Journal of Engineering Science and Technology
Vol. 15, No. 5 (2020) 3013 - 3024

HYBRID CIPHERING METHOD BASED ON CHAOS LOGISTIC MAP AND FINGERPRINT INFORMATION

SALLY A. JERJEES[1,*], BASHAR A. ESTTAIFAN[2], TARIK Z ISMAEEL[3]

[1]College of Computer Engineering Department - University of Baghdad, Al-Jadirya, Baghdad, Iraq
[2]College of Electronic and Communication Engineering Department - University of Baghdad, Al-Jadirya, Baghdad, Iraq
[3]College of Electrical Engineering Department - University of Baghdad, Al-Jadirya, Baghdad, Iraq
*Corresponding Author: sally.jerjees@coeng.uobaghdad.edu.iq

Abstract

In modern era, which requires the use of networks in the transmission of data across distances, the transport or storage of such data is required to be safe. The protection methods are developed to ensure data security. New schemes are proposed that merge crypto graphical principles with other systems to enhance information security. Chaos maps are one of interesting systems which are merged with cryptography for better encryption performance. Biometrics is considered an effective element in many access security systems. In this paper, two systems which are fingerprint biometrics and chaos logistic map are combined in the encryption of a text message to produce strong cipher that can withstand many types of attacks. The histogram analysis of ciphertext shows that the resulted cipher is robust. Each character in the plaintext has different representations in the ciphertext even if the characters are repeated through the message. The strength of generated cipher was measured through brute force attackers, they were unable to deduce the key from the knowledge about pairs of plaintext- ciphertext due to the fact that each occurrence of characters in the message will have different shift value, and as a result a diverse representation will be obtained for same characters of the message.

Keywords: Chaos pseudo random bit generation, Ciphering, Fingerprint, Logistic map, Minutiae.

1. Introduction

Chaos systems are widely used with cryptography, whereas chaos maps had a great attention and are developed by researchers through many years ago. Characteristics of chaos maps are important and achieve requirements of cryptosystems. Shujun et al. [1] generated pseudo-random bit generator based on chaotic systems and used in many stream-cipher cryptography applications. Another pseudo-random Bit Generator based on chaotic logistic map is generated using two logistic maps and the generated stream passed all NIST tests [2]. Many encryption algorithms are developed based on chaos transformation. Rani et al. [3] proposed a symmetric encryption algorithm with logistic map and the resultant cipher can resist all types of cryptanalysis attacks. The other symmetric text encryption algorithm is proposed by Murillo-Escobar et al. [4], in which 128-bits are the secret key and two logistic maps are used to provide best optimized randomness sequence. The resultant cipher has strength to resist chosen/known plaintext attack. A text encryption scheme is proposed by Kumar et al. [5] based on the position substitution, shuffling and a diffusion processes. The scheme uses a Logistic map for matrix generation and position shuffling. When a single symbol is changed, the whole cipher text is affected. It is inferred that using chaos systems with cryptography either as a pseudo random bit generation or as nonlinear function involved with encryption process can produce powerful cipher that resists many different types of attacks. Encryption and decryption operations are used to ensure secrecy of information through unsecure communication channels. Secrete key schemes are widely used in data encryption [6]. Many new proposed methods are developed to increase security. Volos et al. [7] used chaos map to encrypt text message, due to the fact that characteristics of chaos systems are used to provide security requirements [8]. Zhang et al. [8], Priya et al. [9] and Nguyen et al. [10] used biometrics based encryption methods to resist many types of recognition systems attacks.

2. Chaos Logistic map

The logistic map is one of the many chaotic mapping functions; it is widely used in the chaotic cryptosystems. It is important to understand the characteristics and behavior of logistic map. It has a great sensitivity to the initial value and the iterative parameter must have a specific value to show chaotic properties [11], as shown in Fig. 1. The mathematical representation of logistic map is illustrated in Eq. (1).

$$X_{n+1} = r(X_n)(1 - X_n) \tag{1}$$

where X_n represents initial value, r is iteration parameter and X_{n+1} is the output of logistic map.

