Chaos Encryption Algorithm using Key Generation from Biometric Images

Ali M. Meligy
Prof. Dr. of Computer Science
Faculty of science-Menoufia University-Mathematics Department

Hossam Diab
Assistant Professor of Computer Science-Faculty of Science-Menoufia University.
College of Computer Science & Engineering-Taibah University

Marwa S. El-Danaf
Researcher in Academy of Scientific Research and Technology

ABSTRACT
Recently, chaos based encryption techniques introduce several merits over the classical techniques such as extensive security levels, complexity and fast speed. In this paper, a chaotic based cipher that incorporates both Logistic chaotic map and Tent map is proposed. An external biometric key of length 256-bits is employed to derive the initial seeds of the applied chaotic maps. In the encipher stage, the pixels information are masked based on an iterative structure using a data-dependent feedback mechanism that mixes the current cipher parameters with the previously enciphered pixels. Accordingly, the relation of the enciphered image and the original image is confused and the suggested cipher can defeat any attack. The experiments reveal the high efficiency of the proposed algorithm in addition to its sensitivity to secret key changes and its resistance to different types of attacks.

Keywords
Stream Cipher, Chaos Cryptography, Tent Map, Logistic Map, Statistical Tests, Security analysis.

1. INTRODUCTION
With the growth of the digital communication technologies, new challenges for securing digital media from illegal access are arising. Thus, intensive research works in the cryptography field are mandatory to achieve the demand of secure encryption algorithms. Specifically, digital images as a representative information resource require special type of encryption algorithms to cope with the special image features. So, image security researches have become a hot issue in the current digital world. Accordingly, several algorithms are proposed for protecting digital images [1-18]. Among them, chaotic based systems present several desired cryptographic characteristics such as an efficient and simple implementation which ensures a high encryption rate. Further, the chaotic maps possess several essential characteristics such as ergodicity, initial conditions sensitivity, and mixing property, which meet the fundamental requirements of good encryption techniques such as confusion and diffusion properties of classical encryption schemes [5, 6, 7]. Generally, chaotic systems have numerous desired features which are appropriate for designing new image cryptosystems.

Indeed, several chaos-based ciphers have been suggested in the last decade. Some of them exploit 1-D chaotic systems for generating the required secret keys [7, 12, 18]. After generating the key, the image pixels are then shuffled and modified according to the obtained key. On the other hand, some encryption algorithms depend on two-dimensional maps to directly handle the digital image which is represented as 2D array of pixels [19, 20]. Similarly, chaotic based ciphers are utilized for solving the security issues of biometric templates in which the encryption keys are produced randomly for each session. Therefore, the encrypted biometric information is highly protected by chaotic schemes which save them from attacks [15].

One of the simplest chaotic mappings that have been used for image encryption applications is the chaotic Logistic map which can be expressed as:

$$x_{n+1} = r\, x_n (1 - x_n) \tag{1}$$

where $x_n \in [0, 1]$ and $r \in [0, 4]$. Further, when the control parameter (r) falls in the interval $[3.57, 4]$, the map reveals a random behavior [12].

Also, the proposed cipher utilizes the chaotic Tent map which can be depicted as follows:

$$f_u(x_{n+1}) = \begin{cases} u x_n & if \quad x_n < 0.5 \\ u(1 - x_n) & if \quad x_n \geq 0.5 \end{cases} \tag{2}$$

For the chaotic Tent map [17], the control parameter $u = 2$ yields a chaotic sequence $x_n \in [0, 1]$ with a random behavior.

In this paper, an efficient encryption algorithm to protect digital images with a fast performance speed and a high level security is proposed. The proposed stream cipher incorporates both Logistic chaotic map and Tent map to produce the cipherimage. The core idea of the suggested scheme is the utilization of an external biometric image to get an external secret key of length 256-bits. Consequently, the generated external key is employed to deduce the initial seeds of the applied chaos mappings. Further, the pixels are masked based on an iterative module which exploits a data-dependent feedback mechanism to mix the current cipher conditions with the previously masked pixels to get the encryption results.

