Bio-Chaotic Stream Cipher-Based Iris Image Encryption

Abdullah Sharaf Alghamdi, Hanif Ullah, Maqsood Mahmud, Muhammad Khurram Khan
Department of Software Engineering and Information System
King Saud University, Riyadh, Kingdom of Saudi Arabia
{ghamdi, hanif, maqsood.m, mkhurram}@ksu.edu.sa

ABSTRACT-Conventional cryptography uses encryption key, which are long bit strings and are very hard to memorize such a long random numbers. Also it can be easily attacked by using the brute force search or technique. Instead of traditional cryptography, biometric e.g. fingerprint, iris, face, voice etc uniquely identifies a person and a secure method for stream cipher, because Biometric characteristics are ever living and unstable in nature (with respect to recognition). In this paper we used the idea of bio-chaotic stream cipher which encrypts the images over the electronic media by using a biometric key and a bio-chaotic function. It enhances the security of the images and it should not be compromised. The idea also gives birth to a new kind of stream cipher named bio-chaotic stream cipher. The paper also describes how to generate a key from a biometric string and how to encrypt and decrypt the desired data by using the bio-chaotic function.

Keywords: *Biometric, stream cipher, bio-chaotic algorithm (BCA), cryptography, key.*

1. Introduction:

Image encryption techniques are extensively used to overcome the problem of secure transmission for both images and text over the electronic media by using the conventional cryptographic algorithms. But the problem is that it cannot be used in case of huge amount of data and high resolution images [1].

Instead of using the traditional way of cryptography for image encryption we can also use biometric e.g. fingerprint, iris, face, voice etc for the same purpose. The main advantage of a biometric is that it is ever living and unstable characteristics of a human being and it cannot be compromised. However it also suffers from some biometric specific threats and that is the privacy risk in biometric systems. An attacker can interpret a person's biometric data, which he can use for many illegal operations such is to masquerade like a particular person or monitor the person's private data [2].

Similarly some chaos-based cryptosystems are used to solve the privacy and security problems of biometric templates. The secret keys are randomly generated and each session has different secret keys. Thus biometric templates are encrypted by means of chaotic cryptographic scheme which makes them more difficult to decipher under attacks [3].

Moreover some chaotic fingerprint images encryption techniques are also proposed which combines the shuttle operation and nonlinear dynamic chaos system. The proposed image encryption technique provides an efficient and a secure way for fingerprint images encryption and storage [4].

In order to improve the security of the images we proposed a better idea about a new type of algorithm called Bio-Chaotic stream cipher algorithm (BCA) for image encryption which overcome the problems of some of the algorithms used previously for the same purpose. In this algorithm we used the iris images and extract their features by using the L.Rosa [6] iris feature extraction code. These features are then used to generate the initial condition for the secret key using the Hamming Distance technique, which is then Xored to the iris extracted features to generate another secret key called biometric key. This biometric key is then used in the chaotic function to generate the bio-chaotic stream cipher for further encryption.

978-0-7695-3823-5/09 $26.00 © 2009 IEEE
DOI 10.1109/CSE.2009.317

The rest of the paper is organized as in section 2 we will discuss the basic working and idea of the BCA. Section 3 presents the graphical representation of the key generation process and logistic map for the algorithm. Section 4 shows some mathematical comparisons with other algorithms. Section 5 consists of related work, and finally section 6 draws a conclusion.

2. Bio-Chaotic Algorithm (BCA)

The basic idea of the algorithm is such that we took an iris image and extract its features by using L.Rose code[6]. By using this template we create the initial condition for the secret key.

Fig 1 presents the block diagram of the proposed bio-chaotic algorithm. Basic steps of the algorithm are as follows.