Jakimoski [12] proposed a block encryption cipher based on two chaotic maps which are exponential and logistic by using another method of creating S-boxes by involving chaotic maps. The authors claimed that their cipher is strong against attack except brute force attack. Another encryption method based on chaos and DNA was proposed by Babaei [13]. The authors chose logistic map because of its simple mathematical implementation, their proposed method were used for image and text encryption and they used DNA to encode the binary sequence of plaintext then using one time pad for encryption. The chaotic encryption algorithm proposed by Wang and Gu [14] used logistic map, in which the encryption key consists of a combination between logistic map output and plaintext, so that the encryption algorithm's security

is improved and strengthened. They declared that the only way to crack the cipher text is through using force-to-attack method. The proposed encryption system by Voloset al. [7] is used for encrypting text files. Two Logistic maps were used with different initial conditions and system's parameters, for achieving better randomness of the produced bits sequence. They used well-known statistical test suite which is FIPS-140-2 to test their generated binary sequence.

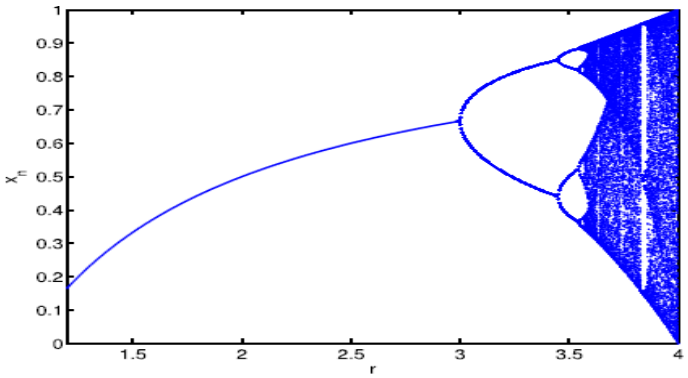


Fig. 1. Characteristics of logistic map [5].

3. Fingerprint Feature Extraction

Biometrics is widely used nowadays in the security systems. There are two types of biometrics: physiological and behavioural types [15]. Fingerprint is one of the known types of physiologic biometric. Fingerprints are unique for every person and are less life time distortion. A fingerprint image needs to be processed to override the problem of noise, scanner resolution, environmental circumstances and fingerprints poses [16]. Figure 2 shows the feature extraction processes which are used in this work.

Fig. 2. Feature extraction processes. [5].

3.1. Pre-processing

Enhancement of fingerprint image is necessary to improve quality of image and to reinforce regions between furrows and valleys of fingerprint ridges [17]. Fast

Fourier Transform (FFT) enhancement method and histogram equalization were used for this purpose. Enhancement and Binarization will be used as preprocessing techniques before feature extraction.

3.1.1. Fast Fourier transform (FFT) technique

The enhancement was done by dividing the image into blocks of size (32×32) pixels. FFT form is obtained for each block according to Eq. (2). Then the enhanced block would be computed as in Eq. (3). This filtering technique depends on enhancement of each block by its dominant frequency [18].

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-2j\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (2)$$

$$g(x,y) = F^{-1}\{F(u,v) \times |F(u,v)|^k\} \quad (3)$$

3.1.2. Histogram equalization

In this method the intensity of pixels is adjusted so that the contrast of fingerprint image is enhanced, such that the histogram of equalized image is more uniform distributed. The procedure of enhancement method is illustrated in Fig. 3.

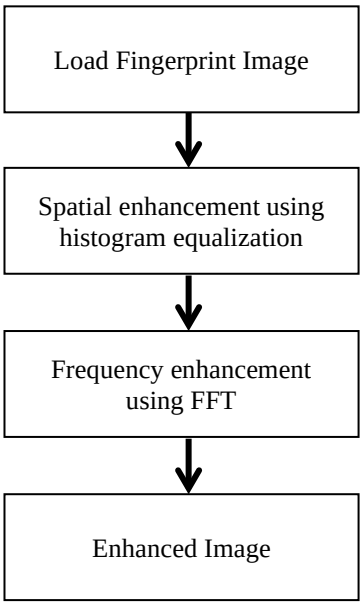


Fig. 3. Block diagram of image enhancement.

