INFORMATICA, 2017, Vol. 28, No. 4, 629–649

DOI: http://dx.doi.org/10.15388/Informatica.2017.149

An Improved Image Encryption Scheme Based on a Non-Linear Chaotic Algorithm and Substitution Boxes

Jan Sher KHAN[1]*, Muazzam Ali KHAN[2], Jawad AHMAD[3], Seong Oun HWANG[4], Waqas AHMED[5]

[1]*Department of Electrical and Electronics, University of Gaziantep, 27310 Gaziantep, Turkey*
[2]*Department of Computing, School of Electrical Engineering and Computer Science National University of Sciences and Technology, Islamabad, Pakistan*
[3]*Glasgow Caledonian University, School of Engineering and Built Environment Glasgow, United Kingdom*
[4]*Department of Computer and Information Communication Engineering, Hongik University Sejong, South Korea*
[5]*Department of Electrical Engineering, HITEC University, Taxila, Pakistan*
e-mail: jskm893@gmail.com, khattakmuazzam@gmail.com, jawad.saj@gmail.com, sohwang@hongik.ac.kr, imwaqasahmed@live.com

Received: January 2017; accepted: July 2017

Abstract. World has become a global village after introduction of social media and social networks. However, it extensively increased the demand for network resources, particularly multimedia traffic like images, videos and audio. The medium for this extensive traffic is always public networks such as internet or cellular networks. But the open nature of such network like internet always creates security threats for data during transmission. Due to many intrinsic features and higher correlation in multimedia traffic, existing encryption algorithms are not very convincing to perform well under critical scenarios. Therefore, many people in the research community are still working to propose new encryption schemes which can address these issues and handle multimedia traffic effectively on public networks. In this paper, we explore the weaknesses of existing encryption schemes, which compromise in many scenarios due to high correlation of multimedia traffic. To tackle this issue we proposed certain enhancements in an existing scheme. Our enhanced modification includes addition of bitwise XORed operation using non-linear chaotic algorithm. Performance of enhanced scheme is tested against state of the art security parameters. Efficiency of the proposed scheme is also validated via entropy, correlation, peak signal to noise ratio, unified average change intensity and number of pixels change rate tests.

Key words: non-linear chaotic algorithm, substitution box, chaos, uniform average change intensity, number of pixel change.

*Corresponding author.

1. Introduction

Over the past few decades, advancement in digital technologies has made people's lives more comfortable and faster. With all their charms, digital technologies, however, possess certain limitations to their robust utilization. Data transmission and reception over the internet is not secure in most cases. The problem can be resolved by applying encryption procedures to ensure that the data is only received by the intended user and even if the data is intercepted by an unauthorized or unintended user, the contents of the data should not make sense to him/her. Encryption is a process to disguise the information in such a way that only the intended user with a certain private key or code could be able to retrieve the actual data from the encrypted information (Acharya *et al.*, 2008; Jakimoski and Subbalakshmi, 2008; Schneier, 1996; William, 2006), which is called decryption, the reverse process of encryption. Symmetric key algorithms use the same keys for encryption and decryption, whereas different keys are used for encryption and decryption in public key algorithms. The traditional symmetric algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES) and International Data Encryption Standard (IDES) encrypt text data in an efficient way (Bruce, 1996; Stallings, 2006; Leong *et al.*, 2000). These traditional algorithms, however, fail to provide efficient encryption of image data due to its associated high redundancy, strong correlation and bulk capacity (Khan *et al.*, 2017a; Ahmad *et al.*, 2017). In 1989, Mathews presented the concept of chaotic encryption (Matthews, 1984). Following Mathew's novel idea, many researchers have turned their attention towards chaos-based image encryption and S-box construction techniques (Ahmad and Hwang, 2016; Anees *et al.*, 2014a; Khan *et al.*, 2015a; Ahmad and Hwang, 2015; Ahmad *et al.*, 2015; Younas and Ahmad, 2014; Anees *et al.*, 2014b; Dawei *et al.*, 2004; Ahmad *et al.*, 2016; Huang and Guan, 2005; Li and Zheng, 2002; Ahmad and Ahmed, 2010; Rehman *et al.*, 2016; Khan *et al.*, 2015b; Habib *et al.*, 2017). These chaos-based image encryption algorithms have lots of merits, such as the large key space, ergodicity and sensitivity to the secret keys. Chung and Chang (1998) designed a new approach for encrypting binary images. They utilized different scan patterns at the same level in the scan tree structure and then applied a $2D$ run-encoding technique ($2DRE$). However, Chang and Yu (2002) present cryptanalysis of the above scheme. Belkhouche and Qidwai proposed binary image encoding based on $1D$ chaotic map (Belkhouche and Qidwai, 2003). In 2014, Amir *et al.* utilized the chaotic behaviour of Logistic map and used more than one substitution box. Logistic chaotic map generates random values that randomly select S-box which is employed in the substitution process. In this paper, we first examine Amir *et al.*'s algorithm (Anees *et al.*, 2014a) and then improve it on the basis of the security parameters suggested in Ahmad *et al.* (2015), Khan *et al.* (2017b). To improve the security characteristics of the Amir's scheme for binary images, bitwise XOR operation is applied on image pixels. In order to verify the security of the proposed algorithm, various statistical analyses and histogram tests are applied on encrypted images.

The rest of the paper is organized as follows. Section 2 explains fundamental knowledge and defines problem statement. Section 3 presents the proposed scheme. Section 4 presents simulation results and comparative analysis. Section 5 concludes this paper.

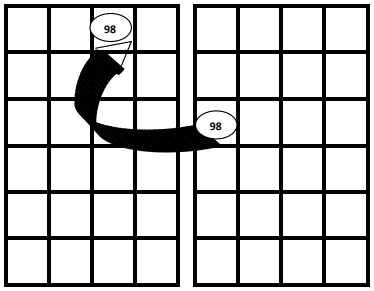


Fig. 1. Substitution process.

2. Fundamental Knowledge

In order to help readers to fully understand our modification to the Amir's algorithm, we explain S-box, Non Chaotic Algorithm (NCA) and Logistic chaotic map. The Amir's scheme works well for high number of gray scale values, but it totally fails in the case of small number of gray scale values. In this paper, we add diffusion to the Amir's algorithm via XORed operation to validate the C. Shannon theory of SP-Network (Kam and Davida, 1979).

2.1. *Substitution Box*

In the paper of Anees *et al.* (2014a), a novel chaotic scheme was proposed. Substitution is done using the technique of multiple substitution boxes (S-boxes). This paper addresses drawbacks of single S-box for substitutions in encryption algorithm and proposes a novel chaotic substitution scheme. For symmetric key algorithms of cryptography, S-box is a core component. S-box is basically a lookup table which is constructed by a boolean function taking n bits as input and producing m bits as output (Yildiz, 2004). The substitution refers to the replacement of plaintext image data with another data set. The resulting substituted data is called the ciphertext image. The plaintext image can be retrieved when the substitution process is reversed. Figure 1 shows the substitution of a single unit of data. Different algebraic structures exist in literature to construct S-boxes (Nyberg, 1992; Weister and Tavares, 1986; Kurosawa *et al.*, 1997; Johansson and Pasalic, 2003). Several S-boxes are used in the field of cryptography and their performance varies by using algebraic and statistical analysis. S-box exhibits the property of non-linearity and several researches have been undertaken to increase this phenomenon (Hussain *et al.*, 2012, 2013a, 2013b). Despite its high non-linearity, S-boxes tend to exhibit low substitution results in highly correlated data set. To resolve this issue, chaotic behaviours of different set of equations are utilized to induce diffusion in the encryption algorithm. This chaotic nature of different functions are known as chaotic maps. As the name implies, the theory refers to the states of confusion, randomness, lack of order, lack of predictability and so on.

