Computer and Information Science; Vol. 7, No. 4; 2014
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Novel Encryption Scheme for Digital Image - Based on One Dimensional Logistic Map

Obaida M. Al-hazaimeh[1]

[1] Computer Science Dep., Al-Balqa Applied Univ., Salt, Jordan

Correspondence: Obaida M. Al-hazaimeh, Computer Science Dep., Al-Balqa Applied Univ., Salt, Jordan. E-mail: dr_obaidam@yahoo.com

Received: January 3, 2014 Accepted: February 3, 2014 Online Published: September 3, 2014

doi:10.5539/cis.v7n4p65 URL: http://dx.doi.org/10.5539/cis.v7n4p65

Abstract

In this paper, an implementation of digital image encryption scheme based on one dimensional logistic map is proposed. The chaotic cryptography technique concentrates in general on the symmetric key cryptographic technique. In the proposed algorithm, a random key table lookup criterion was combined with a one-dimensional chaotic map were used for high degree 2-stage security image encryption while maintaining acceptable overhead delay time. The proposed algorithm is based on image row shuffling and pixel-wise XOR encryption. To increase the security of row shuffling variable rotation and inversion were applied to each shuffled row, based on the difference between old and new row location. The experimental results showed that the proposed algorithm is effective and applicable. The combination of logistic map and key table lookup shows advantages of large random key space and high-level of security. The resulting cipher image is suitable for practical use in secure image storing and transmission.

Keywords: image encryption, logistic map, chaos-based cryptography, pixel shuffling process

1. Introduction

Image encryption has become emergency research in recent years due of the multimedia technology and internet. Images are classified by high correlation between the adjacent pixels, for practical image encryption the traditional cryptographic algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) are not satisfy the standard security analysis tests against different types of attacks. In other words, the outline of the encrypted images using the traditional algorithms is clear, and some of them cost more time while the others cannot resist certain attacks, so there is a is a needed and a room and a wide space for more efficient method for image encryption (Hao, 1993).

In 1990 digital chaotic ciphers gained enormous attention. Brown and Chua (1996) have noticed that there exists the close relationship between chaos and cryptography. Chaotic systems have several significant features favorable to secure communications, which can be connected with some conventional cryptographic properties of good ciphers, such as sensitive dependence on initial condition, psudo-randomness, periodicity, reproduction, confusion, and diffusion (Fridrich, 1998). With all of these features researchers expected to introduce new and powerful tools for image encryption based on chaotic cryptography. In term of digital images, cryptography is the science of using mathematics which play major role by converting the plain-images to cipher-images. Typically, cryptographic algorithms are divided between those that are symmetric key cryptography and those that are asymmetric key cryptography (Parker & Chua, 1995; Fridrich, 1998). In this paper, we are going to use symmetric key cryptography.

Parker and Chua (1995) showed theoretically that the image encryption algorithms can be classified into three parts, position permutation, value transformation, and chaotic systems. This paper chiefly focuses on the chaotic digital encryption algorithms because the security of digital images becomes increasingly important issue since the communications of digital images over network (i.e. internet) occur more frequently (Teng & Zengqiang, 2008). However, image encryption system used randomization systems to increase the uncertainty of the encryption process. Chaotic is one of the most important theories that used to create a random sequence that firstly used in the computer by Edward Lorenz in 1963. Therefore, in this paper a new algorithm for image encryption is proposed based on one dimensional chaotic maps (i.e. logistic map). Logistic map is used because of its basic characteristics, such as sensitivity to the initial conditions, unpredictability, and very simple

non-linear dynamical equations which reduce a significant overhead delay in both encryption and decryption processes (Obaida M. et al., 2014; Yong et al., 2008) as described in the following section.

