Intrinsic Authentication of Multimedia Objects Using Biometric Data Manipulation

Maqsood Mahmud[1, 2, 3], Muhammad Khan[1], Khaled Alghathbar[1, 2], Abdul-Hanan Abdullah[3], and Mohammad Bin-Idris[3]
[1]Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
[2]Department of Information Systems, King Saud University, Saudi Arabia
[3]Faculty of Computer Science and Information Systems, University Technology Malaysia, Malaysia

Abstract: *The Biometric Gaussian Stream (BGS) cryptosystem was extended by extensive research experimentation. Using this system, complexity is added to an image by passing it through a Gaussian noise function. This function is applied with specific parameters for the mean and variance, which also works as a parallel key. To implement a stream cipher BGS with help of biometric images, the Initial Condition (IC) for Linear Feed Back Shift Register (LFSR) from is extracted iriscode. A comparison between various stream ciphers is also made to measure the strength of the BGS cryptosystem. The previous experimentation work has been extended by formulating the algorithmic runtime complexity of the BGS Cryptosystem which proves to be O(n) algorithmically. New techniques to encrypt and assess multimedia objects have been introduced.*

Keywords: *Cryptosystem, LFSR, gaussian noise, computational runtime complexity, stream ciphers.*

Received February 14, 2010; accepted May 20, 2010

1. Introduction

The term biometrics refers to methods and techniques for uniquely recognizing a human being, based on one or more intrinsic physical or behavioral traits. In information technology, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups under surveillance [25, 29].

Stream ciphers represent a diverse approach to symmetric encryption in comparison with block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. The difference is not always clear-cut: In some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to serious security problems if handled incorrectly. The same starting state must never be used twice [22]. In cryptography, the avalanche effect refers to a desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions. The avalanche effect is evident, by a significant change in the output (e.g., half the output bits flip) when an input is changed slightly (for example, flipping a single bit). In the case of block ciphers, a small change in either the key or the Plain text will cause a drastic change in the ciphertext. The term was first used by horst feistel (Feiste l1973), although the concept dates back to at least Shannon's diffusion [1, 27]. Diffusion dissipates the statistical structure of plaintext over the bulk of ciphertext. Confusion makes the relationship between the ciphertext and key as complex as possible.

1.1. Related Work

The papers [5, 6, 7, 8, 9, 10, 11] were found to be the most relevant to the proposed work. Some papers are closely related to biometric image authentication while some are related to stream ciphers. The ideas from both sets of references were combined to conceive the idea of the Biometric Gaussian Stream (BGS) cipher the authors described the relationship between chaotic characteristic and cryptography, putting forward a chaotic algorithm for image encryption with double keys. Discrete logistics maps were used and were implemented in MATLAB like the BGS cipher. The original value of the sequence was regarded as a secret key. In [4], the authors discuss biometric encryption. They state that password management is the weakest point of any cryptosystem, as a password can be guessed, found with a brute force search or stolen by an attacker. Moreover, because of variability the biometric image or template itself cannot serve as a cryptographic key. The authors used user-specific biometric information instead of using PINS and passwords. They also presented the generation of stable crypto graphic keys from biometric data that are stable in nature. A longer and more stable

biostream is generated as the cryptographic key. The authors proposed a novel two factor authentications based on iterated inner products between a tokenized pseudo-random number and the user specific fingerprint feature, which is generated from the integrated wavelet and fourier-mellin transform, and hence produced a set of user specific component code that they called Biohashing. The authors presented recent researches on chaotic systems. They further stated that the drawbacks of a small key space and weak security in one-dimensional chaotic encryptions were obvious.

