J. Basic. Appl. Sci. Res., 2(2)1678-1684, 2012

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Speech Signal Encryption Using Chaotic Symmetric Cryptography

M. Ashtiyani *, P. Moradi Birgani, S. S. Karimi Madahi

Department of Electrical Engineering, Damavand Branch, Islamic Azad University, Damavand, Iran

ABSTRACT

With development of Information and Communication Technology, data transmission becomes more critical day by day. Higher security for transmitting data is especially required. Therefore, we propose an encryption scheme for the speech signal encryption based on combination of scrambling and confusion. Chaotic cat map is used for the scrambling the addresses of the speech signal samples. In order to provide security for the scheme, a modified form of Simplified version of Advance Encryption Standard (S-AES) is introduced and applied. The modification is that we make use of chaos for S-box design and replace it with that of S-AES. The so called Chaotic S-AES has all cryptographic characteristics and requirements of S-AES. Hence, the main contribution of this work is that we make use of chaos in both signal diffusion and confusion parts. In order to check the performance of the method, experimental implementation has been done. It worth be noting that the resistance of the scheme against differential and linear cryptanalysis is at least as of S-AES.
KEY WORDS: Chaos, Encryption, S-box design, speech signal, Symmetric cryptography.

INTRODUCTION

Nowadays human beings need to communicate more than ever. At present, secure communication plays an increasing and ever-growing role in many fields of common life, such as banking, commerce, telecommunication and networking. Some communications must be reliable and have the best security as possible as they can. There are many different methods for communication in security like cryptography.

With the rapid development of the internet and the multimedia technology, the traffic of speech signal has grown rapidly and speech signal is becoming important carrier of information communion for people.

Nowadays, the transmission of speech signal is a daily routine, especially over wireless networks. The chaos and cryptography makes chaos based cryptographic algorithms. As a natural candidate for secure communication and cryptography chaos based encryption techniques are considered good for practical use as these techniques provide, a good combination of speed, high security, complexity, reasonable computational overheads and computational power.

The chaos based cryptographic algorithms, and suggested some new and efficient ways to develop secure signal encryption techniques. Towards this direction, we design an efficient chaos based symmetric cryptography system for speech signal encryption. In this paper, a new speech signal encryption system is proposed, in this system we use symmetric cryptography and chaos for encrypt speech signal. Symmetric cryptography algorithm that we used in this project is Simplified Advance Encryption Standard (S-AES).

CHAOS AND CRIPTOGRAPHY

Chaos functions have mainly used to develop mathematical models of non linear systems. They have attracted the attention of many mathematicians owing to their extremely sensitive nature to initial conditions and their immense applicability to modeling complex problems of daily life [1].

Chaotic functions which were first studied in the 1960's show numerous interesting properties. The iterative values generated from such functions are completely random in nature, although limited between bounds [2]. The most fascinating aspect of these functions is their extreme sensitiveness to initial conditions. For example even if the initial start value of iterations is subjected to a disturbance as small as 10^{-100}, iterative values generated after some number of iterations are completely different from each other [3]. This extreme sensitivity to the initial conditions makes chaotic functions very important for application in cryptography and in this cryptosystem the key sensitivity is determined by the parameter sensitivity of chaotic map and the initial-value sensitivity of diffusion function [4]. The characteristics of the chaotic maps have attracted the attention since it has many fundamental properties such as ergodicity, sensitivity to initial condition, system parameter, mixing property, etc. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography. The chaos is a process of definite pseudo-random sequence produced by nonlinear dynamics system. It's non-periodic and non-astringe.

PROPOSED ALGORITHM

Our proposed method for speech signal encryption consists of three parts, namely sampling, scrambling and encryption. Both of scrambling and encryption use chaos for design process as we will explain hereafter. Figure 1 illustrates the block diagram of our algorithm. The scrambling block, which provides confusion for our scheme, is in

***Corresponding Author:** Meghdad Ashtiyani, Department of Electrical Engineering, Damavand Branch, Islamic Azad University, Damavand, Iran, phone: +98 912 3079886, Email: m.ash.80@gmail.com

essential a chaotic map. Each chaotic mapping is a set of differential equations which often design to represent an unpredictable phenomenon of the environment. Parameters of the mapping, i.e. differential or difference equations should be chosen so that the outputs of the system have an adequate level of unpredictability. Any chaotic mapping which attains required level of security can be used here. Our approach differs with all previous works in the sense that we use chaos to provide both diffusion and confusion. That is, we also make use of chaos in encryption process by utilizing it in S-box design procedure. As depicted, the speech signal first scrambled via Cat Map chaotic mapping. Then the second stage provides diffusion for bits modification in the speech signal by applying S-AES algorithm (with chaotic S-box) to every sample. As it was also shown in [5], combining cat map with block cipher system can provides additional features for the system. We will explain these three sub blocks of scheme in figure 1.

