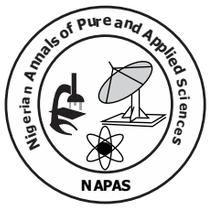

A Chaos based image Encryption Scheme using one Dimensional Exponential Logistic Map.

Gbaden Terlumun
Mathematics/Statistics/Computer Science
University of Agriculture, Makurdi, Nigeria
gbaden2014@gmail.com, +2347037381034

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.

Keyword: Encryption, Decryption, Chaos, Cryptography and Images.

Introduction

Images and other multimedia files are frequently transmitted via computer networks. The transmission of information across untrusted 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 (Forouzan, 2010; Huang *et al.*, 2012). 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 well suited for image encryption. Because in these encryption schemes there exist high correlation among pixels, so it takes high computation time and power. While few researchers such as (Wu *et al.,* 2019; Turk *et al.*, 2016 and Gao *et al.*, 2016) have applied the scatter and disorder characteristics of the chaotic system to encryption and security communication, few have used these characteristics to the encryption of digital images. Although the application of the chaotic one-dimension logistic map for image encryption is convenient and quick, it is not able to provide sufficient security. Therefore, a modification of the logistic map into a one-dimensional exponential chaotic system is approached in order to enhance communication security.

Related Works

Cryptography and Image Encryption

The security of digital images is attracting much attention nowadays and many image encryption algorithms have been proposed by different authors (Rajput and Gulve, 2014). According to Amber (2015) 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 dissimilar cryptographic tasks in a cryptographic system. Reviewing some recent work on chaos – based cryptography, the researcher discovered that cryptographic methodologies are critically important for storage of secured media content and transmission over exposed systems, for example, the web. For high security, encryption is one of the approaches to guard the information from leakage. Image encryption is transformation of image to an inaccurate form so that it can be secured from unauthorized users (Rhee, 2003 and Ramadan *et al.,* 2016).

Exploring application of encryption in time samples pattern, the researcher recommended a secured approach to code input signals by introducing a new encryption algorithm. The algorithm mechanism is such that the transmitter, an input signal was received and coded into a lengthier series of numbers. At the receiver, the coded signal by the transmitter was received and changed back into its original values. This was done based on the idea that the hidden input signal samples using a specific pattern, could only be recoverable by a trusted receiver (Sneyers, 1997and Kumar, *et al.,* 2015). Fu *et al.* (2012) observed that Chaos-based image cipher has been widely investigated over the last decade or so to meet the increasing demand for real-time secure image transmission over public networks. Shah and Saxena (2011) proposed an improved diffusion strategy to promote the efficiency of the most widely investigated permutation-diffusion type image cipher. By using the novel bidirectional diffusion strategy, the spreading process was significantly accelerated and hence the same level of security was achieved with fewer overall encryption rounds. Moreover, to further enhance the security of the cryptosystem, a plaintext related chaotic orbit turbulence mechanism was introduced in diffusion procedure by perturbing the control parameter of the employed chaotic system according to the cipher-pixel. Extensive cryptanalysis has been performed on the proposed scheme using differential analysis, key space analysis, various statistical analyses and key sensitivity analysis. Results of their research indicated that the new scheme was a satisfactory security level with a low computational complexity, which renders it a good candidate for real-time secure image transmission application.

A system for efficient image encryption-then-compression was designed by Nimbokar *et al.* (2014). Image encryption has to be conducted prior to image compression. The researchers considered how to design a pair of image encryption and compression algorithms such that compressing encrypted images can still be

efficiently performed. The work introduced a highly efficient image encryption-then-compression (ETC) system. The proposed image encryption scheme operated in the prediction error domain is able to provide a reasonably high level of security. More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency.

An efficient, secure color image coder based on color Set Partitioning in Hierarchical Trees (C-SPTHT) compression and partial encryption was presented by Karl *et al.* (2005). The use of a stream cipher and encryption of a small number of bits keeps computational demands at a minimum and makes the technique suitable for hardware implementation (Pritchard, 1996). By varying k, the level of confidentiality vs processing overhead can be controlled. It was found that using k = 2 achieved an adequate level of security for test images coded at 0.8 bits per pixel (bpp), resulting in an average of only 0.33% of the coded image been encrypted (Amig *et al.*, 2015).

Aljazaery (2013) 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. This method depends on extracting the important features which are distinguished these signals and images and then discarding them. The next step is encrypting the lowest dimensions of these data. Discrete Wavelet transform (DWT) is used as a feature extraction because it is a powerful tool of signal processing for its multiresolutional possibilities Xiang *et al.* (2008). The chosen data is encrypted with one of conventional cryptographic algorithm (Permutation algorithm) after shrinking its dimension using suitable encryption key. The encrypted data was 100% unrecognized, besides, the decryption algorithm returned the encrypted data to its original dimension efficiently.

Image applications have been increasing in recent years. According to Gotz *et al*. (1997) encryption is used to provide the security needed for image applications. Shah and Saxena (2011) 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. Kartalopoulos (2008) 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. Schimtz (2001) proposed a secure and computationally feasible algorithm called Optimized Multiple Huffman Tables (OMHT) technique. OMHT depends on using statistical-model-based compression method to generate different tables from the same data type of images or video to be encrypted leading to increase compression efficiency and security of the used tables. A systematic study on how to strategically integrate different atomic operations to build a multimedia encryption system was presented. The resulting system can provide superior performance over other techniques by both its generic encryption and its simple adaptation to multimedia in terms of a joint consideration of security, and bit rate overhead. 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 (El-Said *et al.*, 2011).