Our paper is organized as follows: Section 2 introduces the structure of the proposed encryption scheme. Experimental tests and numerical computations to confirm the encryption quality of the suggested scheme are illustrated in Section 3. Section 4 argues the various security analyses of the suggested cipher including statistical analysis and sensitivity analysis related to plaintext and key changes. Finally, Section 5 draws the conclusions.

2. PROPOSED IMAGE ENCRYPTION ALGORITHM
The proposed cipher is a symmetric key stream cryptography technique in which three main functions (the key expansion, encryption and decryption modules) are employed by the

sender and receiver to obtain the encrypted and the decrypted image, respectively. First, a secret biometric image is exploited by the sender/receiver to generate the secret key. The encryption operations are applied to the plainimage to get the cipherimage. The structure of the proposed cipher relies on a data-dependent feedback mechanism in which the encipher of each pixel is made dependent on the encryption properties of the previous cipher pixel, which in turn, makes the cryptosystem robust against any type of attacks. The following subsections present the three phases of the proposed algorithm.

2.1 Key Expansion

In view of the essential needs of cryptology, the enciphered image must be strongly related to the secret key and the security of the encryption scheme only relies on obscuring this key. Further, the cipher should be strictly sensitive to tiny variations in the secret keys. Thus, the strategy of randomly generating the key ensures these requirements. The proposed mechanism for key scheduling utilizes a selected biometric image to produce the required key. The steps for key generation can be depicted as follows:

Step 1: Input an r × c biometric image *BI*.

Step 2: Merge the pixel information of the shared biometric image horizontally as follows.

$$BI(i,j)=BI(i,j)\oplus\Psi,\ 1\le i\le r\ \&1\le j\le c \tag{3}$$

where Ψ is the value of the previous pixel.

Step 3: Divide the obtained matrix from step 2 into h×h blocks.

Step 4: Calculate the mean value of each block which is denoted by *M(s)* for the s^{th} block and approximate *M* to the nearest integer value.

Step 5: Calculate the median value of the main diagonal for each block which is denoted by *N (s)* for the s^{th} block.

Step 6: Obtain the secret biometric key by BitXoring *M* and *N*.

$$Key=M\oplus N \tag{4}$$

The test suite from National Institute of Standard and Technology (NIST) [21] was selected to test the randomness of the sequence (secret key) created by the suggested key expansion mechanism. This suite consists of a set of tests. Each test is independently applied to an *n* bits sequence (the same sequence in each test) to get a P-value. Namely, the P-value indicates to the probability of the randomness of the generated sequence under a certain test. If the obtained P-value for a certain test equals one, then the sequence emerges a perfect randomness. On the other hand, when the P-value is zero; this indicates that the sequence reveals a complete non random behavior. Specifically, the statistical package consists of 16 tests [21]. To perform the statistical analysis of the generated key stream, a significance level α = 0.01, as proposed by NIST, is used and then compute the P-values for various tests. If the obtained P-value ≥ 0.0001, then the P-values are distributed uniformly in the interval [0, 1]. These tests are performed on our proposed key generator and the obtained results are summarized in Table 1. The estimations values confirm that the proposed generator can pass many of the underlying statistical tests and the basic requirements for the uniform distribution are met. Thus, the generated key stream is uniformly distributed and cannot be predicted by an adversary.

Table 1: The NIST Statistical Tests for the proposed key expansion

No.	Statistical tests	P_Value
1	Frequency (Monobit)	0.7237
2	Block Frequency (M =22)	0.3938
3	Runs	1.7029
4	Longest Runs of Ones(M=22)	0.0681
5	Binary Matrix Rank(M = 22)	0
6	Spectral DFT	0.8185
7	Non-overlapping, M=12,B= [1 0 1]	0.2359
8	Overlapping, M =22,B =[1 1 0 1 1]	0.4197
9	Maurer's Universal, (L=7,Q=1280)	0
10	Approximate Entropy	0.2096
11	Linear Complexity (M = 22)	0.8088
12	Cumulative Sums (Backward) Zero & One	1.000& 0.6317
13	Random Excursions	0.0199
14	Random Excursions Variant	0.8084
15	Serial (m = 16)	0
16	Serial (m = 16)	0

Now, the proposed scheme generates the initial seed of the employed chaotic system, X_0 and the initial cipher pixel C_0 from the extracted external biometric key *K*. Assume that the external secret key is represented as follows:

$$K=K_1K_2\cdots K_{32} \tag{5}$$

where K_i represents a block of 8-bit of the overall 256-bit biometric key *K*.

