Generalized Scheme For Fractal Based Digital Signature (GFDS)

Mohammad Ahmad Alia and Azman Bin Samsudin,

School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia.

Summary
This paper describes a new development in the cryptographic digital signature scheme based on Mandelbrot and Julia fractal sets. Recently it has been shown that it is possible to have digital signature scheme based on fractal due to the strong connection between the Mandelbrot and Julia fractal sets. The link between the two fractal sets is used for the conversion of the private key to a public key. However in the previous work the verification can be done only by a specific party. In this paper we introduce a new variation of the fractal public-key digital scheme (GFDS), whereby the verification of the digital signature can be done by any member of the public.

Key words:
Fractals Cryptography, Digital Signature Scheme, Mandelbrot Fractal Set, and Julia Fractal Set.

1. Introduction

Digital signature is an electronic verification mechanism based on the public-key scheme and is considered as a type of the asymmetric cryptography that is focusing on message authenticity. The digital signature scheme is used to provide a guarantee that the original content of a message is unchanged by unauthorized party which is known as the data integrity, the assurance that the source of data is as claimed which is known as message authentication, and the assurance that an entity cannot deny commitments which is known as non-repudiation [1, 2]. The output of the signature process is called the digital signature [3] (see Figure 1). In digital signature based on public-key algorithms, the private key is used to sign a message, while the public key is used to verify the authenticity of the message.

In 1976, Whitfield Diffie and Martin Hellman gave the first notion of a digital signature scheme although at that time they only conjectured the existence of such scheme [4, 5]. Soon after that, in 1978 Rivest, Shamir, and Adleman proposed the first digital signature scheme that is called RSA digital signature algorithm [6]. Subsequently, few more proposed digital signature algorithms based on different 'hard problems' were soon developed after RSA, such as ElGamal signature scheme [7], Undeniable signature [8] and others.

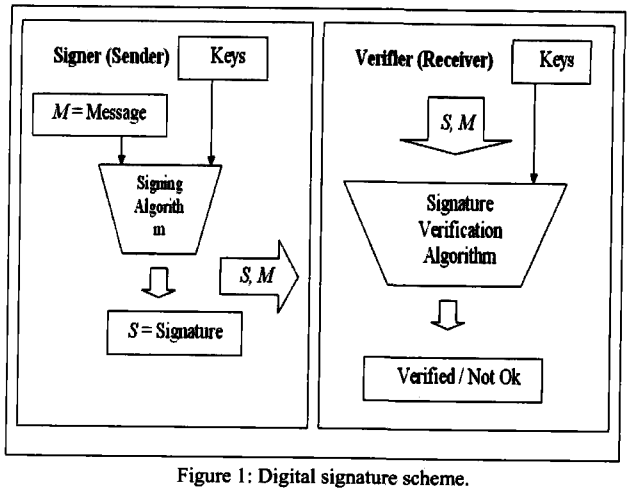


Figure 1: Digital signature scheme.

The well known digital signature schemes can be classified according to the inherited mathematical problems. As of now, there are three main different NP-hard problems (Non-Deterministic Polynomial) where well known digital signature schemes have been derived from.

1. Integer Factorization (IF) schemes. The security in integer factorization schemes are based on the complexity of the integer factorization problem. Examples of IF scheme implementation are RSA digital signature scheme [6] and Rabin digital signature scheme [9].

2. Discrete Logarithm (DL) schemes. Discrete logarithm schemes are based on the complexity of the discrete logarithm problem in a specific finite field. Examples of DL scheme implementation are ElGamal [7], and DSA [10].
3. Elliptic Curve (EC) schemes. The security in elliptic curve schemes is based on the complexity of the elliptic curve discrete logarithm problem. Examples of EC scheme is the elliptic curve digital signature [11].

This paper proposes a new variation of fractal public-key digital signature (FPKDS) scheme to sign and verify the corresponding message. Similar to the original work [12], the functionality of the proposed scheme depends on the strong connection between the Mandelbrot (see Figure 2) and Julia (see Figure 2) sets [13]. Special functions, *Mandelfn* and *Juliafn* functions [14] are used to generate the corresponding private and the public keys.