The need of exchanging messages and secretly over unsecure networks promoted the creation of cryptosystems to enable receivers to interpret the exchanged information (Dachselt and Schwarz, 2001). In the presentation of Hashim and Neamaa (2014), a particular public key cryptosystem called the ElGamal Cryptosystem was considered with the help of MATLAB program used over images. Since the ElGamal cryptosystem over a primitive root of a large prime was used in messages encrypted in the free GNU Privacy Guard software, recent versions of Pretty Good Privacy (PGP), and other cryptosystems. The work shows a modification of this cryptosystem by applying it over gray and color images. That would be by transforming an image into its corresponding matrix using MATLAB program, then applying the encryption and decryption algorithms over it. Actually, this

modification gives one of the best image encryptions that have been used since the encryption procedure over any image goes smoothly and transfers the original image to completely undefined image which makes this cryptosystem really secured and successful over image encryption. As well as, the decryption procedure of the encrypted image works very well since it transfers undefined image to its original. Therefore, this new modification can make 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 (de Oliveira and Sobottka, 2008; Bertuglia, 2005).

Vector Quantization (VQ) is an efficient technique for image encryption (Chen and Chang, 1997). 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 (Guan and Guan, 2005). 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 (Kanso and Smaoui, 2009).

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 (Kocarev and Lian, 2011). This frustrates the attempts to study the ciphertext looking for redundancies and statistical patterns. Diffusion involves many transformations (or permutations) to dissipate the redundancies of the plaintext by spreading it out over the ciphertext. In addition to confusion and diffusion techniques, we also use some number theorems for our new image cryptosystem.

The new cryptosystem consists of the following three basic phases: encryption, transmission and decryption phases. In the encryption phase, we first apply VQ to compress our original image into a set of indices. Next, we diffuse and confuse the codebook, and encrypt these parameters of the codebook by a symmetric cryptosystem. In transmission phase, our scheme sends the set of indices and the above encrypted data of the codebook by a public channel. The scheme also sends the secret key K to the receiver by a secret channel. Since K is the secret key to decrypt the cipher image, we must send it to the legal receiver in secret. In general, there are two methods that can be used to distribute the secret key K. one is by a secure channel. The other is based on the computational difficulty of computing discrete logarithms (Kotulski and Szczepanski, 1997).

Kang *et al.* (2013) 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. The researchers proposed a scalable lossy compression scheme for images having their pixel value encrypted with a standard stream cipher. The encrypted data are simply compressed by transmitting a uniformly sub sampled portion of the encrypted data and some bit planes of another uniformly sub sampled portion of the encrypted data. At the receiver side, a decoder performs content-adaptive interpolation based on the decrypted partial information, where the received bit plane information serves as the side information that reflects the image edge information, making the image reconstruction more precise. When more bit planes are transmitted, higher quality of the decompressed image can be achieved. The experimental results show that the proposed scheme achieves much better performance than the existing lossy compression scheme for pixel-value encrypted images and also similar performance as the state-of-the art lossy compression for pixel permutation based encrypted images. In addition, the proposed scheme had the following advantages: at the decoder side, no computationally intensive iteration and no additional public orthogonal matrix were needed. It works well for both smooth and textured-rich images.

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

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

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 $x_{1,2} = 1 - \frac{1}{r}$.

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 observation.

The Proposed System

The One-Dimensional Exponential Logistic Map

The proposed one dimensional exponential logistic map is defined by

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

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.

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.

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.

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.

Results

Simulation Results

We conducted this experiment using Hp 250 G5 computer with a processing speed of 1.6GHZ and a RAM size of 2048MB. 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.

Flowchart diagram for the encryption/decryption using the exponential logistic map