To compute X_0 and C_0, the following two steps are carried out:

Step1: Compute the intermediate quantities a_1, a_2, a, b_1, and b_2 as follows:

$$a_1=\sum_{i=1}^{31}K_i,\ a_2=\bigoplus_{i=1}^{31}K_i,\ a=\frac{a_2}{a_1} \tag{6}$$

$$b_1=(a+\frac{K_{32}}{255})\bmod 1,\ b_2=(\frac{a_2+K_{32}}{255})\bmod 1 \tag{7}$$

Step2: The values of C_0 and X_0 are determined by

$$C_0=(b_1\times b_2\times 10^4)\bmod 256 \tag{8}$$

$$X_0=\left(\sum_{i=1}^{32}\frac{FIB(K_i)}{255}\right)\bmod 1 \tag{9}$$

Where the symbol *FIB* in Eq. 9 denotes the Fibonacci function [22].

2.2 Encryption Algorithm

The proposed encryption handles the plainimage as a stream of pixels, each pixel is represented by 8-bit, and encrypts the input image pixel by pixel according to the following steps:

Step1: Convert the 2D plainimage *P* into 1D vector by reading the pixels from top left to bottom right sides. The obtained plainimage vector and its corresponding cipher vector are denoted by *P* and *C*, respectively.

$$P = P_1 P_2 \cdots P_m \tag{10}$$

$$C = C_1 C_2 \cdots C_m \tag{11}$$

Step2: Encrypt the current pixel P_i to obtain its corresponding cipher pixel C_i according to

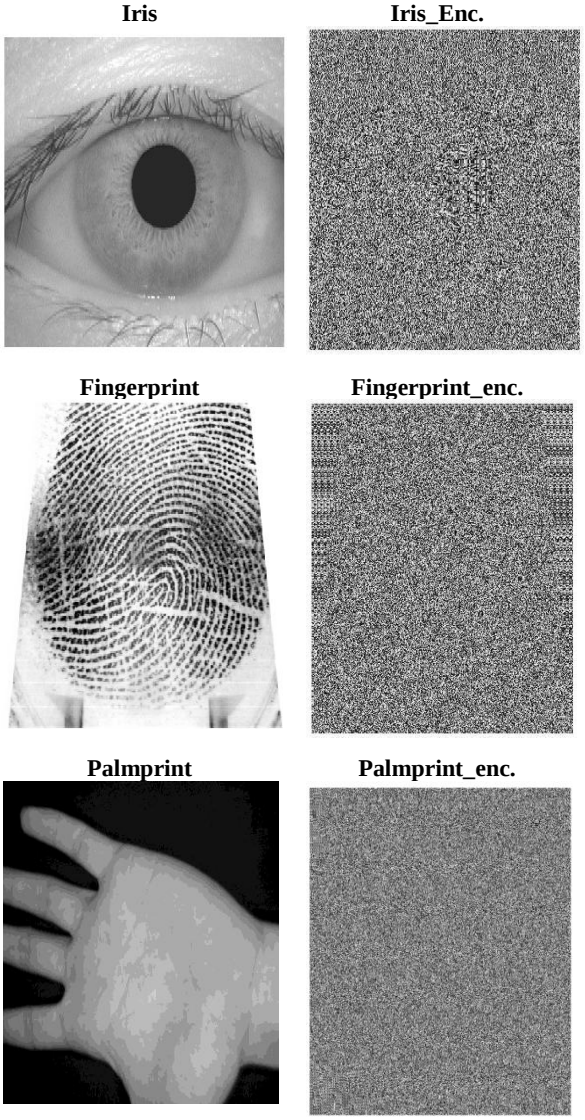


Fig 1: Encryption results for the proposed scheme

$$C_i = \left(\left(P_i \oplus C_{i-1} \right) >>> round \left(10^4 \times \sum_{j=1}^{rounds_j} T(X_j) \right) \right) \bmod 256 \tag{12}$$

