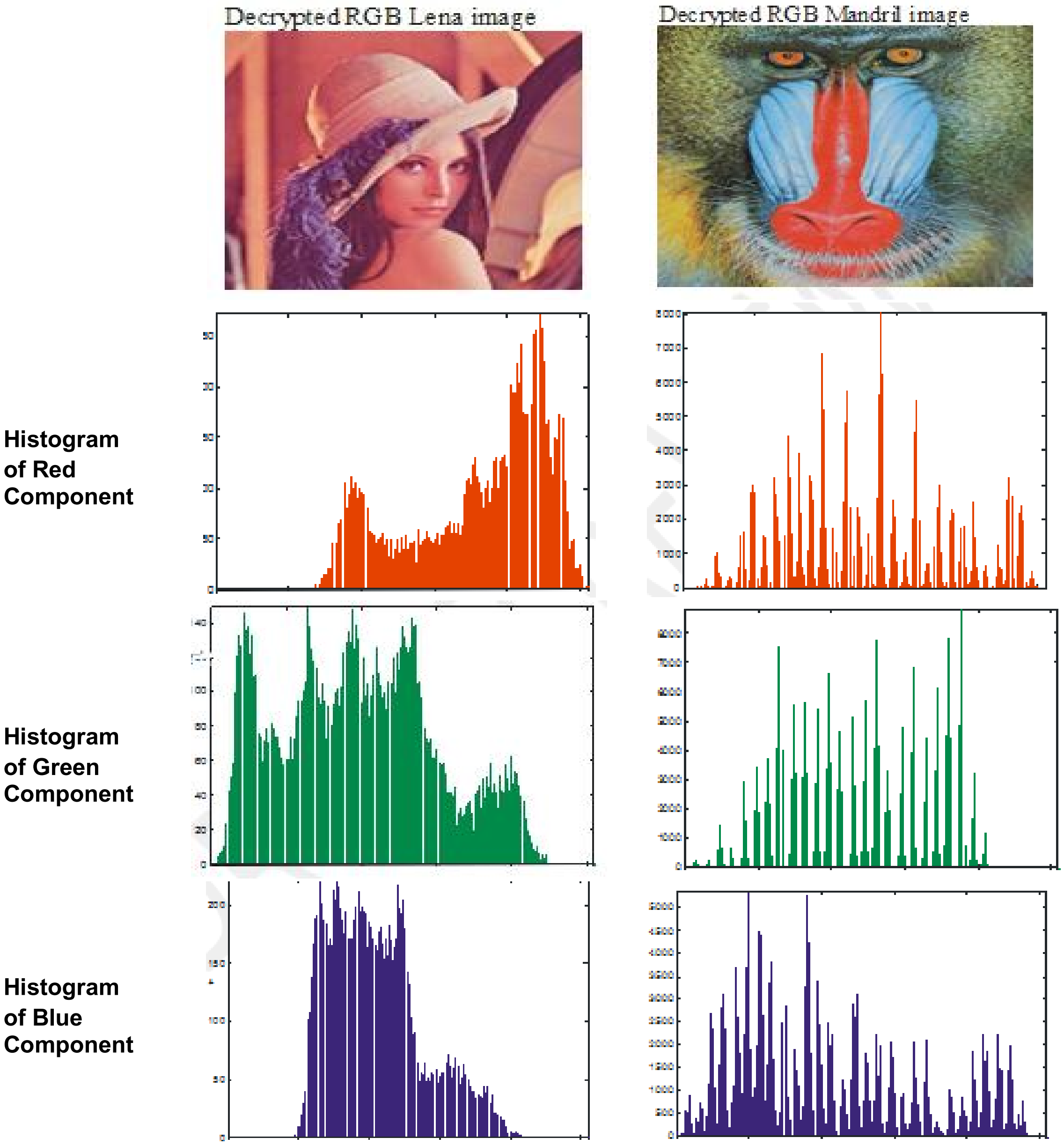

Fig. 7. Histogram of decrypted RGB lena and mandril images using 1-dimensional exponential logistic encryption algorithm

are shown in Figs. 2 and 3. The performance analysis was also carried out on the proposed encryption algorithm using the specified images and the results are shown in Fig. 4.