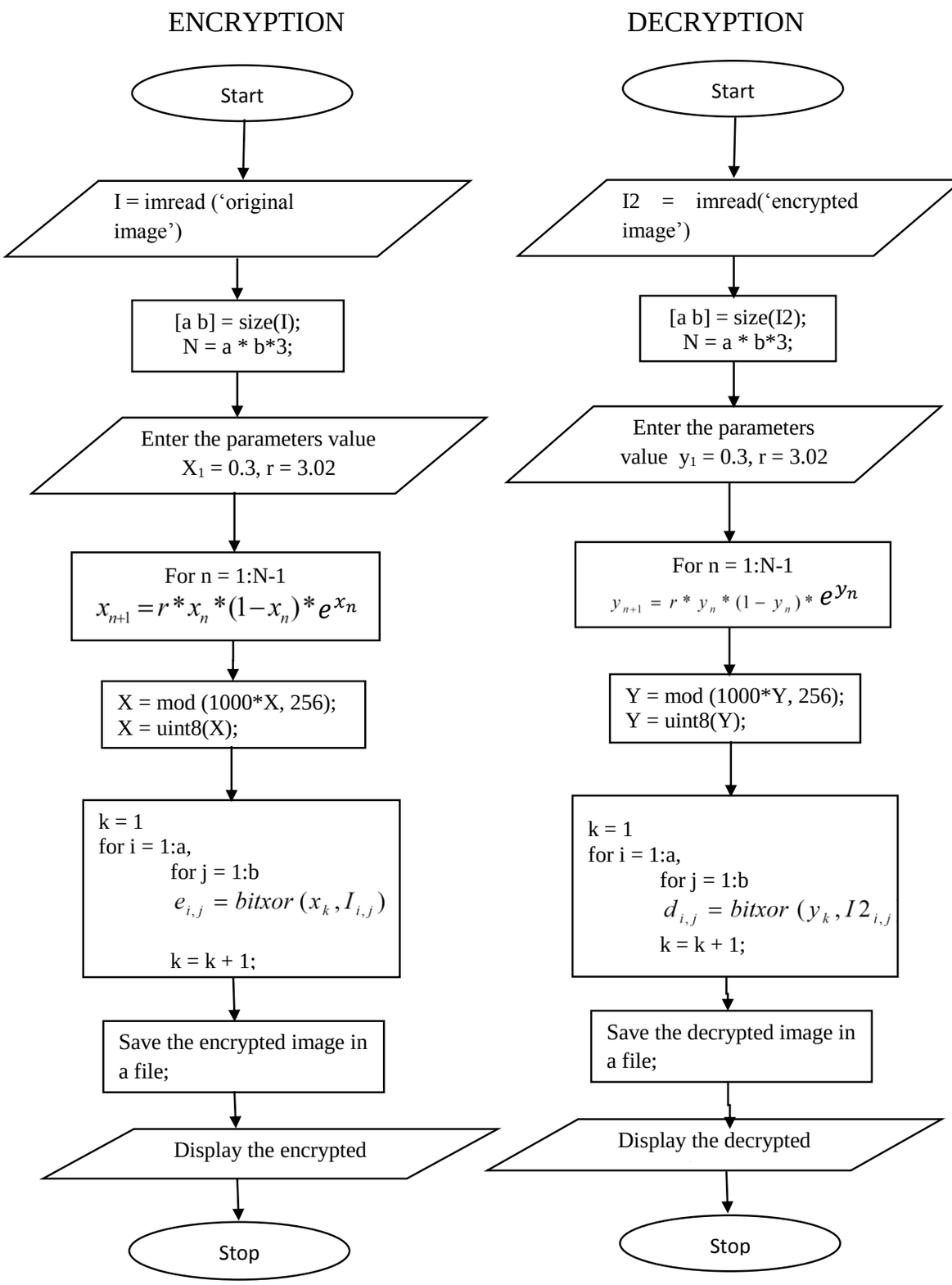

Figure 1: gives the flow diagram for image encryption and decryption using the exponential logistic map.

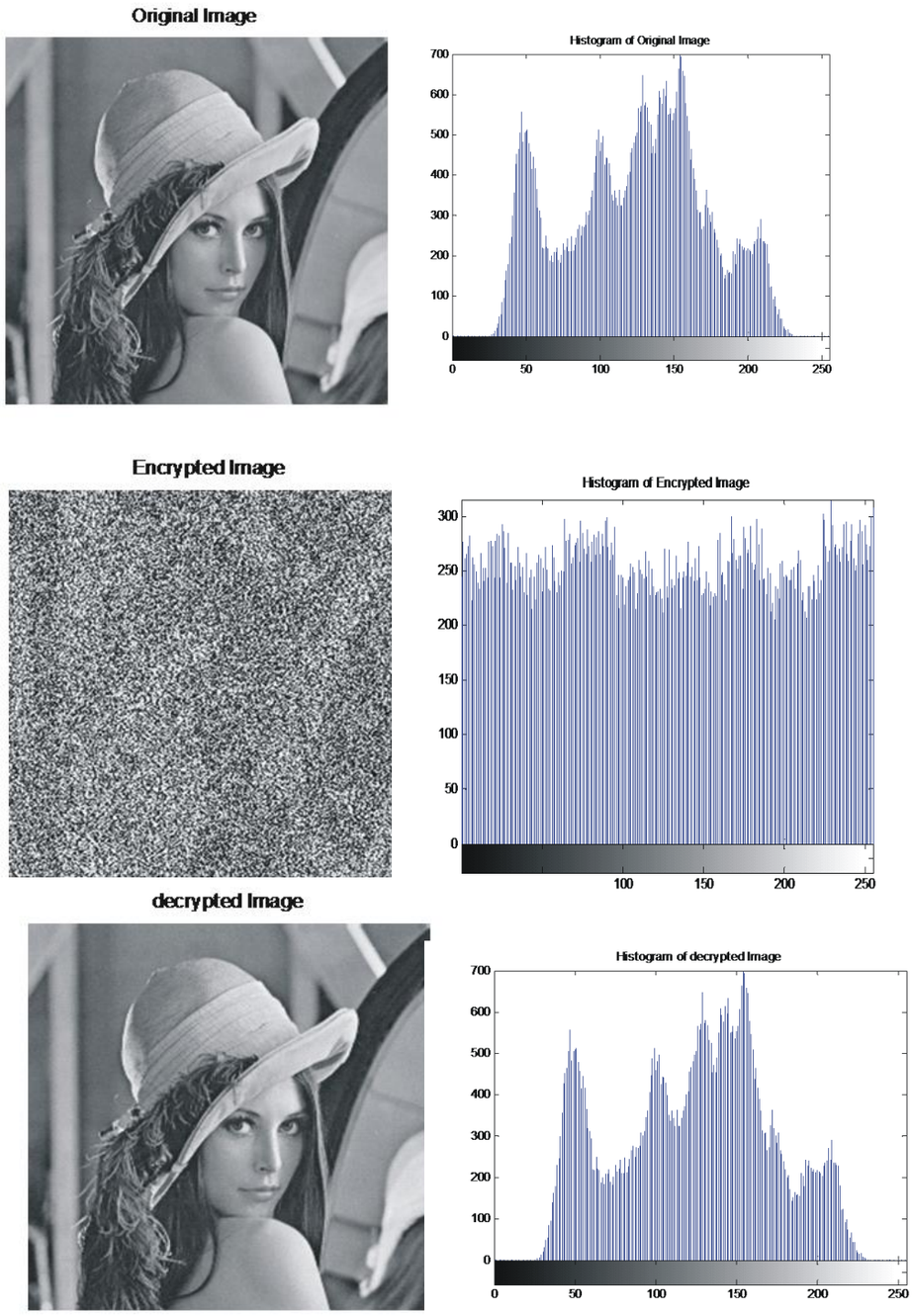

Figure 2: Original, encrypted and decrypted gray Lena images with their histograms using I-Dimensional exponential logistic map image encryption algorithm.