I. Creation or generation of the initial condition from the iris template. The technique used to create the initial condition is that of Hamming Distance i.e.

$$Initial\ Condition = 2^n - 1 \qquad (1)$$

Where n=*1, 2, 3, 4*…... Some other techniques can also be used for the same purpose like

$$I.C = 2k + 1, \qquad 2k - 1, \qquad 2^n$$

II. This initial condition is then converted into secret key by using the LFSR method. An LFSR of length n over a finite field Pq consist of n stages **[a_{n-1},a_{n-2},a_{n-3},……..,a0]** with $a_i \in$ of Pq, and a polynomial

$$B(x) = 1 + c_1x + c_2x_2 + .. + c_nx_n \text{ over Pq } (2)$$

III. The secret key and iris template is then Xored in parallel to generate the biometric key by using the equation,

$$\text{Biometric key} = a_1 \oplus b_1, a_2 \oplus b_2, \ldots.., a_n \oplus b_n \ (3)$$

IV. This biometric key is further Xored with different blocks of the iris template (divided into blocks of 128 bits/block) which encrypts the image in such a way that no intruder or attacker can easily decrypt the image.

V. To make the algorithm stronger and more secure we add the chaotic function to the biometric key and apply it over the iris image which encrypts it in a more secure way. We use the following logistic equation [3].

$$x_{n+1} = rx_n(1 - x_n) \qquad (4)$$

Where n=1, 2, 3,… is the map iteration index and r is the value taken from the algorithm. On the basis of equation 4 we generate the logistic map for different values of the algorithm the detail of which will be given in the next section.

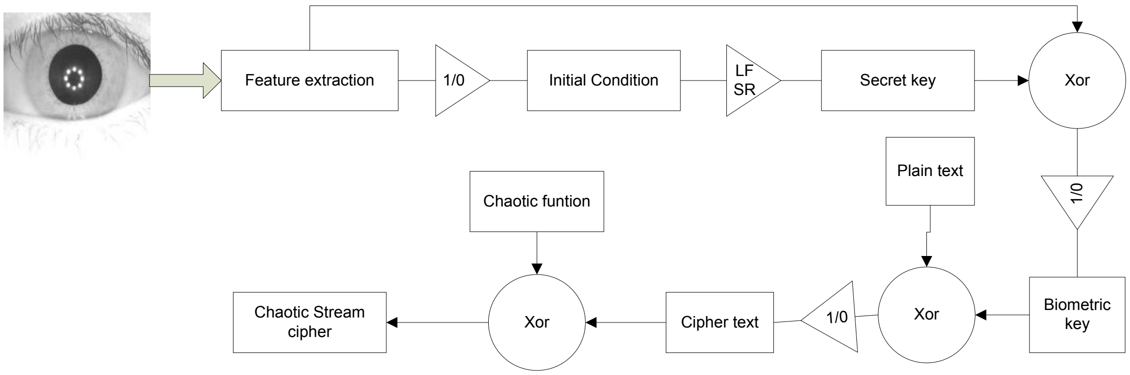

Fig 1: Block Diagram of Bio-Chaotic Algorithm

2.1 Decryption Process

The decryption process of the taken image is carried on by the same way using the same key used for the encryption process but in the opposite direction i.e. the ciphered image is Xored with the biometric key to get the image back in its original form.

$$Plain\ Image = Ciphered\ Image \oplus \text{Key}$$

$\oplus$ It shows the Exclusive OR operation.

3. Experimental Analysis of the Algorithm

In order to evaluate and check the performance of the proposed algorithm i.e. Bio-chaotic algorithm we took iris images from one of the renowned database CASIA (Chinese Academy of sciences and institute of Automation) [7]. The database contains a lot of iris images taken from different people eyes. In our case we use 2 or 3 of the iris images from this database to carry out our experimental process. These images are shown in fig.2.

