Image Encryption Using Hyper Chaos and Symmetric Cryptography

Mozhgan Mokhtai*, Meghdad Ashtiyani[#] , Hassan Naraghi**
Department of Mathematics, Ashtian Branch,Islamic Azad University, Ashtian, Iran[*,**]
Tehran University of Medical Science, International Campus (TUMS-IC) Tehran, Iran[#]
mozhganmokhtari@yahoo.com*, naraghi@aiau.ac.ir**, m-ashtiyani@razi.tums.ac.ir[#]

Abstract— **In recent years, a large amount of work on chaos-based cryptosystems has been published. However, most of them encounter some problems such as low level of security and small key space. The key stream generator is the key design issue of an encryption system. In this paper a new approach to image encryption based on hyper chaotic map is proposed in order to meet the requirements of the secure image transfer. In the proposed encryption scheme, 4D hyper-chaotic system is used in key scheming, this encryption scheme is also based on combination of scrambling and confusion. Chaotic cat map is used for the scrambling the addresses of the image pixels. In order to provide security for the scheme, a modified form of Simplified version of Advance Encryption Standard (S-AES) is 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 image 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 [3,4].**

Keywords-hyper chaos; cat map; cryptography; Advance Encryption Standard (AES);

I. 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, networking and so on. 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.

Over the past decade, there has been tremendous interest in studying the behavior of chaotic systems. Chaotic functions are blessed with properties like sensitivity to the initial condition, and ergodicity which make them very desirable for cryptography [1]. The close relationship between 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, etc.

Unlike the conventional cryptographic algorithms which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Therefore, it can provide a fast and secure means for data protection, which is crucial for data transmission over fast communication channels, such as the broadband internet communication [2].

The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure data encryption techniques. Towards this direction, we design an efficient chaos based symmetric cryptography system for image encryption. In this paper we use symmetric cryptography and chaos for encrypt images. Symmetric cryptography algorithm that we used in this project is Advanced Encryption Standard (AES) [3, 4].

II. CRYPTOGRAPHY AND CHAOS

The chaos is a process of definite pseudo-random sequence produced by nonlinear dynamics system. It's non-periodic and non-astringe. 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. 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. 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. This extreme sensitivity to the initial conditions makes chaotic functions very important for application in cryptography.

The chaos-based encryption was first proposed in 1989 [11], since then, many researchers have proposed and analyzed a lot of chaos-based encryption algorithms, these work all have been motivated by the chaotic

properties such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc.[9]

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.

Recently, in [13], a fast chaotic cryptographic scheme based on iterating a Logistic map was proposed, and no random numbers need to be generated and the look-up table used in the cryptographic process is updated dynamically. In [14], a 2D chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme, which employs the 3D cat map to confuse the relationship between the cipher-image and the plain-image. To overcome the drawbacks such as small key space and weak security of one-dimensional chaotic map, a nonlinear chaos algorithm is proposed in [18], which shows high-level security and acceptable efficiency. Recently, because hyper-chaos has more than one positive Lyapunov exponent, and have more complex dynamical characteristics than chaos, so secure communication schemes based on hyper-chaotic systems have been investigated [20], but at present, there is little work about the study of encryption algorithm based on hyper-chaos. In general, as the prediction time of a chaotic system is longer than that of a hyper-chaotic system [21], so it may be more valuable to study the application of hyper-chaos in encryption algorithms[9]

III. PROPOSED ALGORITHM

Our proposed scheme for image encryption consists of two processes, namely scrambling and encryption. Firstly, we scramble the image based on total image scrambling matrix generated by using 2D chaotic map, and then encrypt the scrambled image by using hyper chaos. Both of processes 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 essential a chaotic map [3].

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 [4].

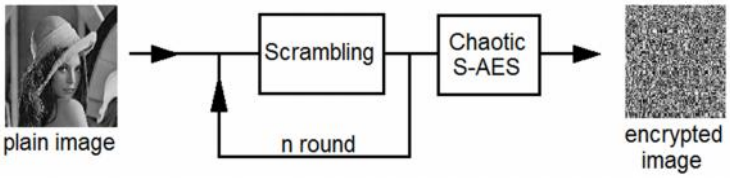

Figure 1. Block diagram of this project

As depicted, the image pixels first scrambled via Cat Map chaotic mapping. Then the second stage provides diffusion for pixels values modification in the image by applying S-AES algorithm (with chaotic S-box) to every pixel. As it was also shown in [7], combining cat map with block cipher system can provides additional features for the system. We will explain these two sub blocks of scheme in following.