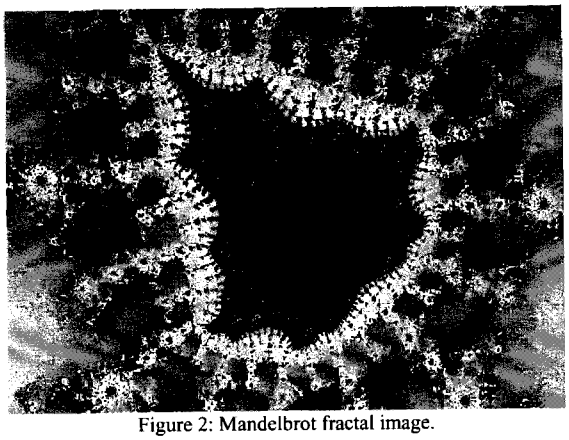


Figure 2: Mandelbrot fractal image.

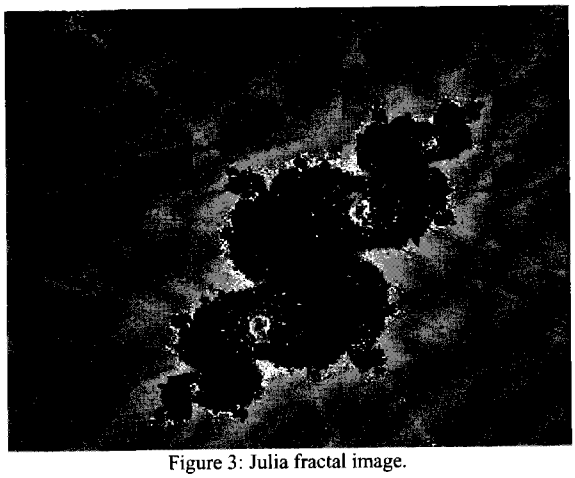


Figure 3: Julia fractal image.

2. Existing Digital Signature Based on The Mandelbrot and Julia Fractal Sets

According to [12], and with the aid of Figure 4, we describe in brief the idea of the fractal digital signature scheme based on fractal set by using Mandelbrot function "*Mandelfn* (see Equation 1) and Julia function *Juliafn* (see Equation 2) [15].

$$z_n = c \times f(z_{n-1});\ z(0) = c;\ c,z \in \mathbf{C}; n \in \mathbf{Z}. \quad (1)$$

$$z_n = c \times f(z_{n-1});\ z(0) = y;\ y,c,z \in \mathbf{C}; n \in \mathbf{Z}. \quad (2)$$

In Figure 4, sender and receiver must agree and use the public domain value, c. The receiver, Bob, generates e and n as the private keys, while the sender, Alice, generates k and d as her private keys. Sender and receiver use their private values as well as the value c as inputs to the Mandelbrot function to produce the public keys z_nd (see Equation 3) and z_ke (see Equation 4). Bob and Alice exchange their public keys. Alice then obtains Bob's public key, z_nd and uses these values together with her private key and the plaintext as inputs to the Julia function to produce the signature s, illustrated by Equation 5. Alice will then send a message to Bob. Bob then obtains Alice's public key, z_ke, the signature s and the message m from Alice which will be used as input values together with his own private key to the Julia function, to verify the message v illustrated in Equation 6.

One limitation of such approach is that, when Alice creates a message, the message can only be verified by a specific individual (in this case the individual is Bob). In the following Section we introduce a new variation to this protocol, such that the verification is not limited to a specific individual but can be made by any member of the public instead.

$$z_nd = z_{n-1} \times c^2 \times d; z,c,d \in \mathbf{C}; n \in \mathbf{Z}. \quad (3)$$

$$z_ke = z_{k-1} \times c^2 \times e; z,c,e \in \mathbf{C}; k \in \mathbf{Z}. \quad (4)$$

$$s = c^{k-x} \times (z_nd)_k e \times m; \quad s,c,e,d \in \mathbf{C};\ n,x,k \in \mathbf{Z};\ m \in \mathbf{R}. \quad (5)$$

$$v = c^{n-x} \times (z_ke)_n d \times m; \quad v,c,e,d \in \mathbf{C};\ n,x,k \in \mathbf{Z};\ m \in \mathbf{R}. \quad (6)$$

