Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 9, September 2019, pg.172 – 181

Retina Random Number Generator for Stream Cipher Cryptography

Murooj Aamer Taha[1]; Naji Mutar Sahib[2]; Taha Mohammed Hasan[3]
Department of Computer Science, College of Science, University of Diyala, Iraq
murooj.aamer.taha@gmail.com; al.sehib@sciences.uodiyala.edu.iq; dr.tahamh@sciences.uodiyala.edu.iq

Abstract— Biometric is the measurement of behavioral and physiological characteristics for the human, generally used either for identification or verification, but it is also can be used as a key for different security applications. Among different biometric characteristics such as ears, voice, fingerprint, face, retina, iris, palm print, hand geometry, etc., the retina biometric can provide a higher level of security because of its inherent robustness. The main aim of this paper is to design and build a pseudorandom number generator based on the retina for stream cipher cryptography. The proposed system is based on the use of hybrid technology that consists of the characteristics of human retina and logistic functions to generate keys with high-quality specifications in terms of unpredictability, randomization, and non-re-generation. The NIST Package and correlation statistical tests prove that the generated keys are random, unpredictable, uncorrelated, and robust against different kinds of attack. The retina image keys are capable of passing most of the NIST statistical tests with high success rates also the average security test prove that the encrypted text is secure against entropy attack.
Keywords— Retina, Random number generator, Logistic function, Linear interpolation

I. INTRODUCTION

Biometrics is a term for body measurements and calculations. It indicates to metrics related to the individual's characteristics. The biometrics authentication is employed in computer science as a fashion of identification and access control. Also, it is used to identify persons in groups that are under control [1]. With the rapid growing of the E-crimes and the related cases, diffusing a reliable user authentication system that became an important job for securing user's private data and access control. People characteristics like voice, face, iris, retina, signature, and other features supply a dependable level of security to public and personal utilize. For a long time, different biometric authentication systems have been used. Because of the uniqueness of human biometrics that taken the main role in decaying imposters' attacks. These models of authentication have beat other conventional security systems such as PIN number and password [2].

Due to computer security, there is an increasing interest in the generating of a random key for digital signatures, cryptography, and protected communication protocols. Stream ciphers are fast cryptographic primitives to provide confidentiality of electronically transmitted data. They can be very suitable in environments with restricted resources, such as mobile devices or embedded systems. Actually, the stream cipher security completely bases on the key stream. stream ciphers security depend entirely on the "suitable" key stream S0, S1, S2,….. . while randomness plays a main role, so the random number generator (RNG) are significant for that purpose[3].The random bit sequence can be taken out from biological data and because of the uniqueness of biometrics; it is very hard to generate the duplicate [4]. Due to using biometric as seeds for pseudorandom number generators or, directly, like random number sequences, this would eliminate the security problems that arise when anyone utilizes software random generators on the basis of the content of the input/output buffers, the system clock, et cetera. due to their disadvantages versus intruder's attacks [5].

The retina as a biometric has specific priorities when compared to other biometrics. It is so secure and utilizes a stable physiological feature. It is so hard to fraud. Retinal patterns are variant for right and left the eye. They are different even for

© 2019, IJCSMC All Rights Reserved

identical twins. Further, retinal patterns do not alter with age. Opposite other biometric behaviors, the image will not sign on the retina for a dead person. As the retina is current deep within a person's eyes it is very unlikely to be damaged by any temporal or environmental conditions. So retina is an important biometric feature for highest security systems [6]. The biometric data can be utilized to seek the randomness of the biometric data in order to utilize them after the codification in the format of integer or bit like random number sequences. The biometric data generate robust random numbers [7].

In this paper, a pseudorandom number generator has been designed and built (based on the characteristics of human retina and logistic functions) for text encryption. This paper consists of the following sections; the related works are explained in the second section, the third section defines and explains the basic concepts and related subjects of logistic function, the fourth section presents the design of the proposed system, experimental results are explained in section five, the last section presents the conclusions of this work and recommendations for future works.

