A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm

Abdullah Sharaf Alghamdi[1], Hanif Ullah[2]
Department of Software Engineering,
College of Computer and Information Sciences,
King Saud University, Riyadh, Kingdom of Saudi Arabia
ghamdi@ksu.edu.sa , hanif@ksu.edu.sa

Abstract: ***Due to dramatic enhancement in computers and communications and due to huge use of electronic media, security gains more and more importance especially in those organizations where information is more critical and more important. The older techniques such as conventional cryptography use encryption keys, 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 attack technique. Instead of using the traditional cryptographic techniques, Biometrics like Iris, fingerprints, 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 and also used to encrypt the images to store it into the databases to make it more secure 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 an initial key also called initial condition 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

Due to dramatic enhancement in computers and communications and due to huge use of electronic media, security gains more and more importance especially the security of biometric images become a hot issue. Biometric images are mostly used for the authentication system because of there ever living and unstable (with respect to recognition) characteristics. Conventional or traditional symmetric or asymmetric cryptography is limited only to text files but it cannot be used in case of huge files like images and videos.

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 [2].

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 [3].

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 [4].

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 [5].

Similarly some new image encryption technique based on hyper-chaos is also proposed, which uses an image total shuffling matrix to shuffle the pixel positions of the plain image and then the states combination of hyper-chaos is used to change the gray values of the shuffled image [6].

In order to improve the security of the images we proposed a better idea which is a new type of algorithm called Bio-Chaotic stream cipher algorithm (BCA) for image encryption which overcomes 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 [9] 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.

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

2. Related work

The same work is carried out in our conference paper already published. The same algorithm is used for the encryption of the Iris images. In this paper we elaborate the algorithm with more detail and add some new features to the existing proposed system [19].

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[2]. 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 [2].

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 [5]. 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 [5].

Also the work done by Muhammad Khurram Khan and Jiashu Zhang for implementing templates security in remote biometric Authentication systems seems relevant to us [4]. 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 [4].

Similarly a new image encryption technique was introduced by Tiegang Gao and Zengqiang Chen in their paper based on the image total shuffling matrix to shuffle the position of the image pixels and then uses a hyper chaotic function to complex the relationship between the plain image and the cipher image. The suggested image encryption algorithm has the advantage of large key space and high security [6].

Moreover a coupled nonlinear chaotic map and a novel chaos-based image encryption technique were used to encrypt the color images by Sahar Mazloom and Amir Masud Eftekhari-Moghadam in their paper [10]. They used the chaotic cryptography technique which is basically a symmetric key cryptography with a stream cipher structure. They used the 240 bit long secret key to generate the initial condition and to increase the security of the proposed system [10].

3. Proposed System 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.Rosa code [9]. L. Rosa used a code to generate a binary pattern from the given iris image. The binary pattern is further divided into small blocks of binary data to make the process simplified, because it is very difficult to encrypt the binary pattern of hundreds of thousands of bits at once. In our case we made each block of 128 bits to make it simpler and to encrypt each block easily. A random block is then selected to create the initial condition for the secret key. The random selection of the block is preferred because of the attackers, so that no one can easily understand that which block is selected for the initial condition.

At the transmission time of the image the bits of this random selected block is encrypted by using Quantum Encryption Technique [8]. Quantum encryption uses light particles, also call photons instead of bits at communication time. A photon can have one of the four orientations or shapes, 45^0 diagonal, -45^0 diagonal, horizontal or vertical. Each of these represents a bit, - and / represents a 0, while | and \ represents a 1[8].

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

I. Generation of the initial condition from the randomly selected block taken from the binary pattern of the iris image. 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

