American Journal of Mobile Systems, Applications and Services
Vol. 1, No. 1, 2015, pp. 20-29
http://www.aiscience.org/journal/ajmsas

Enhanced Encryption Algorithm Based on a Modified Confusion and Diffusion Scheme

Isiaka A. Alimi[1, *], Oluyomi Aboderin[2]

[1]Department of Electrical and Electronics Engineering, School of Engineering and Engineering Technology, Federal University of Technology, Akure, Nigeria
[2]Department of Engineering and Space Systems, National Space Research and Development Agency, Abuja, Nigeria

Abstract

There have been significant developments in computer networking which have result in high rate of internet and multimedia application usage. However, transmission of images and other relevant information over such network can be compromised if adequate security is not employed. Consequently, security is a technical challenge in transmission and storage of digital images. Therefore, image encryption has been noted to be an efficient means of securing digital images and various encryption methods have been proposed in the literature. One of such method is chaos based image encryption technique in which random sequence is employed. This technique is relatively an efficient means of achieving fast and reliable encryption. Nevertheless, it has limited precision which necessitate an improved scheme to be developed. This paper presents image encryption algorithm with improved precision, confidentiality and security that exploits the existing algorithms. The effectiveness of the algorithm is evaluated by comparing the plaintext and the decrypted text using MATLAB®. The simulation results show that, the proposed scheme is viable and offers a reasonable degree of security. Also, there is no loss in the quality of digital images during the process.

Keywords

Cryptography, Encryption, Decrypting, Key, Chaotic Map, Security

Received: May 29, 2015 / Accepted: June 13, 2015 / Published online: July 13, 2015

1. Introduction

The internet is the major channel for information transmission for various applications and without an effective security scheme, the information in the channel is vulnerable to unauthorized users and it can be compromised at various levels of transmission as well as while in storage [1]. Therefore, an end-to-end data encryption is require to create a secure environment for various types of applications such as pay-per-view cable TV, medical imaging systems, industrial imaging systems and military imaging systems on the internet. An image encryption is a process of converting a plaintext (original image) to a ciphertext (encrypted image) so as to protect the information in an open network systems from being compromised by unauthorized parties. This process takes place during the transmission of information. The process scrambles the contents of the message and the original information can only be retrieve through the decryption process [2]. Decryption process is the reverse of the process at the transmitter (sender) and it takes place at the receiver [1], [3].

There are various encryption techniques which have been extensively employed to get around the issues of insecure transmission for both images and texts over an open network systems such as the internet. The encryption techniques can be realized by the implementation of cryptographic algorithms [4]. There are different cryptographic algorithms that can be used for information confidentiality and security;

* Corresponding author
E-mail address: compeasywalus2@yahoo.com (I. A. Alimi), jayyomi@yahoo.com (O. Aboderin)

however, the algorithms differ in speed and efficiency [4], [5].

In the literature, various encryption methods have been proposed [1–5]. It has been observed in [4] that, an efficient and high throughput encryption and decryption algorithms are of high importance in the area of high-speed networking for seamless transmission of multimedia data. However, the conventional standards seem not to be as secure and fast to be able to cope with the current advanced technological demands [4]. Also, inefficiency of the conventional encryption algorithms such as DES, IDES for digital image encryption are discussed in [5]. Furthermore, viability and suitability of the chaos image encryption algorithms have been presented in the literatures [5]. Nevertheless, chaotic encryption algorithms have issues of limited precision and weak security function that requires attention. This paper presents an image encryption algorithm that is based on one-dimensional piecewise linear chaotic maps (PLCM). The level of confusion and diffusion in the encryption system is increased by first shifting the elements of the image before applying one-dimensional PLCM.

The rest of the paper is organized as follows: Section 2 gives the system overview of encryption algorithms. Section 3 discusses chaotic schemes and its advantages over conventional image encryption schemes. The system methodology is presented in Section 4. Discussions on some experimental results obtained with the implementation of the proposed scheme are presented in Section 5. Section 6 concludes the paper.

2. System Overview

Cryptography is an art and study of techniques for secure communication over any untrusted medium in the presence of third parties. Through cryptography, information can be stored and transmitted in a specific form that can only be processed by whom it is intended [3], [6]. Therefore, it has been used to protect credit card information, e-mail, corporate data and classified information in an insecure network. Furthermore, cryptography involves encryption of the plaintext into ciphertext and decryption of the ciphertext [1], [3].

The two main types of cryptography that is usually employed are block and stream ciphers [7]. The block ciphers accept blocks of plain text and produce blocks of cipher text. Similarly, the stream ciphers operate on stream of data bit by bit and its main components are the key stream generator and the mixing function. Data encryption algorithms are classified into hashing, symmetric-key algorithm, and asymmetric-key algorithm [3]. Asymmetric and symmetric encryption techniques are based on the type of security keys used for encryption and decryption [7].

2.1. Symmetric Cryptography

The symmetric cipher is a type in which a single key is used for both encryption and decryption processes [3], [7]. The name symmetric is due to the fact that both the sender and the receiver use the same key in the process. Furthermore, it is also known as secret key cryptography (SKC) because both stations have to keep the key secret and properly protected. Fig. 1 illustrates the SKC system. In this type of encryption, the sender encrypts the message before it is transmitted to the receiver. In a situation where the decryption key is not known at the receiver, the sender sends the key and ciphertext independently to the receiver [8]. Mainly, the security level of the SKC method totally depends on how well the users keep the keys protected. If the key is known by an intruder, then, the encrypted data can be decrypted by unauthorized parties. This is the main weakness of SKC scheme. Some common SKC algorithms include; data encryption standard (DES), triple DES and Rijndael [4], [9].