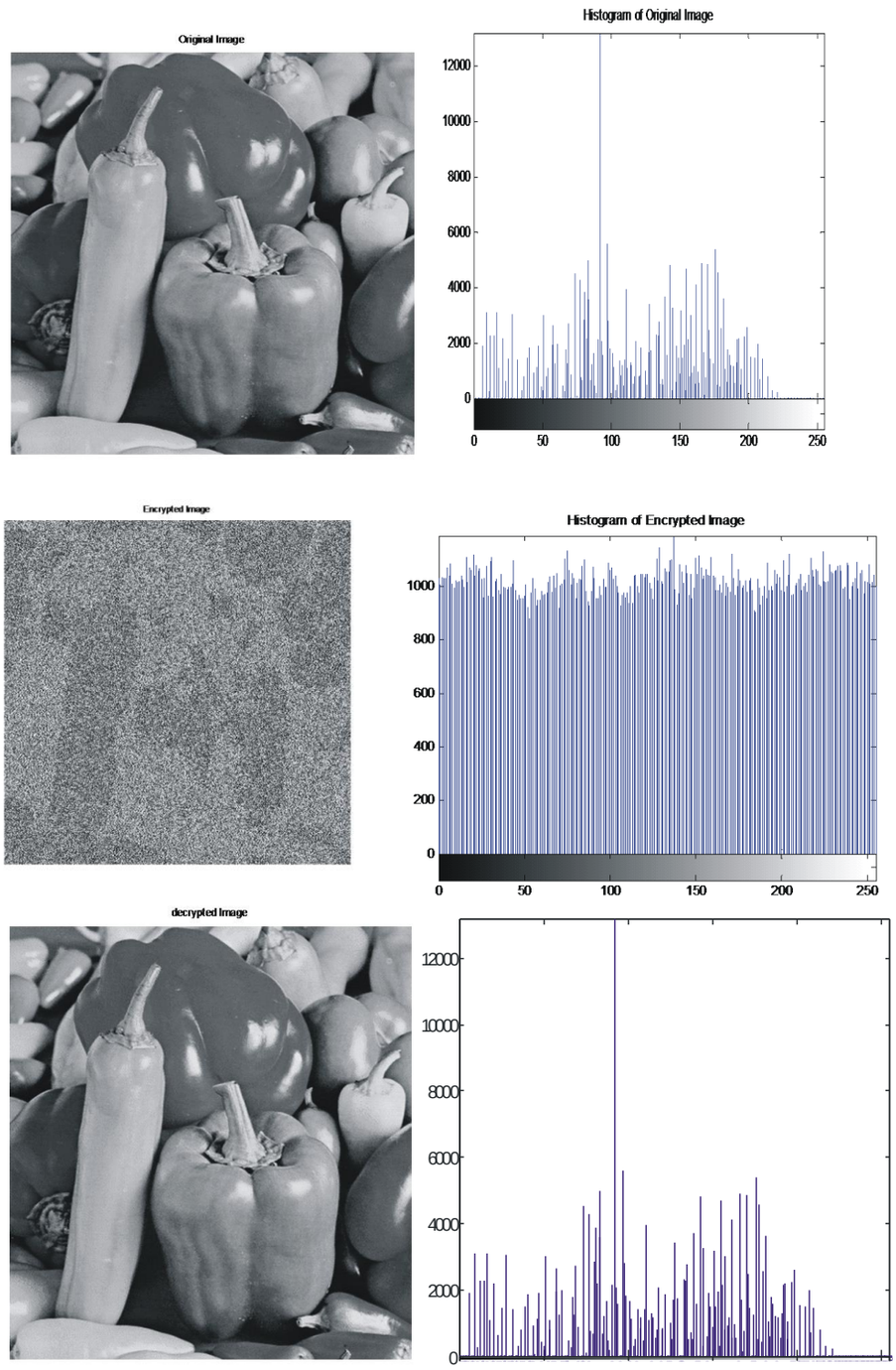

Figure 3: Original, encrypted and decrypted gray Peppers images with their histograms using I-Dimensional exponential logistic map image encryption algorithm.