2.2. *Logistic Map*

The nature of chaotic systems is such that any change in its initial conditions results in an unpredictable change in its outcome. These systems are therefore highly sensitive to the initial conditions. These systems bear the property that any change in the input, however it is infinitesimal, would result in extremely diverging outputs. This lowers the predictability of the outcomes to sufficiently impossible level. Diverse chaotic maps are practically deployed in various systems. Some of them are Arnold Cat map, Chen Lee system, Chirikov–Taylor map, Gauss map, Henon map, Horseshoe map, and Logistic map. The most popular is Logistic map. Mathematically, Logistic map can be written as:

$$f : IR \to IR$$
$$X_{n+1} = f(X_n) = r.X_n(1 - X_n). \tag{1}$$

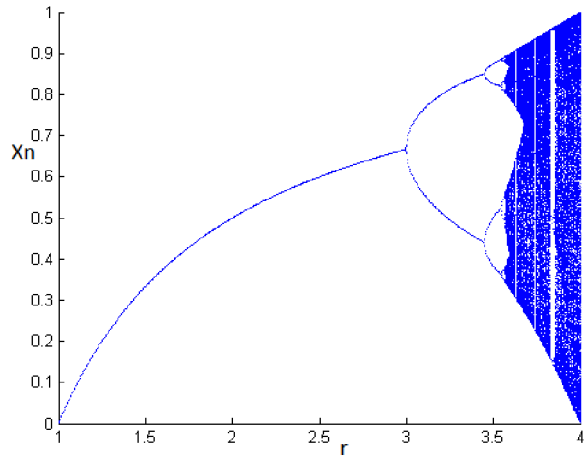
In Eq. (1), $r \in (0, 4)$ is the control parameter and x_0 is the initial condition in range $(0, 1)$. In Li *et al.* (2017), Gao *et al.* examined r and divided the interval r into three slices. For $r \in (0, 3)$, one will get the same x after a number of iterations with no chaotic behaviour. The periodicity still appears for $r \in (3, 3.6)$, but phase space has different values and when $r \in (3.6, 4)$, the periodicity totally disappears and random phenomenon starts. Figure 2 shows the bifurcation and discrete domain plot of Logistic chaotic map. The Amir's scheme utilizes chaotic behaviour of the Logistic map and uses more than one substitution box to substitute data. All S-boxes have values at altered positions and thus increase the probability of randomness in the algorithms. As the chaotic map generates random values, random selections of S-boxes are carried out.

2.3. *Non-Linear Chaotic Map*

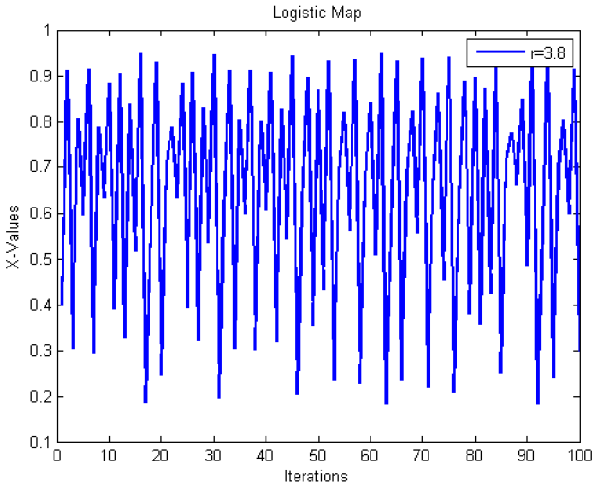
In order to improve the security of and overcome some limitations in chaotic maps, the authors in Gao *et al.* (2006) designed a Non-Linear Chaotic Map (NCA). Due to the limitation of linear functions, the authors used power function $(1 - x)^{\beta}$ and tangent function. Mathematically, NCA can be written as:

$$x_{n+1} = \left(1 - \beta^{-4}\right) \cot\left(\frac{\alpha}{1+\beta}\right)\left(1 + \frac{1}{\beta}\right)^{\beta} \tan(\alpha x_n)(1 - x_n)^{\beta}, \tag{2}$$

where the seed parameters are defined as:



(a)



(b)

Fig. 2. (a) Bifurcation diagram of Logistic map. (b) Logistic map values for $x_0 = 0.4$ and $r = 3.8$.

$$
\begin{cases}
x_n \in (0, 1), \\
\alpha \in (0, 1.4], \\
\beta \in [5, 43], \\
\text{or} \\
x_n \in (0, 1), \\
\alpha \in (1.4, 1.5], \\
\beta \in [9, 38], \\
\text{or} \\
x_n \in (0, 1), \\
\alpha \in (1.5, 1.57], \\
\beta \in [3, 15].
\end{cases}
$$

NCA map has more large key space than other chaotic maps. Detailed map can be found in Gao *et al.* (2006).

Problem Statement

As binary images are very easy to process, they are actively used in many applications such as identification of objects on a conveyor belt or identification of object orientations. Due to the widespread use of binary images, an image encryption scheme should be strong enough to conceal pixelwise information. The plaintext Cameraman and Pepper binary images shown in Figs. 5(a), and 9(a) are encrypted using the Amir's scheme (Anees *et al.*, 2014a). As seen from Figs. 5(b) and 9(b), an encrypted binary image is still recognizable. The histogram results obtained from the Amir's scheme shown in Figs. 5(d), and 9(d) are not flat. To support the observation, numerical results for entropy and correlation coefficient can be seen from Tables 1, 2, 3 and 4. The Amir's algorithm has sufficient efficiency for the gray scale images. It, however, fails in the case of binary images. As binary data consists of just 0's and 1's, the substitution is done using five values only. As it does not conceal the original pixels in a binary image, the Amir's scheme is vulnerable in high correlation scenarios.

3. The Proposed Scheme

A new algorithm is proposed in order to improve the results of the Amir's scheme (Anees *et al.*, 2014a). Our main focus is on high correlated images, i.e. binary images. We added NCA based XORed operation to the existing Amir's algorithm. Detailed steps of the modified Amir's scheme are given as:

First, convert the pixel value of plaintext image I to binary value of 8 bits and store that binary value in I'.

$$I' = dec2bin(I(i, j), 8), \tag{3}$$

where i and j are the positions of pixel value plaintext image I and 8 represents that the binary number are in range of 8 bits.

Split 8 bits pixels value into 4 bits frames, i.e. MSBs and LSBs.

$$MSBs = I'(1, 4), \tag{4}$$

$$LSBs = I'(5, 8). \tag{5}$$

The binary value of MSBs and LSBs are again converted to decimal value, where the decimal value of MSBs and LSBs represent the row and column positions, respectively.

The Amir's scheme utilizes chaotic behaviour of the Logistic map and uses more than one substitution box. Logistic chaotic map generates random values that randomly select S-box which is employed in the substitution process. The proposed modification is as follows:

Random values obtained from Eq. (2) are multiplied with a higher number, i.e. $(10)^{14}$ and stored in a variable Y. Pixels values obtained via the Amir's scheme are XORed with Y to get Z. In order to restrict values between 0–255, modulo 256 operation is applied and obtained results are stored as a final ciphertext image C. The stepwise flowchart for the proposed algorithm is shown in Fig. 3. The decryption process is reverse of the aforementioned scheme. All the steps shown in Fig. 3 can be applied in reverse order to obtain the plaintext Cameraman image I from encrypted Cameraman image C.