II. RELATED WORKS

Biometric-based random number generator systems for security applications have been heavily studied and improved for overcoming the drawbacks of traditional systems. H. Zhu et al. [8] presented a random number generator system based on the unique randomness of the human iris and chaotic function. In this system, the chaotic function is used for eliminating a similar pattern in the iris of the same person to obtain the unpredictable random sequences. S. Gerguri et al. [9] presented a random number generation system from repeated measurements of fingerprints as an alternate system to the proposed biometrics systems in cryptography application, and for analyzing its properties. This system could supply a worthy source of randomness in mobile devices equipped with a scanner for fingerprints. S. Barman et al. [10] proposed a key generation system based fingerprint for cryptographic application. The features of the fingerprint are extracted from a fingerprint image to be processed for deriving a cryptographic key. This generated key is utilized for encrypting the message. At the time of message decryption, the key is regenerated from a fresh sample of the same fingerprint. The generated key can be revoked if needed and it does not reveal exact information about features of fingerprint as the key noninvertible. P. Yankanchi and S. A. Angadi [11] proposed a steganographic system based on one of the biometric traits i.e. Hand geometry. The features are extracted from hand images of individuals and by utilizing these features unique key is generated. This generated key is employed to find a particular pixel position from which, for embedding the secret data in the least significant bits of the cover image. The embedded secret message is extracted from the stego-image by utilizing the generated unique key. R. Dwivedia et al. [12] presented a biometric system based a fingerprint for secure communication. This system provides a framework for secure communication between two users utilizing fingerprint. The algorithm of Diffie Hellman (DH) is utilized for generating public keys from private keys of sender and receiver that are shared and further utilized for producing symmetric cryptographic key at both ends. In this system, the revocable key for symmetric cryptography is generated from the irrevocable fingerprint.

Most of these related systems used the biometrics features as a direct source for key generation, and that lead to making these systems are not able to satisfy the terms unpredictability, randomization, and non-re-generation. Therefore, the proposed system is based on the use of hybrid technology includes the human retina and logistic functions to generate keys with high-quality specifications of the required terms.

III. STREAM CIPHER CRYPTOGRAPHY

Stream ciphers are fast cryptographic primitives to provide confidentiality of electronically transmitted data. They can be very suitable in environments with restricted resources, such as mobile devices or embedded systems. It is depend on the thought of the one-time pad (OTP) cipher, which known as Vernam cipher. OTP uses a whole random keystream, and every digit of the keystream is jointed with one digit from the plaintext to create a digit of ciphertext. The keystream digits have to be totally random, and furthermore, the keystream must own the same length such as the plaintext.[3][13]

IV. AVARAGE SECURETY

It is also called Information Entropy Analysis; in the study of statistical analysis, the Information Entropy factor is used to measure the secure value of a cipher. A secure cryptosystem should be performing a condition on the information entropy that is the ciphertext should not provide any information about the plaintext[14]. Secrecy of ciphers is calculated in terms of the key equivocation (conditional entropy of key given cipher)[15]:

$$H(^{k}/_{c}) = \sum_{j=1}^{L} \quad \sum_{i=1}^{n} \quad q_i P_{ij} \log P_{ij}$$

where,
q_i = Pr (C = ci)
P_{ij} = Pr (K= ki/C = ci)
L = The key length
n = The cipher text length

V. LOGISTIC FUNCTION

The logistic map is usually used in most of pseudorandom generators and cryptosystems. It is employed in the chaos-based secure communication system and for the generations of binary numbers [16]. In 1976, (Robert May) mentioned that the logistic map instructs to the chaotic dynamics. Logistic maps are polynomial maps. It is frequently cited as a symbol of how complex behaviors can rise from so simple nonlinear dynamical equations. it is a one-dimensional map that utilizes to shape easy nonlinear discrete systems. It clarifies by a recursive function as follows:

© 2019, IJCSMC All Rights Reserved

$$x_{n+1} = f(x_n, \lambda) = \lambda x_n(1 - x_n),\ \lambda \in R^+, x_n \in [0,1] \quad (1)$$

wherever λ is the fertility coefficient or population growth rate and x_nis a relative population size in a discrete-time instant n [17]. Precisely, the applications of the logistic map have grown during the last years, for example, in fields as chemistry, biology, physics, image transfer and secure data, random number generators for chaos-based communication, financial modeling, circuit applications, traffic, and business cycle theory . Where $0 \leq x_n \leq 1$ and $0 \leq \lambda \leq 4$. The chaotic behavior is achieved with $3.57 < \lambda \leq 4$ as shown in Figure 1 [18].

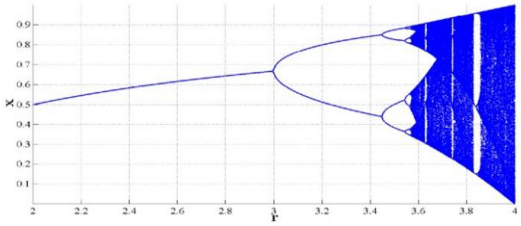


Fig. 1. The bifurcation diagram of the 1D logistic map [44].

VI. The Proposed Key Generation System

In the proposed system, firstly, the retina image is loaded from the database and then the key will be extracted based on several stages, figure 2 illustrates the overall retina based pseudorandom number generator system. Figure 3 illustrates the first three stages of the proposed system.