In [23], the authors proposed a novel chaos based cryptosystem to solve the privacy and security issues of biometric templates in remote biometric authentication over a network. Secret keys are randomly and dynamically generated without any human intervention, and each transaction session has different secret keys. Chaotic encryption scrambles the biometric templates into an intangible form and chaotic modulation spreads the encrypted templates across a wide band of frequencies. This makes them more difficult to decipher under attacks. The authors described a secure fingerprint verification system based on the fuzzy vault scheme, where a transformed version of the sensitive biometric template is stored. Thus a high unlock complexity for attackers with an acceptable unlock rate for the legal users is achieved. A chaotic algorithm for image encryption with double keys is described. It used logistic maps to produce a chaotic sequence, where the original value of the sequence is regenerated as a secret key.

In this paper, the BGS cryptosystem gives a new dimension to the field of cryptography. This idea emerged by manipulating the existing stream ciphers and biometric security features and considering their strength in the current scenarios of the insecure world of communication.

The idea is a combination of three security aspects: Biometrics (Iris), gaussian noise, and stream ciphers. A gabor wavelet was used to generate iriscode for iris bits (Θ) generation. The key used in the BGS is generated with the help of biometrics (Iris code) [5, 12, 23]. This key is further used to encrypt multimedia objects like a picture or even the Iris image itself as in our case. The selection of bits for the inputs of the LFSR key is done by hamming code method. Daugman's proposed algorithm for iriscode generation was used in BGS. He used the gabor wavelet equation to extract the phase of the iris image. Iris bits were further used to extract specific bits using the hamming method to feed LFSR [9, 12]. Gaussian noise was added using a gaussian function with variance (v) and mean LFSR [9, 12]. This Gaussian noise with the already added image was further passed through the LFSR to encrypt it. The decryption was performed in the reverse order as is usually done in cryptosystems [30]. The mean (m) and variance (v) were taken as parallel keys in addition to the Initial condition of LFSR [23]. The BGS was extended by formulating its runtime complexity algorithmically.

1.2. Research Methodology

The following method was adopted in our research.

1. Literature review of biometrics and existing stream ciphers.
2. Selection of one biometric feature (fingerprint, palm geometry, speech, gait, iris etc).
3. Finding the Iris code from the Iris image and extracting it using the gabor wavelet equation given in equation 1, [19].

$$G(x, y) = \frac{1}{2\pi\sigma\beta} e^{-\pi\left(\frac{(x - y_\sigma)}{\sigma^2}\right)} \quad (1)$$

   Where (*xo, yo*) is the center of the receptive field in the spatial domain and (*ξo, vo*) is the optimal spatial frequency of the filter in the frequency domain. α and β are the standard deviations of the elliptical gaussian along x and y. The 2D Gabor function is thus a product of an elliptical Gaussian and a complex plane wave.

$$F(x) = \left(((2\pi)^n \, det\, k)^{-1/2} \, exp\, (-(x-\mu)^T K^{-1} \frac{(x-\mu)}{2}\right) \quad (2)$$

   Where x is a length-n vector, K is the n-by-n covariance matrix, μ is the mean value vector, and the superscript T indicates matrix transpose.
4. Finding confusion and diffusion elements.
5. Determining the avalanche effect between (Plain text and cipher text), (cipher text and key) and (plain text and key).
6. Comparisons between RC2, RC4, DES, 3DES and our BGS cipher with respect to speed (Mbps) were also performed.
7. Extending the BGS cryptosystem by formulating its algorithmic runtime complexity.

The paper is organized as introduction in section1. Proposed BGS cipher model Figure 1, is presented in section 2. Section 3 discusses the mechanism of biometric-g-stream cipher BGS. Section 4 elaborates the implementation part of our work. Section 5 describes the assessment and evaluation of our proposed algorithm. Simulation results are focused in Section 6. Limitations are discussed in section 7. Cryptanalysis perspective is shown in section 8. Finally, sections 9 and 10 depicts the future work and conclusion respectively.

2. Proposed BGS Cipher Model

Figure 1 describes our proposed model for the BGS cryptosystem. An iris image is taken and iris bits are generated using the gabor wavelet equation. The Initial Condition (IC) will be chosen using the hamming method for LFSR to generate the keystream for encryption. The same or another image may be taken for encryption purposes as an object. Image bits are generated by the imread () function in MATLAB. It is passed through gaussian noise to make it more complex.