3.1.3. Binarization

Binarization is a method which is used to convert grey image of 256 levels into an image of only two levels [19]. This conversion is performed by dividing image into (16 ×16) pixels, and determines the mean value of each block, then the new pixels value is computed as in Eq. (4). The binarized image is obtained and ready to be used in the next stage of processing.

$$I_B(x,y) = \begin{cases} 1 \; if \; I(x,y) & \geq threshold \\ 0 & otherwise \end{cases} \quad (4)$$

3.2. Feature extraction

The main prosperity of biometrics is their unique information that extracted using many different methods. Minutiae are the features of fingerprint biometrics. Many types of minutiae are there in a fingerprint but the most used types are: ending and bifurcation ridge type [20]. In order to obtain these minutiae Crossing Number (CN) method is used on a thinned image [21]. Thinning is a process of making the ridge to become one pixel width. It is implemented using MATLAB built-in function to obtain thinned image. The final step for indicating minutiae types is done by applying CN. The method includes sliding a square window of nine pixels over entire thinned image, the central pixel is ridge pixel and its value equals to one (black). The surrounding pixels are numbered from right counter clock wise and their values depend on the thinned image. Eq. (5) represents how CN values are calculated.

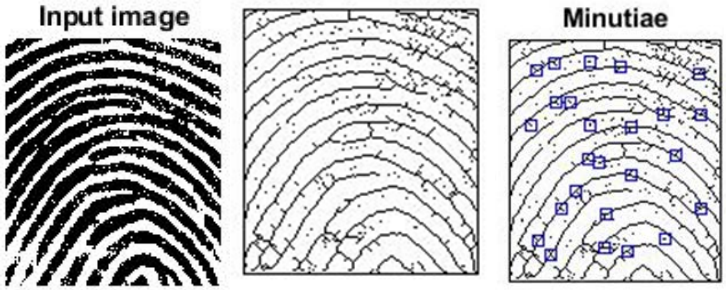
$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i-1}| \quad (5)$$

where P_i is eight neighbor Pixels of pixel P.

3.3. Post processing

The post processing operation is performed to eliminate any false and redundant minutiae which do not have any useful usage. The elimination is achieved by using threshold value and compares the spatial distance between two minutiae points if the distance less than threshold then these minutiae points are neglected, if the distance is greater or equal to the threshold then the minutiae points are considered. The spatial distance is calculated using Eq. (6). The results of feature extraction are illustrated in Fig. 4.

$$d = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2} \quad (6)$$



(a) Binarized image, (b) thinned image (c) minutiae points

Fig. 4. Fingerprint image processing.

4. Proposed Method

The new proposed method depends on both biometrics and chaos systems in ciphering and producing strong encryption key, so that the resulted cipher is robust. The secrete key consists of merging between minutiae points positions and output of two chaos logistic maps as shown in Fig. 5. The key is random due to the fact that it does not submit to any equation and the minutiae distribution of each fingerprint is in a scattered manner and different. Logistic map has three parameters and is very sensitive to the initial value so that it is preferable in cryptography.