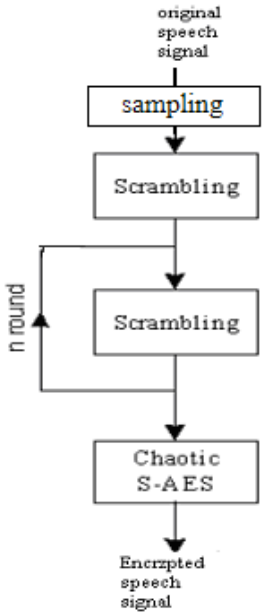

Fig. 1. Block diagram of this project

SAMPLING

The typical method of obtaining a discrete-time representation of a speech signal is through periodic sampling, wherein a sequence of samples x[n], is obtained from a continuous-time speech signal $x_c(t)$ according to the equation (1).

$$x[n] = x_c(nT), \qquad -\infty \le n \le \infty \tag{1}$$

It is convenient to represent the sampling process in the two stages depicted in figure 2. The stages consist of an impulse train modulator followed by conversion of the impulse train to a sequence. Figure 3 show a continuous-time speech signal $x_c(t)$ and result of impulse train sampling for T sampling rate. Figure 4 depicts the corresponding output sequence. The periodic impulse train defines as equation (2) [6-9].

$$s(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT) \tag{2}$$

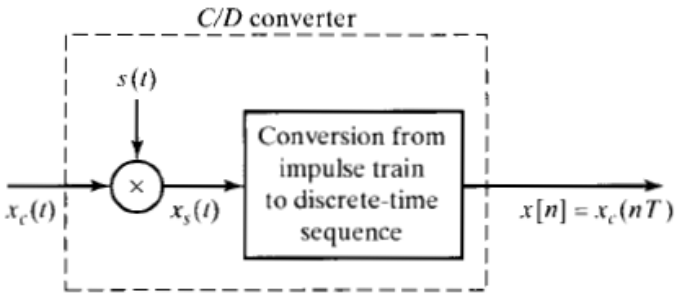

Fig. 2. Sampling of speech signal with a periodic impulse train

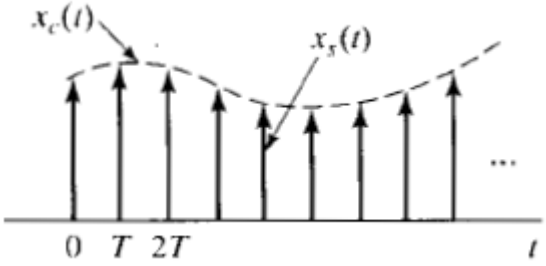

Fig. 3. Continuous-time speech signal

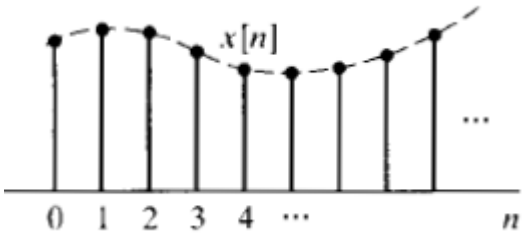

Fig. 4. Discrete-time speech signal

SCRAMBLING

In this project for advancing the quality of encryption effectively, we have used position scrambling method before encryption. This stage is called confusion stage that permutes the bits in the discrete-time speech signal without changing its values by applying scrambling algorithm.

Some classical scrambling algorithms are cat map [2], baker map [10], knight-tour transformation [11], affine transformation [12], magic-square transformation [12], standard map, tent map etc. Among these maps, baker map and cat map attract much attention. Cat map is a two- dimensional chaotic map introduced by Arnold and Avez. Baker map is another two dimensional chaotic map based on which Pichler and Scharinger first introduced their encryption schemes. The 2-D chaotic cat map was generalized to 3-D for designing a real-time secure symmetric encryption scheme, which employed 3-D cat map to shuffle the positions of signal sample and used another chaotic map to confuse the relationship between the cipher-signal and the plain-signal [13]. In [14], baker map was further extended to 3-D. An alternative chaotic signal encryption based on baker map that supports a variable-size signal and includes other functions such as password binding and bit shifting to further strengthen the security of the cipher-signal was proposed [15]. In [16], Baptista proposed a chaotic encryption based on partitioning the visiting interval of chaotic orbits of the logistic map. In this project we apply cat map for scrambling of speech signal.