2. Logistic Map

In order to understand the chaotic behavior, logistic map is presented in this section. The logistic map is one dimensional chaotic system with X output and input variable and two initial conditions $X0$ and α (Patidar et al, 2009; Yong et al.,2008; Behnia et al, 2007), the basic form of the one dimensional logistic map is:

$$Xn+1 = \alpha\, Xn(1-Xn) \tag{1}$$

Where $\alpha \in [0\text{-}4]$, $X \in (0\text{-}1)$ in which, the chaotic behavior is achieved when $\alpha \in [0\text{-}4]$ as shown in Figure 1. In this paper, logistic map is used in the proposed algorithm because it has the advantages of high level efficiency and simplicity in term of mathematical models with very complicated dynamics in the key table size and very good random like properties (Behnia et al, 2007).

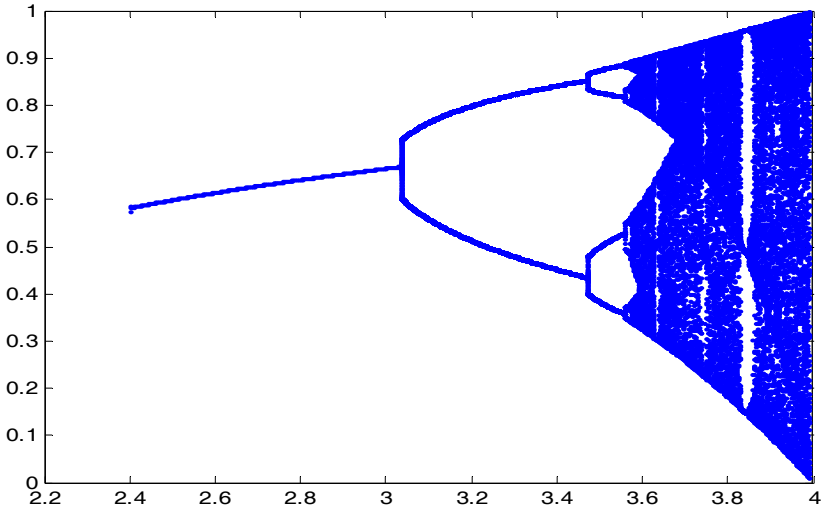


Figure 1. Logistic map diagram

3. Proposed Algorithm

In this section, a new proposed cryptosystem is presented. The proposed algorithm is a symmetric key block cipher algorithm in which one dimensional logistic map is used. Diagrammatically, the steps are represented in Figure 3. Generally, the proposed algorithm is mainly consists of the following steps:

Step 1: Initialization. In this step, the input image is converted into a two dimensional gray level matrix with i, j represents the pixel location and r is row number, then, an empty cipher matrix C, a flag array size is the number of rows, empty key table are created, and finally initiating table pointer to 0 is performed.

Step 2: The initial input condition is set for the logistic map ($X_{n+1} = \alpha\, X_n(1\text{-}X_n)$, where $\alpha = 3$), and then iterate logistic map for 100 times in order to remove the transient effect.

Step 3: Checking, if rows are completely shuffled, go to step 7.

Step 4: In this step, the logistic map is iterated once, and then converting result into row indexes r_{in} is done based on ($r_{in} = x_{n+1} * 10^{14} \bmod r$).

Step 5: In this step, the flag bit of the new row location generated from the previous step is tested, if the flag bit is true (1), go back to step 3. Otherwise r_{in} will be used as new location for row shuffling process.

Step 6: Compute the difference between the new and old row location. Modify the row according to diff value (rotate left, right, or invert), store it in new location and go to step 3.

Step 7: At the end, after completing row shuffling and generating key table processes, for each pixel logistic map is iterated once, and then converting result into key table index to encrypt pixel value based on C (i_i, j) = Key_Table (Key_Ptr)⊕C(i, j).