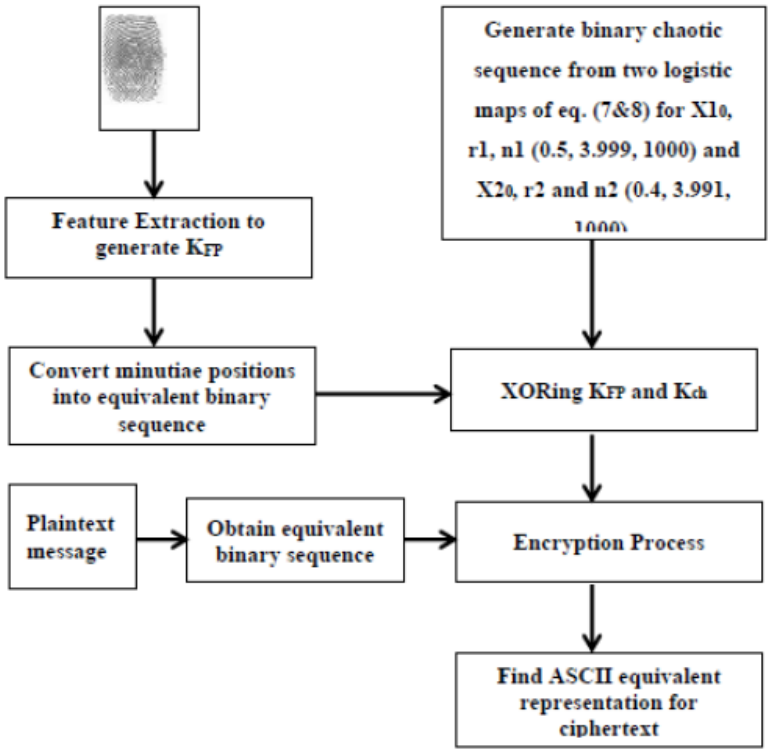


Fig. 5. Block diagram for generation of key and ciphertext.

The proposed method will be explained in the following steps:

Step (1): Input fingerprint image with size (M, N) pixel and message (M_{ss}) with length L_{ss} characters.

Step (2): Add signature (with length L_{ds}) to the end of the message (M_{ss}), the total length will be ($L_{ss} + L_{ds}$) characters.

Step (3): Enhance image to remove noise.

Step (4): Extract features from enhanced image where mp (i) is a minutiae point represented by x_i, y_i, Θi position where i= 1…L_{mp} and L_{mp} is the total number of minutiae extracted from fingerprint.

Step (5): Two logistic maps will be used and represented in the Eqs. (7) and (8):

$$X1_{n+1} = r_1 \times X1_n(1 - X1_n) \quad (7)$$

$$X2_{n+1} = r_2 \times X2_n(1 - X2_n) \quad (8)$$

Both $X1_n$ and $X2_n$ are the initial values and equal to $X1_0$=0.5 and $X2_0$=0.4. r_1 and r_2 are the iteration parameters and equal to r1= 3.999 and r2= 3.991.

Step (6): Obtain pseudo random bits by calculating the mean value ($\bar{x}$) for the outputs of two logistic maps and then compare output of each map with the mean value according to the following equation

$$b_n = \begin{cases} 0 \; if \; x_n \leq \bar{x} \\ 1 \; if \; x_n > \bar{x} \end{cases} \tag{9}$$

where $\bar{x}$ is the mean value, b_n is the bit generated from the logistic map after n-th iterations. The outputs of two maps will be **XORed** for good randomness sequence.

Step (7): XOR operation is done between binary sequence that is generated from CPRNG and binary sequence of minutiae positions to produce the binary key which will be used for encryption.

Step (8): The encryption is done by XORing plaintext (message) with key obtained from previous step. The final ciphertext is obtained by converting each decimal numbers to its ASCII representations.

For decryption, the recipient obtains the key that embedded in the random text, which also contain the ciphered message. This key is an index for the fingerprint used in encryption. The previously mentioned steps are followed to extract the plaintext (original message). As illustrated in Fig. 6.

The encryption time in proposed method is more than that of location based method. This is due to the shift operation and LUT, but Pal et al. [22] used XOR operation which is simplest than other operations. Our method need more time to be broken using Brute Force Attacks (BFA). Also, ciphertext entropy is better in the proposed method.