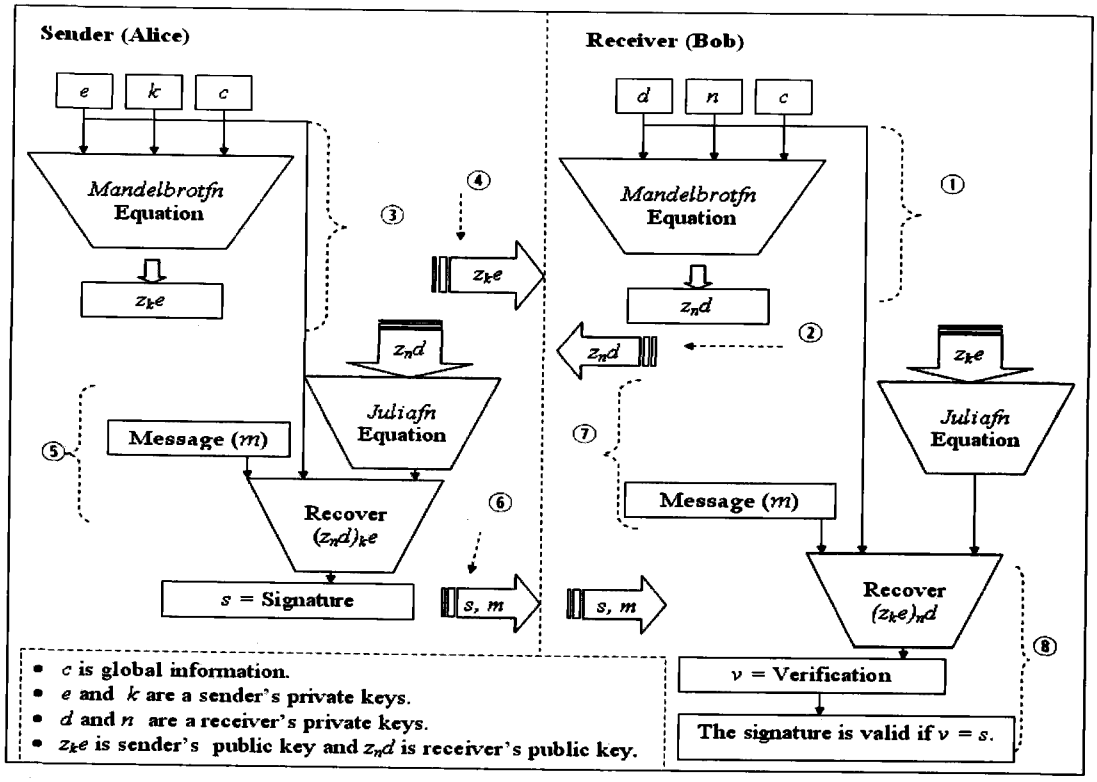


Figure 4: Existing Fractal digital signature algorithm [12].

3. Generalized Scheme of Fractal Based Digital Signature

In this Section, we describe the idea of the generalized fractal public-key digital signature scheme based on fractal set, by using Mandelbrot function "*Mandelfn* (see Equation 7) and Julia function *Juliafn* (see Equation 8) [15].

In Figure 5, sender Alice, choose her private keys k and e and generate c, d and n as public keys. Alice uses her keys as inputs to the Mandelbrot function to produce the private keys $z_n d$ (see Equation 3) and the public key $z_k e$ (see Equation 4). In addition, Alice, generates k and d as her private keys, and then generates her public key for the public. Also, Alice uses her keys together with the message as inputs to the Julia function to produce the signature s which is also illustrated by Equation 5. The signature s will be sent with the message to Bob (a member from the public). After Bob obtains Alice's public key, $z_k e$, c, d, n, the signature s and the message m from Alice, which he will uses as input to Julia function in the verification process to verify the message v. This step is illustrated further by Equation 6. Therefore with this protocol, the general public is able to verify Alice's signature by using Alice's public key. This is an enhancement over the previous method where the verification can only be done by a specific party which needs to be identified by Alice before Alice can create the signature.

4. Key Size Analysis

The chaotic nature of the fractal functions ensures the security of the proposed GFDS scheme is similar to the first digital signature scheme based on fractal Mandelbrot and Julia sets [12]. However, to prevent a brute force attack, the choice of the key size becomes essential. The key space in fractal digital signature depends on the size of the key. For example in 128 bits key, there are 2^{128} possible key values, as is the case in the symmetric scheme. RSA and DSA keys are basically different from fractal keys, where the choice of key is influence by the prime number which exist sparsely in a given finite field.