5.1 Discussion of the Results Obtained from the Application of the Proposed Encrption Algorithm

Figs. 2 and 3 present the plain, cipher and decrypted gray images of Lena and Peppers respectively using the one-dimensional exponential logistic chaotic map encryption algorithm. The visual inspection of the encrypted images from these Figures show that the aplication of the encryption algorithm on the original images not only works well but gives a good encrypted (cipher) images that do not provide any hint on the original image to the attacker and the decrypted images are as clear as the original image. This shows that the proposed image encryption algorithm using the modified one-dimensional exponential logistic chaotic map is effective.

Figs. 5, 6 and 7 shows the plain, cipher and decrypted colour images of the mandril, Lena and decrypted images of Mandril and Lena using the modified one-dimensional exponential logistic algorithm. From the figures, the images have very good mixing that do not reveal any hint about their original images. Their decrypted images are also good as the original images. This shows clearly that the encryption algorith really works.

5.2 Discussion of the Performance Analysis Results

5.2.1 Discussion of the histogram uniformity analysis result

Figs. 2 and 3 show original, encrypted and decrypted gray images of Lena and Peppers along side with their histograms. Comparing the histograms of the cipher images with the histograms of their original images shows that they are completely different from each other. It can also be seen that the histograms of encrypted images are fairly uniformly distributed. It therefore shows that the histogram unifrmity analysis conditions are satisfied, hence the proposed algorithm achieved part of the required level of security.

Figs. 5 and 6 shows the original and encrypted colour Mandril and Lena images along side with their histograms. Looking at their histograms closely in comparison with the histograms of the original images, it can be seen that the histograms of the encrypted images are unifrmly distributed showing that the hacker will find it difficult to know about the plain image from the encrypted image. Also, we see from Fig. 7 that the histograms of the decrypted images look exactly the same with the histograms of their original images. This suggest that the image quality is retained. Thus, the proposed algorithm is a good algorithm.

5.2.2 Discussion of the correlation coefficient analysis results

Fig. 4 show the result of correlation coefficient analysis of the modified one dimensional exponential logistic image encryption algorithm on gray images of Lena and Peppers. The Fig. 4 show that both plain Lena and plain Peppers are strongly correlated in all the three directions with an average coefficient of 0.9243in the plain Lena and 0.9842 in the plain Peppers. We see from these figures that both the plain Lena and plain Peppers are strongly correlated in all the three directions. We also see from Fig. 4 that the correlation coefficients of the cipher Lena along the three directions are very low with a highest correlation coefficiet of 0.0445 as compared to their plain image. Similarly, the correlation coefficient of the cipher Peppers along the three directions has the highest correlation coefficient of 0.0479 as compared to the correlation coefficient of plain Peppers. These results indicate that the proposed algorithm is effective. Since attackers cannot easily get any information regarding the plain image from the cipher image. Hence, the proposed system is efective.

6. CONCLUSION

In this paper, an image encryption algorithm using the modified one-dimensional exponential logistic chaotic map was presented. The one-dimensional exponential logistic chaotic image encryption algorithm was tested on gray images of Lena and Peppers and their results are as shown in Figs. 2 to 4. Standard images of Lena, Peppers and Mandrill of size 256x256 stored in tif format were used as inputs. Two metrics were used in evaluating the performance of the proposed algorithms, the histogram uniformity analysis and the correlation coefficient analysis, results are presented in Fig. 4.

The modified 1-D exponential logistic chaotic map encryption algorithm satisfied the histogram uniformity analysis conditions and the correlation coefficient between adjacent pixels in the cipher image of Lena and Peppers is very low as presented in Fig. 4. This shows that the proposed encryption algorithm is effective.