Where X_j denotes the current input for the selected map (Tent map or Logistic map T) and can be calculated as follows:

$$X_j = \left(\frac{abs\left(K_{j \bmod 32+1} - X_{j-1} \right)}{255} \right) \bmod 1 \tag{13}$$

Also, the scheme will be switching between the Tent map and the Logistic map to select one of them as a mapping T according to the current value X_j as follows:

$$T = \begin{cases} r\,x(1-x) & if\ 0.5 \le X_j \le 0.7 \\ ux & if\ X_j < 0.5 \\ u(1-x) & if\ X_j > 0.7 \end{cases} \tag{14}$$

Further, the selected function T is iterated for $rounds_j$ which is calculated as

$$rounds_j = \left(K_{j \bmod 32+1} + C_{i-1} \right) \bmod 256 \tag{15}$$

Step3: Set *i=i+1* and apply the *step 2* until all pixels are encrypted.

Step4: Convert C into 2D array to get the final enciphered image.

2.3 Decryption Algorithm

The decryption phase returns the original image from the corresponding enciphered one using the same biometric image (accordingly, the same 256-bit external key is generated). The decryption algorithm applies the same steps with the replacement of the encryption mapping with the inverse mapping of Eq. 12.

3. EXPERMENTAL RESULTS

To demonstrate the efficiency of the suggested cipher, several experiments are performed on a set of biometric images downloaded from CASIA (Chinese Academy of science and institute of Automation) database [23]. Also, for the numerical evaluation of the enciphering quality, the correlation coefficient (C.C) between the plainimage and the cipherimage is estimated. Mathematically, C.C can be expressed according to [10, 12] as follows:

$$C.C = \frac{N \sum_{j=1}^{N} (x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N \sum x_j^2 - (\sum_{j=1}^{N} x_j)^2) \times (N \sum y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \tag{16}$$

where x and y denote the grey values of the pixels for the plainimage and the corresponding encryption result.

The encrypted images which are illustrated in Fig. 1 emphasize the feasibility of the proposed scheme. Obviously, the proposed scheme effectively conceals all features of the plainimage which means that the encrypted image is visually indistinguishable. Also, the results are compared with the standard encryption algorithms (AES, RC5, and RC6) in Table 2, where the proposed scheme retains the smallest Correlation Coefficients (C.C).

Table 2: Numerical Evaluation of Encryption Quality

Images	Correlation Coefficient			
	RC5	RC6	AES	Proposed Cipher
Iris001_1_1	0.0118	0.0225	0.0152	0.0134
Iris001_2_1	-0.0258	0.0091	-0.0884	-0.0074
Fingerprint100_L0_0	0.0400	0.0078	-0.0119	-0.0055
Fingerprint100_R0_0	0.0386	0.0056	0.0183	-0.0043
Palmprint0001_m_L_01	-0.0284	0.0067	0.0040	-0.0057
Palmprint0001_m_R_01	-0.0061	0.0050	0.0031	-0.0054

4. SECURITY ANALYSIS

An acceptable encryption algorithm must thwart all types of cryptanalytic threats such as statistical attacks and exhaustive search attacks, differential attacks and related key attacks [7, 10, 12]. In this section, several security tests are applied to the proposed cipher to demonstrate its satisfactory security level.

4.1 Statistical Analysis

From cryptanalysis point of view, statistical analysis may enable an attacker to crack the cipher and recover the plainimage from its cipherimage. Indeed, several cryptography schemes have been successfully broken through the statistical analysis such as permutation based ciphers. Hence, to confirm the strength of the proposed cryptosystem, the statistical analysis based on histogram and adjacent pixel correlations analysis are performed. The obtained results demonstrate the ideality of the proposed scheme regarding the statistical attacks.

4.1.1 Correlation of Two Adjacent Pixels

The correlations between neighboring pixels are tested for horizontal, diagonal, and vertical adjacent pixels for the plainimage and the associated cipherimage. First, several pairs of neighbor pixels in different directions are randomly selected. Then, calculate the correlation coefficient between them according to Eq. 16. The results of the adjacent correlation analysis for horizontal pixels for iris image and its related cipherimage are illustrated in Fig. 2. The obtained values for the correlation coefficients in the plainimage and cipherimage are tabulated in Table 3 for different directions. Obviously, there is an extraneous correlation between adjacent pixels in the cipherimage. On the other hand, the plainimage appears well correlated adjacent pixels which prove that the success of the proposed scheme in decreasing such correlation.