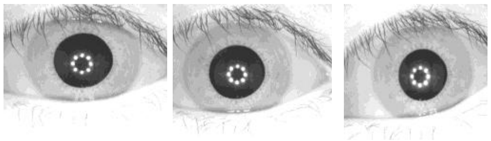

Fig.2. iris images used for experiments

The algorithm is analyzed and tested by using different values for x where x is any real value between 0 and 1. Some of the logistic maps based on the experimental analysis performed over sample and encrypted iris images are included in this section. The logistic maps are derived on the basis of the following mathematical function.

$$Y_K = \begin{cases} 1 & x(i) > 0.5 \\ 0 & x(i) < 0.5 \end{cases} \qquad (5)$$

On the basis of the above equation we generate different logistic maps using different values. Fig.3 and 4 shows the statistical correlation curves of the sequence. By observing the maps carefully it's clear that even changing in a small part of the value the whole map become different.

Fig.5 shows the encrypted images by using different chaotic values.

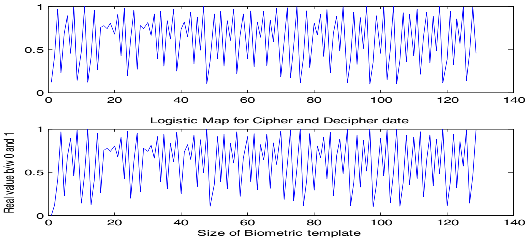

Fig.3: Logistic map when value= 0.54000000000001

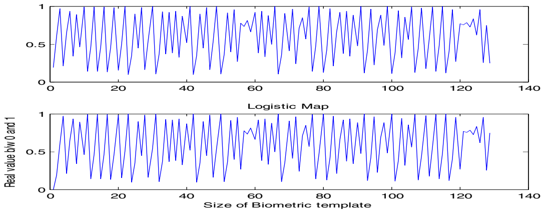

Fig.4: Logistic map when value= 0.58000000001

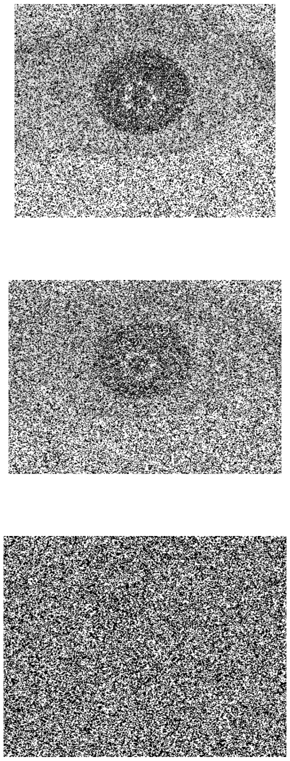

Fig.5: (a) Encrypted image at value= 0.5800000000001
(b) Encrypted image at value= 0.7000000000001
(c) Encrypted image at value= 0.9800000000001

Table 1: Avalanche effect of the BCA

NO	AvalanchePC Effect for BCA	AvalanchePK Effect for BCA	AvalancheCK Effect For BCA
1	47.6563 %	46.8750 %	50.7813 %

From the figure it is clear that how strong the encryption process is that by changing even a small part of the value the image become more and more invisible. Similarly the decryption process is more sample as like the encryption by just Xoring the Ciphered image with the key and we will get the original image.

4.Mathematical observation of the Algorithm

In this section some of the mathematical observations like Avalanche effect, confusion and diffusion, and entropy of the proposed algorithm are mentioned.

4.1 Avalanche Effect

The Avalanche effect refers to a desirable property of the cryptographic algorithms. The Avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip). In the case of quality block ciphers, such a small change in either key or the plain text should cause a drastic change in the cipher text. In our case the Avalanche effect of the proposed system is determined by using the following mathematical equation [8].

$$AvalanchePC = 100 - percentPC \qquad (6)$$

Where percentPC (percent difference between plain image and ciphered image) could be find out by using the equation

$$percentPC = \frac{Acc}{128} * 100 \qquad (7)$$

Where Acc is basically an Accumulator and it could be find out by

$$Acc = plus(DiffPC, Acc) \qquad (8)$$

In equation 8 DiffPC means the difference between plain image and ciphered image and it is basically the Xor operation between plain image and cipher image. Similar methodology is used to find out the avalanche effect between plain image and key and ciphered image and key. The results of the above equations are tabulated in the above table.