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

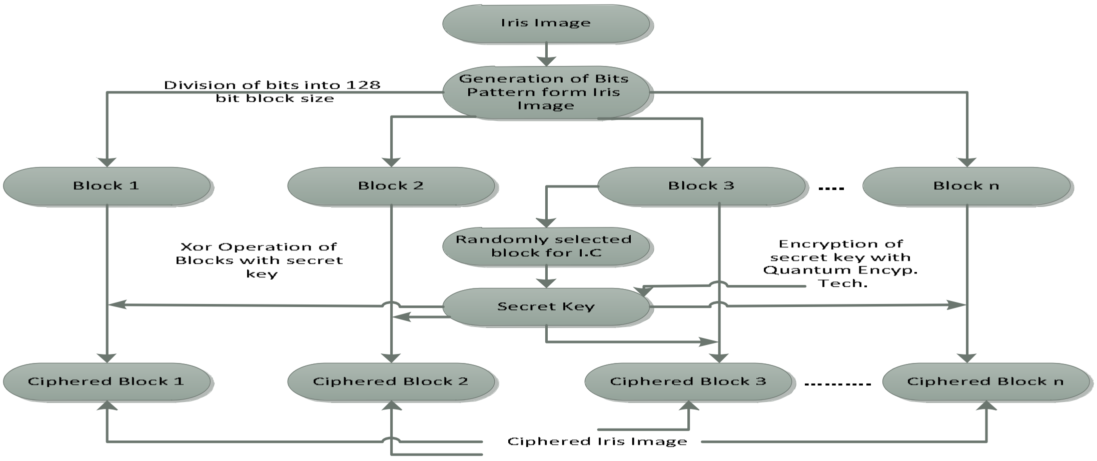
Iris Image
Generation of Bits Pattern form Iris Image
Division of bits into 128 bit block size
Block 1
Block 2
Block 3
....
Block n
Randomly selected block for I.C
Xor Operation of Blocks with secret key
Encryption of secret key with Quantum Encyp. Tech.
Secret Key
Ciphered Block 1
Ciphered Block 2
Ciphered Block 3
....
Ciphered Block n
Ciphered Iris Image

Figure 1. Block Diagram of Bio-Chaotic Algorithm

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

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

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

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

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 [4].

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

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.

3.1 Decryption Process

The decryption process of the used 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. The receiver will first decrypt the randomly selected block by using the same technique used for the encryption process i.e. Quantum Decryption technique [8]. After decrypting the selected block the receiver will generate the initial condition with the same procedure used for the encryption process and will decrypt the image. The equation used for the decryption process is as follows.

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

$\oplus$ It shows the Exclusive OR operation.

4. 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) [11]. 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.

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. 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.

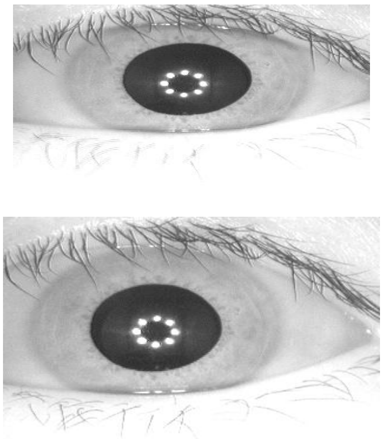

Figure 2. iris images used for experiments

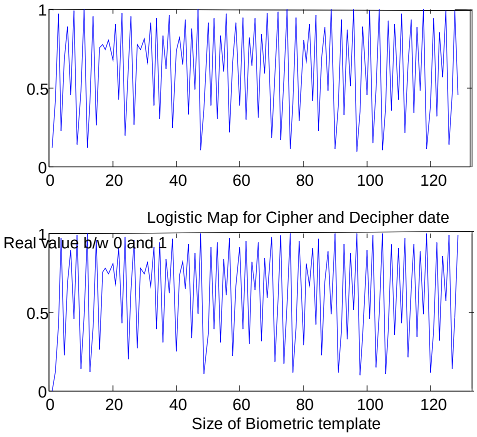

Figure 3. Logistic map when value= 0.54000000000001

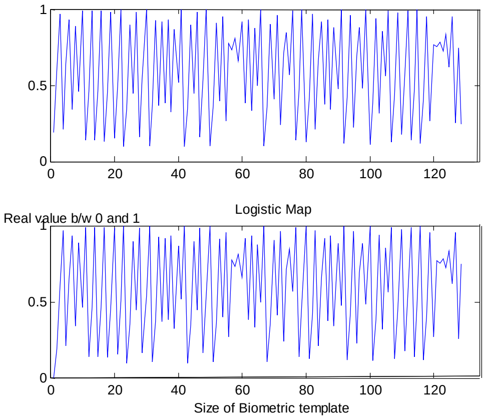

Figure 4. Logistic map when value= 0.58000000001

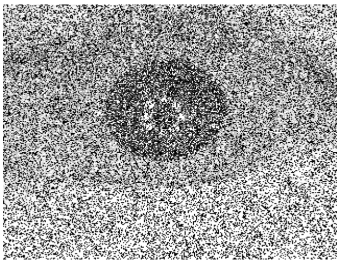

Figure 5. (a) Encrypted image at value= 0.580000000000

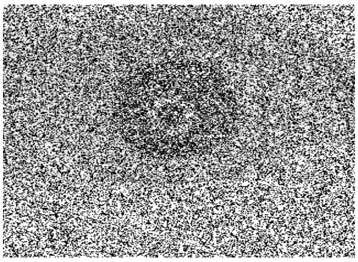

Figure.5. (b) Encrypted image at value= 0.7000000000001

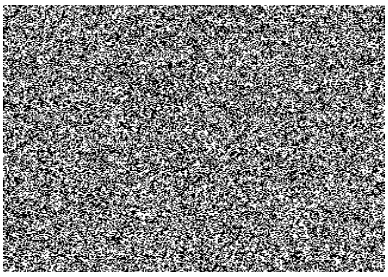

Figure 5. (c) Encrypted image at value= 0.9800000000001

Table 1: Avalanche effect of the BCA

NO	AvalanchePC Effect for BCA	AvalanchePK Effect for BCA	AvalancheCK Effect For BCA
1	48.8758 %	47.9530 %	52.9465 %

5. Statistical Analysis of Bio-Chaotic Algorithm (BCA)

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

5.1 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 [12].