IV. IMAGE SCRAMBLING

In this project for advancing the quality of encryption effectively, we have used pixel position scrambling method before encryption. This stage is called confusion stage that permutes the pixels in the image without changing its values by applying scrambling algorithm.

Some classical scrambling algorithms are cat map [6], knight-tour transformation [12], affine transformation [11], 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 [35]. Baker map is another 2D chaotic map based on which Pichler and Scharingfirst 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 image pixels and used another chaotic map to confuse the relationship between the cipher-image and the plain-image. In [13], baker map was further extended to 3-D. An alternative chaotic image encryption based on baker map that supports a variable-size image and includes other functions such as password binding and pixel shifting to further strengthen the security of the cipher-image was proposed [31]. In [15], 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 image [3].

A. Image scrambling using cat map

Image data has strong correlations among adjacent pixels. In order to disturb the high correlation among pixels, an image total scrambling matrix is used to scramble the position of the plain image. Without loss of generality, we assume that the dimension of the plain image is $N \times M$, the position matrix of pixels is $P_{x_n,y_n}(I)$, $x_n \in \{0, 1, 2, .., N-1\}$, $y_n \in \{0, 1, 2, .., M-1\}$, where $P_{x_n,y_n}(I)$ is the grey value of the image.

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 [7] described by:

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

where (x_n, y_n) is the pixel position in the $N \times M$ image so that :

$$\begin{aligned} x_n &\in \{0, 1, 2, .., N-1\} \\ y_n &\in \{0, 1, 2, .., M-1\} \end{aligned} \tag{2}$$

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. Image position is scrambled via the iteration of cat map, consequently realizing the image encryption. The result of scrambling is different for difference of the iteration times. For a 256× 256gray image, it is hard to find out the trace of original image after iterating 30 times, reaching the effect of scrambling; the image after iterating 64 times is the same as the original image, so cat map has the periodicity. With the differences of the parameter and the image's size, the periodicity is different. Image can be scrambled via keeping the value of a and 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 image's position, however the pixels' values have not been changed [4].

I. CHAOTIC 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 image 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 image information is provided with this block. Many renowned block ciphers, such as DES, AES, MISTY etc, 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 [34], are of this family. That is they utilize block ciphers in conjunction with scrambling for image encryption. It applies cat map for scrambling of pixel contents and simplified AES for encryption. Our approach differs with 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 [3, 4].

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 [32] and produce chaotic-based S-box for S-AES. S-AES is simplified version of AES algorithm [33]. It operates on 16-bit plaintexts and generates 16-bit cipher texts, using the expanded key k_0,.., k_{47}.

For more information about S-AES, we recommend taking a look at [33]. 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 hyper-chaotic mapping [18], in the procedure of S-box design

The first and most necessary characteristic to check is that the obtained S-box should be 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 in comparison with the formers [3, 4].

II. HYPER CHAOTIC KEY SPACE

While classical encryption algorithms are sensitive to keys, so some elaborated constructions are need to achieve satisfying and safer chaos-based encryption. It is well known that a good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible [12].

The difference between hyper-chaos and chaos is that the further is unstable in at least two directions, while the latter only diffuses in one certain direction. In other words, the hyper-chaos has at least two positive Lyapunov exponents, while the latter has only one. For security, because hyper chaotic systems have more complicated phase space than chaotic systems, it is difficult to use those methods based on chaos synchronization to attack them [9].

Compared with one-dimensional chaotic map, for example, logistic mp and skew tent map, 4D hyper chaotic system defined as (1) has more control parameters and initial conditions. It can enlarge the key space when it is combined in the image encryption algorithm.

In the proposed encryption scheme, this 4D hyper-chaotic system generated from Chen's chaotic system [30] is used in key scheming, which is modeled by:

$$\begin{cases} x' = a(y - x) \\ y' = -xz + bx + cy - w \\ z' = xy - dz \\ w' = x + k \end{cases} \tag{3}$$

Where when a = 36, b = −16, c = 28, d = 3, and k [−0.7, 0.7], the system can be in chaos phenomena (Figure 2, 3 and 4), and its Lyapunov exponents are $a_1 = 1.499$, $a_2 = 0.019$, $a_3 = 0$, $a_4 = -10.54$. More details can be seen and studied in [5] with some other properties.