An Xor operation is applied between the keystream bits and image gaussian noise added bits. An encrypted image multimedia hiding is thus achieved. Now it could be securely transferred on a channel. For the decryption process the encrypted image is first XORed using the keystream from LFSR. The decrypted image is then passed through the Gaussian function to achieve the original image.

The image bits can be reconstructed to the original image by the imshow (I) function of MATLAB. Note: The two dimensional aspects of the image are converted into one dimension and then transferred to a binary format to attain plain binary text to perform the encryption.

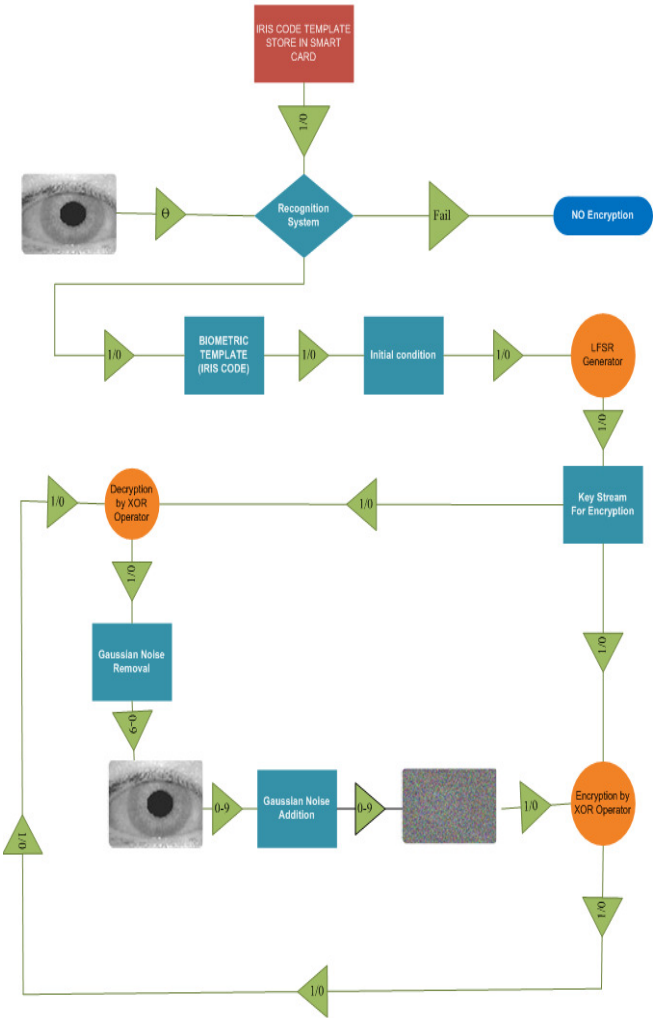

Figure 1. Proposed BGS cipher model.

3. Mechanism of BGS Cipher

The BGS mechanism is described bellow with the help of an example.

3.1. Description of BGS Cipher Algorithm

The following example is given to provide an in-depth understanding of the idea behind BGS ciphers. The algorithm is mentioned in section 6.1. An Iris code template is taken in binary. This image is converted into iris code for the purpose of simulation in MATLAB.

The Gabor Wavelet equation was used for iris code generation. It is stored in a biometric string called "Bio" on line 2. First an initial condition is generated by the hamming method (i.e., 20, 21, 22, 23, 24, 25, and 26….) from string "b" and stored in another string called "IC" on line 4. The LFSR [22] "For" loop is run to generate the key stream for our bio-stream cipher. The loop starts in step 7 and ends in step 10 to generate the key stream.