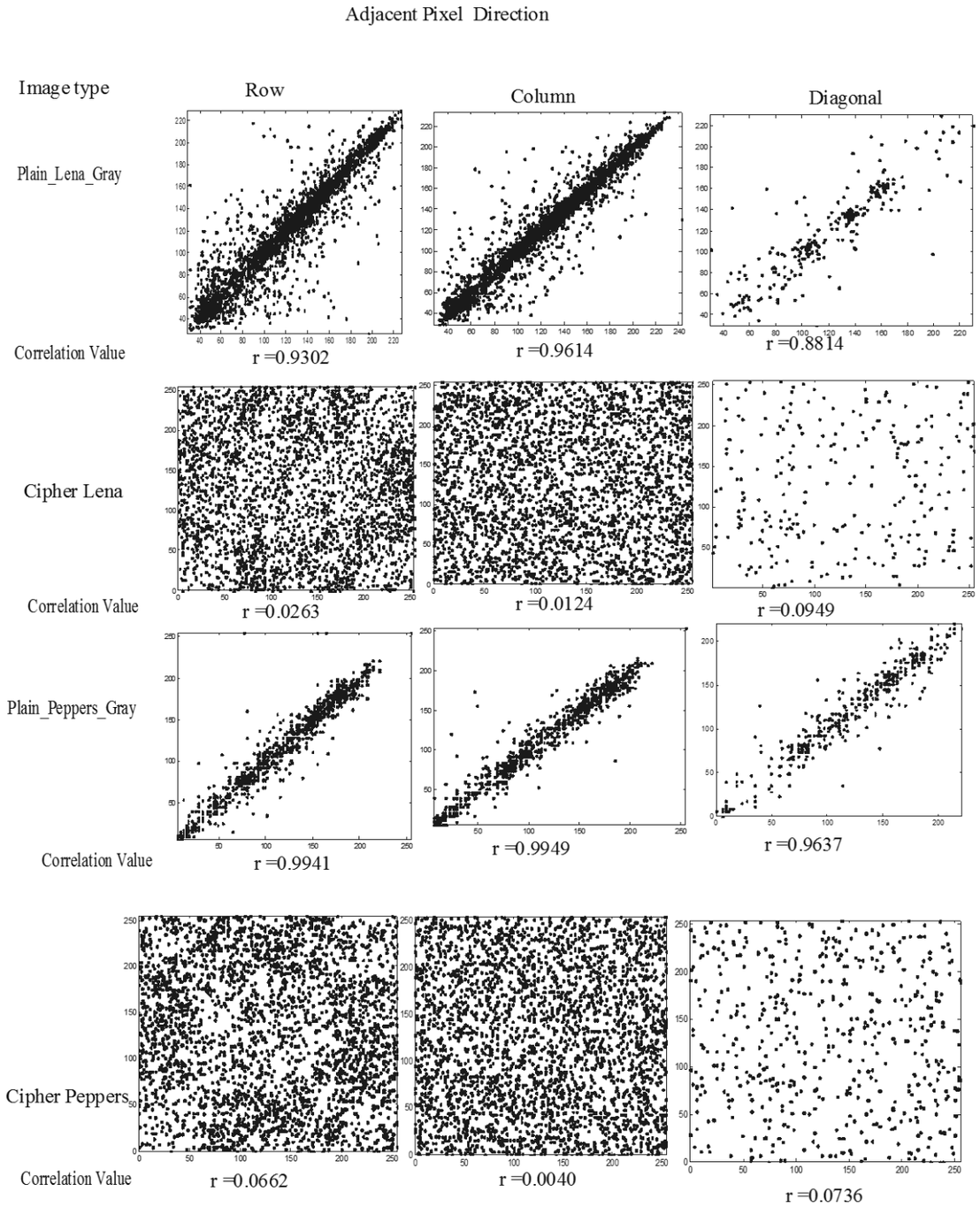

Figure 4: Correlation coefficient between adjacent pixels of plain and cipher gray images of Lena and peppers using exponential logistic encryption algorithm