4. Results and Comparative Analysis

Comparison needs to be done between the results of the Amir's scheme (Anees *et al.*, 2014a), Li's scheme (Li *et al.*, 2017) and the proposed scheme. The Li's scheme is based on single dimension Skew tent chaotic map which cannot resist many differential attacks. In our proposed scheme, the Logistic chaotic map is utilized for the selection of S-box only. This would allow supporting the effectiveness of the proposed algorithm. As shown in Figs. 6, 7, 10 and 11, results are improved visually. To strengthen this argument, comparative results of the two algorithms are shown in Tables 1, 2, 3 and 4. As the correlation coefficients improve, similarity between the plaintext image and the ciphertext image decreases. Mathematically, correlation coefficients can be calculated as

$$C.\,C = \frac{Cov(x, y)}{\sqrt{VAR(x) \times VAR(y)}}, \tag{6}$$

where

$$VAR(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2,$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big).$$

In the above equation, E stands for expected value operator. From Fig. 12, one can see that the original plaintext Cameraman image has correlation in horizontal, vertical and diagonal directions, respectively. When the Cameraman image is encrypted via the proposed scheme, a disorder distribution without regular pattern appears shown in Fig. 13. Special attention must be given to the information entropy analysis, where the value of the security parameter approaches to 8 in the proposed algorithm. Entropy value close to 8 is considered as ideal which was proposed in the Shannon theory of information entropy. Entropy is the measure of unpredictability of the information content. The closer the value of entropy to ideal value, i.e. 8 bits, the more effective is the algorithm. As outlined in the problem statement, our objective is to improve the encryption results for a binary

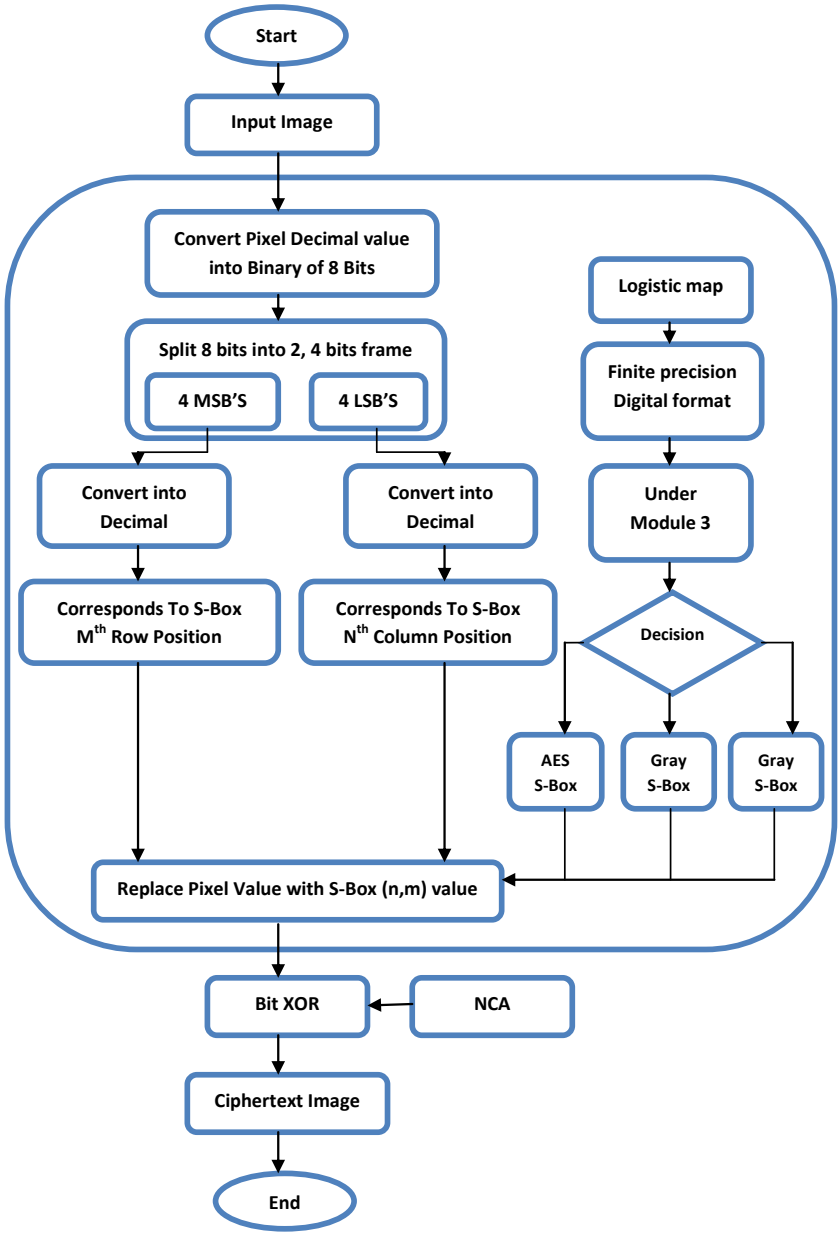
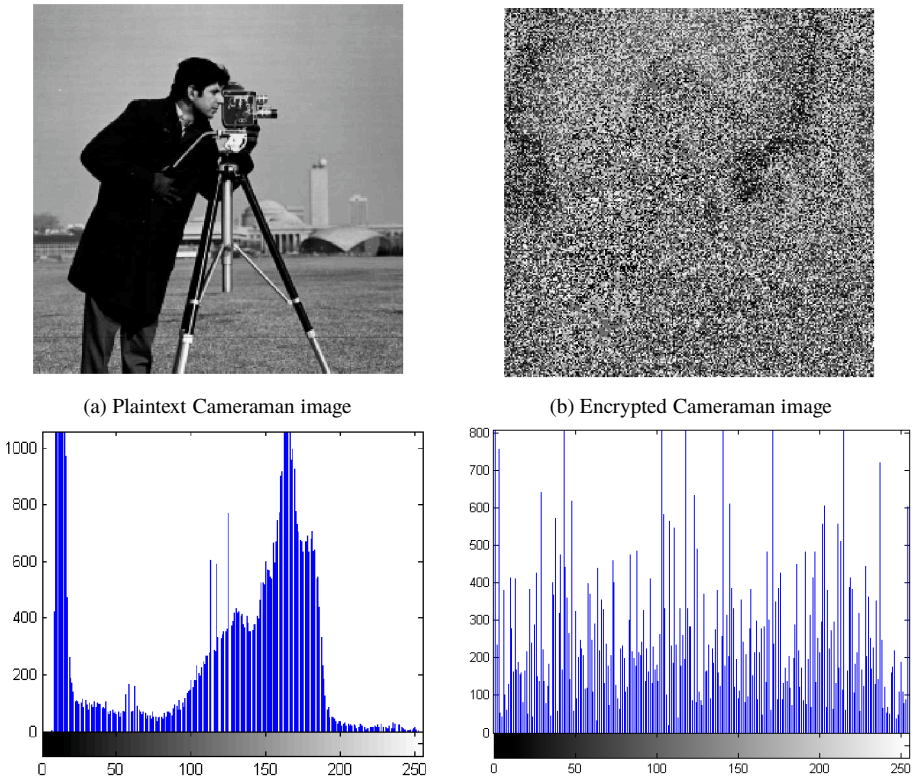


Fig. 3. Flowchart for proposed encryption algorithm.

image. The entropy value has significantly increased from 2 to around 7.9. Mathematically, entropy can be written as:

$$H = -\sum p(x_i) \log_2 p(x_i), \tag{7}$$



(a) Plaintext Cameraman image

(b) Encrypted Cameraman image

(c) Histogram of plaintext Cameraman

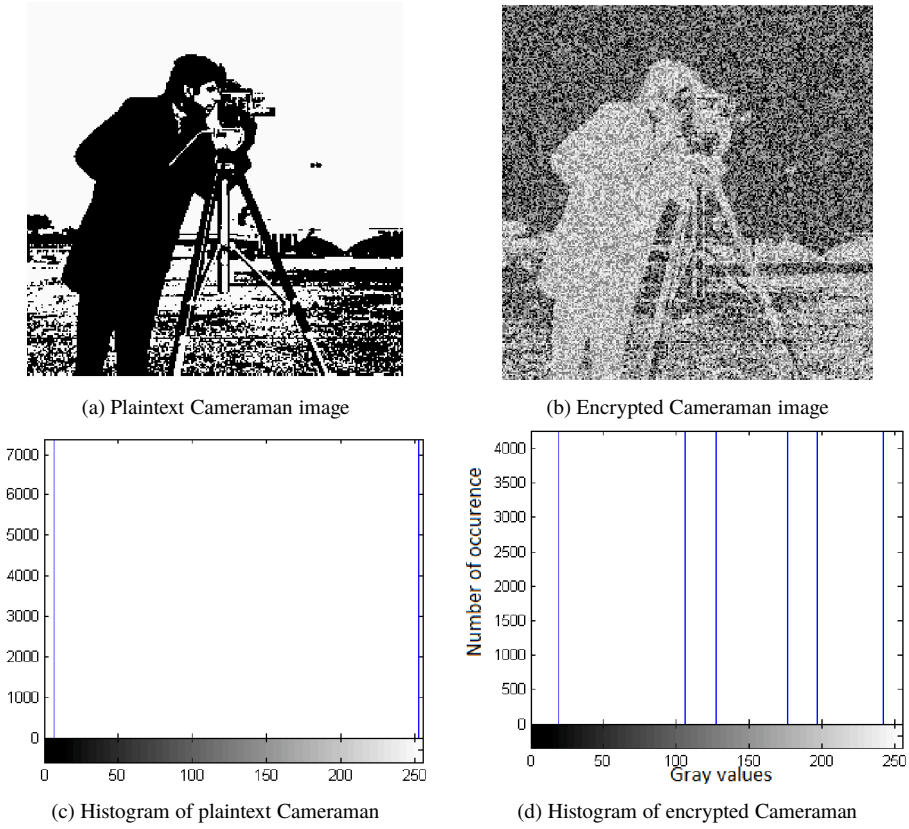
(d) Histogram of encrypted Cameraman

Fig. 4. Encryption and histogram of gray scale Cameraman image via Amir's algorithm.

where $p(x_i)$ is the probability of random variable x at ith index. Key sensitivity describes the percentage change resulting from a single bit change in the key on the decryption process or the difference in the two cipher images. The results show that the value of the parameter increases significantly, making it difficult to retrieve the contents of the plain image. Likewise, values for Peak Signal to Noise Ratio (PSNR) have also improved. Mathematically, PSNR can be defined as:

$$PSNR = 20 \times \log_{10}\left(\frac{I_{MAX}}{\sqrt{MSE}}\right), \tag{8}$$

where I_{MAX} is the maximum pixel value of the plaintext image. Histogram analysis shows that the pixels values of the encrypted image (resulting from the proposed algorithm) are distributed evenly over the entire range, which can be seen from Figs. 6(d), 7(d), 10(d) and 11(d). The probability of occurrence of each pixel value is therefore the same. This normalizes the image in such a way that the distribution of the information content is evenly distributed and it does not concentrate over certain values.



(a) Plaintext Cameraman image

(b) Encrypted Cameraman image

(c) Histogram of plaintext Cameraman

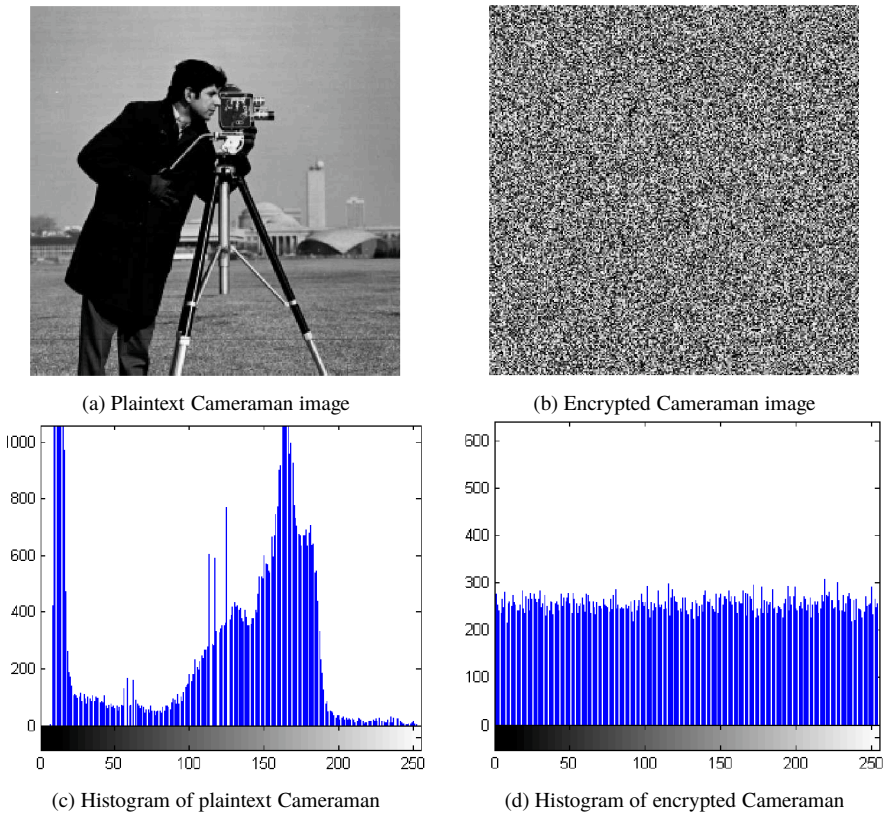
(d) Histogram of encrypted Cameraman

Fig. 5. Encryption and histogram of binary Cameraman image via Amir's algorithm.

Other parameters like Mean Square Error (MSE), Number of Pixel Change (NPCR) and Uniform Average Change Intensity (UACI) are also calculated. MSE basically measures the cumulative square error between two digital images. MSE can be used to find the avalanche effect. NPCR and UACI are used to check the effect of single pixel change on the whole image. Mostly, for any encryption scheme, a small change in the plaintext image pixel value should cause significant change in the ciphertext image. Mathematically, MSE, NPCR and UACI are written as:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left(C(i,j) - C^*(i,j)\right)^2, \tag{9}$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{10}$$



(a) Plaintext Cameraman image (b) Encrypted Cameraman image

(c) Histogram of plaintext Cameraman (d) Histogram of encrypted Cameraman

Fig. 6. Encryption and histogram of gray scale Cameraman image via proposed scheme.

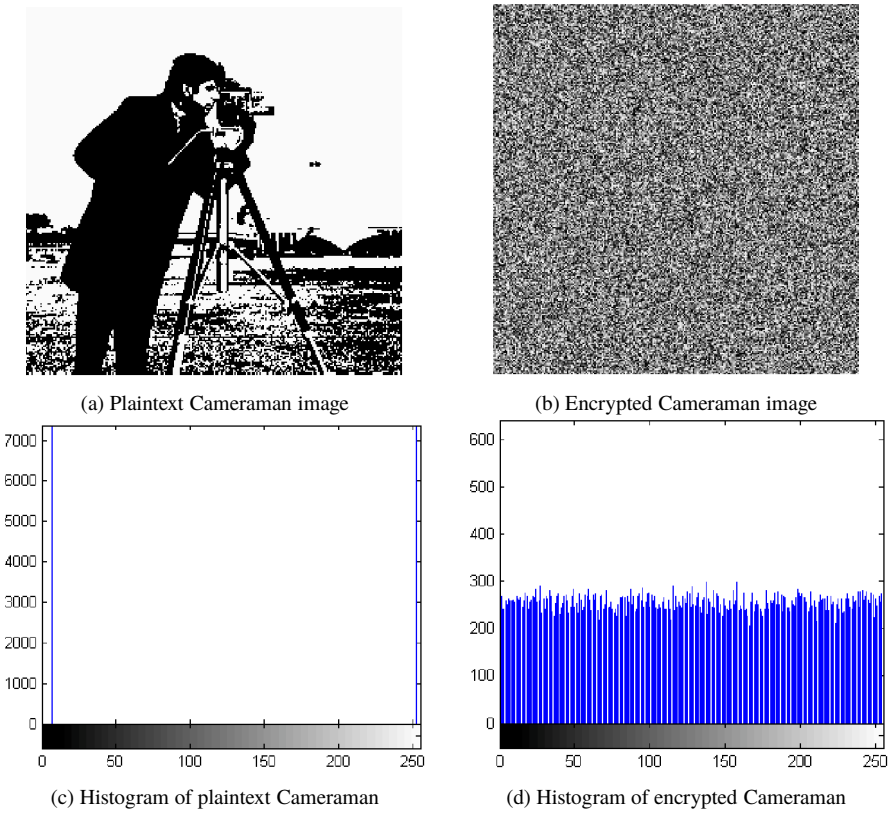
where

$$D(i,j) = \begin{cases} 0 & \text{if } C(i,j) = C^*(i,j), \\ 1 & \text{otherwise.} \end{cases}$$

$$\text{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C(i,j) - C^*(i,j)}{255}\right] \times 100. \tag{11}$$