With randomly chosen initial conditions x_0, y_0, z_0 and w_0, if the system (1) is iterated after many rounds, we can get a chaotic sequence $s = \{x_0, y_0, z_0, w_0, x_1, y_1, z_1, w_1, \ldots\}$.

This chaotic system selects four control parameters for the key, four initial values change with encryption process, so the key space is large enough. We can divide image into many sections, and each section is encrypted with a different key, the key is produced through four dimensional map and AES algorithm, and it is more secure. Due to the randomness of four-dimensional map and the security of AES, it is hard to get internal control parameters even if someone knows the key generator. The probability of obtaining the encryption keys is very low [9].

As the hyper-chaos has two positive Lyapunov exponents, so the prediction time of a hyper chaotic system is shorter than that of a chaotic system [21], as a result, it is safer than chaos in security algorithm. For more detailed analysis of the complex dynamics of the system, please see relative references [30, 9].

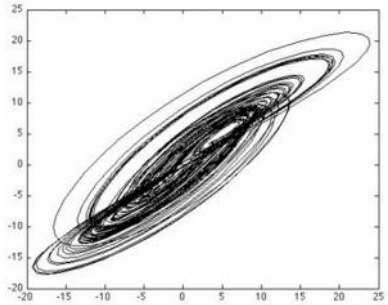

Figure 2. Hyper chotic system (y-x plane)

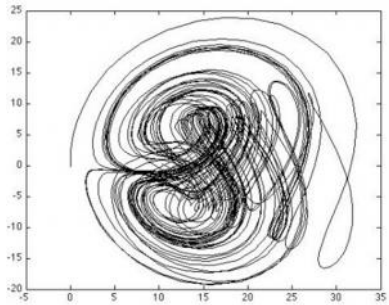

Figure 3. Hyper chotic system (z-y plane)

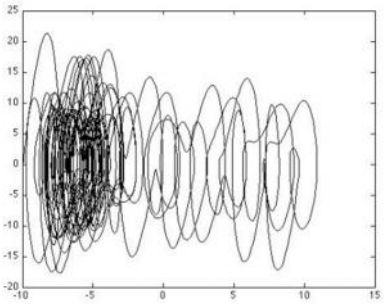

Figure 4. Hyper chotic system (w-x plane)

V. EXPRIMENTAL RESULT

A. Correlation Analysis

To test the correlation between two adjacent pixels (vertically and horizontally) in an encrypted image, some simulations are carried out. Firstly, randomly select 4096 pairs of two adjacent pixels from the image, then calculate the correlation coefficient of each pair by using the following formulas [14]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{n} x_i \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{n} (x_i - E(x_i))^2 \tag{5}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{n} (x_i - E(x_i))(y_i - E(y_i)) \tag{6}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(Y)}} \tag{7}$$

where x and y are grey values of two adjacent pixels in the image. From Table I, it can be seen that the proposed image encryption algorithm based on image total shuffling matrix have better performance compared with algorithm proposed by Ref. [18], which used the same grey image as that in this Letter. In the meantime, as hyper-chaos has larger key spaces than that of chaos used in some literatures [2,3,20], and the image shuffling algorithm proposed here is more secure than that using Arnold cat map transformation, which is periodic [3], so hyper-chaos has some potential application in image encryption algorithms.

TABLE I. CORRELATION OF TWO ADJACENT PIXELS

	Original image	**Encrypted image**
Horizontal	0.9842	0.0098
Vertical	0.9762	0.0003

B. Histogram

The Lena image of size 512×512 and 256 gray levels is employed for experimentation. The original image is shown in figure 5, its histogram is given in figure 8. Figure 6 is the image obtained after confusion process on the plain image. The corresponding histogram is shown in figure 9. It was observed from figure 8 and figure 9 that both histograms are same. It means that the corresponding statistical information depicted in Fig.6 after confusion process is exactly the same as that of the original image. It is due to the fact that cat map does not change the pixel values of the Lena image. The result shown in figure 7 is encrypted image obtained after chaotic S-AES process. The corresponding histogram is shown in Fig.10. From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. It was observed that this histogram is entirely different from one shown in figure 8.