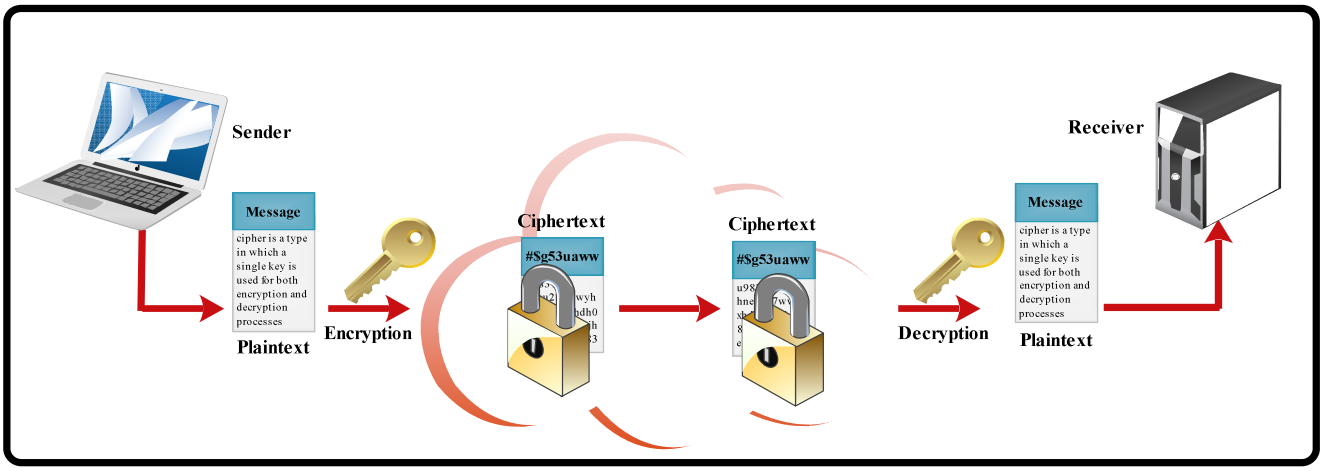

Fig. 1. Symmetric Key Encryption.

2.2. Asymmetric Cryptography

Another type of cryptography in which more than one key is required is asymmetric or public key cryptography (PKC). PKC is a category of cryptography in which two keys namely, a public key and a private key are used to perform encryption and decryption. The public key is known to the public while the private key is known only to the authorized user of ciphertext to decrypt the messages [3], [8], [9]. The implementation of two keys helps in preventing the major weakness in SKC so that a single key does not have to be securely managed among multiple users. However, PKC is comparatively slower [4] and requires more computational processing power. Algorithms that use PKC include Rivest, Shamir & Adleman (RSA), elliptic curve cryptography (ECC) and Diffie-Hellman [9]. Fig. 2 depicts the PKC system.

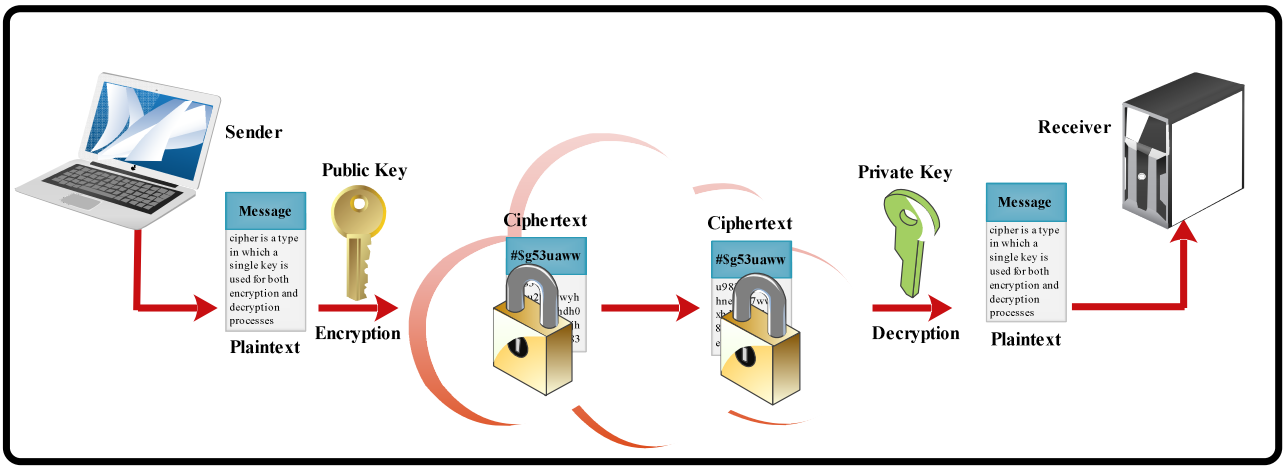

Fig. 2. Asymmetric Key Algorithm.

2.3. Hash Functions

A cryptographic hash function is an algorithm that receives certain arbitrary quantity of input and produces an output of fixed size. In contrast with the SKC and PKC algorithms, hash functions, also known as one-way encryption and message digests, use no key. However, a fixed length hash value is evaluated based on the plaintext which makes it impossible for both the contents and length of the plaintext to be recovered. The effectiveness of the algorithms is based on the fact that the probability of two different plaintext messages to yield the same hash value is low. Hash algorithms are usually employed to provide a digital fingerprint of a file's contents so as to ensure that the file has not been altered by an intruder, virus, or by other means [3]. Therefore, they help in preserving the file integrity [10]. Also, they are normally utilized by various operating systems for password encryptions. There are various hash functions such as hashed message authentication code (HMAC); message digest 2 (MD2); MD4; MD5 and secure hash algorithm (SHA) which have been employed in cryptography for message integrity. The basic operation of hash system is shown in Fig. 3. Furthermore, there are some technical issues such as low key space, weak security and slow performance speed in the conventional encryption algorithms that chaotic image key encryption algorithm addresses [5].