Cat Map

In this structure have three inputs x, y coordinate potential lines and other contamination of different voltage levels for transmission Cat mapping is from Arnold, and it is named because of demonstrating it with a cat's face usually, the classical Arnold cat map is a two-dimensional map [8] described by equation (3).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} . \begin{bmatrix} x_n \\ y_n \end{bmatrix} \mod(N) \tag{3}$$

Where (x_n,y_n) is the position of samples in the NxN data such as image, so that equation (4).

$$(x_n, y_n) \in \{0, 1, 2, .., N-1\} \tag{4}$$

And (x_{n+1},y_{n+1}) is the transformed position after cat map, a and b are two control parameters and are positive integers. Cat map has two typical factors, which bring chaotic movement: tension (multiply matrix in order to enlarge x, y) and fold (taking mod in order to bring x, y in unit matrix). In fact, cat map is a chaotic map. For applying cat map we must transform the discrete-time speech signal to NxN matrix.

First discrete-time speech signal divided to blocks with length 256 (for example the second block consist of x[256], x[257] … x[511]), and then each block of speech signal with size of 1x256, expanded to the 256x256 matrix. The block number λ expands to 256x256 matrix via equation (5).

$$\begin{bmatrix} x[0+256\lambda] & x[1+256\lambda] & \cdots & x[255+256\lambda] \\ x[0+256\lambda] & x[1+256\lambda] & \cdots & x[255+256\lambda] \\ \vdots & \vdots & \ddots & \vdots \\ x[0+256\lambda] & x[1+256\lambda] & \vdots & x[255+256\lambda] \end{bmatrix} \quad \lambda = \{0, 1, 2, .., \infty\} \tag{5}$$

Samples positions of expanded discrete-time speech signal are scrambled via the iteration of cat map, consequently realizing the speech signal encryption. The result of scrambling is different for difference of the iteration times.

For 256x256 expanded speech signals, it is hard to find out the trace of original signal after iterating 30 times, reaching the effect of scrambling; the expanded speech signal after iterating 64 times is the same as the original signal, so cat map has the periodicity. With the differences of the parameter and the signal's size, the periodicity is different. Expanded speech signal can be scrambled via keeping the value of a, b secret, but the periodicity will bring some insecure factors, so applying cat map solely cannot meet the demands of encryption; and cat map only transforms the original signal's position, however the discrete time's values have not been changed [5].

CHAOTIC S-AES

The next, but somehow more important part of our proposed scheme is encryption part. Since high speed for encryption/decryption is a feature of interest in online secure speech signal transmission, we have to apply encryption/decryption scheme which has satisfactory speed in practical implementation.

Besides security level of this block is of great importance as diffusion of the signal information is provided with this block. Many renowned block ciphers, such as DES, AES, MISTY est., can be used based on required level of security, size of the key, speed of implementation and other related design metrics. Some previous works, such as [5], are of this family. That is they utilize block ciphers in conjunction with scrambling for signal encryption. It applies cat chaotic map for scrambling of bit contents and simplified DES for encryption.

Our approach differs with all previous works in the sense that we use chaos to provide both diffusion and confusion. That is, we also make use of chaos in encryption process by utilizing it in S-box design procedure, figure 5.