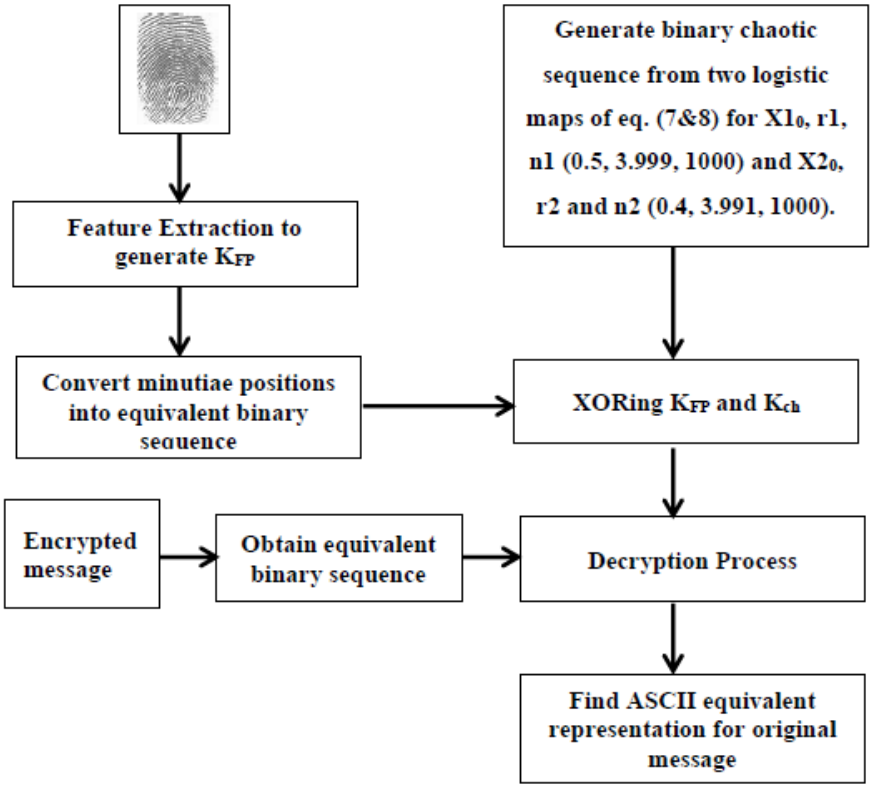


Fig. 6. Block diagram for decryption process.

5. Results and Discussion

The simulation results of an image processing methods were illustrated in Fig 4. Table 1 shows how the key is calculated and the ciphering will be obtained. The strength of the proposed method depends on biometrics and parameters of logistic map so that the attackers must try all possible combination of minutiae and chaos parameters in order to extract the message. One fingerprint may be used, but multiple fingerprints if used will increase ambiguity and enhance security for this method. While the reconstruction of original message were obtained by applying decryption process as shown in Table 2. Table 3 shows incorrect ciphers that are obtained when using incorrect fingerprint image or incorrect logistic map initial condition and iteration parameter. The brute force attackers will try the following computations which are infeasible to be implemented.

($X1_0$, r1 and n1)= [0, 1]* [3.999, 4.0]* [1:10000000]

($X2_0$, r2 and n2)= [0, 1]* [3.991, 4.0]* [1:10000000]

Table 1. Generated key and encryption process.

Plaintext	"Hybrid Encryption Method "
Decoded plaintext to binary	01001000, 01111001, 01100010, 01110010, 01101001, 01100100, …
Minutiae points	M1(91,20), M2(14,28), M3(65,28), M4(157,32), M5(15,35), …
Minutiae key	01011011, 00010100, 00001110, 00001100, 01000001, 00011100, …
Binary Chaos key	01000010, 00110110, 00011000, 11101001, 10100001, 10100100, …
Chaos key XORed by minutiae binary key	00011001, 00100010, 00010110, 11110101, 01110000, 10111000, …
Ciphertext (key XORed with plaintext)	01010001, 01011011, 01110100, 10000111, 10001001, 11011100, …
ASCII Encoding of ciphertext	Q[tŕ%Ü§F¿GÊE□RSÜ?dx…

Table 2. Reconstruction of original message and decryption process.