In section 4.2, the avalanche effect [13, 21, 23, 24] (Shannon's Diffusion) is calculated using the MATLAB tool. String "DiffPC" is declared in line 6. These strings will show the difference between bits in plain text and cipher text. On line 4, DiffPC is calculated. The variable "Accumulator" is used for the summation of the difference in bits using an Xor function. The percentage difference between plain text and cipher text is calculated and stored in accumulator on line 11.

The avalanche effect between the cipher text and key is also calculated and store in the variable "AvalancheCK" and is shown on line 12. The avalanche effect between the plain text and key is shown on line 13. The value is stored in the variable "AvalanchePK". On line 14, the avalanche effect is calculated and stored in the variable "AvalanchePC".

4. Implementation

The implementation of the BGS is performed using the MATLAB tool. The results are discussed in section 7.

4.1. Algorithm for BGS Cipher

The algorithm for the stream cipher is shown below to provide an in-depth understanding of the idea. The code was written in MATLAB [30].

1. *Begin*
2. *"CT"- Cipher Text*
3. *"PT"- Plain Text*
4. *"IC"- Initial Condition*
5. *"I"- Image data*
6. *"p"- Gaussian factor*

7. *"J"- Image data "I" after adding Gaussian Noise*
8. *"Bio"- variable for Biometric (Iris) Data*
9. *IC<--Bio(1), Bio(2), Bio(4), Bio(8), Bio(16), Bio (32), Bio (64), Bio (128)*
10. *N<--128*
11. *LFSR Key Generation*
12. *For i<--1 to n*
13. *Key(i) <--IC(8)*
14. *IC(1)<-- IC (2) Xor IC (5)*
    11Shift each bit forward
15. *End*
16. *Read Image <-- Input Image*
17. *I <-- Image Data*
18. *Input <-- p*
19. *J<-- Gauss Noise(I, p)*
20. *CT<--J Xor Key*
21. *Decryption Process*
22. *PT<-- CT Xor Key*
23. *In Stream Ciphers the Key can be taken as a substring of the Keystream depending upon the size of CT*
24. *Input<-- h*
25. *K <-- Gauss Filter(PT,h)*
26. *Show image <-- K*
27. *End*

4.2. Avalanche Effect

The algorithm below is used to evaluate the avalanche effect for the Biometric-Stream cipher. This code was written in MATLAB [30].

1. *Begin*
2. *Finding the Avalanche*
   Effect/Shannon Diffusion
   DiffCK- Difference between Cipher text and Key
   DiffPK- Difference between Plain text and Key
   DiffPC- Difference between Plain text and Cipher Text
   Accum - Accumulator for Differences
   PercCK- Percentage of Cipher text and Key
   AvalancheCK- Avalanche effect of Cipher and Key
   AvalanchePK- Avalanche effect of Plain text and Key
   AvalanchePC- Avalanche effect of Plain text and Cipher text
3. *DiffCK<--Key Xor CT*
4. *DiffPK(i)<--PT Xor Key*
5. *DiffPC(i) <--PT Xor CT*
6. *Accum-->0*
7. *M<--128*
8. *For i<--1 to m*
   Accum<-- DiffCK (i) + Accum
   Accum<--DiffPK (i) + Accum
   Accum<--DiffPC (i) + Accum
9. *End*
10. *PercCK<--Accum/128*100*
11. *AvalancheCK<--100-PercentCK*
12. *AvalanchePK<--100-PercPK*
13. *AvalanchePC<--100-PercPC*
14. *End*

5. Runtime Complexity of our Algorithm

The complexity of our algorithm is O(n). Step wise runtime calculation is as follows:

Table 1. Runtime complexity of the algorithm.