Figure 5. Original image

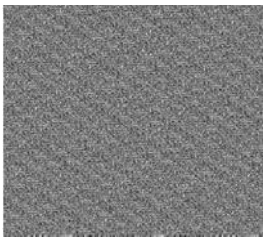

Figure 6. Scrambled image

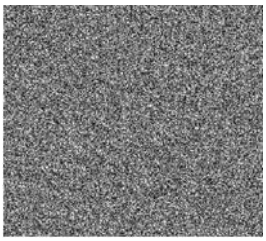

Figure 7. Encrypted image

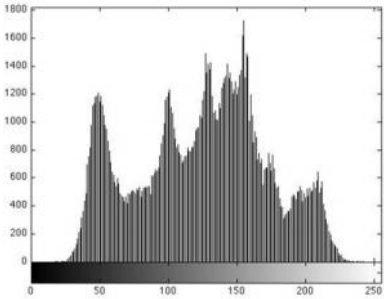

Figure 8. Histogram of original image

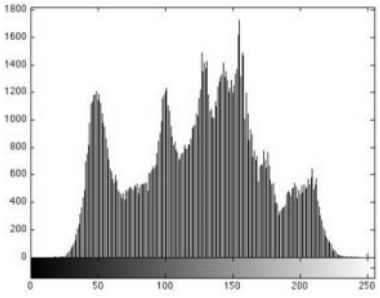

Figure 9. Histogram of scrambled image

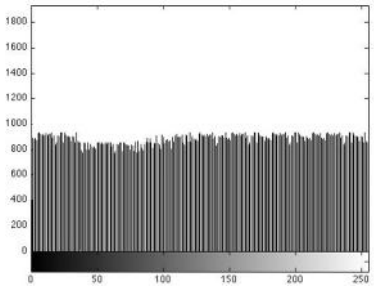

Figure 10. Histogram of encrypted image

C. Key Space Analysis

In our algorithm, the initial values of Logistic map and hyper-chaotic system are used as secret keys, if the precision is 10^{-14}, the key space size is 10^{70}. Also, the initial iteration number N_0 and k can also be used as the secret keys. This is enough to resist all kinds of brute-force attacks. It can be shown that hyper-chaos encryption algorithm is sensitive to the key; a small change of the key will generate a completely different decryption result and cannot get the correct plain-image.

D. Security Analysis

A good encryption should resist all kinds of known attacks, it should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. Some security analysis has been performed on the proposed image encryption scheme, the resistance of the scheme against differential and linear cryptanalysis is at least as of S-AES.

VI. CONCLUSION

In this paper, an image encryption scheme based on the combination of chaotic map for the scrambling the addresses of the pixels and chaotic simplified AES for the encryption is proposed to achieve adequate level of security for image 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 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.

ACKNOWLEDGMENT

The authors acknowledge helpful comments provided by the anonymous reviewers. We benefited from advices by Dr. M. Bagheri, Dr. S. S. Karimi Madahi, Dr. Jalil. Ghahramani, Dr. Hossein Sarabadani and critical readings by Dr. P.M. Birgani and Dr. Meysam Siyahmansoori. The authors are grateful to Tehran University of Medical Science, International Campus (TUMS-IC) and Islamic Azad University, Ashtian branch.

REFERENCES

[1] Bose, R. and Banerjee, A., “Implementing Symmetric Cryptography Using Chaos Functions”, Advanced Computing & Communication Conference, 1999.

[2] H.S. Kwok, Wallace K.S. Tang. " A fast image encryption system based on chaotic maps with finite precision representation", Chaos, Solitons and Fractals 32 (2007) 1518–1529

[3] M. Ashtiyani, P. Moradi Birgani , S. S. Karimi Madahi, “Speech Signal Encryption Using Chaotic Symmetric Cryptography, ” J. Basic. Appl. Sci. Res., 2(2)1678-1684, 2012

[4] M.ashtiyani, P.Moradi Birgani and Hesam M . Hosseini “Chaos-Based Medical Image Encryption Using Symmetric Cryptography” , ICTTA Conference 2008.

[5] Lizhen CHEN, “A Novel Image Encryption Scheme Based on Hyperchaotic Sequences” Journal of Computational Information Systems 8: 10 (2012) 4159-4167

[6] 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).

[7] Kh. S. Singh, S. Devi and S. S. Singh, “Encryption Scheme based on Combination of Cat Map and SDES”, DOEACC Center, Imphal.

[8] Mina Mishra and V. H. Mankar“Review on Chaotic Sequences Based Cryptography and Cryptanalysis”, nternational Journal of Electronics Engineering, 3 (2), 2011, pp. 189–194

[9] Tiegang Gao and Zengqiang Chen“A new image encryption algorithm based on hyper-chaos, ” Physics Letters A 372 (2008) 394–400

[10] Mayank Mishra, Prashant Singh, Chinmay Garg, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping”, International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 741-746

[11] R. Matthews, “On the derivation of a chaotic encryption algorithm”,Cryptologia 8 (1989) 29.