To make it clear, our implementations have been done based on the following pseudo-code as shown in Figure 2.

```
 Image(i,j)=gray_scale(image)
C(I,j)=0;
FlagI=0
Key_Table=Empty
Key_Ptr=0;
α = 3
For 100 times Do
        X_{n+1} = α X_n(1-X_n)
End
While Row not completed
 {
        Lable:
        X_{n+1} = α X_n(1-X_n)
        r_in = x_{n+1}*10^14 mod r).
                If Flage(r_in)=1 go to Lable
                        Diff= r_in=r_old
                        If Diff >0
                                Rotate old row to the right
                        Else if Diff<o
                                Rotate old row to the left
                        Else
                                Invert old row
                        End
        C(r_in)=Image(r_old)
}
For all pixels do
        X_{n+1} = α X_n(1-X_n)
        Key_Ptr = x_{n+1}*10^14 mod size(Key_Table).
        C_i (i_i, j) = Key_Table (Key_Ptr)⊕C(i, j).
End
```

Figure 2. Pseudo-code of the proposed algorithm

For decryption process, the ciphered image needs to receive encryption keys and follow the introduced steps in reverse order. It involves converting the ciphered image back to its original form (plain-image) for the receiver to understand.

4. Experimental Results

In general, this section concentrates on the performance evaluation of the proposed algorithm. The MATLAP simulation of the new algorithm has been done with a set of gray scale images (i.e. Cameraman, and Baboon) sized 256 x 256 as shown in Figure 4(a) and 4(e). The main encryption keys are the logistic map parameter $\alpha = 3$ and *X0* as initial condition utilized for shuffling Image rows, the second key is the difference between each row and its new shuffled location utilized to rotate (left or right) or invert row as described in the previous section. In addition, a set of chaotic values which is not used in shuffling process will form the key table. The key table has a random size and content depending on the main encryption keys and image size. Also key selection process is based on logistic map

The performed experiments were implemented through MATLAB application tool on a 1.6 GHz core i5 (IV), 8 GB memory and 750 GB hard disk capacities.

With a statistical analysis of Cameraman, and Baboon images and its encrypted image, their grey-scale histograms are given in Figure 4© and 4(g). Figure 4(d) and 4(h) shows grey-scale histogram distribution of the ciphered image after applying the steps of the proposed algorithm.

5. Security Analysis and Discussion

In this paper, we have proposed a new scheme for digital image encryption based on one dimensional logistic map to increase the security level of the digital images.