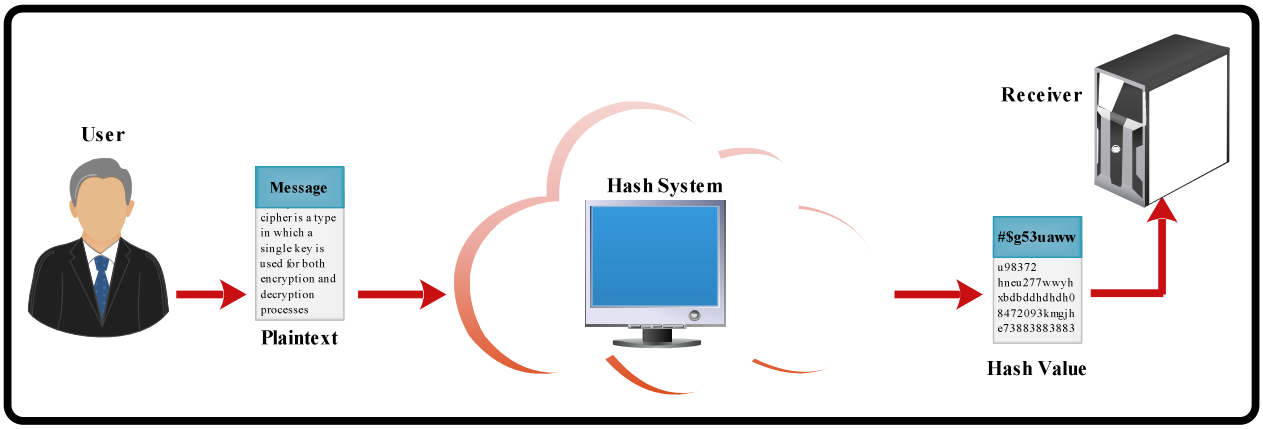

Fig. 3. Hash Function.

3. Chaotic Cryptographic Algorithms

It has been observed in the literature that, there is a close relationship between cryptography and chaotic system [11]. Also, chaotic systems have some characteristics that are similar to the conventional cryptosystems. Chaotic based image encryption schemes have wide feasible implementation in cryptosystems because of their significant advantages such as ease of implementation, high sensitivity to initial conditions and system parameters. Also, they have pseudo-random property and are non-periodic in nature which makes them to be noise-like [11], [12].

These properties enable chaotic system to be a viable alternative to the conventional cryptographic algorithms. Compare to the conventional algorithms which are primarily based on discrete mathematics, chaos-based cryptography is developed from complex dynamics of nonlinear systems or maps which are deterministic but simple [13]. Consequently, chaos-based cryptography provides a fast as well as secure means of information protection. This is essential for multimedia data transmission over the broadband internet communication [13]. Therefore, the combination of chaotic theory and cryptography is an essential part of information security systems [12].

There are a number of simple chaotic systems such as logistic map, piecewise linear chaotic map (PLCM) and piecewise nonlinear chaotic map that have been employed in developing chaotic cryptosystems. It has been observed in [14] that the PLCMs are usually employed in digital chaotic ciphers because they have perfect dynamic properties and are easy to implement in both hardware and software. The major advantages of one-dimensional chaotic system is in its high-level efficiency and simplicity, however, there are certain fundamental issues such as small key space, slow performance speed and weak security function that require consideration [14]. In this paper, the level of confusion and diffusion in the encryption scheme is increased in order to achieve a more secure cryptosystem. This is realized by first shifting the elements of the image before applying one-dimensional PLCM.

4. Methodology

The proposed scheme uses an iterative process to encrypt sequence of bits. The elements of the image are first circularly shifted to improve the level of system security. The system model is given by:

$$X = \begin{bmatrix} x_0 & \cdots & x_{n-1} \\ \vdots & \ddots & \vdots \\ x_1 & \cdots & x_0 \end{bmatrix} \quad (1)$$

Where each row is a cyclic shift of the row above it and the (i,j) entry of X, that is $X_{i,j}$ is given by

$$X_{i,j} = x(i,j)\ mod\ n \quad (2)$$

Furthermore, a one-dimensional PLCM which is defined on the interval $I = [\,0,1]$ is employed for the cryptosystem. This is due to the fact that it is ergodic, viable, simple and has unique invariant density function on the defined intervals. The map is given in [15] as:

$$F(x_n,p) = \begin{cases} {x_n}/{p}, & x_n \in [0,p] \\ (x_n - p)/\left(\frac{1}{2} - p\right) & x_n \in \left[p, \frac{1}{2}\right] \\ F(1 - x_n, p), & x_n \in \left[\frac{1}{2},\ 1\right] \end{cases} \quad (3)$$

The chaotic map is executed from the initial condition x_0 with the control parameter p and $0 < p < \frac{1}{2}$. The scheme employs simple key generation method that is based on random number generation and combination which is achieved by the application of the secret key $K = (x_0, p)$. Then, the maximal block size of plaintext is selected as an integer b_{max}. Also, the threshold T_i is chosen in order to generate a bit chain C_i. The position at which the plain-block P_i appears in C_i is estimated and the cipher-block corresponding to the plain-block is noted as b_i by keeping T_i and n_i constant to simplify the system operation. The factor n_i, is the number of iterations of the chaotic map from x_0. After the first iteration, the encryption procedure for the subsequent plain-block will not start from x_0 but from where the initial operation ended.

5. Experimental Results and Discussion

This section presents some experimental results based on the implementation of the proposed scheme in MATLAB® so as to study its feasibility and effectiveness. To achieve this, different analyses such as number of pixel change rate analysis, visual information analysis and statistical analysis are carried out on the images. The results obtained are presented in the following sub-section.

5.1. Number of Pixel Change Rate (NPCR) Analysis

The general requirement for the image encryption schemes is that, the encrypted image should have high distinction from

its original form. The number of pixel change rate (NPCR) is employed to quantify this requirement [13]. The $NPCR_{R,G.B}$ is adopted to measure the difference in the number of pixels of the colour components in two images and according to [13], its expected value is expressed as:

$$\epsilon\left[NPCR_{R,G.B}\right] = (1 - 2^{-L_{R,G,B}}) \times 100\% \quad (4)$$

where $L_{R,G,B}$ is the number of bits used to represent the colour component of red, green or blue. A 24-bit colour with 8-bit for each RGB colour component has $L_R = L_G = L_B = 8$. Therefore, the expected value of each component is;

$$\epsilon[NPCR_R] = \epsilon[NPCR_G] = \epsilon[NPCR_B] = 99.609375\% \quad (5)$$

5.2. Visual Analysis

Five different images are analysed for visual information. The plaintext images that are employed in the visual analysis and their properties are presented in Table 1. Fig. 4(a) -8(a) illustrate the original images that are employed in the visual analysis while 4(b) -8(b) show the corresponding encrypted images. A close comparison of the original and the encrypted images in the figures shows that there is no visual information that can be observed in the encrypted image. Therefore, the proposed scheme is able to achieve a high-level encryption because; the encrypted images do not reveal any information about the original images.