Ciphertext	Q[tŕ%Ü§F¿GÊE□RSÜ?dx…
Decoded ciphertext to binary	01010001, 01011011, 01110100, 10000111, 10001001, 11011100, …
Minutiae points	M1(91,20), M2(14,28), M3(65,28), M4(157,32), M5(15,35), …
Minutiae key	01011011, 00010100, 00001110, 00001100, 01000001, 00011100, …
Binary Chaos key	01000010, 00110110, 00011000, 11101001, 10100001, 10100100, …
Chaos key XORed by minutiae binary key	00011001, 00100010, 00010110, 11110101, 01110000, 10111000, …
Plaintext (key XORed with ciphertext)	01001000, 01111001, 01100010, 01110010, 01101001, 01100100, …
ASCII Encoding of Plaintext	"Hybrid Encryption Method "

Table 3. Incorrect cipher for different cases of plaintext 'Fingerprint'.

Correct fingerprint and correct chaos parameters	' _Kx' …Ê÷q¶£XØ '
Incorrect image with correct chaos parameters	' 8RÔš ØÃws_¶Î¤äÞ '
Correct image with incorrect initial condition of first LM	' _ïÚ\q:ê;V}iŒxÞ '
Correct image with incorrect iteration parameters of first LM	' c{IFÛ R^- ääÏ ¾'
Incorrect fingerprint and incorrect chaos parameters	' 1 4EjÜ ßƊ]ðsy‡ '

Figures 7 and 8 show histogram of original message characters and the message encrypted form. From the diagram it can be inferred that the histogram has flat distribution, and this means that each character of plaintext has different mapping in ciphertext at each occurrence. For this reason cryptanalytic attacks are unable to estimate and conclude the plaintext from given ciphertext. It is necessary to compare the performance of the proposed method with other methods to specify the points of weakness and strength. For this purpose, text encryption method that proposed by Pal et al. [22] is used. Authors used fingerprint with location of sender and recipient to generate the encryption key. Table 4 shows differences in some features between location-based method and the proposed method in this paper.

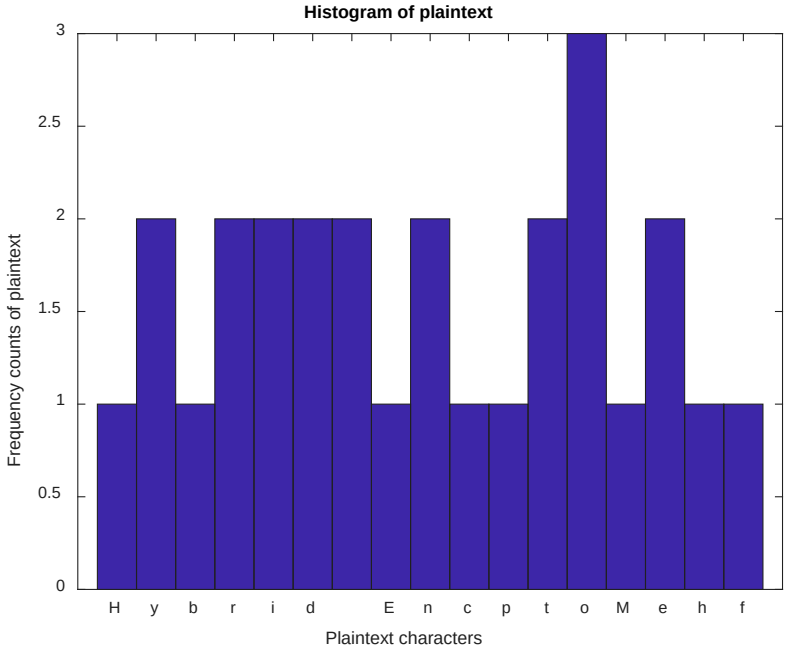


Fig. 7. Histogram of plaintext.