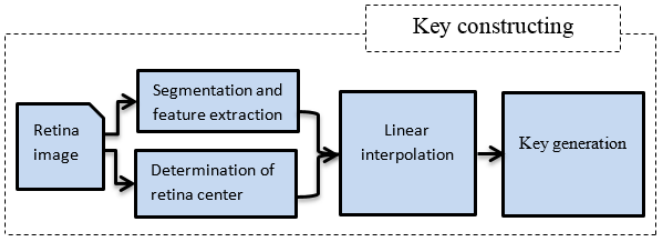


Fig. 2. The structure of retina based pseudorandom number generator system.

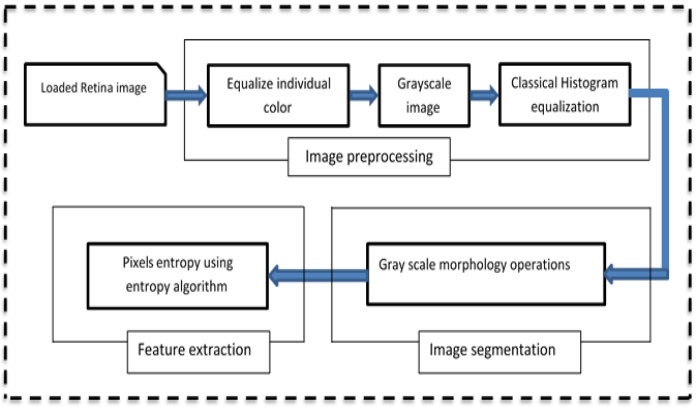


Fig. 3. The block diagram of the retina image preprocessing, segmentation and feature extraction stages.

A. Retina Image Preprocessing Stage

In this stage, the loaded retina image is preprocessed using the following steps;

- ***Step1: Equalize individual color***. The pixel is represented with three ingredients, i.e. the amount of red, green, and blue which organize the presented color. The histogram equalization is performed in each of the three color elements separately. The procedure of color image equalization causes the local features of the image to become visible after equalization.
- ***Step2: Grayscale conversion***. The retina colored image is converted to the grayscale image to have minimal data because the domain of grayscale has one channel instead of three channels of a color domain that tend to fast processing and less influenced by the brightness that refers as noise in many cases.
- ***Step3: Classical histogram equalization (CHE).*** The CHE stretches the histogram over the total spectrum of pixels (0 – 255). It is a contrast enhancement process with the target to obtain a new enhanced image for the uniform histogram. The CHE attempt to create an output image which has a flat histogram, i.e., a regular distribution. A histogram merely plots the frequency at every grey-level exist from black (0) to white (255).

© 2019, IJCSMC All Rights Reserved

B. Retina Image Segmentation Stage

In this stage, the segmentation technique is presented using grayscale morphological operations. It is more simple and easy method than other segmentation methods. The grayscale morphological operations are dilation, erosion, opening, closing, and top and hat; in this search, only two operations are used opening, and top-hat with structure element shape as diamond and size 5×5. First opening operation is performed on the processed image which starts with the erosion operation, where the light regions which are less than the structuring element are removed. The operation of dilation which follows ensures that light regions that are larger than the structuring element retain their original size.

The gray image *I* is a function that it's domain is a subset of two-dimension digitized space *m*×*m*. For each point $p \in m \times m$, the translation of *I* by *p* is defined by:

$$(I)_p = \{\alpha + p | \forall \alpha \in I\} \qquad (2)$$

And the erosion and dilation by structuring element *J* are respectively offered by:

$$I \ominus J = minimum\{(I)_p | p \in J\}^{\underset{p \in J}{minimum}}(I)_p, \qquad (3)$$

$$I \oplus J = maximum\{(I)_p | p \in J\}^{\underset{p \in J}{maximum}}(I)_p. \qquad (4)$$

The opening can be defined as the dilation of the erosion of the set *I* by the structuring element *J*:

$$I \circ J = (I \ominus J) \oplus J \qquad (5)$$

Opening removes small objects from the foreground (commonly taken as the dark pixels) of an image, placing them in the background. Secondly, perform image subtraction operations on the image for better foreground extraction. Finally, the morphological top-hat operation is performed. White top-hat computes the morphological opening of the image and then subtracts the result from the original image (after processing) to extract the white image reigns. The white top-hat transform is offered by:

$$Top - Hat(I) = I - (I \circ J) \qquad (6)$$

C. Retina Image Feature Extraction Stage

The main goal of this stage is to extract some important features of the retina image. Entropy algorithm is used for analyzing the human retina patterns and extracting features from them. Entropy is used to measure the amount of information. Entropy is defined in terms of the probabilistic behavior of a source of information.

After the retina image is preprocessed and segmented, the image will be input for the entropy algorithm. The entropy algorithm will extract the pixel entropy feature, as in the following steps;

- ***Step 1:*** Find the histogram for the input retina image.
- ***Step2:*** Normalize the histogram and calculate the entropy function in the range of (0-255).