Table 1. Properties of different images analysed.

Image	Properties				
	Width (pixels)	Height (pixels)	Horizontal Resolution (dpi)	Vertical Resolution (dpi)	Bit Depth
Lena	512	512	73	73	24
Glass Apples	672	372	96	96	24
Bird	1024	683	96	96	24
Frog	620	438	96	96	24
Cubes	1300	975	72	72	24

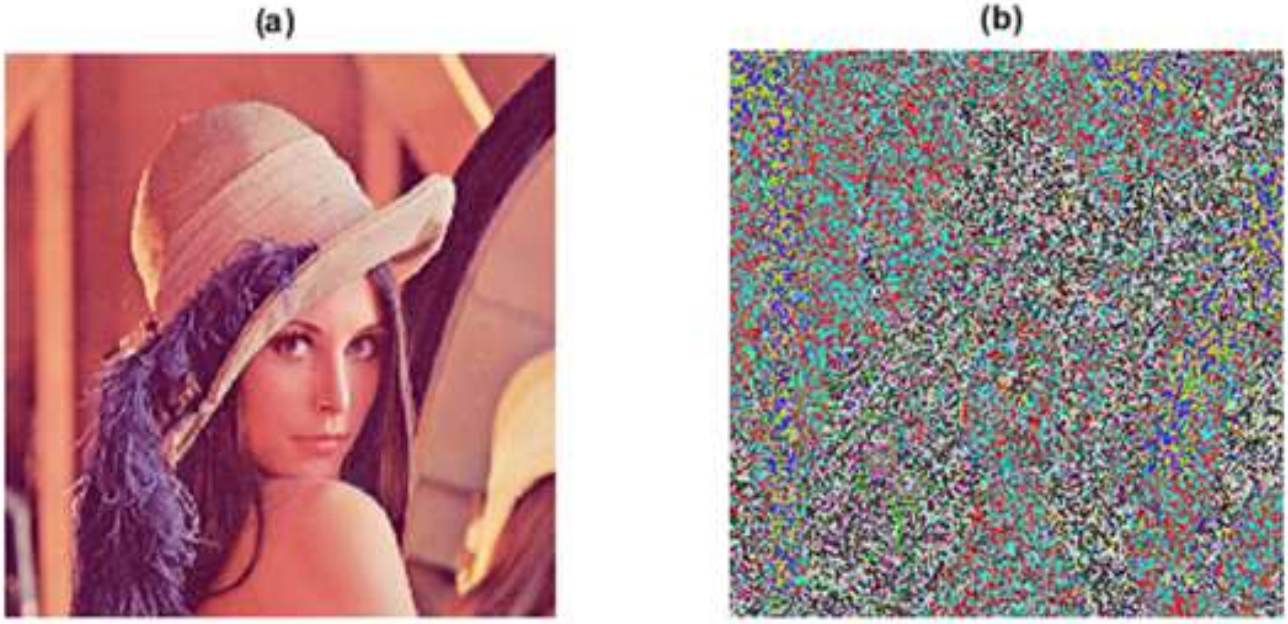

Fig. 4. (a) Lena's Original Image, (b) Lena's Encrypted Image.

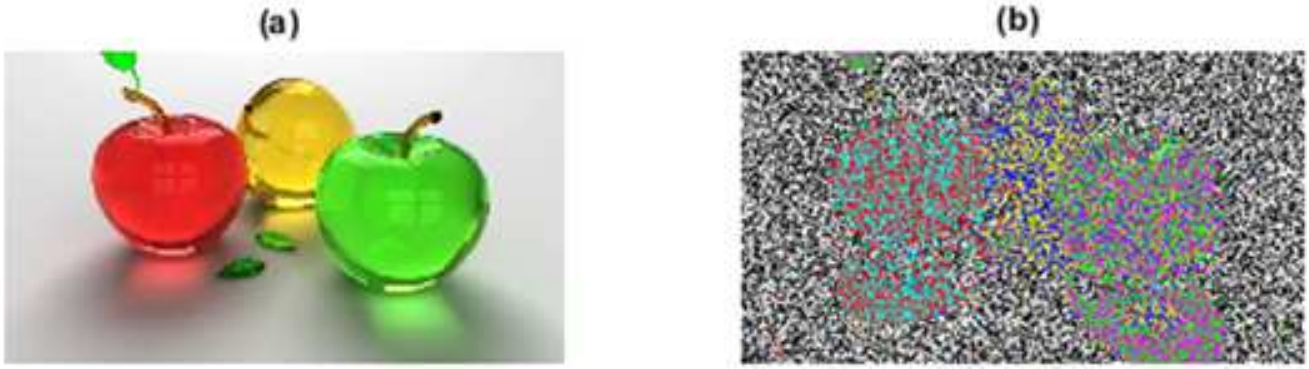

Fig. 5. (a) Glass Apples' Original Image, (b) Glass Apples' Encrypted Image.

Fig. 6. (a) Bird's Original Image, (b) Bird's Encrypted Image.