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

Where percentPC (percent difference between plain image and ciphered image) could be found 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 table1.

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.

5.2 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 [12]. Confusion and diffusion are the same properties like Avalanche effect which is elaborated in the previous section. The confusion and diffusion of the proposed algorithm is round about 49%, which shows the strength of the proposed system.

5.3 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 [12]. Entropy can be found by using the equation

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

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.

Table 2: Entropy of Bio-chaotic Algorithm

Bio-chaotic Algorithm	Entropy(H(X))
1	64.67

5.4 Histogram of the Images

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

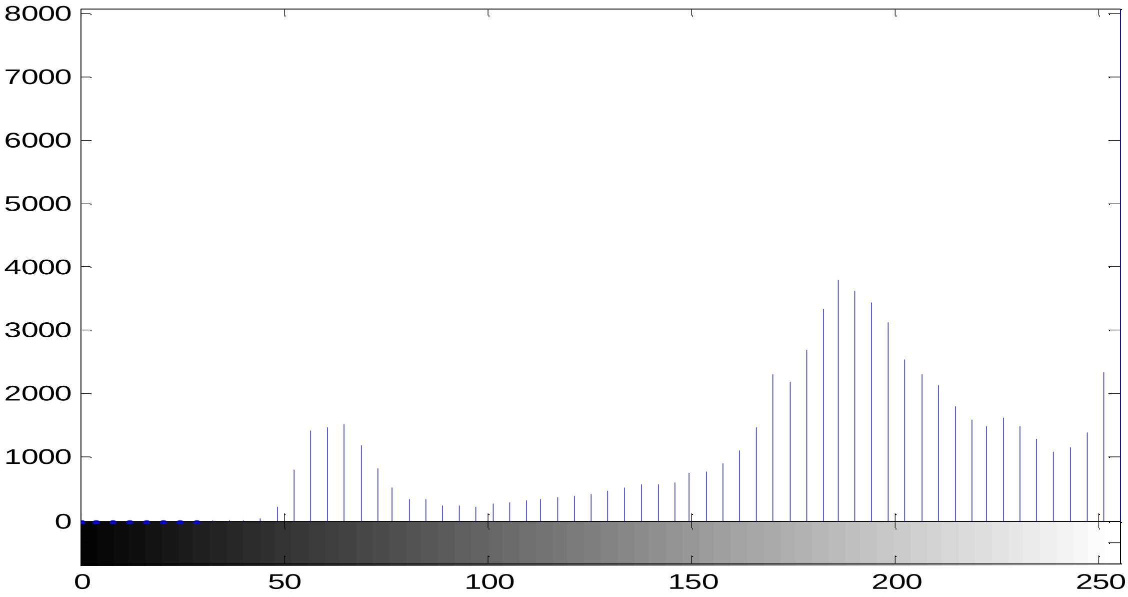

Figure 6. (a) histogram of the plain image

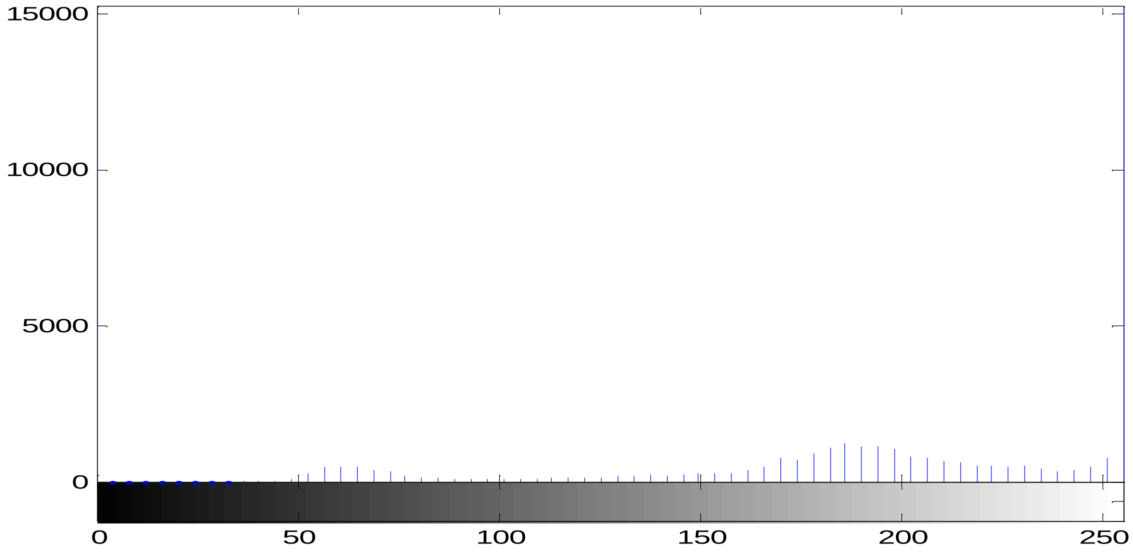

Figure 6. (b) histogram of the ciphered image

6. Conclusion

This paper presents a new and novel idea for the encryption and decryption of the iris images. The proposed algorithm called the Bio-Chaotic Algorithm (BCA) takes an iris image and with the help of L.Rosa code generates the iris features or the binary bits pattern for the image. This binary bits pattern is then divided into small blocks of bits to simplify the process. Each block is that of 128 bits long. Then a random block is selected from all these blocks to create the initial condition. This initial condition is then passed from the LFSR to generate the secret key. A secret key of 128 bits is generated from the result of the LFSR. This secret key is then used for the encryption of the iris image. A Quantum encryption technique is also used to encrypt the randomly selected block, so that no one can easily attack the block used for the generation of the secret key. The same procedure is then used at the receiver end to decrypt the iris image. Chaotic function is used to make the algorithm more secure and make the process of the encryption and decryption more complex. Experimental and statistical analysis of the algorithm shows that the algorithm is stronger and more secure and can be used for the practical implementation of the iris images encryption.

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 use a block size more than 128 bits to make the algorithm stronger and more secure.

References

[1] Arroyo David, Li Chengqing, Li Shujun, Alvarez Gonzalo, Halang A. Wolfgang," Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm", Elsevier , Science Direct, Volume 41, Issue 5, 15 September 2009, Pages 2613-2616

[2]Haojiang Gao, Yisheng Zhang , Shuyun Liang , Dequn Li, "A new Chaotic Algorithm for image Encryption", Elsevier , Science Direct , Aug 2005.

[3] 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.