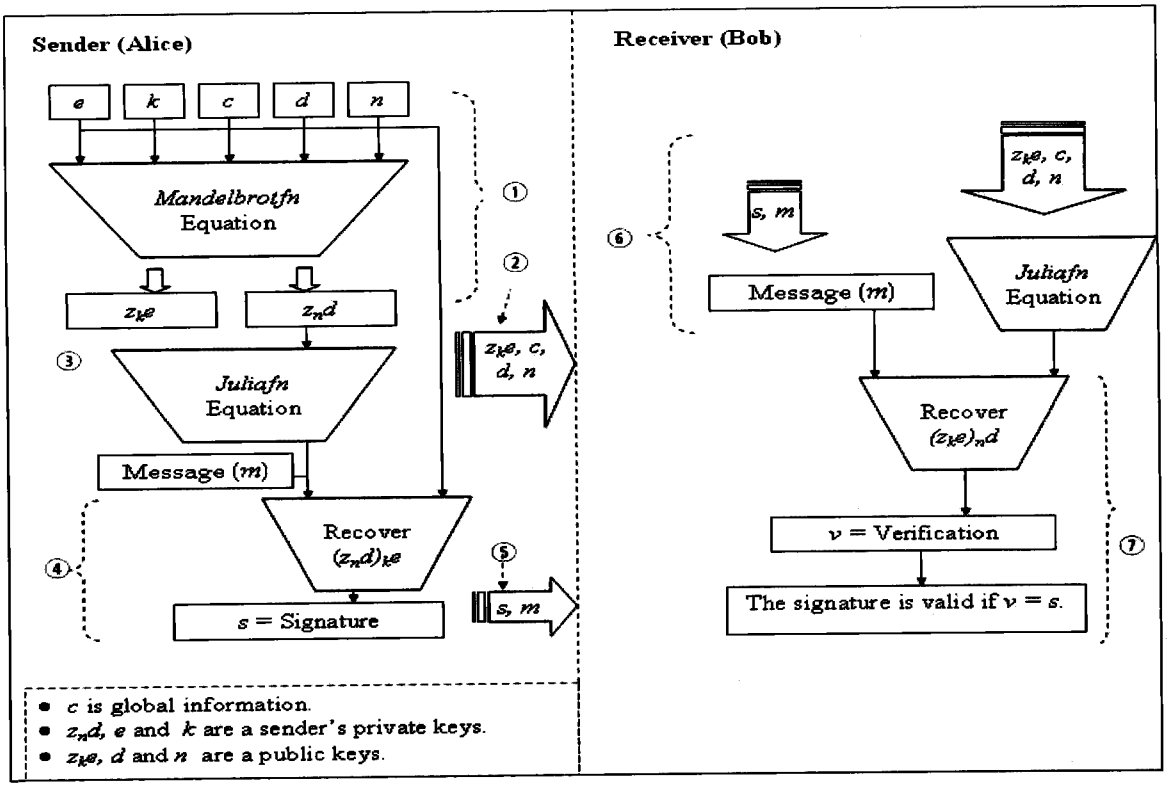


Figure 5: The new generalized version of fractal public-key digital signature.

5. Performance Evaluation

As shown in Figure 4 earlier, the first fractal digital signature scheme involves a sender and a receiver. The receiver must generate the public key from the chosen private key and then sends the public key to the sender. The sender will then generate his public key by using *Mandelfn* function and sends it to the specific receiver who generated his public key. But in our new scheme (see Figure 5), the sender generates his private and public keys and then sends the public keys together with the signed message through the mechanisms of communication to the public. Thus, any receiver could verify the validity of the message if there is no changing in the content. The comparison in terms of algorithm speed and key size is equivalent to the first digital signature scheme based on Mandelbrot and Julia fractal sets.

6. Statistical Analysis

A powerful statistical analysis can be use to test the histogram for the signatures and check correlation coefficient of the statistical analysis [16]. It is well known that many previous digital signature schemes have been successfully analyzed by using statistical analysis. An ideal digital signature should be resistant to the brute force of any statistical attack. Statistical analysis has been performed to prove the strength of the proposed digital signature scheme based on Mandelbrot and Julia fractal sets by calculating the histogram analysis and the correlation coefficient analysis of two adjacent points.