Here, M and N denote the number of rows and columns, respectively. $C(i,j)$ corresponds to ciphertext image pixel at ith row and jth column position and $C^*(i,j)$ corresponds to the ciphertext image pixel at ith row and jth column position; they differ by only a single bit. Similarly, quality analysis is also done to figure out the quality of the proposed image encryption scheme. The quality of an algorithm can be calculated via Irregular Deviation $I - D$ and Deviation from Uniform Histogram $D - P$. Mathematically, these parameters can be defined as:

$$I - D = \sum_{i=0}^{255} \big(|H_i - A_h|\big), \tag{12}$$



(a) Plaintext Cameraman image (b) Encrypted Cameraman image

(c) Histogram of plaintext Cameraman (d) Histogram of encrypted Cameraman

Fig. 7. Encryption and histogram of binary Cameraman image via proposed scheme.

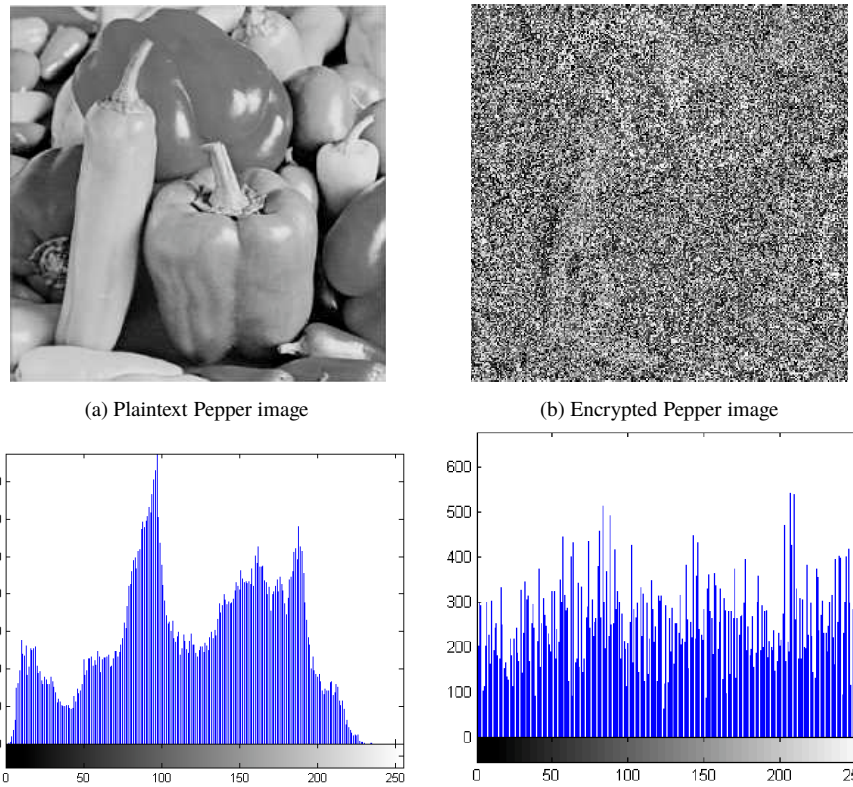
$$D - P = \frac{\sum_{i=0}^{255}(|H_{Ei} - H_E|)}{M \times N}, \tag{13}$$

$$H_{Ei} = \begin{cases} \frac{M \times N}{256} & \text{if } 0 \leqslant E_i \leqslant 255, \\ 0 & \text{elsewhere,} \end{cases}$$

where H_i computes the amplitude of histogram difference between plaintext image and encrypted image at index i and A_h calculates the average sum of histogram values. H_{Ei} is the ideal while H_E is the real histogram value of encrypted image at index i. Smaller value of $I - D$ and $D - P$ represents the high quality of an image encryption scheme. Likewise, contrast analysis is also carried out to allow an observer to strongly recognize the entity in texture of an image. Mathematically, contrast can be computed as:

$$C = \sum_{i,j=1} N|i - j|^2 \times \Gamma(i, j), \tag{14}$$

where $\Gamma(i, j)$ represents the number of Gray-Level Co-Occurrence Matrices (GLCM). High contrast value shows that the image gray levels are considerably different. Using the



(a) Plaintext Pepper image

(b) Encrypted Pepper image

(c) Histogram of plaintext Pepper

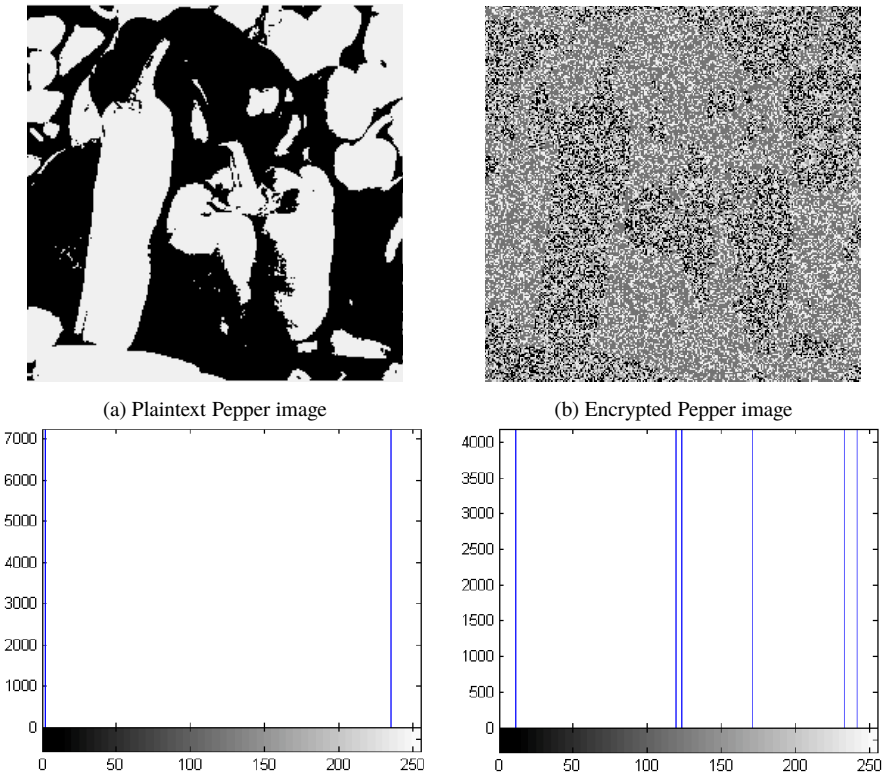
(d) Histogram of encrypted Pepper

Fig. 8. Encryption and histogram of gray scale Pepper image via Amir's algorithm.

aforementioned parameters, we compute the simulation results for our encryption scheme. Simulation results of gray and binary images for both Cameraman and Pepper images are shown from Tables 1 to 4. All simulation results are in favour of the proposed scheme. Apart from tabular values, we have also shown the correlation plots for the plaintext and ciphertext Cameraman image in Figs. 12 and 13, respectively. From these plots, one can see lower correlation between adjacent pixels.