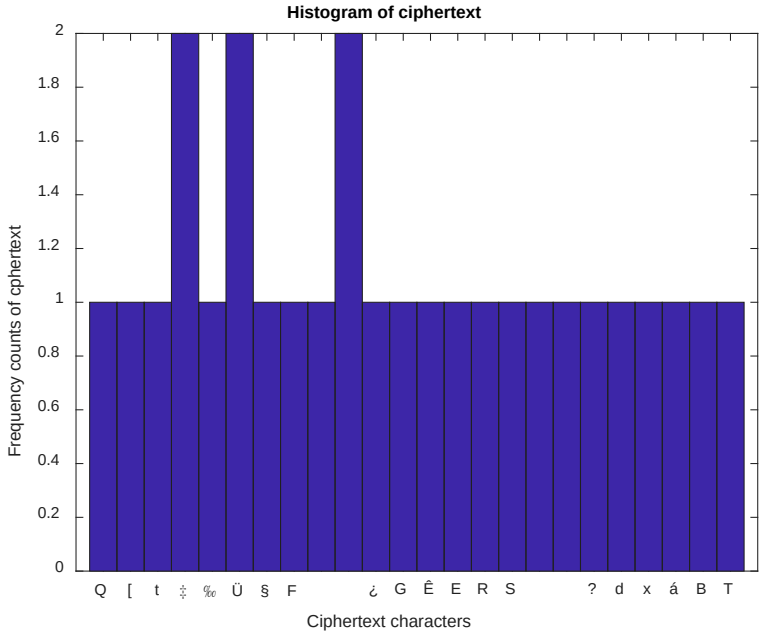


Fig. 8. Histogram of ciphertext.

Table 4. Comparison of proposed method with location based and fingerprint biometric method.

	Encryption Methods	
Feature	**Proposed Fingerprint based Encryption Method**	**Location based and Fingerprint Biometric Method**
Key Type	Symmetric	Symmetric
Key Length	Variable 16×32= 512	Constant 8×54=432 bit
Key Feature	Not repeated	Repetition
Encryption Type	Block of size 1 byte	Stream
Encryption Time	0.067039 second	0.015081 second
Entropy	4.4366	4.3219
Encryption Operation	Shift operation	Xor operation
BFA Time	5.9×10^{129} year	4.88×10^{105} year

6. Conclusion

Simulation results show that the encrypted message is hard to be broken, and the secret key is very strong. The generated key consists of merging between characteristics of chaos and biometrics. So that the construction of the key requires not only to estimate the fingerprint minutiae but also needs to estimate chaos parameter. Brute force attacks are computationally infeasible because any fingerprint except the previously used will give incorrect minutiae set. Beside that the chaos maps have high precision and sensitivity towards initial condition.

Nomenclatures

b_n	Bit generated from the logistic map after n-th iterations
d	Euclidian distance
I_B	Binary Image
$F(u,v)$	Function in frequency domain
$f(x,y)$	Function in time domain
$g(x,y)$	Function in time domain after inverse of Fourier
K_{ch}	Key generated from chaos logistic map
K_{FP}	Key generated from fingerprint
k	Variable measured by experiments
n	Number of iterations
P_i	Neighbour pixels
r	Iterative parameter
$\bar{x}$	Mean value
X_n	Initial value
X_{n+1}	Output of chaos

Abbreviations

CN	Crossing number
CPRNG	Chaos pseudo random number generation
FFT	Fast Fourier transform
FIPS- 140-2	Federal Information Processing Standard
MSG	message
NIST	National Institute of Standards and Technology