Table 3: C.C for original image and its related enciphered image

Direction	Plainimage	Cipherimage
Horizontal	0.9740	-0.1494
Vertical	0.9709	0.0403
Diagonal	0.9681	-0.0013

Horizontally adjacent pixels for plainimage **Horizontally adjacent pixels for enciphered image**

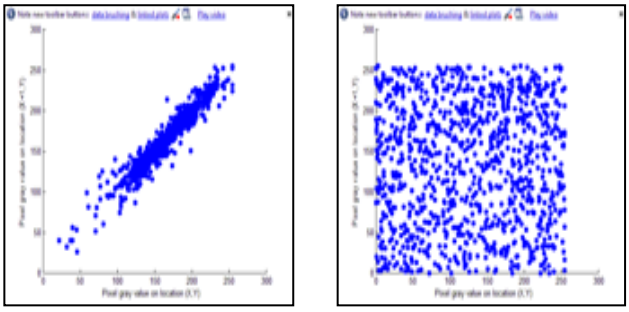
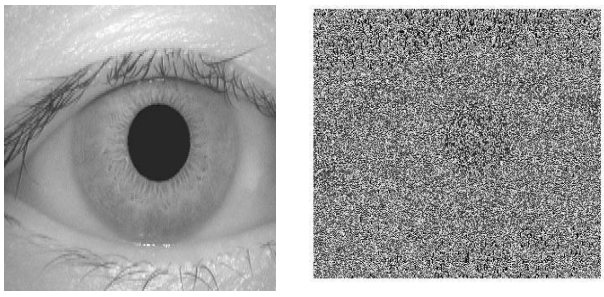


Fig. 2. The horizontal adjacent pixels distribution for plainimage and its related cipherimage

4.1.2 Gray Histograms Analysis

Additionally, to prevent an opponent from exploiting the statistical features of the cipherimages to obtain valuable information about the plainimage, the cipherimage must bear a high dissimilarity to the original image. The histogram of several encrypted biometric images and its related original biometric images are studied. One of these examples shown in Fig. 3 presents the histogram of a cipherimage and the histogram of corresponding original image denoted by iris image. It is clear that the enciphered image histogram is uniformly distributed and notably dissimilar to the relevant histogram of the corresponding original image and consequently does not afford any indication about the original plainimage. Thus, an opponent cannot apply any statistical analysis on the proposed cipher.

Iris plainimage **Enciphered iris image**



Histogram of plainimage **Histogram of enciphered image**

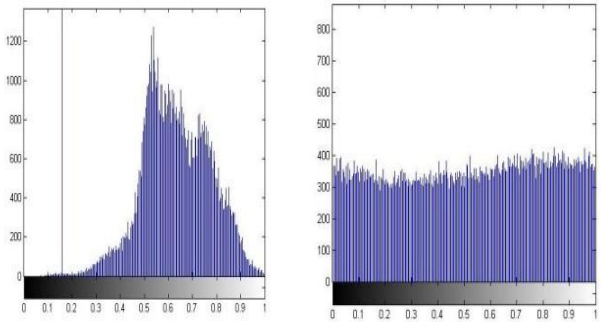


Fig. 3. Histogram of the iris image and its encryption

4.2 Information Entropy Analysis

Information entropy is considered as a major indicator to randomness degree. According to Shannon's theory [19], the entropy of an information source IS can be defined as follows:

$$H(IS) = -\sum_{i=0}^{2^L-1} P(IS_i) log_2 P(IS_i) \quad (17)$$

Where $P(IS_i)$ denotes the probability of symbol IS_i, and L is the number of bits used in representation of symbols of the source *IS*. According to this definition, it is found that the idea entropy value for a random image with 2^8 (256) grey levels equals 8. To test the safety of the suggested scheme against the entropy attack, the entropy values for several images encrypted by the proposed scheme are estimated and are displayed in Table 4. The achieved estimations are too close to the expected value of 8 for a perfect random image. Thus, the proposed image cipher can defy the entropy attacks.