5. Conclusion

We proposed a new algorithm on the basis of weaknesses found in the Amir's scheme. Non-Linear Chaotic Algorithm (NCA) is employed for removing correlation and diffusion in plaintext image. The proposed algorithm enhances the security of the Amir's scheme. In high correlated images such as binary images, the proposed scheme works very well. Desired results are achieved and performance upgrade is verified by comparing the results with the original scheme. Numbers of security parameters to evaluate the effectiveness of an image encryption algorithm are used to compare both modified and original schemes.



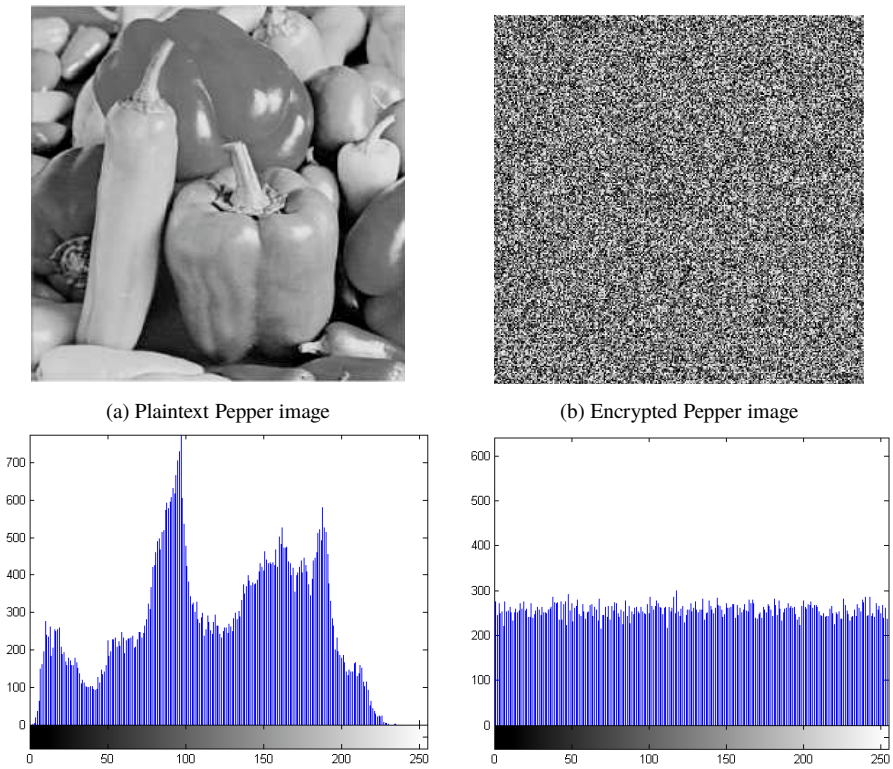
(a) Plaintext Pepper image (b) Encrypted Pepper image

(c) Histogram of plaintext Pepper (d) Histogram of encrypted Pepper

Fig. 9. Encryption and histogram of binary Pepper image via Amir's algorithm.

Table 1
Evaluation of the proposed scheme for gray scale Cameraman image.

Parameter	(Anees *et al.*, 2014a)	(Li *et al.*, 2017)	Proposed
MSE	38.3683	40.3293	**40.3774**
PSNR	16.8046	6.7754	**16.8233**
Entropy (H)	7.9000	7.9901	**7.9966**
NPCR	98.8251	9.545	**99.4537**
UACI	33.1335	33.1907	**33.6723**
I-D	48,834	44,765	**39,003**
D-P	0.3446	0.3290	**0.0678**
Contrast	7.9935	8.6755	**10.0678**
Key Sensitivity Difference	66.2567	99.5453	**99.6353**
Horizontal Direction Corr Coff	**−0.0171**	0.0132	0.0536
Vertical Direction Corr Coff	0.0449	0.0019	**−0.0047**
Diagonal Direction Corr Coff	0.0250	0.0141	**0.0089**
Time (Second)	**7.46**	7.88	7.50



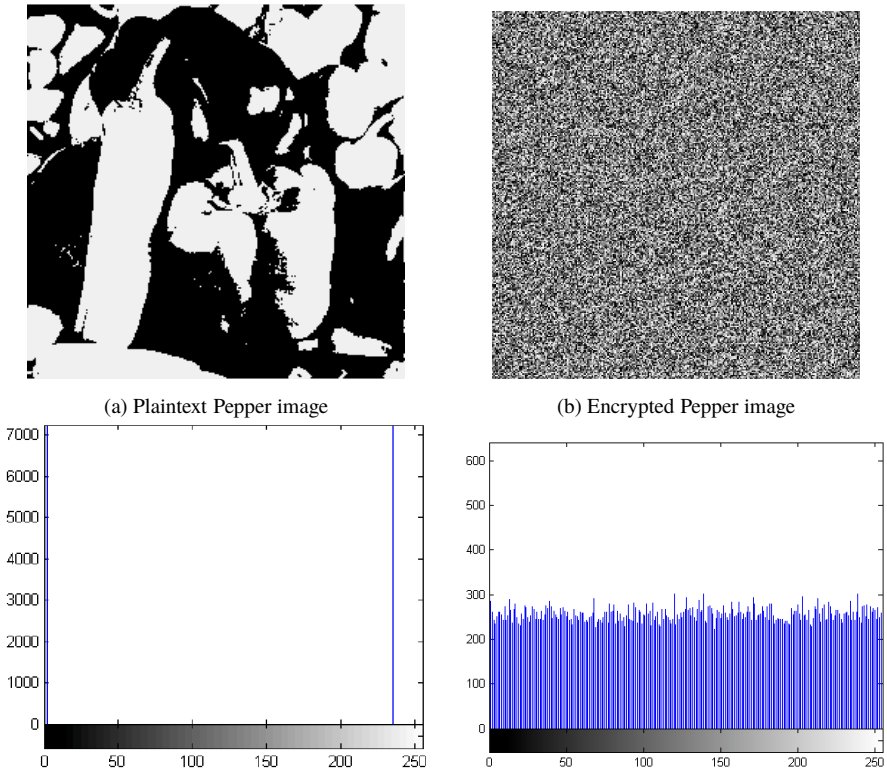
(a) Plaintext Pepper image (b) Encrypted Pepper image

(c) Histogram of plaintext Pepper (d) Histogram of encrypted Pepper

Fig. 10. Encryption and histogram of gray scale Pepper image via proposed scheme.

Table 2
Evaluation of the proposed scheme for binary Cameraman image.

Parameter	(Anees *et al.*, 2014a)	(Li *et al.*, 2017)	Proposed scheme
MSE	39.0926	40.0739	**40.4153**
PSNR	8.3952	8.7952	**9.4948**
Entropy (H)	2.2599	7.8867	**7.9973**
NPCR	66.7236	98.5453	**99.2365**
UACI	24.31205	33.2334	**33.8234**
I-D	122,876	98,745	**20,554**
D-P	2.0021	0.5587	**0.0512**
Contrast	5.7745	7.8876	**10.1254**
Key Sensitivity Difference	66.3325	98.4867	**99.0452**
Horizontal Direction Corr Coff	0.0091	0.0099	**-0.0046**
Vertical Direction Corr Coff	0.0918	0.0418	**−0.0122**
Diagonal Direction Corr Coff	0.0443	0.5280	**0.0328**
Time (Second)	**7.48**	7.67	7.51



(a) Plaintext Pepper image (b) Encrypted Pepper image

(c) Histogram of plaintext Pepper (d) Histogram of encrypted Pepper

Fig. 11. Encryption and histogram of binary Pepper image via proposed scheme.

Table 3
Evaluation of the proposed scheme for gray scale Pepper image.