[12] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, second ed., Wiley, New York, 1995

[13] K.W. Wong, “A fast chaotic cryptographic scheme with dynamic look-up table”, Phys. Lett. A 298 (2002) 238.

[14] G. Chen, Y.B. Mao, C.K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps”,Choas Solitons Fractals 21 (2004) 749.

[15] M.S. Baptista, “Cryptography with Chaos”, Phys. Letters, A, 240 (1-2), (1998).

[16] Birgani P M and Ashtiyani M, “Wireless real time Brain mapping, Biomed 06, IFMBE Proceeding, pp. 444-446.

[17] Salim M. Wadi and Nasharuddin Zainal“Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption”, 4th International Conference on Electrical Engineering and Informatics, ICEEI 2013.

[18] XIAO Yong-Liang and XIA Li-Min, “An Image Encryption Approach Using a Shuffling Map”, Theor. Phys. (Beijing, China) 52 (2009) pp. 876–880.

[19] Meghdad Ashtiyani, Saeed Asadi, Pedram Hassani Goudarzi, “A New Method in Transmitting Encrypted Data by FCM Algorithm”, Second IEEE international conference on information and communication from theory to application, Syria 2006.

[20] J.P. Goedgebuer, L. Larger, H. Port, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode" ,Phys. Rev. Lett. 80 (1998) 2249.

[21] S. Yanchuk, T. Kapitaniak, "Symmetry-increasing bifurcation as a predictor of a chaos-hyperchaos transition in coupled systems",Phys. Rev. E 64 (2001) 056235.

[22] Meghdad Ashtiyani, Parmida Moradi Birgani and Saeed Asadi "MRI Segmentation Using Fuzzy C-means Clustering a Algorithm Basis Neural Network" ICTTA Conference 2008.

[23] Meghdad Ashtiyani, soroor behbahani, Saeed Asadi and Parmida Moradi Birgani, "Transmitting Encrypted Data by Wavelet Transform and Neural Networks" Signal Processing and Information Technology, 2007 IEEE International conference.

[24] MS Mansoory, M Ashtiyani, TN Hojjat "Cardiac motion evaluation for disease diagnosis using ICA basis neural network", Computer Science and Information Technology-Spring Conference, 2009.

[25] MS Mansoory, M Ashtiyani, H Sarabadani"Automatic Crack Detection in Eggshell Based on SUSAN Edge Detector Using Fuzzy Thresholding" Modern Applied Science 5 (6), p117

[26] SS Karimi Madahi and P. Salah,"A Neural Network Based Method for Cost Estimation 63/20kV and 132/20kV Transformers" Journal of Basic and Applied Scientific Research, 2012.

[27] Jalil Ghahramani and Seyed Siavash Karimi Madahi"Adjusting the Transient Stability of Power System Using STATCOM-SMES Combined Compensator" Applied Mechanics and Materials, p.1115-1119, 2012

[28] SS Karimi Madahi, M Hassani"Optimal design of insulators of using Artificial Neural Network (ANN)" Journal of Basic and Applied Scientific Research 2 (1), 2012.

[29] Meghdad Ashtiyani, Saeed Asadi and Parmida Moradi Birgani, "ICA-Based EEG Classification Using Fuzzy C-mean Algorithm", ICTTA Conference 2008.

[30] T.G. Gao, Z.Q. Chen, Z.Y. Yuan, G. Chen, "Hyperchaos generated from Chen's system", Int. J. Mod. Phys. C 17 (2006)471

[31] 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)

[32] P. Amani, H. Khalozadeh, and M. R. Aref, "S-box design for AES block cipher with chaotic mapping", inProceeding of 4th Iranian Society of Cryptology Conference(ISCC07), Tehran, Iran, 16-18 Oct, pp.91-98, (2007).

[33] Musa, E. Schaefer, and S. Wedig, "A simplified AES algorithm and its linear and differential cryptanalyses", inCryptologia 27, p.148–177, April (2003)

[34] Kh. S. Singh, S. Devi and S. S. Singh, "Encryption Scheme based on Combination of Cat Map and SDES",DOEACC Center, Imphal.

[35] http://mathworld.woffram.com/arnoldsCatMap.html

[36] www.mathworks.com