Begin	Cost	Times
1. Input Biometric Data in 0/1	0	1
2. "Bio" variable	0	1
3. IC<-- Bio(1), Bio(2),Bio (4), Bio(8),		
4. Bio(16), Bio (32), Bio,(64), Bio (128)	C1	1
5. N<-- 128	C2	1
6. LFSR Key Generation	0	1
7. For i<-- 1 to n	C3	n
8. Key(i)<-- IC(8)	C4	n-1
9. IC(1)< -- IC(2)XOR IC(5)	C5	n-1
10. Shift each bit forward	C6	n-1
11. End		
12. Read Image <-- Input Image	C7	1
13. I <-- Image Data	C8	1
14. Input <-- p	C9	1
15. J<-- Gauss Noise(I, p)	C10	1
16. CT<-- J XOR Key	C11	1
17. Decryption Process	0	1
18. PT<-- CT XOR Key	C12	1
19. Input<-- h	C13	1
20. K <-- Gauss Filter(PT,h)	C14	1
21. Show image <-- K	C15	1
22. End		

Table 2. Runtime complexity of the algorithm.

No.	T(n)=∑ Cost * Times
1	= 0(1)+ 0(1)+ 0(1)+ 0(1)+C1(1)+C2(1)+C3(n)+C4(n-1)+C5(n-1)+C6(n-1)+ C7(1)+ C8(1)+ C9(1)+ C10(1) +C11(1) +C12(1)+C13(1)+C14(1)+C15(1)
2	=0(1)+0(1)+0(1)+0(1)+C1(1)+C2(1)+C3(n)+C4(n-1)+C5(n-1)+C6(n-1)+C7(1)+C8(1)+ C9(1)+ C10(1) +C11(1) +C12(1)+C13(1)+C14(1)+C15(1)
3	=0{1+1+1+1}+(1){C1+C2+C7+C8+C9+C10+C11+C12+C13+C14+C15}+(n){C3}+(n-1){C4+C5+C6}
4	=0{1+1+1+1}+(1){C1+C2+C7+C8+C9+C10+C11+C12+C13+C14+C15}+(n){C3}+nC4+nC5+nC6-C4-C5-C6
5	=0{1+1+1+1}+(1){C1+C2+C7+C8+C9+C10+C11+C12+C13+C14+C15}+(n){C3+C4+C5+C6}-C4-C5-C6
6	=0{1+1+1+1}+(1){C1+C2+C7+C8+C9+C10+C11+C12+C13+C14+C15-C4-C5-C6}+(n){C3+C4+C5+C6}
7	=0+{b}+ n{a}
8	=a(n)+b
9	=O(n)

6. Simulation Result /Finding

The results of our simulation from the perspective of shannon's diffusion or the avalanche effect can be viewed bellow.

6.1. Description of Table 3

Table 3 describes the entropy of a specific image under consideration. We took a human picture to encrypt and found its entropy to be 5.8784. The entropy varies with the picture, size and contents.

Table 3. Entropy of human image.

Image	Entropy (H(x))
Human Image	5.8784

6.2. Description of Table 4

Table 4 shows two different avalanche effects between two different variables i.e., plain text with cipher text and key stream with cipher text. The idea was conceived by considering permutation phenomena, where order matters, like PK, PC, and CK. The first permutation takes two variables, Plain text (P) and Cipher text (C). The second permutation considers the Plain text (P) and Key Stream (K). The third permutation takes the Cipher text (C) and Key Stream (K). In Table 4, the AvalanchePC and AvalancheCK values are close to 50% change. These results can be further improved by using other biometric aspects or a more complex stream cipher like the alternate step generating stream cipher, RC6, A5, etc., A comparison is also shown in Figure 2 with DES. Since the avalanche effect of DES is a bit higher than the BGS Cipher, BGS is better in the sense that our cipher is light weight, with one XOR operation and a gaussian function, which takes less time to encrypt and decrypt.

Table 4. Avalanche effect (shannon's diffusion).