  Consider *m*×*m* image *I* with gray $\{x_1, x_2, \ldots, x_j\}$. If the probability of every pixel value x_i in image f is $p(x_i)$. Then, the amount of information included within every pixel can be represented like this:

$$h(x_i) = -p(x_i) \times \log p(x_i) \qquad (7)$$

  for an image *I*, the total amount of information will be gotten as follows:

$$H(I) = -\sum_{i=1}^{j} h(x_i) \qquad (8)$$

- ***Step 3:*** Compute the new histogram for the results of the entropy function.
- ***Step 4:*** Equalize the histogram and take the maximum entropy value from the result.

D. Retina Center Determination Stage

The traditional Canny edge detector goal is to detect edges even in images that are intensely contaminated by noise. It smooth image using one mask Gaussian filter. Adaptive Canny Edge Detection (ACED) goal is to find the important points in retina vessels and this is achieved using two kernels. The required steps are as follows;

- ***Step1:*** Convert the color image to grayscale image, then to remove the noise, 2D Gaussian filter will be performed; the first mask parameter is segma1=2, then with the second mask and its parameter segma2=2, then the gradients GX, GY, and the magnitude will be computed.
- ***Step2:*** Locate the theta as theta1=2, theta2=0 in order to highlight regions with high spatial derivatives.

© 2019, IJCSMC All Rights Reserved

- ***Step3:*** Locate the threshold parameter as alpha=0.7 to determine the final set of pixels. The pixels that are greater than the threshold will be determined as black and the pixels that are lower than the threshold will be determined as white.
- ***Step4:*** Apply linear interpolation between maximum x, y, and minimum x, y, then the resulted x, y will represent the mid-point and its coordinate will be the center of the retina grid.

E. Linear Interpolation Stage

In this stage, the linear interpolation technique is used between retina center point and entropy points to generate new points whose coordinates locate the key values.

Linear interpolation is the simplest method of interpolation. It takes two data points to construct the value of new data points. Two data points in the coordinate frame that are given as (x_0,y_0) and (x_1,y_1) respectively. To find a function that represents these data points, the equation of a straight line can be used that represents a straight line drawn which passes through these two data points. The equation of a straight line is presented by:

$$f(x) = y = mx + c \qquad (9)$$

where m represents the gradient of the line and c represents the y-intercept of the equation, that is the value of y at $x = 0$, and are presented by the following equation:

$$m = \frac{(y_1 - y_0)}{(x_1 - x_0)} \qquad (10)$$

$$c = y_1 - mx_1 \qquad (11)$$

Next, to substitute the values of m and c and rearranging, the interpolating function $f(x)$ is written like:

$$f(x) = y = \frac{y_1 - y_0}{x_1 - x_0}(x - x_0) + y_0 \qquad (12)$$

F. Key Generation Stage

For key generation, the 1D logistic map is used which basically nonlinear and exhibit an apparently random behavior for values of the system. The logistic function produces truly unpredictable random sequences even if the initial conditions are known exactly. Matrix 64 × 64 is used to be filled by the 1 D logistic function values. The coordinates of the retina points (that generated in the linear interpolation step) will locate the key values in the chaotic matrix. Mod function is used for the coordinates of retina image points that exceed 64×64 to be compatible with the chaotic matrix. Each time the chaotic value is taken (as a key) new chaotic value will fill in its position and the chaotic matrix is rotated by 90 degrees anti-clockwise. This approach will overcome the similar patterns collected from the same retina image, so even if two pixels have the same intensity in the retina image, then the generated random sequence is absolutely different. Figure 4 illustrates an example of the key generation process.

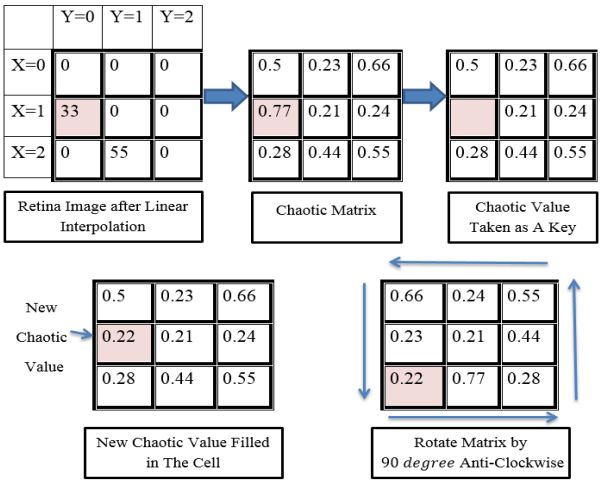


Fig. 4. An example of the key generation process.

G. Encryption using stream cipher

Encryption is the technique of encoding plain text into cipher text before transmitting it over channel for avoiding stealing of confidential data. A stream cipher encrypt bits individually at a time. The crypto-key that generated in(F)is converted to binary stream and xored with the plain text that will be converted to binary stream too. The output is ciphered secret message.