References

1. Shujun, L.; Xuanqin, M.; and Yuanlong, C. (2001). Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. *International Conference on Cryptology in India, Springer-Verlag Berlin Heidelberg*, 316-329.
2. Patidar, V.; Sud, K.K.; and Pareek, N.K. (2009). A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Informatica*, 33(4), 441-452.
3. Rani, P.J.; and Bhavani, S.D. (2012). Symmetric encryption using logistic map. *2012 1st International Conference on Recent Advances in Information Technology (RAIT)*, 1-5.
4. Murillo-Escobar, M.A. ;.Abundiz-Perez, F.; Cruz-Hernandez, C.; and Lopez-Gutierrez, R.M. (2014.). A novel symmetric text encryption algorithm based on logistic map. *Proceedings of the 2014 International Conference on Communications, Signal Processing and Computers*, 32.
5. Kumar, M.; Kumar, S.; Budhiraja, R.; Das, M.K.; and Singh, S. (2017). A cryptographic model based on logistic map and a 3-D matrix. *Journal of Information Security and Applications*, 32, 47-58.
6. Paar , C.; and Pelzl, J. (2009). *Understanding cryptography*. Springer Science & Business Media.

7. Volos, C.; Kyprianidis , I.; and Stouboulos, I. (2013). Text encryption scheme realized with a chaotic pseudo-random bit generator. *Journal of Engineering and Technology Review*, 6(4), 9-14.
8. Zhang, M.; Zhang, J.; and Zhang, Y. (2015). Remote three-factors authentication scheme based on fuzzy extractors. *Security and communication networks*, 8(4), 682-693.
9. Priya, S.S.S.; Karthigaikumar, P.; and Mangai, N.S. (2014). Mixed random 128 bit key using finger print features and binding key for AES algorithm. *Proceedings of IEEE 2014 International Conference of Contemporary Computating and Informatics (IC31)*, 1226-1230.
10. Nguyen, T.H.; Wang, Y.; Nguyen, T.N.; and Li, R. (2013). A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm. *International Conference on Signal Processing, Communication and Computing (ICSPCC 2013). IEEE*, 1-6.
11. Arroyo, D.; Alvarez, G.; and Fernandez, V. (2008). On the inadequacy of the logistic map for cryptographic applications. arXiv preprint arXiv:0805.4355.
12. Jakimoski, G. (2001). Chaos and cryptography : Block encryption ciphers based on chaotic maps. *Ieee Transaction and Systems*, 48(2), 163-169.
13. Babaei, A.M. (2013). A novel text and image encryption method based on chaos theory and DNA computing. *Natural Computing, Springer Science+ Business Media B.V*,12(1), 101-107.
14. Wang , A.X.; and Gu, S. (2014). New chaotic encryption algorithm based on chaotic sequence and plain text. *IET Information Security*, 8(3), 213-216.
15. Bhattacharyya, D.; Ranjan, R.; Alisherov, F.; and Minkyu, C. (2009). Biometric authentication : A review. *International Journal of u- and e- Service Science and Technology*, 2(3), 13-28.
16. Jayapal, R. (2017). *Biometric encryption system for increased security*. M.Sc. Thesis, University of North Florida.
17. Arora; K; and Garg, P. (2011). A quantitative survey of various fingerprint enhancement techniques. *International Journal of Computer Applications*, 28(5), 24-29.
18. Aguilar, G.; Sanchez, G.; Toscano, K.; Salinas, M.; Nakano, M.; and Perez, H. (2007). Fingerprint recognition. *Second International Conference on Internet Monitoring and Protection, ICIMP*,IEEE, 32-32.
19. Bhowmik, P.; Bhowmik, K.; Azam, M.N.; and Rony, M.W. (2012). Fingerprint image enhancement and its feature extraction for recognition. *International Journal of Scientific & Technology Research*, 1(5), 117-121.
20. Zhao, F.; and Tang, X. (2007). Preprocessing and post processing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition*, 40(4), 1270-1281.
21. Chaudhari, A.S.; Patnaik, G.K.; and Patil, S.S. (2014). Implementation of minutiae based fingerprint identification system using crossing number concept. *Informatica Economica*, 18(1), 17-26.
22. Pal, R.; Bhartia, O.; and Sen, M. (2019). *A cryptographic algorithm using location based service and biometrics*. Springer Singapore.