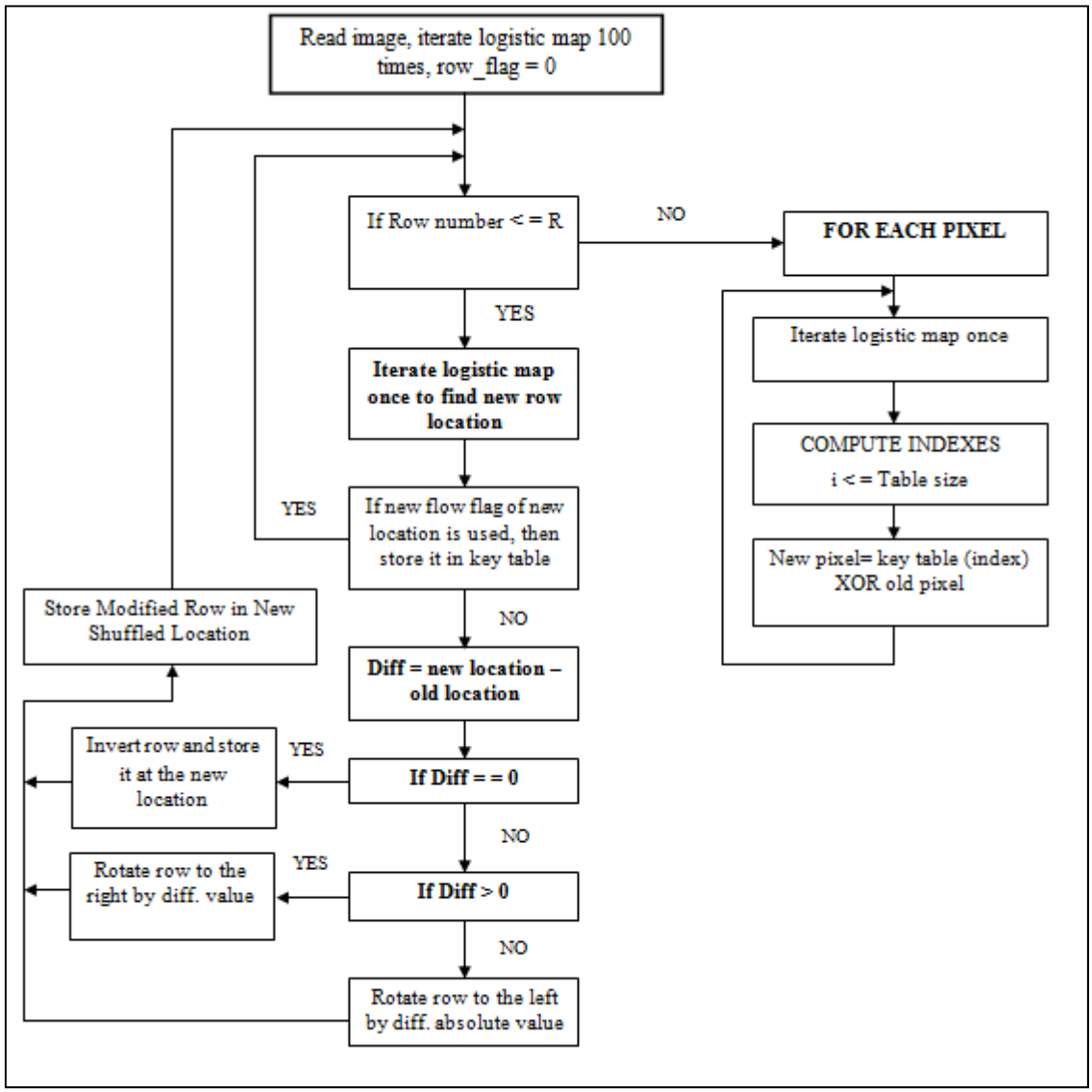
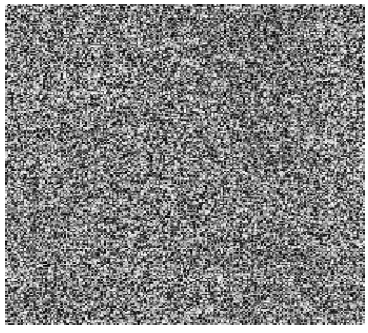
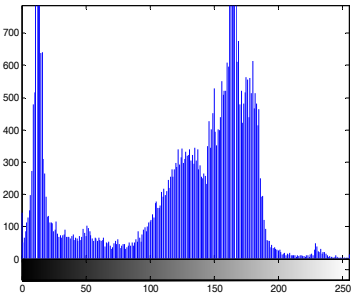


Figure 3. Proposed algorithm architecture

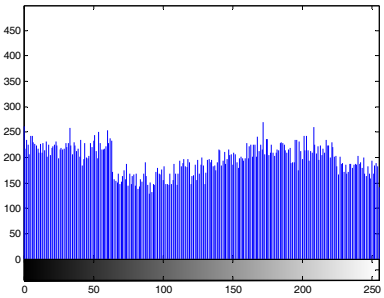
(a) Plain-image.



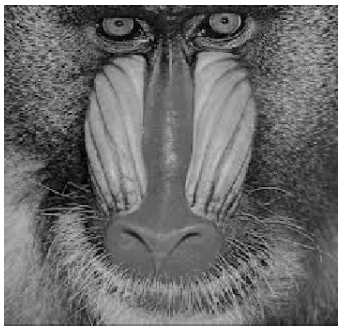
(b) Ciphered image.