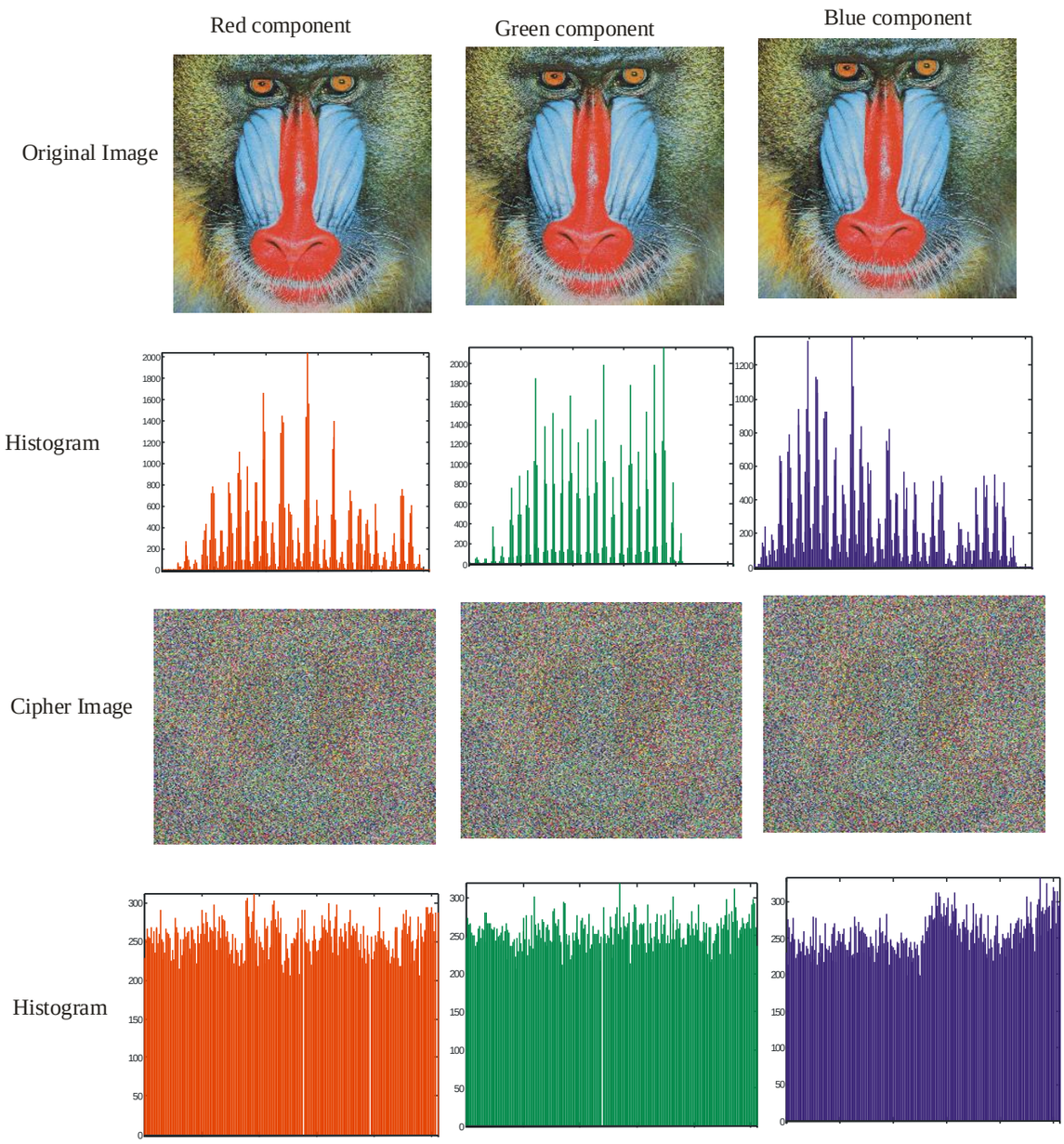

Figure 5: Histogram of original and encrypted RGB Mandril image using 1-Dimensional exponential logistic chaotic map encryption scheme

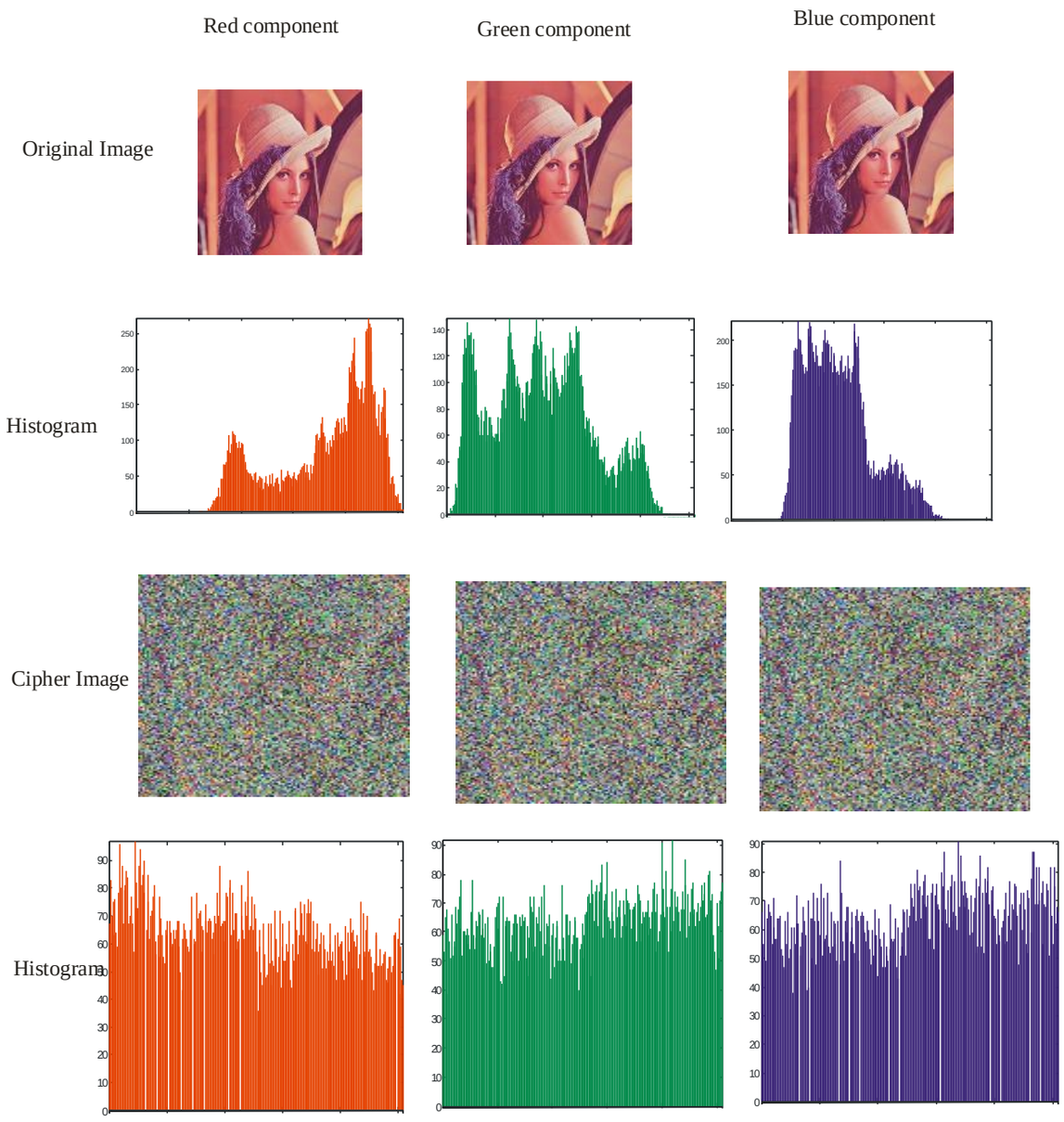

Figure 6: Histogram of original and encrypted RGB lena image using 1-Dimensional exponential logistic chaotic map encryption scheme