Cipher Name	AvalanchePC Effect	AvalancheCK Effect
BGS Cipher	47.6563 %	50.7813 %
DES	53.125 %	54.6875

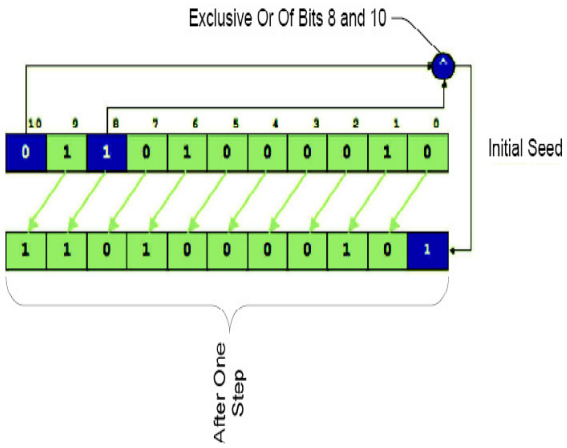

Figure 2. A model LFSR to be used in BGS cipher.

6.3. Description of Table 5

Table 5 shows the speed comparisons of symmetric ciphers. In the BGS cipher, the x* indicates the time taken by the gaussian noise factor which is additional in comparison with RC4. It is concluded from the table below that our BGS is more robust then DES and 3DES with respect to speed.

*Is a gaussian noise factor and depicts a decrease in speed (in Mbps). The value of x is so small that it is negligible. Moreover the speed is bit effected due to the extra layer of Gaussian Noise in BGS, which gives more strength in comparison to RC4 with little trade for speed.

Table 5. Speed comparisons of symmetric ciphers.

Cipher Name	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	variable	0.9
RC4	variable	45
(BGS) Cipher	variable	45-x*

It is a general rule that the longer the key, the harder it will be to crypt-analyze it. Yet, a very long key is used, equal to the size of the image in binary format, for XOR purposes. This was done to have a strengthened key, and hence a strong cipher. The cryptanalytic strength can be further analyzed by using the derivatives of the binary function as [23, 27].

$$V^{(i)}a_1, K, a_i \qquad f(x) = \sum c\zeta[a_1, a_2] \tag{3}$$

7. Limitation and Future Work

The limitation that was found in the experimental phase was the processing of images in binary format, especially colored ones. Since colored images have three phases i.e., RBG, when these images are converted to integers values and then to binary, there is a huge amount of data to handle. The management of image data in binary format some-time creates the problem of memory out of bounds in MATLAB.

This work can be further extended to advanced stream ciphers like the eSTREAM [8] ECRYPT project. Chaotic functions, logistic maps or elliptic curves can be brought into consideration with a combination of biometric features to achieve more desired results, not in only in the field of cryptography but also in the new emerging field of biometrics.

8. Conclusions

The extended BGS Cryptosystem in this paper opens a new dimension to enhance biometric security. The extension of BGS by finding its runtime complexity was performed in this paper. Initially in the paper Gaussian noise was added to the image with specific parameters to make it more complex and secure with less trade off in speed (Mbps), which was negligible. The keystream was extracted from iriscode and then the image was encrypted. The decryption was made in the reverse manner. The BGS proved to be more strengthened in comparison with others ciphers like RC4, 3DES, DES, etc., due to its biometric aspects and inculcation. The runtime complexity of O(n) shows that the algorithm is more efficient and robust with respect to its runtime complexity. The selection of iris code was due to its versatile behavior and its and its universally proven uniqueness. A high entropy

human image was used to take to encrypt human related sensitive data, e.g., hospital data. In conclusion, the proposed system can be easily realized in a real environment and can also enhance the eSTREAM [8, 14, 17, 19] ECRYPT project due its biometric (iris) aspect.

References

[1] Afzal M., Kausar F., and Masood A., "Comparative Analysis of the Structures of eSTREAM Submitted Stream Ciphers," *in Proceedings of 2nd International Conference on Emerging Technologies*, Pakistan, pp. 13-14, 2006.

[2] Ahmed H., Kalash H., and Allah O., "Encryption Quality Analysis of the RC5 Block Cipher," *Algorithm for Digital Images Optical Engineering*, vol. 45, no. 10, pp. 15-23, 2006.