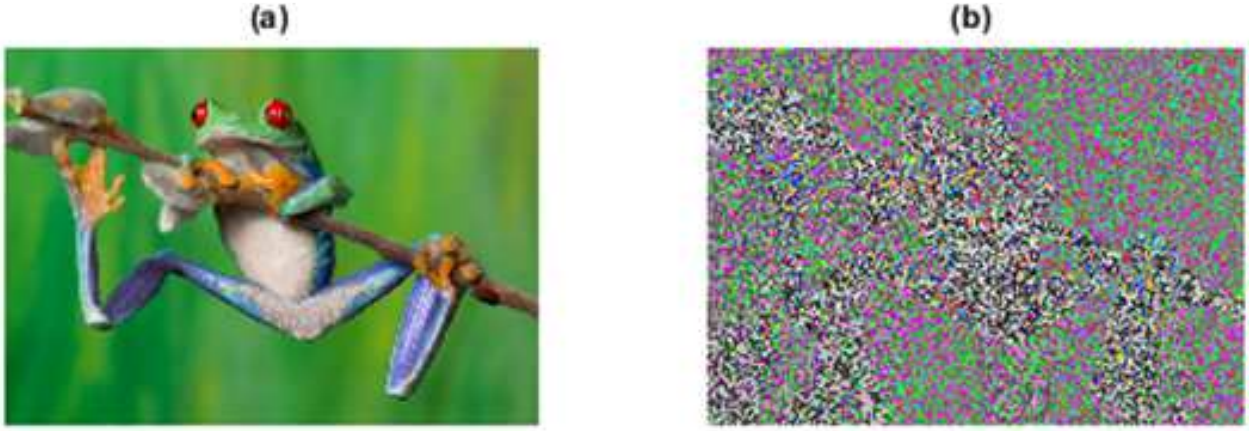

Fig. 7. (a) Frog's Original Image, (b) Frog's Encrypted Image.

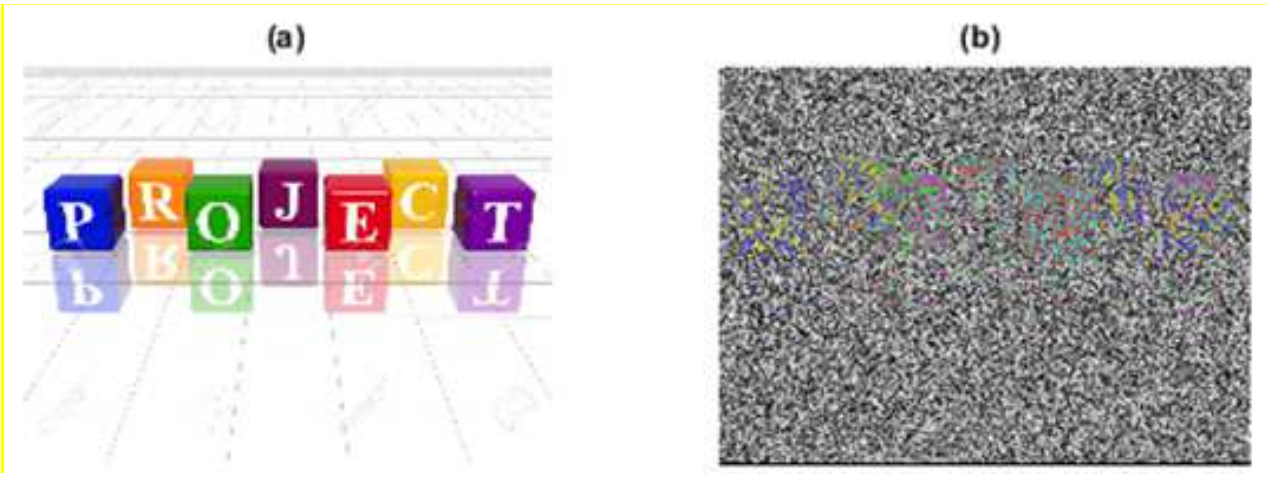

Fig. 8. (a) Cubes' Original Image, (b) Cubes' Encrypted Image.

5.3. Statistical Analysis

It has been noted in [13] that, to resist the statistical attacks, the encrypted images should possess certain random properties that should have no statistical similarity to the original image. The histograms of the five images presented and their corresponding encrypted images have been analysed, however, because of page limitation, only the results for the Lena's image are presented in this sub-section and the subsequent ones. The implementation of the proposed scheme changes the original image pixel values with uneven distribution into uniform distribution in the range [0,255] for the encrypted image. Therefore, the grey-scale histogram of the original image has uneven spikes while that of the encrypted images is flat, thereby, concealing the pixel frequency distribution of the plaintext-image. This makes the grey-scale histogram of the encrypted image to be different from that of the original image. Figure 9 illustrates

the histograms of the original and encrypted images. Furthermore, the colour histograms should be uniformly distributed in all three colour components (Red, Green and Blue) for random appearance. Fig. 10 shows the histograms of RGB colours for the original image with their corresponding band, also, Fig. 11 illustrates that of the encrypted image. Therefore, the results show that the cipher image has no statistical similarity with the plain image, consequently, it is not susceptible to statistical attacks.

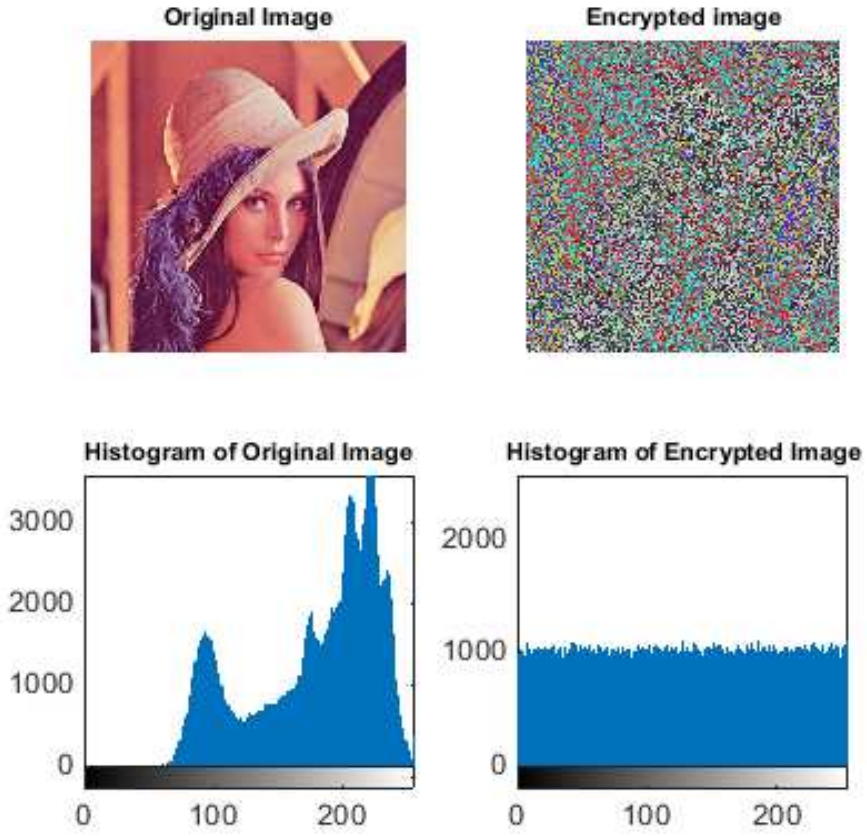

Fig. 9. Histogram of the Original and Encrypted Image.