Table 4: Results of information entropy analysis.

Images	Entropy
Iris 001_1_1	7.9888
Iris 001_2_1	7.9599
Fingerprint 100_L0_0	7.9700
Fingerprint 100_R0_0	7.9586
Palmprint 0001_m_L_01	7.9265
Palmprint 0001_m_R_01	7.9099

4.3 SENSITIVITY ANALYSIS

A perfect cipher must be wholly sensitive to tiny modification in the associated encryption key and the original plainimage. Namely, the trivial variation on a single bit in either the plainimage or the secret key must yield a considerable change in the cipherimage (i.e. totally different enciphered image). To verify the strength of the proposed algorithm, the following analysis is employed.

4.3.1 Key Sensitivity Analysis

One aspect of key sensitivity for a secure cipher is the failure of restoring the plainimage from cipherimage if there is only a minor diversity between decryption and encryption keys. Really, this feature also promises the high resistance of the cryptosystem to brute-force attacks. On the other hand, the resulting cipherimage from a small changing in the encryption key must result in extremely different enciphered image. To test the high sensitivity of the proposed cipher to the modification of the secret key, the following steps are carried out:

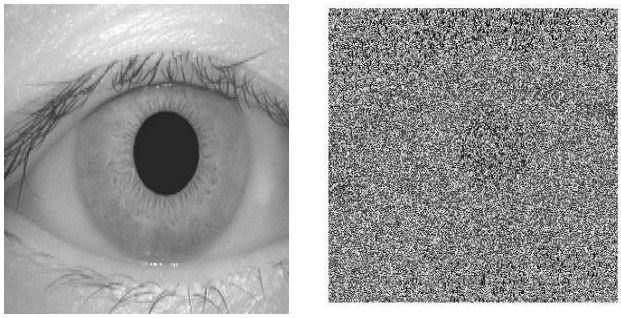
1) Use the secret key K_1 to encrypt the plainimage shown in Fig. 4(a) and the enciphered image is denoted by CI_1 as depicted in Fig. 4(b).
2) The same plainimage is enciphered again by the key K_2 where this key is different from the previous key K_1 in only the most significant bit. The resulting image CI_2 is displayed in Fig. 4 (c).
3) Finally, the same image is enciphered again by the key K_3 where this key is different from K_1 in only the least significant bit. The resulting image CI_3 is illustrated in Fig. 4 (d).
4) Compare the enciphered images CI_1, CI_2 and CI_3 to find their differences.

Fig. 4 shows the plainimage and the three corresponding cipherimages produced from the applications of the aforementioned steps. To computationally compare these encrypted images, the correlation between each pair of them is evaluated. Table 5 lists the obtained results for correlation. It is obvious that modifying only one bit of the secret key yields entirely distinct enciphered images with insignificant correlation between them.

Table 5: C.C analysis obtained for encryption by slightly different secret key.

Image1	Image2	Correlation coefficient
Enciphered image CI_1	Enciphered image CI_2	0.0017
Enciphered image CI_2	Enciphered image CI_3	0.0655
Enciphered image CI_3	Enciphered image CI_1	-0.0017

a) Original image **b) Enciphered image CI_1**



c) Enciphered image CI_2 **d) Enciphered image CI_3**

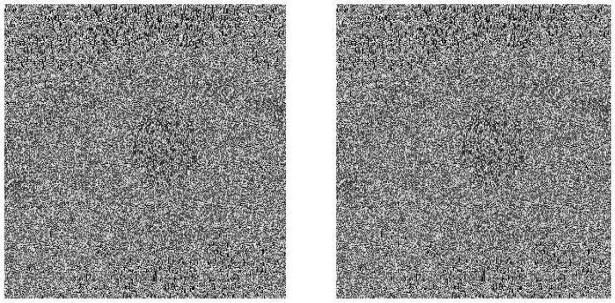
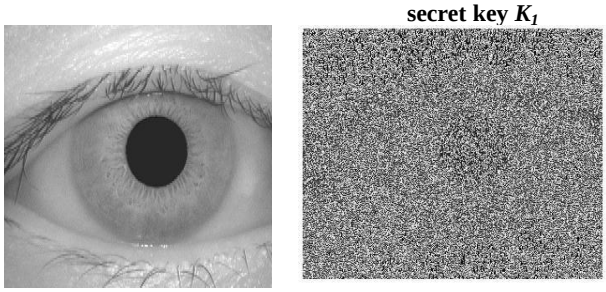