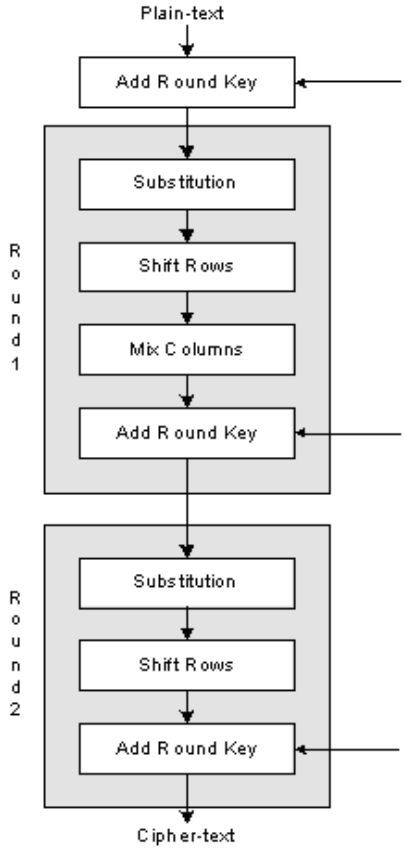

Fig. 5. Block diagram of S-AES

Here, we briefly overview chaotic S-box design. Security of block ciphers mainly relies on the S-boxes, since they are the only nonlinear element in block cipher algorithm. So designing S-boxes to maintain cryptographic requirements is actually the heart of block cipher design. S-box design criterion of the most famous block cipher, DES, have been mysterious for decades, after its adaptation as a federal standard in 1977 and have not been published till now. On the other hand, new block cipher designers often clarify their assumed criterion for picking up an S-box. For, S-box of AES, new selected block cipher in replacement of DES has been chosen mathematically. Due to lack of space, we cannot review this subject anymore and just comes up to our used scheme. Some papers employ chaos for S-box design. We use the presented approach in [17] and produce chaotic-based S-box for S-AES. S-AES is simplified version of AES algorithm [18]. It operates on 16-bit plaintexts and generates 16-bit cipher texts, using the expanded key k0, k1, …, k47.

For more information about S-AES, we recommend taking a look at [18]. In order to produce an S-box with chaos, it is necessary to choose a chaotic mapping with good level of unpredictability and irregularity. Then one of the outputs should be selected, quantized and sampled. Numbers of quantization levels are equal to the S-box size. We make use of Lorenz chaotic mapping [19-22], in the procedure of S-box design. We will review Lorenz chaotic mapping in more details in the preceding part of this section.

The first and most necessary characteristic to check is that the obtained S-box is reversible. The other essential cryptographic characteristics and requirements for obtaining good S-box have been check and S-box with satisfactory level of them has been chosen. It must be noted that some parameters of the chaotic mapping and sampling rate should be tuned well in order to reach acceptable S-box. This S-box then replaced with the S-box of S-AES to attain chaos-based block cipher, which we name it chaotic S-AES hereafter. That the chaos is also used in the design of encryption algorithm is the main prominence of our work comparing with the formers.

Lorenz Chaotic Function

The Lorenz equation is commonly defined as three coupled ordinary differential equation (6).

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = x(\tau - z) - y$$
$$\frac{dz}{dt} = xy - \beta z \tag{6}$$

Where the three parameters σ, τ, β are positive and are called the Prandtl number, the Rayleigh number, and a physical proportion, respectively. It is important to note that the x, y, z are not special coordinate. The x is proportional to the intensity of the convective motion, while y is proportional to the temperature difference between the ascending and descending currents, similar signs of x and y denoting that warm fluid is rising and cold fluid is descending. The variable z is proportional to the distortion of vertical temperature profile from linearity, a positive value indicating that the strongest gradients occur near the boundaries.

Lorenz equations have some benefits for cryptographic application such as:

- Invariance: The z-axis is invariant, meaning that a solution that starts on the z-axis *(i.e.* x=y=0*)* will remain on the z-axis. In addition the solution will tend toward the origin if the initial condition is on the z-axis. A graph within a graph is an “inset”, not an “insert”. The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
- Symmetry: The Lorenz equation has the following symmetry of ordinary differential equation (7).

$$(x, y, z) \rightarrow (-x, -y, z) \tag{7}$$

This symmetry is present for all parameters of the Lorenz equation.

- Equilibrium points: To solve for the equilibrium points we let, equation (8).

$$\dot{x} = f(x) = \begin{bmatrix} \sigma(y - x) \\ x(\tau - z) - y \\ xy - \beta z \end{bmatrix} \tag{8}$$

And we solve f(x)=0. It is clear that one of those equilibrium points is x_0=(0,0,0) and with some algebraic manipulation we determine equation (9), (10).

$$x_{C1} = (-\sqrt{\beta(\tau - 1)}, -\sqrt{\beta(\tau - 1)}, \tau - 1) \tag{9}$$

$$x_{C2} = (-\sqrt{\beta(\tau - 1)}, -\sqrt{\beta(\tau - 1)}, \tau - 1) \tag{10}$$

are equilibrium points and real when $\tau > 1$.

Solutions stay close to origin: If $\sigma, \tau, \beta > 0$ then all solution of the Lorenz equation will enter an ellipsoid centered at $(0, 0, 2\tau)$ in finite time. In addition the solution will remain inside the ellipsoid once it has entered. It follows by definition that the ellipsoid is an attracting set.