Parameter	(Anees *et al.*, 2014a)	(Li *et al.*, 2017)	Proposed
MSE	39.4456	40.6745	**40.8832**
PSNR	15.9943	16.0045	**16.8809**
Entropy (H)	7.9102	7.9811	**7.9977**
NPCR	98.7824	97.6535	**99.5562**
UACI	33.2564	33.3326	**33.7529**
I-D	118,654	100,342	**25,231**
D-P	1.6432	0.7653	**0.0923**
Contrast	8.4312	8.6523	**9.5678**
Key Sensitivity Difference	66.4432	99.6231	**99.6489**
Horizontal Direction Corr Coff	0.0282	0.0331	**0.0127**
Vertical Direction Corr Coff	0.0481	0.0220	**0.0065**
Diagonal Direction Corr Coff	0.0502	0.0328	**0.0142**
Time (Second)	**7.41**	7.63	7.45

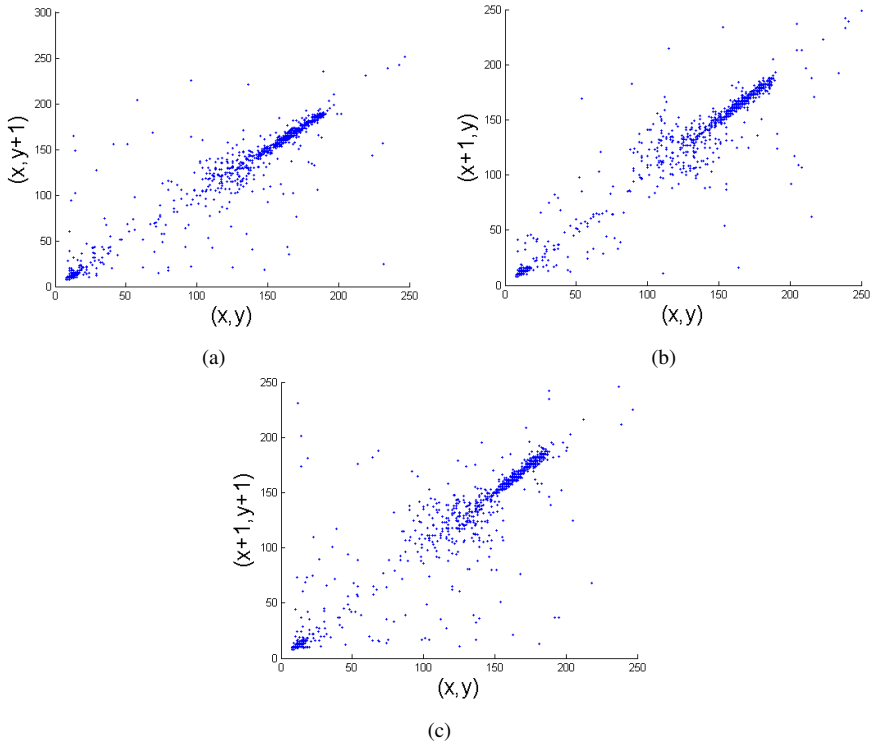


Fig. 12. Plot of randomly chosen adjacent pixel of plaintext Cameraman image at pixel locations x and y (a) horizontal direction, (b) vertical direction, (c) diagonal direction.

Table 4
Evaluation of the proposed scheme for binary scale Pepper image.

Parameter	(Anees *et al.*, 2014a)	(Li *et al.*, 2017)	Proposed
MSE	38.0543	40.1643	**40.4687**
PSNR	8.0065	8.4186	**9.5196**
Entropy (H)	2.3290	7.7156	**7.9920**
NPCR	66.6729	98.6112	**99.5300**
UACI	27.6599	33.7232	**33.8823**
I-D	121,115	101,659	**21,772**
D-P	1.7991	0.5834	**0.1402**
Contrast	3.5234	7.3332	**9.6645**
Key Sensitivity Difference	66.7705	98.5522	**99.3001**
Horizontal Direction Corr Coff	0.0101	0.0221	**0.0058**
Vertical Direction Corr Coff	0.0432	0.0664	**−0.0239**
Diagonal Direction Corr Coff	0.0551	0.1200	**0.0211**
Time (Second)	**7.44**	7.61	7.47

These parameters include the correlation, information entropy, Unified Average Change Intensity (UACI), Peak Signal to Noise Ratio (PSNR), key sensitivity difference, avalanche effect and Number of Pixel Change Rate (NPCR). Although the computational complexity

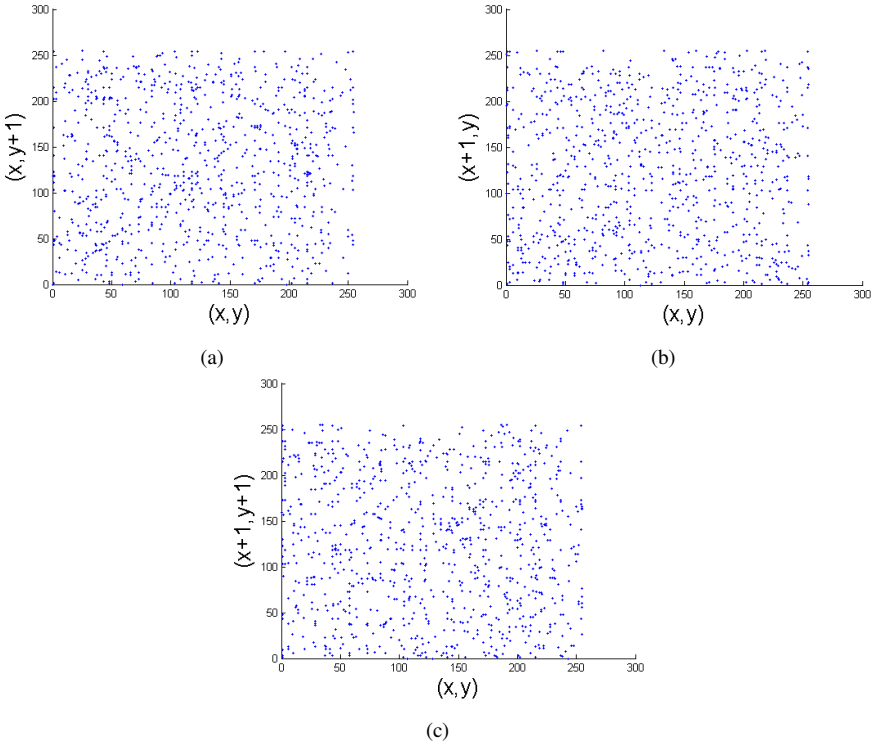


Fig. 13. Plot of randomly chosen adjacent pixel of encrypted Cameraman image at pixel locations x and y (a) horizontal direction, (b) vertical direction, (c) diagonal direction.

of the proposed scheme is a bit higher due to NCA based diffusion, this additional overhead provides higher security for the proposed scheme.

References

Acharya, B., Patra, S.K., Panda, G. (2008). Image encryption by novel cryptosystem using matrix transformation. In: *First International Conference on Emerging Trends in Engineering and Technology, 2008, ICETET'08.* IEEE, pp. 77–81.

Ahmad, J., Ahmed, F. (2010). Efficiency analysis and security evaluation of image encryption schemes. *Computing*, 23, 25.

Ahmad, J., Hwang, S.O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dynamics*, 82(4), 1839–1850.

Ahmad, J., Hwang, S.O. (2016). A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, 75(21), 13951–13976.

Ahmad, J., Hwang, S.O., Ali, A. (2015). An experimental comparison of chaotic and non-chaotic image encryption schemes. *Wireless Personal Communications*, 84(2), 901–918.

Ahmad, J., Khan, M.A., Hwang, S.O., Khan, J.S. (2016). A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural Computing and Applications*, 1–15.

Ahmad, J., Khan, M.A., Ahmed, F., Khan, J.S. (2017). A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation. *Neural Computing and Applications*, 1–11.

Anees, A., Siddiqui, A.M., Ahmed, F. (2014a). Chaotic substitution for highly autocorrelated data in encryption algorithm. *Communications in Nonlinear Science and Numerical Simulation*, 19(9), 3106–3118.