© 2019, IJCSMC All Rights Reserved

VII. EXPERIMENTAL RESULTS

The proposed system is tested on (DRIONS-DB) database [15]. The database contains 110 color digital retinal images. 124 eye fundus images are chosen randomly from an eye fundus image base which belonging to the Ophthalmology Service at Miguel Servet Hospital, Saragossa (Spain). For this first image base, whole these eye images (14 in total) that had some kind of cataract (moderate and severe) were eliminated and, in the end, it was acquired the image base with 110 images.

The results of the retina image preprocessing stage are demonstrated in figure 5.

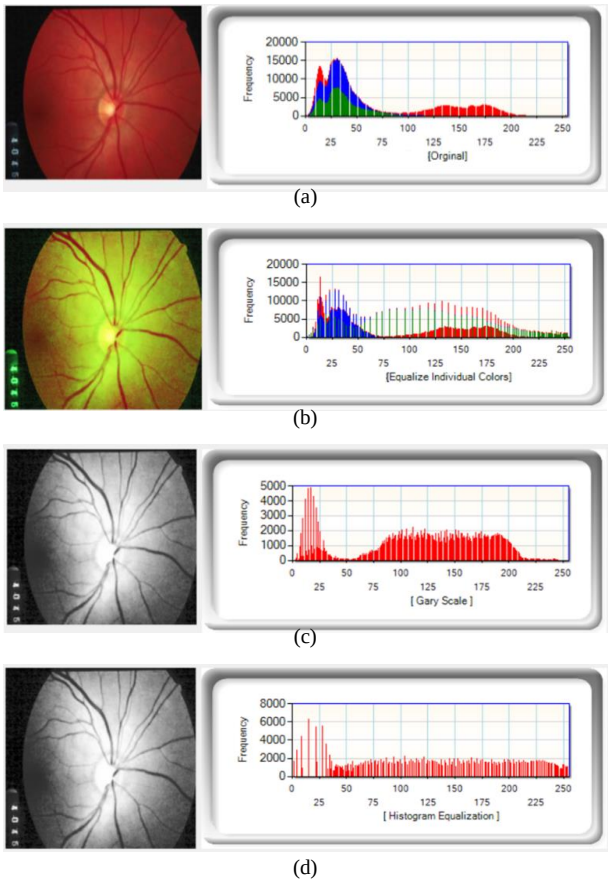
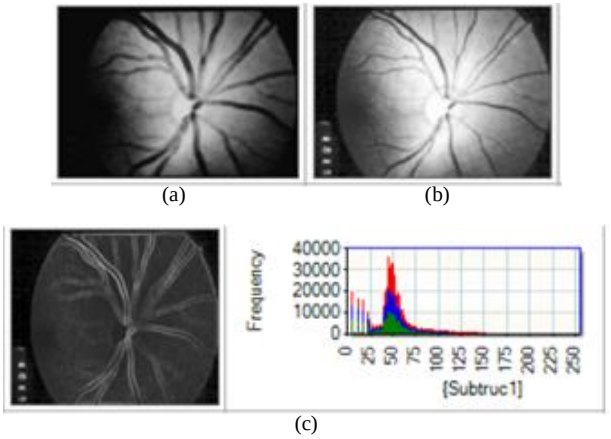
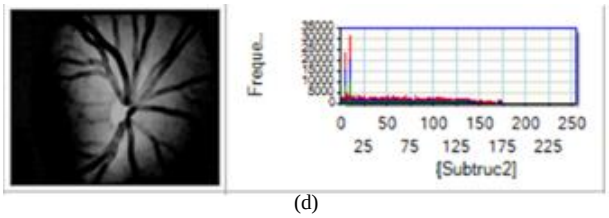


Fig. 5. The results (image and its histogram) of the first stage in the retina based key generation system, (a) The original loaded image, (b) Enhanced image with equalizing individual color method, (c) The grayscale image, (d) The grayscale image histogram equalization.

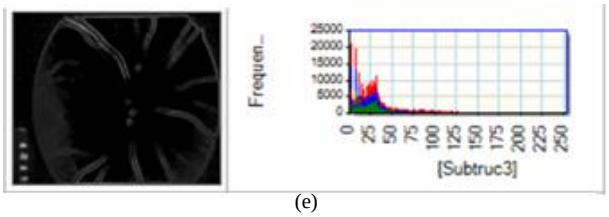
After the preprocessing stage, the resulted image is segmented using grayscale morphology operations. In opening operation, the white regions will be smoothed where light features which are smaller than the structuring element are removed as shown in figure 6 (b). For image enhancement, multiple subtractions will be performed on the image. In figure 6, the first subtraction: opening image (a) is subtracted from the preprocessing image (b) the result of subtraction is demonstrated in (c). Then, second subtraction is: image (a) is subtracted from (c) and the resulted image is shown in (d). The third subtraction is the opposite of the second subtraction and the result is shown in (e). The last subtraction is subtracting image (e) from (d). Finally, the white top-hat operation is performed to return the bright spots in the image which are smaller than the structuring. Figure 6 shows the overall segmentation stage results.