6.1 Histograms Analysis

The histogram image illustrates how the values of the original message signature and the changed message signature are distributed by graphing the number of repeated characters. The histograms have been applied to several signatures. In this Subsection we use the histogram as one of the tools of statistical analysis to clarify the strength of the digital signature scheme based on Mandelbrot and Julia fractal sets. This strength is shown through the histogram distribution of the original message signature and the changed message signature. Figure 6, shows the difference between the signature values before and after the changing in the message content. These changes have been applied on the proposed fractal digital signature. As shown by Figure 7, the histogram presents the distribution for the original message signature value.

The original message before the changing:
CRYPTOGRAPHY_IS_THE_SCIENCE_OF_KEEPING_
THE_MESSAGES_
AND_ENSURING_AUTHENTICATION

Message after the change (removing the first character 'c')
RYPTOGRAPHY_IS_THE_SCIENCE_OF_KEEPING_
THE_MESSAGES_
AND_ENSURING_AUTHENTICATION

Figure 6: An example for the GFDS.

Figure 8, shows the histogram for the changed message signature value. The change between the previous messages is only the first character 'c' which is removed from the original message, which caused the differences in the value of signatures. As shown, those Figures show big differences in the distribution for the signatures histograms.

6.2 Correlation Coefficient Analysis

Correlation coefficient analysis is used in this Subsection to find the correlation between two distributed histogram adjacent points for the signatures that has been used to perform the statistical analysis on the proposed fractal digital signature scheme. The process for the correlation coefficient analysis depends on the random selection of the original message signature and the changed message signature values as pairs of two adjacent points. Calculation for the correlation coefficient is done by using Equations 7, 8, 9, 10 and 11.

$$\mathrm{cov}(x,y) = E(x - E(x)(y - E(y)) \tag{7}$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \tag{8}$$

where x and y are the values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{10}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{11}$$

The correlation result (r) between two adjacent points for distributed signature values was calculated by Equation 8 [17] which was applied in the proposed digital signature scheme based on Mandelbrot and Julia fractal sets. The correlation coefficient value is 0.109138. However, the correlation between the two adjacent points for original message signature and the changed message signature is very close to zero. This represents a non correlation and can be defined as uncorrelated. The uncorrelated result highlights the difficulty of attacking the signature by changing the message content.

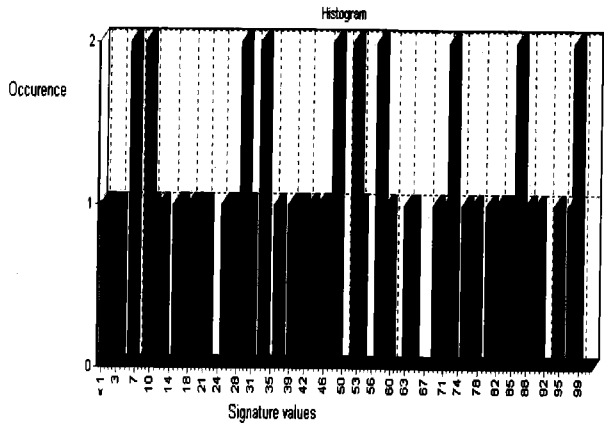


Figure 7: Histogram signature of the original massage.

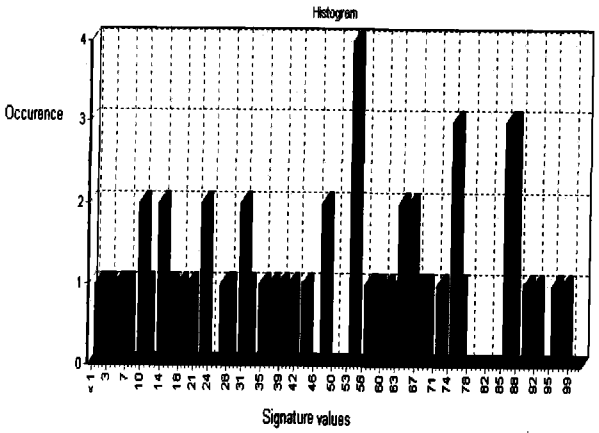


Figure 8: Histogram signature of the changed massage.