The simulation results show that the proposed chaotic image encryption algorithm has high operation efficiency and good encryption effect. We therefore conclude that the modified one-dimensional exponential logistic map image encryption algorithm can withstand various forms of attacks ensuring for confidentiality and security. Thus, the new map is suitable for image encryption and can be used for real time applications.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Farouzan BA. TCP/IP protocol suite. 4th Edition. Boston: McGraw Hill. 2010;667.
2. Huang CK, Liao CW, Hsu SL, Jeng YC. Implementation of grey image encryption with pixel shuffling and grey-level encryption by single chaotic system. Telecommunication System. 2012;10(1): 247-256.
3. Amber SN. Chaos based cryptography and image encryption. M.Sc Thesis. Ryerson University, Canada. 2015;98.
4. Rajput S, Gulve AK. A comparative performance analysis of an image encryption technique using extended hill cipher. International Journal of Computer Applications. 2014;95(4):0975-987.

   Available:www.citeseerx.ist.psu.edu/

   (Accessed on 1st March, 2017)
5. Rhee MY. Internet security cryptographic principles, algorithms and protocols. Republic of Korea: John Wiley & Sons Ltd. 2003;600.
6. Ramadan N, Ahmed HE, Elkhami SE, El-Samie FE. Chaos-based image encryption using an improved quadratic chaotic map. America Journal of Signal Processing. 2016;6(1):2165-2179.
7. Sneyers R. Climate chaotic instability: Statistical determination and theoretical background. Environmetrics. 1997;8(5): 517-532.
8. Kumar RR, Sampath A, Indumathi P. Enhancement and analysis of chaotic image encryption algorithms. Journal of Computer Science and Information Technology. 2015;1:143-152.
9. Fu C, Chen J, Zou H, Meng W, Zhan Y, Yu Y. A chaos-based digital image encryption scheme with an improved diffusion strategy. Optics Express. 2012;20(3):2363-2387.
10. Shah J, Saxena V. Performance study on image encryption schemes. International Journal of Computer Science. 2011;8(4): 800-814.
11. Aljazaery IA. Encryption of images and signals using wavelet transform and permutation algorithm. Oriental Journal of Computer Science and Technology. 2013;7(1):745-758.
12. Xiang T, Wong K, Liao X. An improved chaotic cryptosystem with external key. Communications in Nonlinear Science and Numerical Simulation. 2008;13(9):1879-1889.
13. Gotz M, Kelber K, Schwarz W. Discrete – time chaotic encryption system I. Statistical design approach. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions. 1997;44(120):963-970.
14. Kartalopoulos SV. Chaotic quantum cryptography in information assurance and security. ISIAS'08 Fourth International Conference. 2008;320-327.
15. Schmitz R. Use of chaotic dynamical systems in cryptography. Journal of the Franklin Institute. 2001;338(4):429-440.
16. El-Said SA, Hussein FA, Fouad MM. Securing image transmission using in-compression encryption technique. International Journal of Computer Science and Security. 2011;4(5):466-481.
17. Dachselt F, Schwarz W. Chaos and cryptography. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions. 2001;48(12):1498-1513.
18. Hashim HR, Neamaa IA. Image encryption and decryption in a modified ELGamal cryptosystem in MATLAB. International Journal of Sciences: Basic and Applied Research. 2014;14(2):141-147.
19. de Oliveira LP, Sobottka M. Cryptography with chaotic mixing. Chaos, Solitons & Fractals. 2008;35(3):446-468.
20. Bertuglia CS, Vaio F. Nonlinearity, chaos and complexity. The dynamics of natural and social systems. United States: Oxford University Press Inc. 2005;350.
21. Chen T, Chang C. An image cryptosystem based upon vector quantization. IEEE Transactions on Image Processing. 1997;7(10):1485-1488.
22. Guan Z, Huang F, Guan W. Chaos-based image encryption algorithms. Physics Letters. 2005;346(1-3):153-170.
23. Kanso A, Smaoui N. Logistic chaotic maps for binary numbers generations. Chaos, Solitons & Fractals. 2009;40(5):2557-2568.
24. Kocarev L, Lian Y. Chaos–based cryptography: A brief overview. Circuits

and Systems Magazine, IEEE. 2011;1(3): 6-14.

25. Kotulski Z, Szczepanski J. Discrete Chaotic Cryptography (DCC). Annalen der Physik. 1997;6(5):381-394.

26. Kang X, Peng A, Xu X, Cao X. Performing scalable lossy compression on pixel encrypted images. EURASIP Journal on Image and Video Processing. 2013;20(13): 1687-1698.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/46191