Fig. 4: Key sensitive

Moreover, the attempt to restore the original image from the enciphered one with slightly different key fails. Particularly, Fig. 5 (a) and Fig. 5 (b) illustrate the original plainimage and the associated enciphered image obtained by the secret key K_1, respectively, whereas Fig. 5 (c) and Fig. 5 (d) depict the recovered images from the decryption procedure with a correct key K_1 and a slightly different key K_2, respectively. Obviously, the deciphering with a somewhat distinct key cannot succeed.

a) Original image **b) Enciphered image With secret key K_1**



c) Recovered image with Secret key K_1 **d) Recovered image by slightly different key K_2**

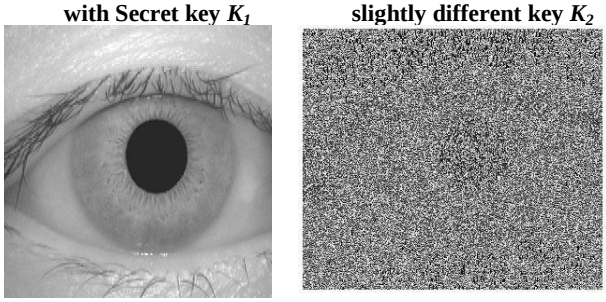


Fig. 5: Key sensitive test

4.3.2 Plainimage Sensitivity Analysis

Another requirement for a good encryption technique is its high sensitivity to tiny changes of the plainimage. To test the proposed algorithm in this direction, two criteria can be used. The first one is the Number of Pixels Change Rate (NPCR) and the second is the Unified Average Changing Intensity (UACI). Assume that P_1 and P_2 are two images with only one pixel different, and the secret key used is denoted by K, the following steps are employed:

1) Use the secret key K to encrypt the first plainimage P_1 displayed in Fig. 4(a) and the related enciphered image is denoted by C_1.
2) The same secret key K is used to encrypt the second plainimage P_2 which is different from P_1 in only one pixel. The resulting image is named C_2.
3) Finally, compute the values of UACI and NPCR according to the following equations[7-10]:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{|C_1(i,j) - C_1(i,j)|}{255}\right] \times 100\% \quad (18)$$

$$NPCR = \sum_{i,j}\frac{D(i,j)}{W \times H} \times 100\% \quad (19)$$

where W and H are the width and height of C_1 or C_2 and $D(i, j)$ is estimated as follows:

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{otherwise} \end{cases} \quad (20)$$

The test is performed on iris biometric image of size 280 x 320, and the result of NPCR estimator is found to be over 99.60%. Also, the value of UACI estimation is estimated to be over 33.46%. The obtained values for NPCR and UACI prove that the suggested cipher is strongly sensitive to changes occurred in the plainimage.

5. CONCLUSION

A novel methodology for securing digital images which utilizes two types of chaotic systems (Logistic map and Tent map) is proposed in this paper. The suggested scheme switches between the two chaotic systems based on cipherimage information. This switching is based on a chaos-feedback mechanism. The main feature of the proposed scheme lies on the utilization of a biometric secret image to drive an external secret key, which in turn deduces the control parameters of the maps. The cipher of each pixel relies on the secret key, the previous encrypted information and the yield of the Tent map or the Logistic map. The conducted experimental results illustrate that the encrypted image has a small correlations among neighbor pixels, nearly uniform image histogram (approximately random image). Moreover, the security analyses also confirm that the suggested cipher is especially sensitive to variations in the encryption key and the plainimage. Thus, the proposed scheme has a sufficient robustness against common attacks.

6. REFERENCES

[1] Z. H. Guan, F. Huang, and W. Guan. 2005. Chaos-Based Image Encryption Algorithm. Physics Letter A. vol. 346. pp. 153-157.