7. Conclusion

This paper shows the possibility of establishing a fractal based digital signature with public verification, derived from the logical connection between the Mandelbrot and Julia fractal sets. The security protection of the proposed generalized fractal digital signature depends on the changes of the public keys values ($z_n d$, $z_k e$) which are affected by the signer's private keys (e, k). The GFDS presents the possibility of verifying the message by any member of the public which is enhancement over the previous fractal digital signature, where the signature van only be verified by a specific verifier.

Acknowledgments

The authors would like to thank the Universiti Sains Malaysia (USM) for supporting this study.

References

[1] W. B. Schultz, "Electronic Records; Electronic Signatures," *Federal Register* , vol. 62, no. 54 , pp. 13430-13466, 2007.

[2] A., Menezes, P. Van Oorschot, and S. Vanstone, "*Handbook of Applied Cryptography*," CRC Press, pp. 4 - 15, 516, 1996.

[3] Public Law, "Electronic Signatures in Global and National Commerce Act," *Weekly Compilation of Presidential Documents*, vol. PUBLIC LAW 106-229, no. 36, pp. 464-476, 2000.

[4] W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no.6, pp. 644-654, 1976.

[5] A. A. Lysyanskaya, "Signature Schemes and Applications to Cryptographic Protocol Design," PhD thesis, MIT, Massachusetts Institute of Technology, pp. 1-3, 2002.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on*, vol. 31, no. 4, pp. 469 – 472, 1985.

[8] C. David, and H. V. Antwerpen, "Undeniable Signatures," *Crypto'89, LNCS 435, Springer-Verlag, Berlin*, pp 212-216, 1990.

[9] K. Kaoru and W. Ogata, "Efficient Rabin-type Digital Signature Scheme," Designs, Codes and Cryptography, Springer Netherlands, vol. 16, no. 1, pp. 53-64, 1999.

[10] J. Burrows, "Digital Signature Standard (DSS)," *Federal Information Processing Standards Publication 186, Computer Systems Laboratory, National Institute of Standards and Technology*, Fips Pub 186, pp. 1-5, 1994.

[11] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Certicom*, 2001.

[12] M. Alia, and A. Samsudin, "A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Set," American Journal of Applied Sciences, vol. 4 , no. 11, pp. 850-858, 2007.

[13] B. Mandelbrot, "*Fractal Geometry of Nature*," San Francisco: W. H. Freeman, 1982.

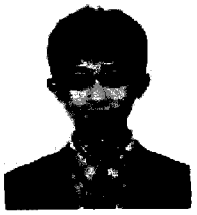
[14] N Giffin, "Fractint," *The University of British Columbia Campus in Vancouver B.C. Canada*, TRIUMF project, pp. 1-7, 2006.

[15] M. Alia, and A. Samsudin, "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Set," *International Journal of Computer Science and Network Security*, vol. 7, no. 2, pp. 302-307, 2007.

[16] S. Behnia, A. Akhshani, A. Akhavan,, and H. Mahmodi, "Applications of Tripled Chaotic Maps in Cryptography," *arXiv.org, The Cornell University*, 2007.

[17] H. E. H. Ahmad, H. M. Kalash, and O. S. FaragAllah, "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption," *Informatica*, vol.4, no. 31, pp. 121-129, 2007.

Mohammad A. Alia received the B.S. degree in Computer Sciences and M.S. degree in Information Technology from Al-Zaytoonah University in 2000 and 2003, respectively. During 2000-2004, he stayed at Al-Zaytoonah University-Jordan as an instructor of Computer Sciences and Information Technology. Then, he worked as a lecturer at Al-Quds University in Saudi Arabia form 2004 - 2005. Currently he is a PhD student at the School of Computer Sciences, Universiti Sains Malaysia.



Azman Samsudin is a lecturer at the School of Computer Sciences, Universiti Sains Malaysia. He received the B.Sc. degree in Computer Science from the University of Rochester, USA, in 1989. He obtained his M.Sc. and Ph.D. degrees in Computer Science from University of Denver, USA, in 1993 and 1998, respectively. His research interests are in the field of Cryptography, Interconnection Switching Networks, and Parallel Distributed Computing.