[3] Biham E., Granboulan L., and Nguy P., "Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4," *Computer Science Department, Techno Israel Institute of Technology*, vol. 3557, no. 10, pp. 359-367, 2005.

[4] Biometric Encryption, Biometrics and Cryptography, available at: http://www.3Dface.org, last visited 2007.

[5] CASIA Iris Database, available at: http://sinobiometrics.com, last visited 2006.

[6] Chang Y., Zhang W., and Chen T., "Biometrics-Based Cryptogrphic Key Generation," *in Proceedings of International Conference on Multimedia and Expo*, Taiwan, pp. 2203-2206, 2004.

[7] Chapeau F., "Nonlinear Test Statistic to Improve Signal Detection in Non-Gaussian Noise," *IEEE Signal Processing Letters*, vol. 7, no. 7, pp. 205-207, 2000.

[8] Courtois N., "Fast Algebraic Attacks on Stream Ciphers with Linear Feedback," *Computer Journal of Crypto*, *LNCS*, vol. 2729, no. 5, pp.176-194, 2003.

[9] Daugman J., "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161, 1993.

[10] Daugman J., "New Methods in Iris Recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 37, no. 5, pp. 1167-1175, 2007.

[11] Daugman J., "Probing the Uniqueness and Randomness of Iris Codes: Results from 200 Billion Iris Pair Comparisons," *in Proceedings of the IEEE*, USA, pp. 1927-1935, 2006.

[12] Daugman J., "Uncertainty Relation for Resolution in Space, Spatial Frequency, and Orientation Optimized by Two-Dimensional Visual Cortical Filters," *Optical Society of America*, vol. 2, no. 7, pp. 160-169, 1985.

[13] Dawson E., Gustafson H., and Pettit A., "Strict Key Avalanche Criterion," *Computers and Security*, vol. 13, no. 8, pp. 687-697, 1994.

[14] eSTREAM: The Stream Cipher Project, available at: http://www.ecrypt.eu.org/stream/index.html, last visited 2004.

[15] Gao H., Zhang Y., Liang S., and Li D., "A New Chaotic Algorithm for Image Encryption," *Elsevier, Science Direct*, vol. 24, no. 72, pp. 394-399, 2005.

[16] Honge R., "A Chaotic Algorithm of Image Encryption Based on Dispersion Sampling," *in Proceedings of the 8th International Conferences on Electronic Measurement and Instruments,* China, pp. 1396-1400, 2007.

[17] Horan D. and Guinee R., "A Novel Stream Cipher for Cryptographic Applications," *in Proceedings of Military Communications Conference, MILCOM* ,USA, pp. 1-5, 2006.

[18] Khan K. and Zhang J., "Improving the Security of A Flexible Biometrics Remote User Authentication Scheme," *Computer Standards and Interfaces (CSI), Elsevier Science*, vol. 29, no. 1, pp. 84-87, 2007.

[19] Khan K., Xie L ., and Zhang J., "Chaos and NDFT-Based Concealing of Fingerprint-Biometric Data into Audio Signals for Trustworthy Person Authentication," *Journal of Digital Signal Processing (DSP), Elsevier Science*, vol. 20, no. 1, pp. 179-190, 2010.

[20] Khan M. and Zhang J., "Implementing Templates Security in Remote Biometric Authentication Systems," *in Proceedings of IEEE Conference*, China, pp. 1396-1400, 2006.

[21] Lee T., "Image Representation Using 2D Gabor Wavelets," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 18, no. 10, pp. 1-13, 1996.

[22] Mahmud M., "Natural Language (ARABIC) as a Strengthening Layer for Stream Ciphers in Wireless Networks," *in Proceedings of The 17th IASTED International Conference on Applied Simulation and Modeling,* Greece, pp. 23 -25, 2008.

[23] Mahmud M., Khan M., and Alghathbar K., "Biometric-Gaussian-Stream Cipher with New Aspect of Image Encryption (Data Hiding)," *in Proceedings of International Conference Sectech,* LNCS, USA, pp. 97-107, 2009.