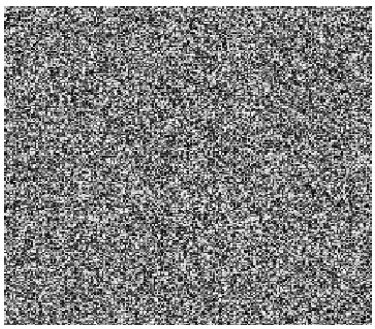
(c) Histogram of plain-image.



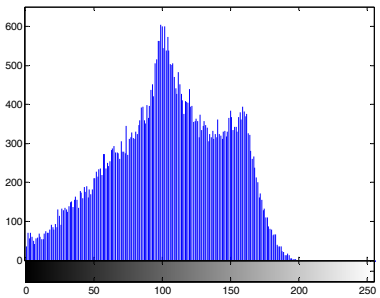
(d) Histogram of ciphered image.



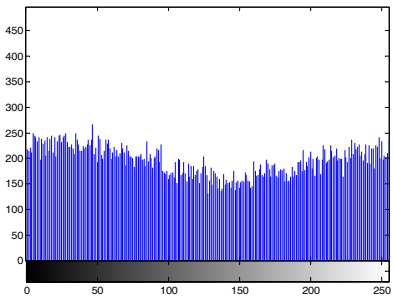
(e) Plain-image.



(f) Ciphered image.



(g) Histogram of plain-image.



(h) Histogram of ciphered image.

Figure 4. Proposed encryption algorithm for some of plain images

In 1998, Shannon carried out a first survey and discussion of the security analysis and evaluation for any image encryption scheme. In this section, several tests have been done to justify the security and performance of the proposed image encryption algorithm such as key space analysis, information entropy, correlation analysis of two adjacent pixels, and differential attack to prove that the proposed image encryption algorithm is effective and secure against the most common attacks (i.e. cryptanalytic, statistical, and brute force attacks).

5.1 Key Space Analysis

Key space size is the total number of different keys that can be used in the cryptosystem (Patidar et al., 2009; Behnia et al., 2008). Cryptosystem should be completely sensitive to all secret keys (i.e. a small change in secret key in the encryption process results into a completely different cipher-image). In this paper, the precision is 10^{-14} which means the key space size for initial conditions and control parameters is over than 2260. Apparently, the key space in the proposed image encryption is large enough and sufficient to resist all kinds of brute force attacks.

5.2 Information Entropy

According to Claude E. Shannon (1949), Information theory is the mathematical theory of data communication and storage. To test the information entropy, the modern information theory is mainly concerned with

error-correction, data compression, cryptography, communications systems. To calculate the entropy H(s) of a source s, we have:

$$H(s) = \sum_{i=1}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)} \quad = 7.997 \tag{2}$$

Where, P contains the histogram counts for gray scale image that have 256 levels, the theoretical value of entropy is 8 bits (Obaida, 2012a; 2012b). The entropy value is calculated and listed in Table 1.

Table 1. Information entropy

Image 256 x 256	Entropy Value
Lena	7.9969
Man	7.9822
Women	7.9928
Baboon	7.9880
Boat	7.9962
Peppers	7.9972

5.3 Correlation Analysis of Two Adjacent Pixels

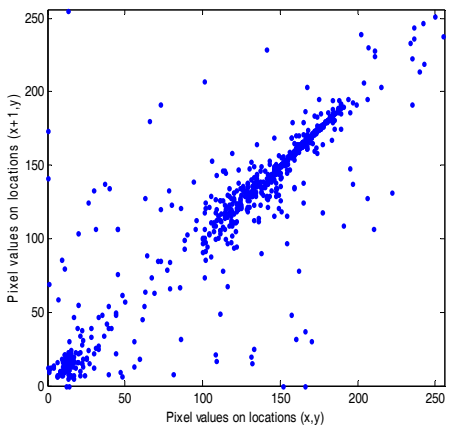
To test the correlation coefficients, Tao et al. (1998) carried out a study to define the relationship between characteristics of plain-image and ciphered image. Typically, to test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, the following procedure was carried out. 1000 pairs of two adjacent pixels from plain-image and their corresponding ciphered image produced using the proposed algorithm were randomly selected in three directions, vertical, horizontal, and diagonal and the correlation coefficients were calculated by using the following two formulas:

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(yi - E(y)\big), r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \tag{3}$$

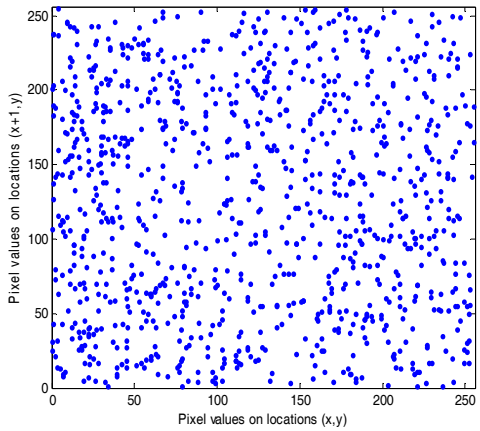
Where,

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \,, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{4}$$

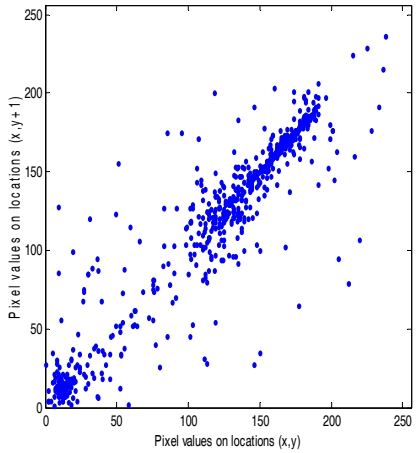
Where, x and y are grey scale values of two adjacent pixels in the image. Figure 5 shows the correlation distribution of adjacent pixels for vertical, horizontal, and diagonal direction respectively in the plain image (a), (c), and (e).



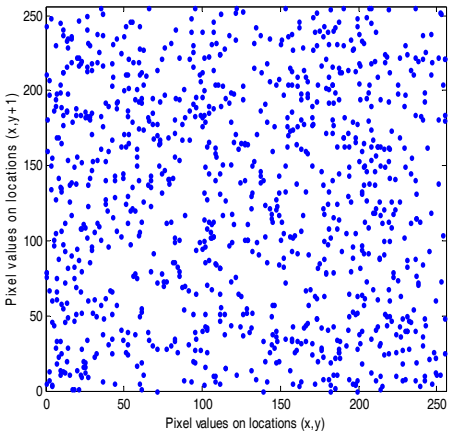
(a) Vertical correlation distribution for plain-image



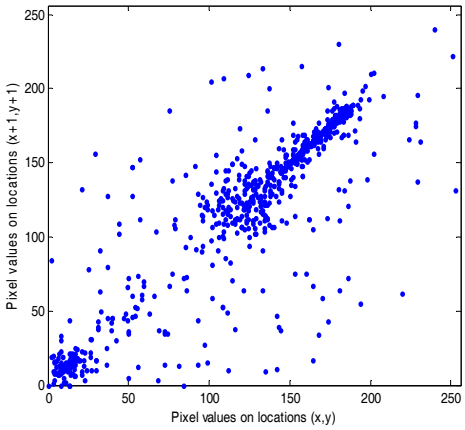
(b) Vertical correlation distribution for ciphered image