RESULTS

A man speech signal employed for experimentation. The original speech signal is shown in figure 6, its histogram is given in figure 7. The histogram of scrambled speech signal is shown in figure 8. It was observed from figure 7 and figure 8 that both histograms are same. It means that the corresponding statistical information of scrambled signal after confusion process is exactly the same as that of the original signal. It is due to the fact that cat map does not change the values of the discrete-time speech signal. The histogram of encrypted speech signal is shown in figure 9. It is more uniform. It was observed that this histogram is entirely different from one shown in figure 7.

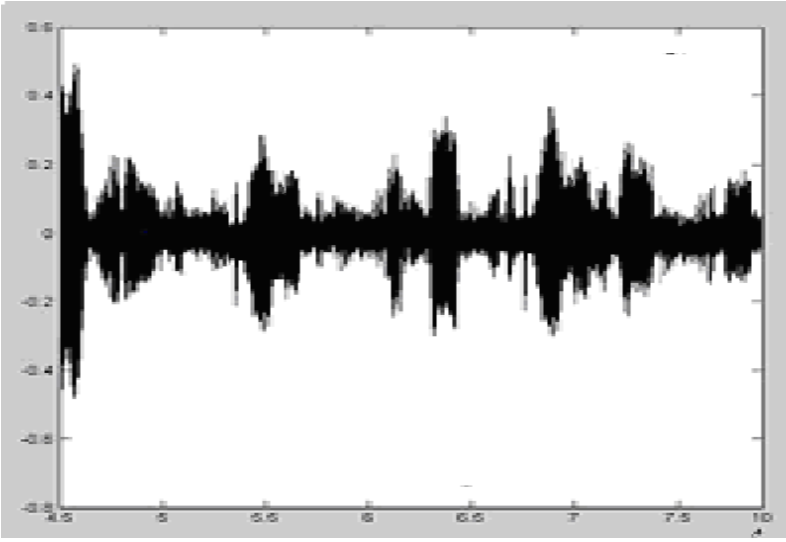

Fig. 6. Original speech signal

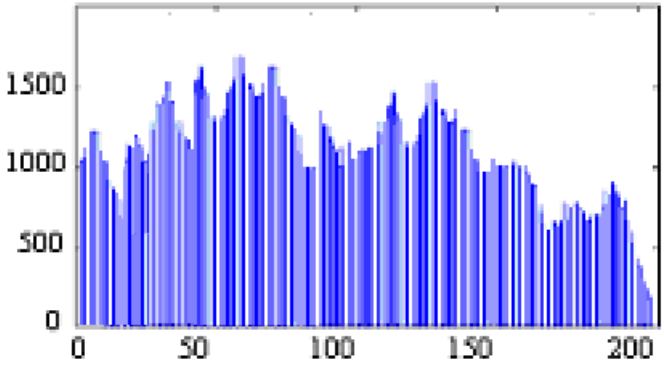

Fig. 7. Histogram of speech signal in fig. 3.