[24] No J., "New Binary Pseudorandom Sequences of Period 2n-1 with Ideal Autocorrelation," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 814-817, 1998.

[25] Paul S. and Preneel B., "A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher," *in Proceedings of the 11th International Workshop, Fast Software Encryption FSE*, India, pp. 245-259, 2004.
[26] Ping Z., Jizhou S., and Xu Z., "A Stream Cipher Algorithm Based on Conventional Encryption Techniques," *in Proceedings of Canadian Conference on Electrical and Computer Engineering*, China, pp. 649-652, 2004.
[27] Schneier B., "The Uses and Abuses of Bi cs," *Communications of the ACM*, vol. 42, no. 8, pp. 136-137, 1999.
[28] Shannon C., "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, no. 1, pp. 379-423, 1948.
[29] Teoh A., David N., and Alwyn G., "Biohashing: Two-Factor Authentication Featuring Fingerprint Data and Tokenized Random Number," *The Pattern Recognition Society, Elsevier*, vol. 37, no. 40, pp. 2245-2255, 2004.
[30] The Math Works TM Accelerating the Pace of Engineering and Science, available at: http://www.mathworks.com, last visited 2009.
[31] What is an LFSR, Texas Instrument SCTA036A, available at: http://www.pld.com.cn/freeip/LFSR.pdf, last visited 1996.
[32] Yang S. and Verbauwhede I., "Secure Fuzzy Vault Based Fingerprint Verification System," *in Proceedings of IEEE International Conference*, Hawaii, pp. 540-523, 2004.

Maqsood Mahmud is a researcher at centre of excellence in Information Assurance College of Computer and Information Sciences, King Saud University, He is pursuing his PhD at University Technology Malaysia. His interest includes information security in general and biometric authentication schemes in special. He has more than 10 international conference and journal papers, mostly in IEEE, ACM and LNCS. Two of his papers are ISI indexed. He is also holder of a US patent in biometric authentication field. He has also served as reviewer of various international conferences and journals.

Muhammad Khan is a manager R & D at the Centre of Excellence in Information Assurance, College of Computer and Information Sciences, King Saud University. He is the founding editor of Bahria University Journal of Information and Communication Technology. He is an associate editor of Journal of Information Hiding and Multimedia Signal Processing. He also plays role of guest editor of several international journals including Springer-Verlag and Elsevier Science He is an active reviewer of many international journals of IEEE, Elsevier Science, Springer-Verlag, and Taylor and Francis, He has been included in the Marquis Who's Who in the World 2010 edition. He has been recently awarded outstanding leadership award at 3rd IEEE NSS'09, Australia. He has published more than 60 research papers. His areas of interest are biometrics, multimedia security, chaotic cryptography, digital data hiding, and cryptology.

Khaled Alghathbar PhD, CISSP, CISM, PMP, BS7799 Lead Auditor, is an associate professor and the director of the Centre of Excellence in Information Assurance in King Saud University, Saudi Arabia. He is a security advisor for several government agencies. His main research interest is in information security management, policies and design. He received his PhD in Information Technology from George Mason University, USA.

Abdul-Hanan Abdullah obtained his PhD degree from Aston University, United Kingdom in 1995. He has been the dean at the Faculty of Computer Science and Information Systems Since 2004. Currently, he is heading Pervasive Computing Research Group, under K-Economy Research Alliances. His research interests include computer network, network security and grid computing.

Mohammad Bin-Idris is a senior lecturer at Faculty of Computer Science and Information System. He obtained his MSc and PhD in the area of software engineering, and information technology security in 1998 and 2008 respectively. He focuses on the research of designing and development of mobile and telecommunication software. His main research activity in IT security is in the area of intrusion prevention and detection. He is currently active in various academic activities and involves in university-industry link initiative in both areas, and recently received a prestigious award in the mobile software invention by the government of Malaysia and telecommunication leading industry.