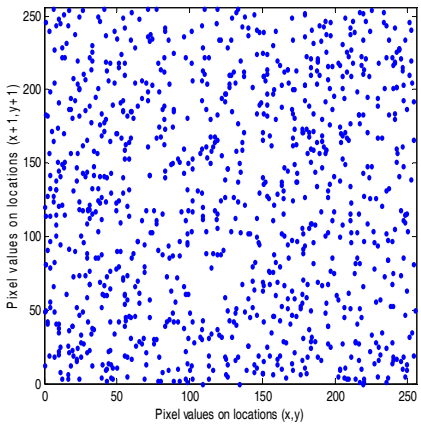
© Horizontal correlation distribution for plain-image



(d) Horizontal correlation distribution for ciphered image



(e) Diagonal correlation distribution for plain-image



(f) Diagonal correlation distribution for ciphered image

Figure 5. Correlation distribution

The correlation coefficients of the plain image and the ciphered image in the vertical, the horizontal, and the diagonal directions were calculated and listed which are shown in Table 2. These correlation analysis prove that the proposed encryption algorithm satisfy zero co-correlation.

Table 2. Correlation coefficients of two adjacent pixels in six images

Image	Plain-image			Ciphered image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9816	0.9578	0.9417	0.0504	0.0531	0.0508
Man	0.9643	0.9655	0.9289	0.0551	0.0557	0.0505
Women	0.9551	0.9576	0.9292	0.0527	0.0523	0.0492
Baboon	0.8511	0.8878	0.8468	0.0475	0.0517	0.0502
Boat	0.9506	0.9374	0.9275	0.0561	0.0508	0.0495
Peppers	0.9653	0.9629	0.9605	0.0501	0.0544	0.0526

Table 2 shows the correlation coefficients for the three dimensions in the ciphered image which resulted from the proposed algorithm are close to zero, while the correlation coefficients for the three dimensions in the plain

image are 1.00. This indicates that the plain image and ciphered image are not correlated, as suggested by Tao Sang et al.

5.4 Differential Attack

For any encryption algorithm, it is desirable property that a small change in plain-image should cause a significant change in the cipher-image. To test the influence of one-pixel change on the whole cipher image encrypted by the proposed algorithm, the most two common measures were used: UACI and NPCR (Chen at al., 2003; Van et al., 2004). Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) are defined by formula 5, and formula 6 respectively.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (5)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \quad (6)$$

In this paper, the values of NPCR and UACI are calculated and listed in Table 3.

Table 3. NPCR and UACI

Image 256X256	NPCR	UACI
Lena	99.6109	12.5946
Man	99.5891	12.8296
Women	99.6247	13.6968
Baboon	99.5990	13.6225
Boat	99.6384	12.8922
Peppers	99.6002	12.8174

In general, higher NPCR values are desired for ideal encryption schemes. The UACI values must be in the range of 13% (Shujun et al., 2002; Parker & Short, 2001; Wei et al., 2000). In our evaluation, six images are taken for comparison. The results demonstrate that the proposed algorithm can survive differential attack.

6. Conclusion

In this paper, a way of improving the security of the digital image cryptosystem is proposed using one dimensional logistic map. The conducted experiments and the statistical analysis of the algorithm show that the proposed algorithm is strong, fast, and secure because it has satisfied the standard security analysis tests against different types of attacks such as correlation coefficient test, differential attack test, key space analysis, and entropy analysis. Thus, we expect that the proposed algorithm will be efficiently employed in serious applications that require a high level of security (i.e. digital images) or it could be considered as a high-quality alternative to the other algorithms because of the high level of security and performance in term of overhead delay time.