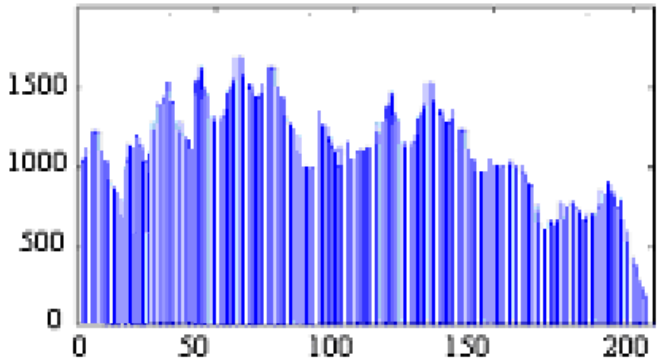

Fig. 8. Histogram of scrambled speech signal

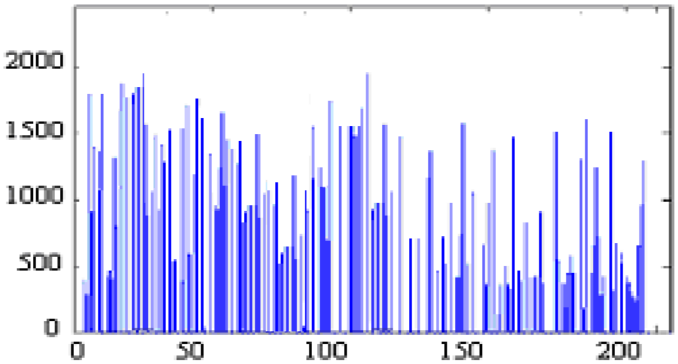

Fig. 9. Histogram of scrambled and encrypted speech signal

CONCLUSION

In this paper, a speech signal encryption scheme based on the combination of chaotic map for the scrambling the addresses of the input data and chaotic simplified AES for the encryption is proposed to achieve adequate level of security for speech signal transmission. Efficiency of the scheme has been confirmed through experimental tests. The main advantage of our approach is that we make use of chaos in both scrambling and encryption procedure. As a result, our proposed algorithm differs with all previous works in the sense that we use chaos to provide both diffusion and confusion. That is, we also make use of chaos in encryption process by utilizing it in S-box design procedure. It worth be noting that the resistance of the scheme against differential and linear cryptanalysis is at least as of S-AES.

REFERENCES

1. M.Ashtiyani, S.Asadi, P.H.Goudarzi, "A New Method in Transmitting Encrypted Data by FCM Algorithm", proceeding of ICTTA06 conference, Syria, (2006).
2. G.R. Chen and Y.B. Mao et al., "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals 21, pp. 749–7612, (2004).
3. J.S. Yen and J.I. Guo, "A New Chaotic Key-based Design for Image Encryption and Decryption", *IEEE Proc. on Circuits and Systems*", vol. 4, pp. 49-52, (2000).
4. X.Y .Yu, J .Zhang, H.E.Ren, G.S.Xu1 and X.Y.Luo. "Chaotic Image Scrambling Algorithm Based on S-DES", Journal of Physics: Conference Series 48, pp. 349–353, (2006).
5. Kh. S. Singh, S. Devi and S. S. Singh, "Encryption Scheme based on Combination of Cat Map and SDES", DOEACC Center, Imphal.
6. S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalysis of an image encryption scheme", *J. Electronic Imaging*, vol. 15, no. 4, p. art. no. 043012, (2006).
7. http://mathworld.woffram.com/arnoldsCatMap.html
8. T.-J. Chuang and J.-C. Lin, "New approach to image encryption", *J. Electronic Imaging*, vol. 7, no. 2, pp. 350–356, (1998).
9. K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3d cat map based symmetric image encryption scheme", *Physics Letters A*, vol. 343, pp. 432–439, (2005).
10. Y. Mao, G. Chen and S. Lian, "A Novel Fast Image Encryption Scheme based on on the 3-D Chaotic Baker Map", *Int. J. ifurcat Chaos*, vol. 14, no. 10, pp. 3613-3624, (2004).
11. T. B. Arthur and Y. Kan, "Magic Squares Indeed", J. the Mathematical Gazette, 108, pp. 152-156, (2001).
12. H.T. Chang, "Arbitrary affine Transformation and Their Composition Effects for Two-dimensional Fractal Sets", *J. Image and Vision Computing*, 22, pp. 1117-1127, (2004).
13. C. Charilaos, S. Athanassios and E. Touradj, "The JPEG2000 Still Image Coding Systems", *IEEE Trans.on Consumer Electronics* 46, pp. 1103-1127, (2000).
14. R. Matthews, "On the Derivation of a Chaotic Encryption", *Cryptologies*, XIII(1), pp. 29-49, (1989).
15. G. Jakimoski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers based on Chaotic Maps", *IEEE Trans. on Circuits and Systems1, fundam. Theory Applic*. vol. 48, no. 2, pp. 163-169, Feb. (2001).
16. M.S. Baptista, "Cryptography with Chaos", *Phys. Letters, A*, 240 (1-2), (1998).
17. P. Amani, H. Khalozadeh, and M. R. Aref, "S-box design for AES block cipher with chaotic mapping", in *Proceeding of 4th Iranian Society of Cryptology Conference(ISCC07),* Tehran, Iran, 16-18 Oct, pp.91-98, (2007).
18. . Musa, E. Schaefer, and S. Wedig, "A simplified AES algorithm and its linear and differential cryptanalyses", in *Cryptologia* 27, pp.148–177, April (2003).
19. B. schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition, John Wiley and Sons, 1996.
20. J. L. Lorenz, and Y. Pomeau, "A simple case on nonperiodic (strange) attractor", in *Journal of Non. Equib. Thermodyn.,* vol. 3, pp. 135-152, (1978).
21. W. Stallings, Cryptography and Network Security, Third Edition, Prentice Hall 1999.
22. D. Stinson, *Cryptography Theory and Practice*, second Edition, CRC Press, 2002.