The table shows that the Avalanche effect between the plain image and ciphered image, and plain image and key is less than 50 percent that is a more desirable value for any algorithm. Similarly the Avalanche effect between ciphered image and key is round about 50 percent which is slightly bigger than the rest of the two, but again it is a desirable value for our proposed algorithm.

4.2 Confusion and Diffusion

Confusion and diffusion are the two properties of the operation of a secure cipher. Confusion refers to making the relationship between the key and the cipher text as complex and as involved as possible. Diffusion refers to the property that redundancy in the statistics of the plain text is dissipated in the statistics of the cipher text [8]. Confusion and diffusion are the same properties like Avalanche effect which is elaborated in the previous section.

4.3 Entropy

Entropy is a measure of the uncertainty or randomness associated with a random variable. It is basically a measure of the average information content one is missing when one does not know the value of the random variable [8]. Entropy can be found by using the equation

$$H(x) = -\sum_{i=1}^{n} \mathrm{p}(x_i) log_b \mathrm{p}(x_i) \qquad (9)$$

By using the above equation we found the entropy of our proposed system which is round about 127.3. The values show better uncertainty and randomness of bits in the algorithm. The probability of each bit is 0.5. The entropy will be high if there is more randomness in the bits used in the ciphered image. Table 2 shows the entropy of our proposed system.

4.4 Histogram of the Images

Figure 6 shows the histogram for the plain and encrypted or ciphered images used in the bio-chaotic algorithm.

Table 2: Entropy of Bio-chaotic Algorithm

Bio-chaotic Algorithm	Entropy(H(X))
1	127.3

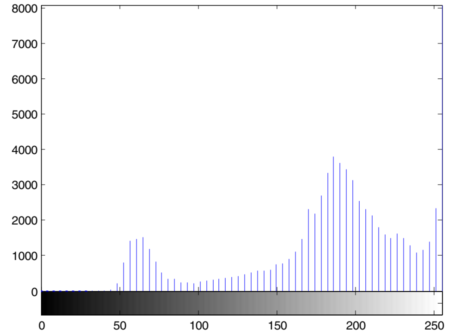

Fig 6: (a) histogram of the plain image

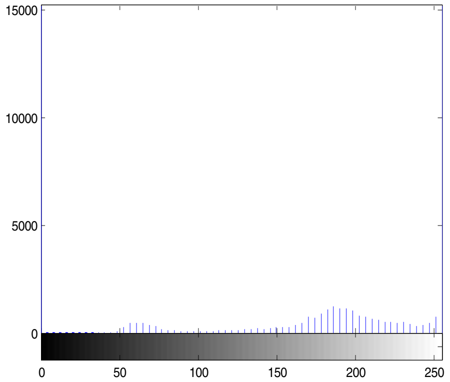

Fig 6: (b) histogram of the ciphered image

5. Related work

The work that we seen relevant to our work is that of Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li which proposed a new chaotic algorithm for image encryption[1]. In this paper they presented a new nonlinear chaotic algorithm (NCA) which uses power function and tangent function instead of linear function. The experimental results demonstrated in this paper for the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency [1].

Similarly the work done by Song Zhao, Hengjian Li, and Xu Yan for the security and Encryption of fingerprint images is more relevant to our work [4]. In this paper they proposed a novel chaotic fingerprint images encryption scheme combining with shuttle operation and nonlinear dynamic chaos system. The proposed system in this paper shows that the image encryption scheme provides an efficient and secure way for fingerprint images encryption and storage [4].

Also the work done by Muhammad Khurram Khan and Jiashu Zhang for implementing templates security in remote biometric Authentication systems seems relevant to us [3]. In this paper they presented a new chaos-based cryptosystem to solve the privacy and security issues in remote biometric authentication over the network. Experimental results derived in this paper shows that the security, performance and accuracy of the presented system are encouraging for the practical implementation in real environment [3].