References

Behnia, S., Akhshani, A., Ahadpour, S., & Mahmodi H. (2008). Chaotic cryptographic scheme based on composition maps. *International Journal of Bifurcation and chaos, 18*, 251-261. http://dx.doi.org/10.1142/S0218127408020288

Behnia, S., Akhshani, A., Ahadpour, S., & Mahmodi, H. (2007). A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. *Physical Letters, 366*(4-5), 391-396. http://dx.doi.org/ 10.1016/j.physleta.2007.01.081

Brown, R., & Chua, L. (1996). Clarifying chaos: Examples and counterexamples. *International Journal Bifurcat Chaos, 6*(2), 219-249. http://dx.doi.org/ 10.1142/S0218127496000023

Chen, H., Guo, J., Lin-Chieh, H., & Cheng J. (2003). Design and Realization of a New Signal Security System for Multimedia Data Transmission. *EURASIP Journal on Applied Signal Processing, 13*, 1291–1305. http://dx.doi.org/10.1155/S1110865703309011

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal Bifurcat Chaos, 8*(6), 1259–84. . http://dx.doi.org/ 10.1142/S021812749800098X

Hao, B. (1993). Starting with parabolas, an introduction to chaotic dynamics. *Shanghai Scientific and Technological Education Publishing House*, Shanghai, 20-25.

Kuhn D., Walsh T., & Fries S. (2005). Security Considerations for Voice over IP Systems, *Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-58.* http://dx.doi.org/10.6028/NIST.SP.800-53r4

Obaida M, A., Nouh A, Sofyan H., & Ammar A, (2014). HANON Chaotic Map - Based New Digital Image Encryption Algorithm, *MAGNT Research Report, 2*(4), 261-266. http://dx.doi.org/14.9831/1444-8939.2014/2-4/MAGNT.33

Obaida M. (2012). A new approach for complex encrypting and decrypting data. *International Journal of Computer Science Issues, 5*(2), 95-103.

Obaida, M. (2012). Increase the Security Level for Real-Time Application Using New Key Management Solution. *International Journal of Computer Science Issues, 9*(3), 240-246.

Parker, A., & Short, K. (2001). Reconstructing the key-stream from a chaotic encryption scheme. *IEEE Trans Circuits System I, 48*(5), 104–12. http://dx.doi.org/10.1109/81.922466

Parker, T. S., & Chua, L. O. (1995). Chaos: a tutorial for engineers. *Proceedings of the IEEE Transactions on Circuits and Systems, 75*(8), 982 - 1008.

Patidar, V., Pareek, N., & Sud, K. (2009). A New Substitution-diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Non-linear Science and Numerical Simulation, 14*(7), 3056-3075. http://dx.doi.org/ 10.1016/j.cnsns.2008.11.005

Shannon, C. (1998) .Communication Theory of Secrecy Systems. Bell Systems, *Technical Journal, MD Computing, 15*, 57 - 64. http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shujun, L., & Zheng, X. (2002). Cryptanalysis of a chaotic image encryption method. *Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium, 2*, 708-711. http://dx.doi.org/10.1109/ISCAS.2002.1011451

Tao, S., Ruli, W., & Yixun, Y. (1998). Clock-Controlled Chaotic Key-Stream Generators. *Institution of Engineering and Technology Electronics Letters, 34*, 1932 - 1934. http://dx.doi.org/10.1049/el:19981377

Teng, G., &Zengqiang, C. (2008). A new image encryption algorithm based on multiple chaotic systems. *Physical Review Letter A, 372*(4), 394-400.

Van, D., Ville, D., Philips, W., Van, R., & Lemahieu, I. (2004). Image scrambling without bandwidth expansion. *IEEE Transactions Circuits and Systems for Video Technology, 14*(6), 892-897. . http://dx.doi.org/10.1109/TCSVT.2004.828325

Wei, D., Wei-qi, Y., & Dong-xu, Q. (2000). A Novel Digital Hiding Technology Based on Tangram Encryption. *IEEE Proceedings of on NEWCAS 2005, and Conways Game. Proceeding of 2000 International Conference on Image Processing, 1*, 601-604.

Yong, W., Kwok-Wo, W., Xiaofeng L., Tao. X.,& Guanrong, C. (2008) A chaos-based image encryption algorithm with variable control parameters. *Chaos solution& Fractals, 41*(4), 1773-1783.