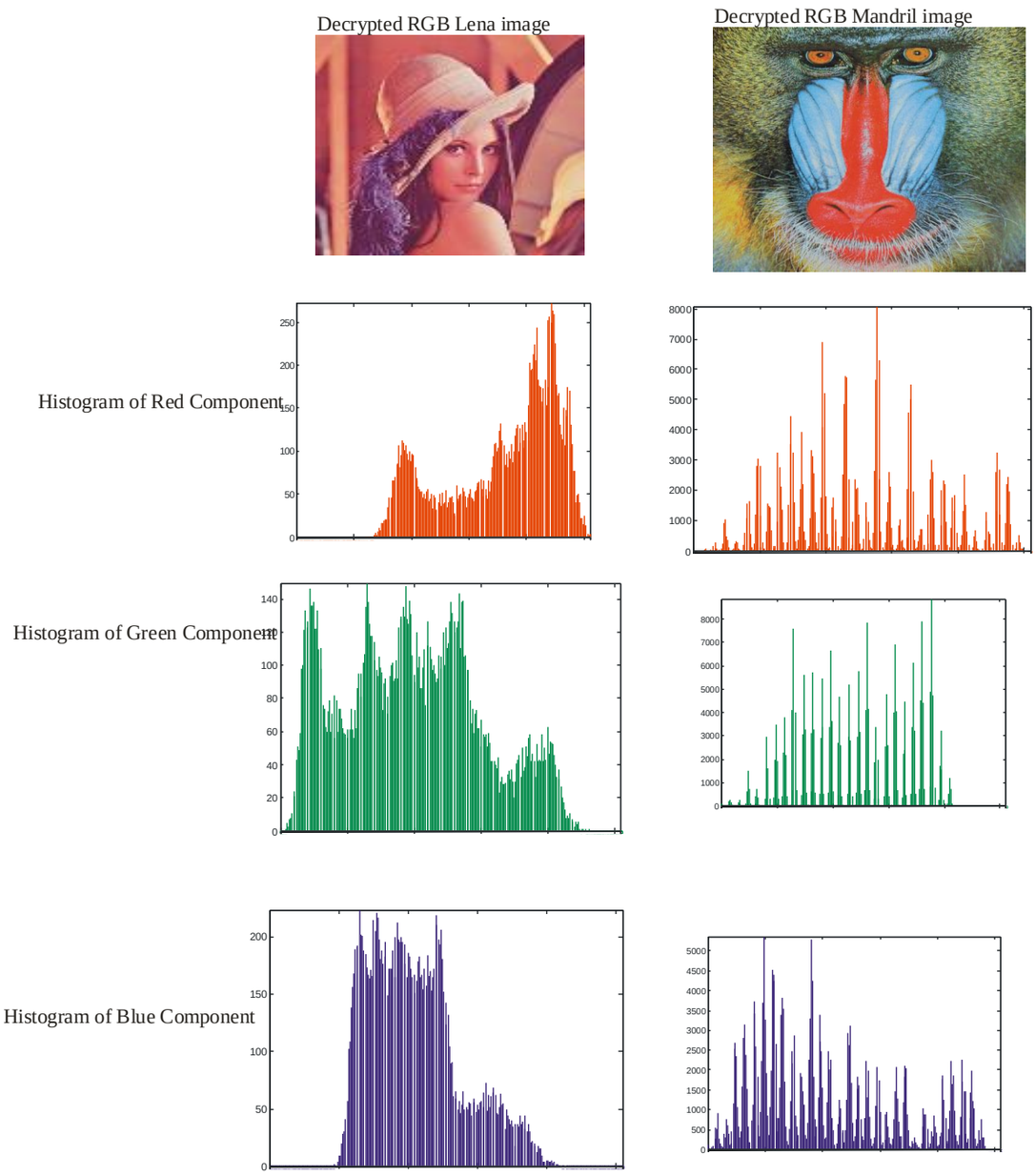

Figure 7: Histogram of Decrypted RGB Lena and Mandril images using 1-Dimensional Exponential logistic Encryption Algorithm

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:

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 Figure 2.

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

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

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

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

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 Figure 4.

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 are shown in Figures 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 Figure 4.

Discussion of the results obtained from the application of the proposed encrption algorithm.

Figures 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.

Figure 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.

Discussion of the Performance Analysis Results
Discussion of the histogram uniformity analysis result

Figure 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.

Figures 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 Figure 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.

Discussion of the correlation coefficient analysis results

Figure 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 figure 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 figure 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.

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 Figures 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 Figures 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 Figure 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.

References

Aljazaery, I.A, (2013). Encryption of Images and Signals Using Wavelet Transform and Permutation Algorithm. *Oriental Journal of Computer Science and Technology.* 7(1): 745- 758.

Amber, S.N. (2015). Chaos Based Cryptography and Image Encryption. *M.Sc Thesis.* Ryerson University, Canada. 98pp.

Amig, J.M., Kocarev, L. and Szczepanski, J. (2015). Theory and Practice of Chaotic Cryptography. *Physics Letters.*366 (3): 211-223.

Bertuglia, C.S and Vaio, F. (2005). *Nonlinearity, Chaos and Complexity. The Dynamics of Natural and Social Systems.* United States: Oxford University Press Inc.350pp.

Chen, T. and Chang, C. (1997). An Image Cryptosystem Based Upon Vector Quantization. *IEEE Transactions on Image Processing.* 7(10):1485-1488.