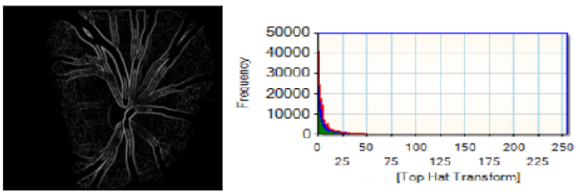
© 2019, IJCSMC All Rights Reserved



(d)



(e)



(f)

Fig. 6. Segmentation stage results using grayscale morphology.

In the stage of features extraction, the results of the pixel entropy feature using entropy algorithm are shown in figure 7.

	Size Entropy	Max Value
▶	Entropy 8	5.62305242068844
	Entropy 4	1.11571832537367

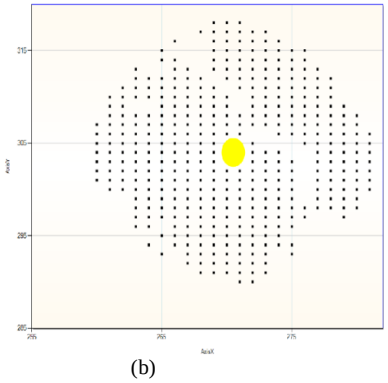
(a)

#	X	Y
1	220	67
2	221	68
3	194	69
4	222	69
5	195	70
6	222	70
7	196	71
8	223	71
9	197	72
10	224	73

(b)

Fig. 7. The results of the pixel entropy feature, (a) Table of calculated maximum entropy. (b) The coordinates of the final highest entropy pixels.

The center of the retina will be determined by; firstly, applying the ACED algorithm as shown in figure 8, secondly, linear interpolation technique is used between retina center point and entropy points to generate new points whose coordinates locate the key values to present more randomness as shown in figure 9.



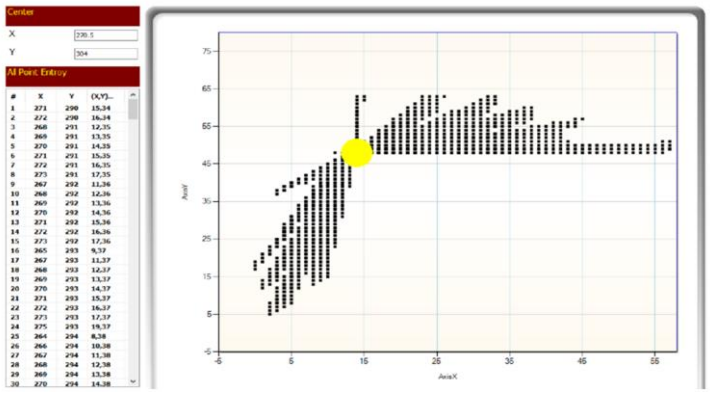
(a)

#	X	Y
1	271	290
2	272	290
3	268	291
4	269	291
5	270	291
6	271	291
7	272	291
8	273	291
9	267	292
10	268	292
11	269	292
12	270	292
13	271	292
14	272	292
15	273	292

(b)

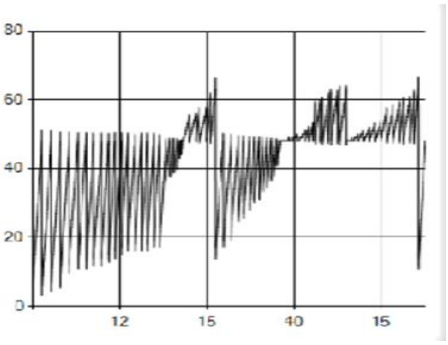
Fig. 8. ACED algorithm implementation. (a) The graph of (ACED) algorithm implementation, and retina center locating which represented by yellow color. (b) Retina points coordinates.