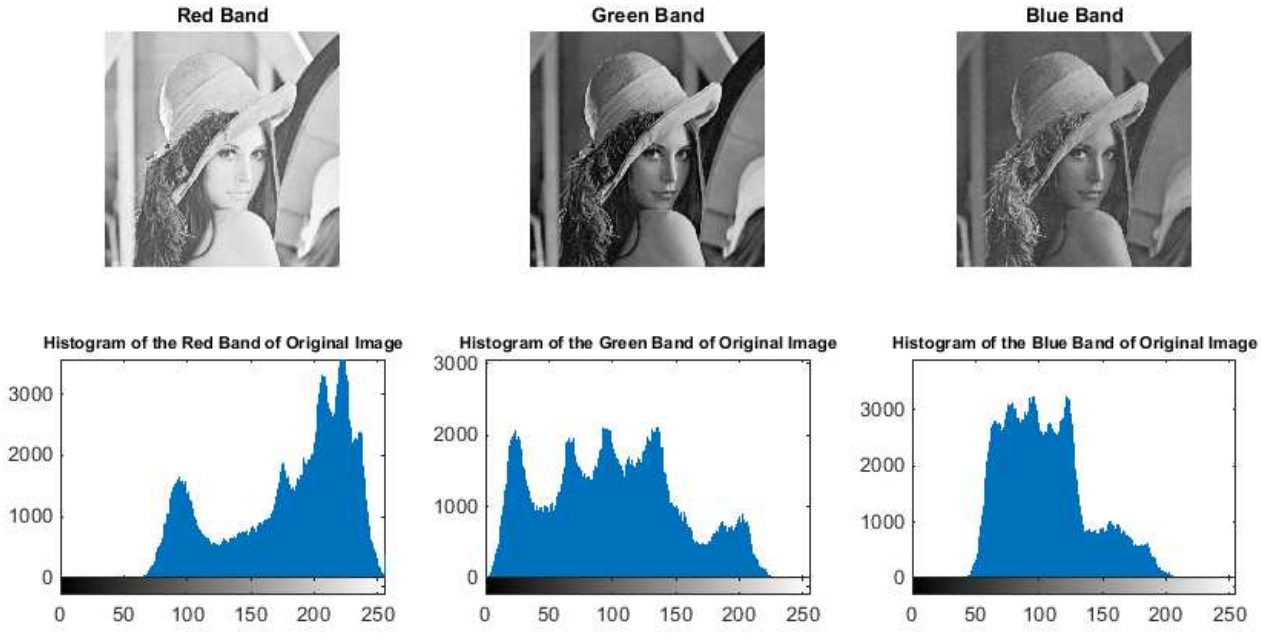

Fig. 10. Histograms of the Colour Components of Original Image.

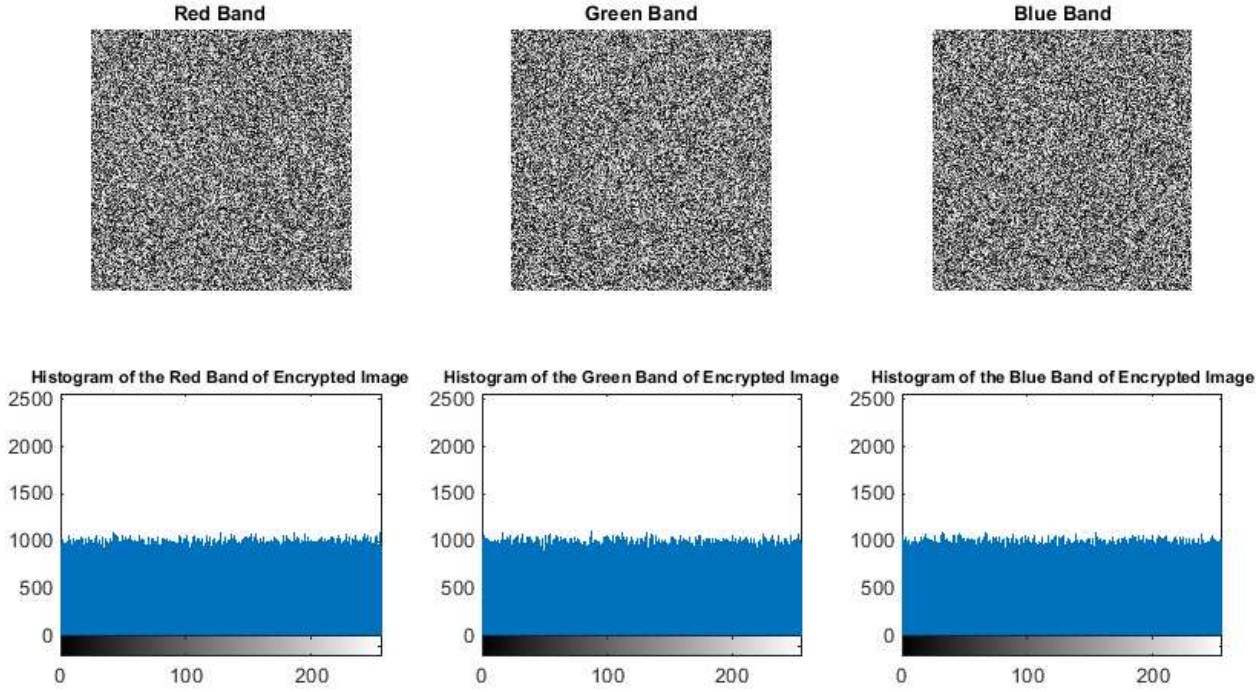

Fig. 11. Histograms of the Colour Components of Encrypted Image.