Dachselt, F. and Schwarz, W. (2001). Chaos and Cryptography. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions.* 48 (12):1498-1513.

de Oliveira, L.P. and Sobottka, M. (2008). Cryptography with Chaotic Mixing. *Chaos, Solitons& Fractals.* 35(3): 446-468.

El-Said, S.A., Hussein, F.A. and Fouad, M.M (2011). Securing Image Transmission Using in-Compression Encryption Technique. *International Journal of Computer Science and Security*. 4(5): 466-481.

Farouzan, B.A. (2010). *TCP/IP Protocol Suite. 4th Edition*. , Boston: McGraw Hill. 667pp.

Fu, C., Chen, J., Zou,H., Meng, W., Zhan, Y and Yu, Y. (2012). A Chaos-based Digital Image Encryption Scheme with an Improved Diffusion Strategy. *Optics Express.* 20 (3):2363-2387.

Gao, J., Shi, D. and Huang, L. (2016). The Design and its Application in Secure Communication and Image Encryption of a New Lorenz-Like System with Varying Parameter. *Mathematical Problems in Engineering.*Vol.2016.

Gotz, M., Kelber, K. and Schwarz, W.(1997). Discrete –Time Chaotic Encryption System I. Statistical Design Approach. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions.* 44 (120): 963-970.

Guan, Z., Huang, F. and Guan, W. (2005). Chaos-Based Image Encryption Algorithms. *Physics Letters.* 346(1-3): 153-170.

Hashim, H.R. and Neamaa, I.A. (2014). Image Encryption and Decryption in a Modified ELGamal Cryptosystem in MATLAB. *International Journal of Sciences: Basic and Applied Research*. 14(2):141-147.

Huang, C.K., Liao, C.W., Hsu, S.L. and Jeng, Y.C. (2012). Implementation of Grey Image Encryption with Pixel Shuffling and Grey-Level Encryption by Single Chaotic

System. *Telecommunication System.* 10(1): 247-256.

Kang, X., Peng, A., Xu, X. and Cao, X. (2013). Performing Scalable Lossy Compression on Pixel Encrypted Images. *EURASIP Journal on Image and Video Processing.* 20 (13): 1687-1698.

Kanso, A. and Smaoui, N. (2009). Logistic Chaotic Maps for Binary Numbers Generations. *Chaos, Solitons & Fractals.* 40 (5): 2557-2568.

Karl, M., Rastislav, L. and Konstantinos, N.P. (2005). Efficient Encryption of Wavelet-Based Coded Color Image. *Pattern Recognition.* 38(5):1111-1115. Retrieved from www.ScienceDirect.com on 1st March, 2017.

Kartalopoulos, S.V. (2008). Chaotic Quantum Cryptography in Information Assurance and Security. *ISIAS'08 Fourth International Conference.2008,* 320-327.

Kocarev, L. and Lian, Y. (2011). Chaos –Based Cryptography: A Brief Overview. *Circuits and Systems Magazine, IEEE.* 1(3): 6-14.

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

Kumar, R.R., Sampath, A. and indumathi, P. (2015). Enhancement and Analysis of Chaotic Image Encryption Algorithms. *Journal of Computer Science and Information Technology.* 1:143-152.

Kumaur, N., Wadhwa, D., Tower, D. and Vijayalakshmi, S. (2015). Review of Different Chaotic Based Image Encryption Techniques. *International Journal of Information and Computation Technology.* 4 (2): 197-206. Retrieved from http://www.irphouse.com/ijict.htm on 2nd March, 2017.

Nimbokar, K.G., Sarode, M.V. and Ghonge, M.M. (2014). A Survey Based on Designing an Efficient Image Encryption-Then-Compression System. *International Journal of Computer science Applications.* 1: 0975-8887.

Pritchard, J. (1996). *The Chaos Cookbook*. Oxford: Butterworth-Heinemann. 400pp.

Rajput, S. and Gulve, A.K. (2014). A Comparative Performance Analysis of an Image Encryption Technique Using Extended Hill Cipher. *International Journal of Computer Applications*. 95(4):0975-987. Retrieved form www.citeseerx.ist.psu.edu/ on 1st March, 2017.

Ramadan, N., Ahmed, H.E. Elkhami, S.E. and El-Samie, F.E. (2016). Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map. *America Journalof Signal Processing.* 6 (1): 2165-2179.

Rhee, M.Y. (2003*). Internet Security Cryptographic Principles, Algorithms and Protocols.* Republic of Korea: John Wiley & Sons Ltd.600pp.

Schmitz, R. (2001). Use of Chaotic Dynamical Systems in Cryptography. *Journal of the Franklin Institute.* 338(4):429-440.

Shah, J. and Saxena, V. (2011). Performance Study on Image Encryption Schemes. *International Journal of Computer Science.* 8(4): 800-814.

Sneyers, R. (1997). Climate Chaotic Instability: Statistical Determination and Theoretical Background. *Environmetrics.* 8(5):517-532.

Turk, M. and Ogras, H. (2016). A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator. *American Journal of Signal Processing.* 6 (3): 67-76.

Wu, Z., Zhang, X., and Zhong, X. (2019). Generalized Chaos Synchronization Circuit Simulation and Asymmetric Image Encryption. *IEEE Access.*

Xiang, T., Wong, K and Liao, X (2008). An Improved Chaotic Cryptosystem with External Key. *Communications in Nonlinear Science and Numerical Simulation*. 13(9): 1879-1889.