© 2019, IJCSMC All Rights Reserved



(a)

#	X	Y
1	2	5
2	2	6
3	2	7
4	2	8
5	3	8
6	3	9
7	3	10
8	3	11
9	3	12
10	4	12
11	4	13
12	4	14
13	4	15
14	5	15
15	5	16

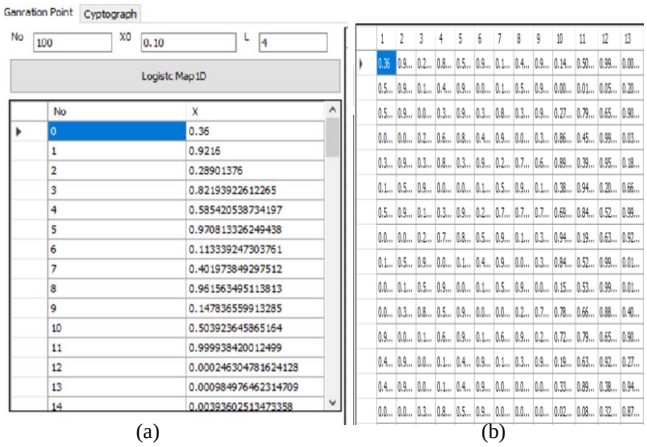


(b) (c)

Fig. 9. Linear interpolation process implementation. (a) graph of the linear interpolation process. (b) The new point coordinates that are generated, (c) The behavior and the distribution of the new points using the above approach.

In the final stage, the coordinates of the retina points that generated in the linear interpolation stage will locate the key values in chaotic matrix. The key is generated by using matrix 64×64 filled by the 1D logistic function values with initial value x=0.1 and the λ=4 as shown in figure 10 (a), (b). The coordinates of the retina points determine the key values in a chaotic matrix as shown in figure 10.

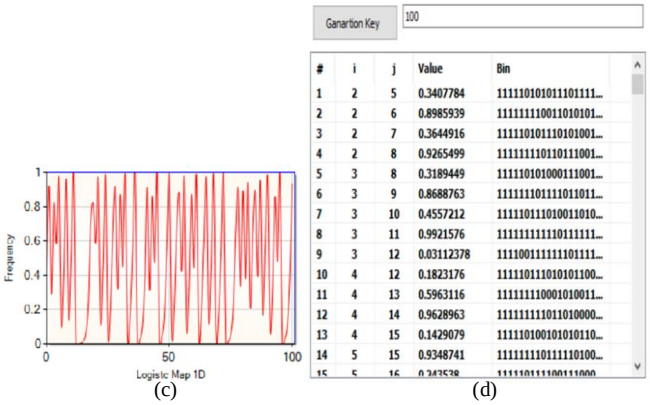
The NIST statistical tests are very useful for studying and estimating the randomness of the binary sequence created by the generator. So as to test the randomness of the keys that are created by the proposed retina image, NIST package is used. The results for (16) the statistical tests of the NIST are shown in table 1. The obtained results show that the generated keys are capable of passing the NIST statistical tests with high success rates. Table 2 shows a comparison between the proposed system and other related existing systems.



No	X
0	0.36
1	0.9216
2	0.28901376
3	0.82193922612265
4	0.58542038734197
5	0.9708133262494 38
6	0.113339247303761
7	0.401973849297512
8	0.961563495113813
9	0.147836559913285
10	0.503923645865164
11	0.999938420012499
12	0.000246304781624128
13	0.000984976462314709
14	0.003936025134733 58

(a) (b)

© 2019, IJCSMC All Rights Reserved



(c) (d)

Fig. 10. The generated key, (a) The numbers generated at the initial conditions of the logistic function. (b) Matrix 64 × 64 filled by the 1D logistic function values. (c) The distribution of the generated random numbers using the chaotic function system. (d) The coordinates of the retina points opposite the key values in the chaotic matrix..

TABLE I. NIST TEST RESULTS FOR THE GENERATED KEY.

Test Name	***Number of tests***	***Number of successes***	***Number of failures***	***Lowest success ratio***	***p-value >0.01***
Frequency	128	128	0	100%	1
Cumulative Sums	256	255	1	99%	0.592517
Runs	128	127	1	99%	0.609751
Longest Run of Ones	128	128	0	100%	1
Binary Matrix Rank	128	128	0	100%	0.39099
Spectral DFT	128	128	0	100%	0.638173
Random Excursion	128	127	1	99%	0.6185
Random Excursion Variant	128	127	1	99%	0.6718
Lempel Ziv Compression	128	128	0	100%	1
Block Frequency	128	127	1	99%	0.859684
Overlapping Template Matching	128	128	0	100%	1
Approximated Entropy	128	128	0	100%	1
Non-Overlapping Template Matching	18944	16681	2263	88%	0.003496
Linear Complexity	128	127	1	99%	0.7461
Serial	128	128	0	100%	1
Universal	1280	1101	179	86%	0.043

AVERAGE SECURITY

The information entropy obtained is relatively high value. This means that information leakage in the encryption process is negligible and the encrypted text is secure against entropy attack. This test prove that the generated keys is unpredictable, random and robust keys. The test is previously described in section (IV).

Plaintext= Hello Nada Open the yellow envelope

Cipher text=
187,127,142,251,179,61,16,159,202,215,147,179,195,249,113,229,122,87,158,
65,94,180,18,119,144,92,94,122,151,137,68,147,128,133,122

Average security = 0.459476845531451

Fig(11) show the average security for ciphered text.