[2] S. Li, X. Zheng, X. Mou, and Y. Cai. 2002. Chaotic encryption scheme for real time digital video. Proceedings of the SPIE on electronic imaging. pp. 149-160. San Jose, CA, USA.

[3] Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, and Abd El Fatah .A. Hegazy. 2010. An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. IJCSNS International Journal of Computer Science and Network Security. VOL.10 No.2.

[4] G. Jakimoski and L. Kocarev. 2001. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. vol. 48, no. 2.

[5] H. El-din, H. Ahmed, H. M. Kalash, and O. S. F. Allah,. 2007. An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption. Informatica. vol. 31. pp. 121-129.

[6] M. S. Baptista. 1998. Cryptography with chaos. Phys. Lett. A. vol.240. pp.50-54.

[7] I. A. Ismail, M. Amin, and H. Diab. 2010. A digital image encryption algorithm based a composition of two chaotic logistic maps. International Journal of Network Security. vol. 11. no. 1. pp. 1-10.

[8] N.K. Pareek, Vinod Patidar, and K.K. Sud. 2005. Cryptography using multiple onedimensional chaotic maps. Commun. Nonlinear Sci. Numer. Simul. 10 (7) 715–723.

[9] Nitumoni Hazarika and Monjul Saikia. 2014. A Novel Partial Image Encryption using Chaotic Logistic Map. International conference on Signal Processing and Integrated Networks (SPIN).

[10] G. Chen, Y. Mao, and C.K. Chui. 2004. A symmetric image encryption based on 3D chaotic maps. Chaos Solitons Fractals. vol. 21. pp. 749-761.

[11] DeWang, and Yuan-Biao Zhang. 2009. image encryption algorithm based on s-boxes substitution and chaos random sequence. International Conference on Computer Modeling and Simulation.

[12] Pareek ,N. K., Patidar , V., Sud, .K .K. . 2006. Image encryption using chaotic logistic map. In Image and Vision Computing 24-926–934. Elsevier.

[13] Rajinder Kaurand Er.Kanwalprit Singh. 2013. Image Encryption Techniques:A Selected Review. IOSR Journal of Computer Engineering Vol. 9. No. 6. pp. 80-83.

[14] Ashwaq T. Hashim, Dr. Rasha Fahim Nathim, and Gaidaa Saeed Mahdi. 2014. Modification of RC5 Algorithm for Image Encryption. IJCCCE Vol.14. No.2.

[15] Abullah Sharaf Alghamdi, Hanif Ullah, Maqsood Mahumd and Muhammed Khurram Khan. 2009. Bio-Chaotic Stream Cipher – Based Iris Image Encryption. International Conference on Computational Science and Engineer.

[16] Z.Yun-peng, and Z. Zheng-jun. 2009. Digital Image Encryption Algorithm Based on Chaos and Improved DES. Proceedings of the IEEE International Conference on Systems. Man, and Cybernetics San Antonio. TX, USA.

[17] Muhammad Khurram Khan, and Jiashu Zhang. 2006. Implementing Templates Security in Remote Biometric Authentication System. IEEE Conf. Proceedings on CIS'06, China. pp. 1396-1400. vol.2.

[18] Fu, Ch., Zhang, Z., Chen, Z., and Wang, X. 2007. An Improved Chaos-Based Image Encryption Scheme. ICCS. Springer-Verlag. Berlin.

[19] Jiri Giesl, Ladislav Behal and Karel Vlcek. 2009. Improving Chaos Image Encryption Speed. International Journal of Future Generation Communication and Networking Vol. 2. No. 3.

[20] Zhai, Y., Lin, S., Zhang, and Q. 2008. Improving Image Encryption Using Multi-chaotic Map. Workshop on Power Electronics and Intelligent Transportationi System.

[21] National Institute of Standards and Technology. 2008. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Special publication 800-22. Revision 1.

[22] Bóna, and Miklós *2011,* A Walk Through Combinatorics (2nd ed.), New Jersey: World Scientific.

[23] CASIA Iris Database. [Online March, 2009] http://sinobiometric.com.