[4] 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.

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

[6] Gao Tiegang, Chen Zengqiang," A new image encryption algorithm based on hyper-chaos" Elsevier, Science Direct, Physics Letters A, Volume 372, Issue 4, p. 394-400, 2007.

[7] 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.

[8] T Morkel 1, JHP Eloff," Encryption Techniques: A Timeline Approach", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa

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

[10] Mazloom Sahar, Eftekhari-Moghadam Masud Amir", Color image encryption based on Coupled Nonlinear Chaotic Map", the journal of Chaos, Solitons and Fractals 42 (2009) 1745–1754, ELSEVIER, 2009.

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

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

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

[14] 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.

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

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

[17] 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

[18] 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.

[19] Alghamdi S. Abdullah, Ullah Hanif, Mahmud Maqsood, Khan K. Muhammad., "Bio-chaotic Stream Cipher-Based Iris Image Encryption," cse, vol. 2, pp.739-744, 2009 International Conference on Computational Science and Engineering, Canada.

[20] 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.

Authors Profile

Dr. Abdullah Alghamdi is a full time associate professor, SWE Department, College of Computer and Information Sciences, KSU. He holds a Ph.D. in the field of Software Engineering from the department of computer science, Sheffield University, UK, 1997. He obtained his M.Sc. in the field of software development technologies from the UK in 1993. In the academic year 2004/5 he worked as a visiting professor at School of IT and Engineering, University of Ottawa, Ottawa, Canada, where he conducted intensified research in Web Engineering as part of his Post-Doc program. He recently published a number of papers in the field of Web engineering methodologies and tools. Dr. Abdullah worked as a part-time consultant with a number of governmental and private organizations in the field of IT strategic planning and headed a number of IT committees inside and outside KSU. Currently he is chairing the Software Engineering Department at KSU and part time consultant at Ministry of Defense and Aviation.

Hanif Ullah received the BIT (Hons) and MSc. Degree in Information Technology from Iqra University Karachi in 2004 and Quaid-e-Azam University Islamabad, Pakistan in 2007 respectively. In January 2008, He joined King Saud University, Saudi Arabia as a Research Assistant and start working on Network and Information security related topics. Currently He is working as a Lecturer in the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Saudi Arabia.