6. Conclusion

In this paper we have presented a new idea and a new method for the iris image encryption and decryption. We proposed a new algorithm for the image encryption named Bio-Chaotic Algorithm (BCA). We extracted the Iris features by using the L. Rose code and create the initial condition by using the Hamming distance technique. From this initial condition we generated the secret key and Xor it with the iris image bits to generate a new key called biometric key. They same key is used for the encryption and decryption process of the iris image. We also used chaotic function to further enhance the security of our proposed system.

7. Future Work

In the future we would like to use the same technique for the encryption of Fingerprint images. Also we would like to embed the algorithm with a stream cipher technique used in our other paper to make it more secure and enhanced.

References

[1]Haojiang Gao, Yisheng Zhang , Shuyun Liang , Dequn Li, “A new Chaotic Algorithm for image

Encryption", ELSEVIER , SCIENCE DIRECT , Aug 2005.

[2] Andrew Teoh Beng Jin, David Ngo Chek Ling, Alwyn Goh, " Biohashing : two factor authentication featuring fingerprint data and tokenized random number " April 2004,"The Journal Of The Pattern Recognition Society " , ELSEVIER , April 2004.

[3] Muhammad Khurram Khan, Jiashu Zhang, "Implementing Templates Security in Remote Biometric Authentication Systems", IEEE Conf. Proceedings on CIS'06, China, pp. 1396-1400, Vol.2, 2006.

[4] Song Zhao, Xu Yan, "A secure and efficient fingerprint images encryption scheme" Proceedings of the IEEE, 2008, pp- 2803-2808.

[5] Muhammad Khurram Khan, Jiashu Zhang, "Improving the Security of 'A Flexible Biometrics Remote User Authentication Scheme'", Computer Standards and Interfaces (CSI), Elsevier Science UK, vol. 29, issue 1, pp. 84-87, 2007.

[6] Iris code by Luigi ROSA, L'Aquila ITALY(19600bits)"http://www.advancedsourcecode.com/irisphase.asp"

[7] CASIA Iris Database. [Online March, 2006] http://sinobiometrics.com.

[8] Shannon, C. E., "A Mathematical Theory of Communication," Bell System Technical Journal, July 1948, p.623.

[9] Yao-Jen Chang, Wende Zhang , and Tsuhan Chen, "Biometrics-Based Cryptogrphic Key Generation" 2004 IEEE, USA.

[10] Ren Honge, Shang Zhenwei, Wang Yuanzhi , Zhang Jian , "A Chaotic Algorithm of Image Encryption Based on Dispersion Sampling" The eight International conference on Electronic Measurement and Instruments" 2007 IEEE.

[11] Shenglin Yang, Ingrid M. Verbauwhede ,"Secure Fuzzy Vault Based Fingerprint Verification System", 2004 IEEE.

[12] The MathWorks^{TM} Accelerating the pace of engineering and science. "www.mathworks.com" Date accessed : 2 Feb 2009

[13] Eli Biham, Louis Granboulan, Phong Q. Nguy "Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4" Computer Science Department, Technion – Israel Institute of Technology, Haifa

[14] J. Daugman,"High confidence visual recognition of persons by a test of statistical independence ",IEEE Transactions on Pattern Analysis and Machine Intelligence vol.15,1993,pp.1148-61.

[15]Mahmud.M "Natural Language (ARABIC) as a Strengthening Layer for Stream Ciphers in Wireless Networks" The *17th* IASTED International Conference on Applied Simulation and Modeling ,ASM 2008,Corfu Greece, June 23 – 25, 2008.

[16] J.G. Daugman, "Uncertainty Relation for Resolution in Space, Spatial Frequency, and Orientation Optimized by Two-Dimensional Visual Cortical Filters," *J. Optical Soc. Amer*., vol. 2,no. 7, pp. 1,160-1,169, 1985.