Anees, A., Siddiqui, A.M., Ahmed, J., Hussain, I. (2014b). A technique for digital steganography using chaotic maps. *Nonlinear Dynamics*, 75(4), 807–816.

Belkhouche, F., Qidwai, U. (2003). Binary image encoding using 1D chaotic maps. In: *IEEE Region 5, 2003 Annual Technical Conference*. IEEE, pp. 39–43.

Bruce, S. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, New York.

Chang, C.C., Yu, T.X. (2002). Cryptanalysis of an encryption scheme for binary images. *Pattern Recognition Letters*, 23(14), 1847–1852.

Chung, K.L., Chang, L.C. (1998). Large encrypting binary images with higher security. *Pattern Recognition Letters*, 19(5), 461–468.

Dawei, Z., Guanrong, C., Wenbo, L. (2004). A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons & Fractals*, 22(1), 47–54.

Gao, H., Zhang, Y., Liang, S., Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons & Fractals*, 29(2), 393–399.

Habib, Z., Khan, J.S., Ahmad, J., Khan, M.A., Khan, F.A. (2017). Secure speech communication algorithm via DCT and TD-ERCS chaotic map. In: 2017 4th International Conference on Electrical and Electronic Engineering (ICEEE). IEEE, pp. 246–250.

Huang, F., Guan, Z.H. (2005). Cryptosystem using chaotic keys. *Chaos, Solitons & Fractals*, 23(3), 851–855.

Hussain, I., Shah, T., Gondal, M.A., Mahmood, H. (2012). Analysis of S-box in image encryption using root mean square error method. *Zeitschrift für Naturforschung A*, 67(6–7), 327–332.

Hussain, I., Shah, T., Gondal, M.A., Khan, W.A., Mahmood, H. (2013a). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, 23(1), 97–104.

Hussain, I., Shah, T., Mahmood, H., Gondal, M.A. (2013b). A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications*, 22(6), 1085–1093.

Jakimoski, G., Subbalakshmi, K.P. (2008). Cryptanalysis of some multimedia encryption schemes. *IEEE Transactions on Multimedia*, 10(3), 330–338.

Johansson, T., Pasalic, E. (2003). A construction of resilient functions with high nonlinearity. *IEEE Transactions on Information Theory*, 49(2), 494–501.

Kam, J.B., Davida, G.I. (1979). Structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*, (10), 747–753.

Khan, J., Ahmad, J., Hwang, S.O. (2015a). An efficient image encryption scheme based on: Henon map, skew tent map and S-Box. In: *2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*, IEEE, pp. 1–6.

Khan, J.S., ur Rehman, A., Ahmad, J., Habib, Z. (2015b). A new chaos-based secure image encryption scheme using multiple substitution boxes. In: *2015 Conference on Information Assurance and Cyber Security (CIACS)*. IEEE, pp. 16–21.

Khan, M.A., Ahmad, J., Javaid, Q., Saqib, N.A. (2017a). An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. *Journal of Modern Optics*, 64(5), 531–540.

Khan, J.S., Ahmad, J., Khan, M.A. (2017b). TD-ERCS map-based confusion and diffusion of autocorrelated data. *Nonlinear Dynamics*, 87(1), 93–107.

Kurosawa, K., Satoh, T., Yamamoto, K. (1997). Highly nonlinearfit-resilient functions. *Journal of Universal Computer Science*, 3(6), 721–729.

Leong, M.P., Cheung, O.Y., Tsoi, K.H., Leong, P.H.W. (2000). A bit-serial implementation of the international data encryption algorithm IDEA. In: *2000 IEEE Symposium on Field-Programmable Custom Computing Machines*. IEEE, pp. 122–131.

Li, S., Zheng, X. (2002). Cryptanalysis of a chaotic image encryption method. In: IEEE International Symposium on Circuits and Systems, 2002, ISCAS 2002, Vol. 2. IEEE.

Li, C., Luo, G., Qin, K., Li, C. (2017). An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics*, 87(1), 127–133.

Matthews, R. (1984). On the derivation of a 'Chaotic' encryption algorithm. *Cryptologia*, 8(1), 29–41.

Nyberg, K. (1992). On the construction of highly nonlinear permutations. In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, Berlin, Heidelberg, pp. 92–98.

Rehman, A.U., Khan, J.S., Ahmad, J., Hwang, S.O. (2016). A new image encryption scheme based on dynamic s-boxes and chaotic maps. *3D Research*, 7(1), 7.

Schneier, B. (1996). *Protocol Building Blocks. Applied Cryptography*, second edition. 20th Anniversary Edition, pp. 21–46.

Stallings, W. (2006). *Cryptography and Network Security: Principles and Practices*. Pearson Education India.

Weister, A.F., Tavares, S.E. (1986). On the design of S-boxes [A], Dvances in Cryptology-CRYPTO?85 [C].

William, S. (2006). *Cryptography and Network Security: for VTU*. Pearson Education India.

Yildiz, S. (2004). *Construction of Substitution Boxes Depending on Linear Block Codes*. Doctoral dissertation, Middle East Technical University.

Younas, M.B., Ahmad, J. (2014). Comparative analysis of chaotic and non-chaotic image encryption schemes. In: *2014 International Conference on Emerging Technologies (ICET)*. IEEE, 81–86.

J.S. Khan is currently pursuing his master of electrical engineering in the Department of Electrical and Electronics Engineering, Gaziantep University, Turkey. He obtained his bachelor of science degree in electrical engineering, from HITEC University in Taxila with highest distinction. As an exchange student, he completed his fourth year of undergraduate studies in the Department of Electric and Electronics Engineering at Istanbul Technical University (ITU), Turkey. His research interest includes chaos based encryption, cryptography and medical imaging.

M. Khan (Senior member IEEE) is an assistant professor in the Department of Computing, SEECS, National University of Sciences & Technology, Islamabad, Pakistan. He received his master with major in mobile networks from IIUI and PhD degree in computer sciences as a sandwich program from IIUI and UMKC, USA, in 2011. He completed his Post doc at University of Ulm, Germany, and University of Missouri, USA, in 2013 and 2016, respectively. He joined Awk University Mardan as an assistant professor/chair CS department in 2011. He has been at School of Computer Science, University of Ulm, Germany, and School of Computer and Electrical Engineering University of Missouri, USA, as post doc fellow with professor dr. G.M. Chaudhry and prof. dr. Frank. Later, dr. Khattak joined College of National University of Sciences & Technology, Islamabad, as an assistant professor in 2013. He worked at the Networking and Multimedia Lab, University of Missouri, Kansas City, USA, as a research fellow. His research interests include wireless networks sensor, body area networks, image processing, image compression, image encryption and data network security.

J. Ahmad received his BS degree in electronics engineering in 2009 from Muhammad Ali Jinnah University, Pakistan, and his MS degree in electrical engineering technology, from HITEC University, Pakistan, in 2012. Currently, he is enrolled as a PhD student at Glasgow Caledonian University, United Kingdom. His interest includes energy efficient systems, neural networks, cryptography and image encryption.

S.O. Hwang received the BS degree in mathematics in 1993 from the Seoul National University, the MS degree in computer and communications engineering in 1998 from the Pohang University of Science and Technology, and the PhD degree in computer science from the Korea Advanced Institute of Science and Technology. He worked as a software engineer at the LGCNS Systems, Inc. from 1994 to 1996. He worked as a senior researcher at the Electronics and Telecommunications Research Institute (ETRI) from 1998 to 2007. Since 2008, he has been working as an associate professor with the Department of Computer and Information Communication Engineering, Hongik University, Korea. His research interests include cryptography, cybernetic security and mobile network. He is a member of the IEEE.

W. Ahmed attained his bachelor degree in communication engineering in the year 2008 from FAST University Islamabad, Pakistan. He did his masters in electrical engineering from HITEC University, Taxila. Currently, he is pursuing his PhD in computer vision from UET, Taxila, Pakistan. His area of interest involves signal processing, image processing, computer vision, and secure communication.