© 2019, IJCSMC All Rights Reserved

CONCLUSION

Random numbers are very significant for stream cipher cryptography. Unpredictability and unique randomness key generation system based retina has been proposed. This system takes advantage of computer processing speeds, biometric data, and chaotic map to produce robust keys without having to remember complicated sequences which might be lost, stolen, or even guessed. By using a 1D logistic map with retina image features to generate the keystream, the resulting key satisfies the following characteristics: Firstly, it seems random, that implies it can pass all the tests. Also, it is unpredictable and cannot be surely recreated. Finally, it xored with the plain text to produce a secure cipher text.

In future work, another biometrics like fingerprint, face, hand also can be used as a random source to generate RNG.

REFERENCES

[1] S. Jaiswal, S. S. Bhadauria, R. S. Jadon, "Biometric: Case Study", Journal of Global Research in Computer Science, Vol. 2, No. 10, 2011, pp. 19-49.

[2] I. M. Alsaadi, "Physiological Biometric Authentication Systems, Advantages, Disadvantages and Future Development: A Review", International Journal of Scientific & Technology Research, Vol. 4, No. 12, 2015, pp. 285- 289.

[3] Bart Preneel. (2010). "Understanding Cryptography". Springer.

[4] M. Tajuddin, C. Nandini, "Cryptographic Key Generation using Retina Biometric Parameter", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 3, No. 1, 2013, pp. 54-56.

[5] J. Szczepanski, E. Wajnryb, J.M. Amigó, M. V. Sanchez-Vives, M. Slater, "Biometric random number generators", Computers & Security, Vol. 23, No. 1, 2004, pp. 77-84.

[6] K. Saraswathi, B. Jayaram, R. Balasubramanian, "Retinal Biometrics based Authentication and Key Exchange System", International Journal of Computer Applications, Volume 19– No.1, 2011, pp. 1-7.

[7] H. M. A. Salman, "Proposal Design: Fingerprint Random Number Generators", The 13th International Arab Conference on Information Technology ACIT'2012 Dec.10-13, 2012, pp. 516- 522.

[8] H. Zhu, C. Zhao, X. Zhang, L. Yang, "A novel iris and chaos-based random number generator", Computers & Security, Vol. 36, 2013, pp. 40-48.

[9] S. Gerguri, V. Matyáš, Z. Říha, L. Smolík, "Random Number Generation Based on Fingerprints", book title "Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices", Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 170-182.

[10] S. Barman, D. Samanta and S. Chattopadhyay, "Revocable key generation from irrevocable biometric data for symmetric cryptography," Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT), Hooghly, 2015, pp. 1-4.

[11] P. Yankanchi, S. A. Angadi, "Biometric Steganography: A New Approach Using Hand Geometry", International Journal of Recent Trends in Engineering & Research (IJRTER), Vol. 02, No. 09, 2016, pp. 96-104.

[12] R. Dwivedia, S. Deya, M. A. Sharmaa, A. Goela, "A fingerprint based crypto-biometric system for secure communication", Cryptography and Security, arXiv:1805.08399 [cs.CR], 2018, pp. 1-29.

[13] Manifavas,C ; Hatzivasilis,G; Fysarakis,K ; and Papaefstathiou,Y. (2015). "A survey of lightweight stream ciphers for embedded systems". SECURITY AND COMMUNICATION NETWORKS, Published online 21 December 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1399.

[14] Mousa. A, Faragallah.O.S, EL-Rabaie.S, and E. M. Nigm. (2013). "Security Analysis of Reverse Encryption Algorithm for Databases". International Journal of Computer Applications (0975 – 8887)Volume 66– No.14.

[15] Sahib.N.M, Fadel.A.H and Ahmed.N.S. (2018). "Improved RC4 Algorithm Based on Multi-Chaotic Maps". Research Journal of Applied Sciences, Engineering and Technology.

[16] E. B. Shahram, S. E. Mohammad, "Modified Logistic Maps for Cryptographic Application", Applied Mathematics, Vol. 6, 2015, pp. 773-782.

[17] M. F. El-Santawy, A. N. Ahmed, "On Comparing Different Chaotic Maps in Differential Evolutionary Optimization", Anale. Seria Informatică, Vol. X, 2012, pp. 25-28.

[18] O. F. Mohammad, M. SM. Rahim, S. R. M. Zeebaree, Y. H. A. Falah, "A Survey and Analysis of the Image Encryption Methods", International Journal of Applied Engineering Research, Vol. 12, 2017, pp. 13265-13280.

[19] http://www.ia.uned.es/~ejcarmona/DRIONS-DB.html.

© 2019, IJCSMC All Rights Reserved