5.4. Image Encryption and Decryption

The decrypted image after reverse operation at the receiver is shown in Fig. 12. It is observed that the decrypted image is the same as the plaintext-image and there is no notable error in the pixel values between the plaintext image and the decrypted image. To further verify this, pixel subtraction operation is employed. The pixel values of the original image are subtracted from the corresponding pixel values of the decrypted image. Fig. 13 shows the result of the analysis and according to the result, there is no quality loss because, the differences are zeros. Furthermore, mean and standard deviation of the images are evaluated as shown in Fig. 14. A mean of 1024 and standard deviation of 674.4882 are obtained for both encrypted and decrypted images.

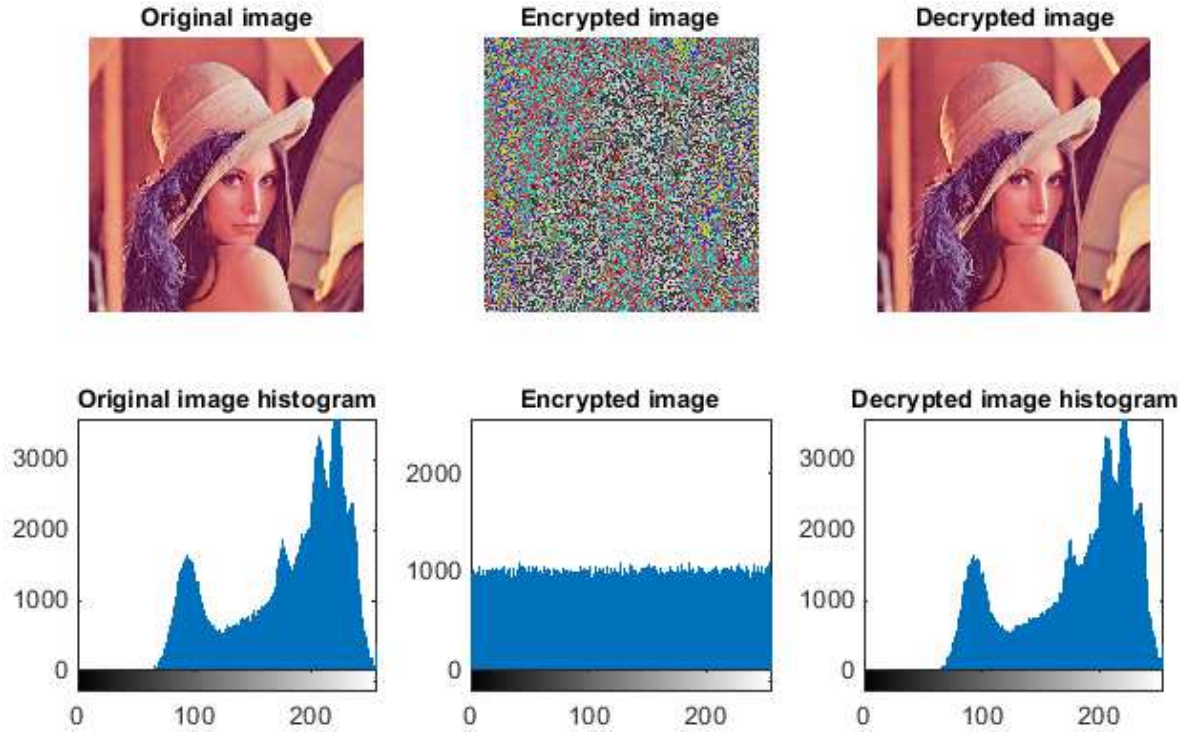

Fig. 12. Image Encryption and Decryption.

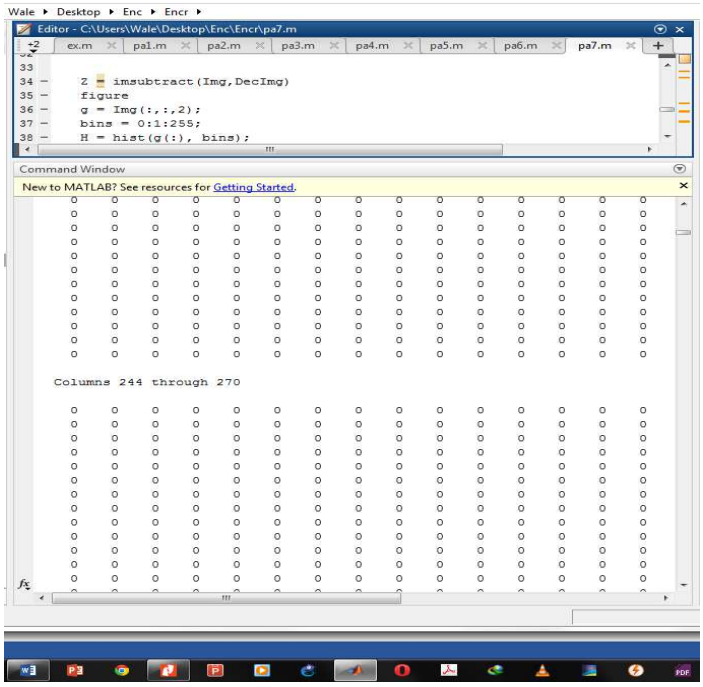

Fig. 13. Pixel Subtraction Operation

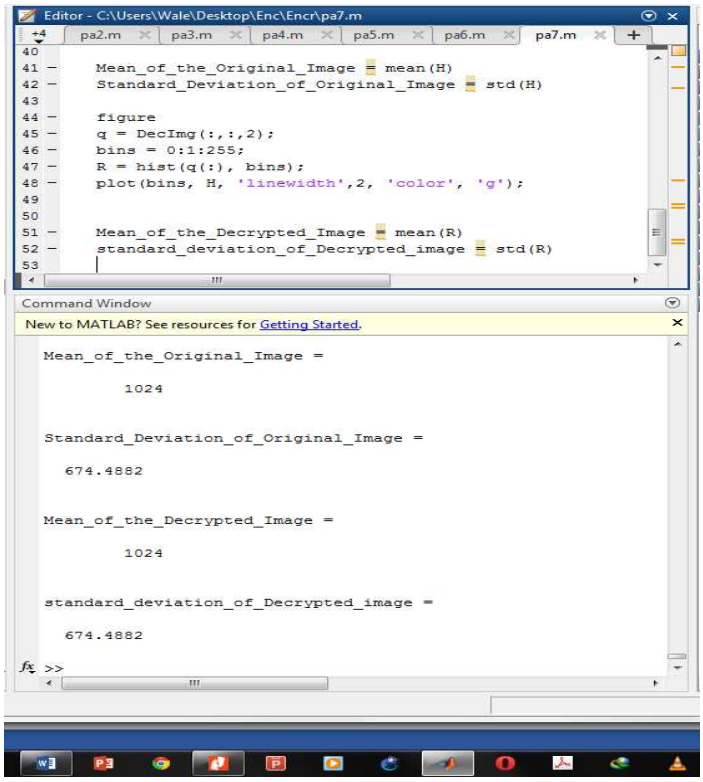

Fig. 14. Mean and Standard Deviation of the Images.

6. Conclusion

This paper presents image encryption algorithm that exploits the existing algorithms in order to have features such as improved precision, confidentiality and security. The level of confusion and diffusion in the encryption scheme is increased by first shifting the elements of the digital images before applying one-dimensional piecewise linear chaotic maps. The effectiveness of the algorithm is evaluated by comparing the plaintext and the decrypted text using MATLAB®. The simulation results show that, the proposed scheme is viable and offers a reasonable degree of security. Also, there is no loss in the quality of digital images during the process.

References

[1] M.P. Leong, S.Z.M. Naziri and S.Y.Perng, "Image Encryption Design Using FPGA," 2013 International Conference on Electrical, Electronics and System Engineering, pp. 27-32.

[2] M. Al-qdah and Lin Yi Hui, "Simple Encryption/Decryption Application," International Journal of Computer Science and Security, vol. 1, issue 1, pp. 33-40, 2007.

[3] S. D. Sadananda, and A. Karkala, "Image Encryption and Decryption Using Image Gradient Technique," International Journal of Emerging Technology and Advanced Engineering vol. 3, issue 1, pp. 511-515, 2013.

[4] V. Shokeen and N. Yadav, "Encryption and Decryption Technique for Message Communication," International Journal of Electronics and Comm. Technology, vol. 2, Issue 2, pp. 80-83. 2011.

[5] Y. Zhang, W. Liu, S. Cao, Z. Zhai, X. Nie and W. Dai, "Digital Image Encryption Algorithm Based On Chaos And Improved DES," 2009 IEEE International Conf. on Systems, Man and Cybernetics, pp.474-479.

[6] R. Venkateswaran and V. Sundaram, "Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography," International Journal of Computer Applications, vol. 3, no.7, pp. 28-31. 2010,

[7] M. Bin Younas and J. Ahmad, "Comparative Analysis of Chaotic and Non-Chaotic Image Encryption Schemes," 2014 International Conference on Emerging Technologies, pp. 81-86.

[8] A. P. Deshmukh and R. Qureshi, "Transparent Data Encryption- Solution for Security of Database Contents," International Journal of Advanced Computer Science and Applications, vol. 2, no. 3, pp. 25-28, 2011.

[9] R. S.Jamgekar and G. S. Joshi, "File Encryption and Decryption using Secure RSA," International Journal of Emerging Science and Engineering, vol. 1, Issue 4, pp. 11-14, 2013.

[10] A. S. Rajput, N. Mishra and S. Sharma, "Towards the Growth of Image Encryption and Authentication Schemes," 2013 Intern. Conf. on Advances in Computing, Communications and Informatics, pp. 454-459.

[11] N. Kumar, D. Wadhwa, D. Tomer and S. Vijayalakshmi, "Review on Different Chaotic Based Image Encryption Techniques," Intern. Journal of Info. and Computation Tech. vol. 4, no. 2, pp. 197-206, 2014.

[12] R. B. Prajapati, "Tutorial Review on Image Hiding," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, issue 11, pp. 8362-8365, 2014.

[13] H. S. Kwok and W. K. S. Tang, "A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation," Elsevier, Chaos, Solitons and Fractals 32, pp.1518–1529, 2007.

[14] [S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavand, "A Fast Chaotic Encryption Scheme Based on Piecewise Nonlinear Chaotic Maps," Elsevier, Physics Letters A, pp. 391–396, 2007.

[15] X. Wu, Y. Xiong, "Adaptive Watermarking Algorithm Based on Chaotic Map," 2010 International Conference on Computer Application and System Modeling, vol. 6, pp. v6-477-v6-480.

Biography

Alimi Isiaka Ajewale earns B.Tech. (Hons) and M.Eng. in Electrical and Electronics Engineering (Communication) from Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2001, and the Federal University of Technology, Akure, Nigeria in 2010 respectively. He is a Lecturer in the Department of Electrical and Electronics Engineering, Federal University of Technology, Akure, Nigeria. He has published 3 refereed international journals. He has extensive experience in radio transmission, as well as in Computer Networking. His areas of research are in Computer Networking and Security, Advanced Digital Signal Processing and Wireless communications. He is a COREN registered engineer.

Oluyomi Aboderin, a COREN registered engineer, received B.Tech. (Hons) in Electronic and Electrical Engineering and M.Sc. in Personal Mobile and Satellite Communication (PMSC) degrees from Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2001, and University of Bradford, Bradford, United Kingdom in 2010 respectively. He is a Research Engineer with National Space Research and Development Agency (NASRDA) Abuja, Nigeria. He is currently enrolled at the Faculty of Engineering University of Porto Porto, Portugal for his Doctoral degree program in Telecommunication. His research interest is in Satellite Channel Estimation and Modeling, Antenna design and Frequency Management for Next Generation Network (NGN).