Chaos-Based Medical Image Encryption Using Symmetric Cryptography

Conference Paper · May 2008

DOI: 10.1109/ICTTA.2008.4530291 · Source: IEEE Xplore

3 authors, including:

Meghdad Ashtiyani
Shahid Beheshti University of Medical Sciences
23 PUBLICATIONS **305** CITATIONS

Chaos-Based Medical Image Encryption Using Symmetric Cryptography

Meghdad Ashtiyani
Electrical Eng. Department,
IHU
Tehran, Iran
m_ash_80@yahoo.com

Parmida Moradi Birgani
Biomedical Eng. Department,
Islamic Azad University
Tehran, Iran
moradi_pa@srbiau.ac.ir

Hesam M. Hosseini
Electrical Eng. Department,
Tarbiat Modares University
Tehran, Iran
hesam.mhosseini@gmail.com

Abstract— **In this paper, we propose an encryption scheme for the medical image encryption based on combination of scrambling and confusion. Chaotic cat map is used for the scrambling the addresses of the medical image pixels. 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 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.**

Keywords-Chaos; Encryption; Medical Image; S-box design; Symmetric cryptography

I. INTRODUCTION

Security is certainly a permanent field of interest at all times. At present, secure communication plays an increasing and ever-growing role in many fields of common life, such as banking, telemedicine, commerce, telecommunication and networking. With the rapid development of the internet and the multimedia technology, the traffic of digital images has grown rapidly and digital image is becoming important carrier of information communion for people. Security of image becomes important for many sectors mainly for medical applications. Nowadays, the transmission of medical images is a daily routine, especially over wireless networks.

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.

The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. Towards this direction, we design an efficient chaos based symmetric cryptography system for medical image encryption. In this paper, a new medical image encryption system is proposed; in this system we use symmetric cryptography and chaos for encrypt medical images such as MRI, X-ray, ultrasound, CT and PET. Symmetric cryptography algorithm that we used in this project is Simplified Advance Encryption Standard (S-AES)

II. CHAOS AND CRYPTOGRAPHY

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 and in this cryptosystem the key sensitivity are determined by the parameter sensitivity of chaotic map and the initial-value sensitivity of diffusion function.

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.

III. PROPOSED ALGORITHM

Our proposed method for image encryption consists of two parts, namely scrambling and encryption. Both of them use of chaos for design process as we will explain hereafter. Fig.1 illustrates the block diagram of our algorithm. The scrambling

block, which provides confusion for our scheme, is in 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 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 [4], 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.

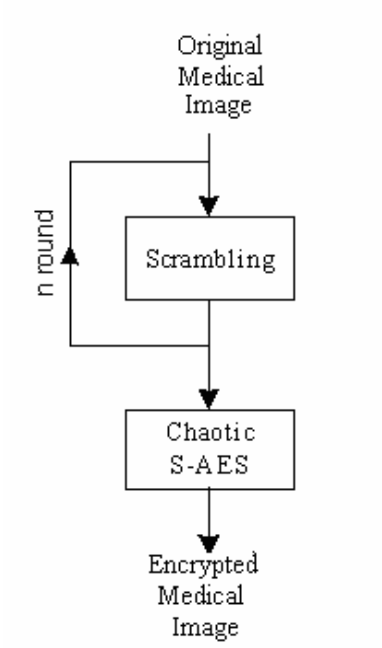

Figure1. Block diagram of this project

IV. 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 medical image without changing its values by applying scrambling algorithm.

Some classical scrambling algorithms are cat map [1], baker map [9], knight-tour transformation [12], affine transformation [11], magic-square 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.

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 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 [14]. 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 medical image.

A. *Cat Map*

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:

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

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

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

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 256×256 gray 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, b secret, but the periodicity will bring some insecure factors, so applying cat map solely can not meet the demands of encryption; and cat map only transforms the original image's position, however the pixels' values have not been changed [4].

V. 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

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 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 [4], are of this family. That is they utilize block ciphers in conjunction with scrambling for image encryption. It applies cat chaotic map for scrambling of pixel 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.

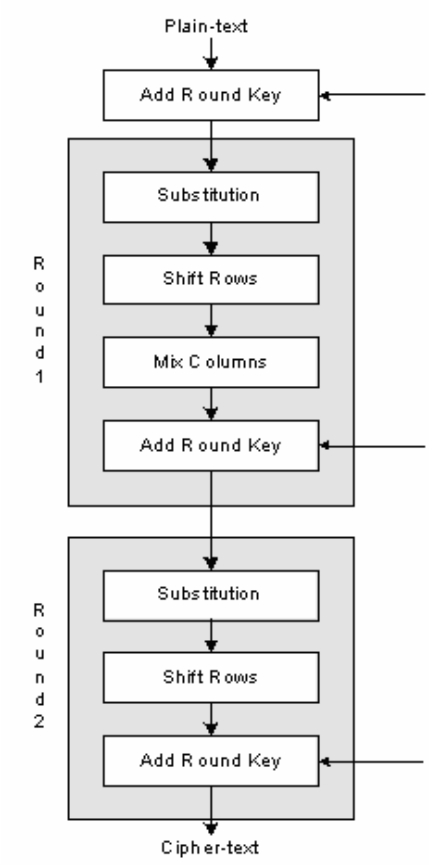

Figure2. Block diagram of S-AES

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 can not 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 [16] and produce chaotic-based S-box for S-AES. S-AES is simplified version of AES algorithm [17]. It operates on 16-bit plaintexts and generates 16-bit cipher texts, using the expanded key $k_0, k_1, .. , k_{47}$.

For more information about S_AES, we recommend taking a look at [17]. 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, [18], 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.

A. *Lorenz Chaotic Function*

The Lorenz equation is commonly defined as three coupled ordinary differential equation like:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(\tau - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \tag{3}$$

where the three parameter 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 spacial 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:

- Symmetry: The Lorenz equation has the following symmetry of ordinary differential equation:

$$(x, y, z) \rightarrow (-x, -y, z) \quad (4)$$

This symmetry is present for all parameters of the Lorenz equation

- 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).
- Equilibrium points: To solve for the equilibrium points we let

$$\dot{x} = f(x) = \begin{bmatrix} \sigma(y - x) \\ x(\tau - z) - y \\ xy - \beta z \end{bmatrix} \quad (5)$$

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 that

$$x_{C1} = (-\sqrt{\beta(\tau - 1)}, -\sqrt{\beta(\tau - 1)}, \tau - 1) \quad (6)$$

$$x_{C2} = (-\sqrt{\beta(\tau - 1)}, -\sqrt{\beta(\tau - 1)}, \tau - 1) \quad (7)$$

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.

VI. RESULTS

The plain mammography image of size 256×256 and 256 gray levels is employed for experimentation. The original image is shown in Fig.3 (a); its histogram is given in Fig. 4(a). Fig. 3 (b) is the image obtained after confusion process on the medical image. The corresponding histogram is shown in Fig.4(b). It was observed from Fig.4 (a) and Fig.4(b) that both histograms are same. It means that the corresponding statistical information depicted in Fig.3(b) 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 medical image. The result shown in Fig.3(c) is encrypted image obtained after chaotic S-AES process. The corresponding histogram is shown in Fig.4(c). It is more uniform. It was observed that this histogram is entirely different from one shown in Fig.4 (a).

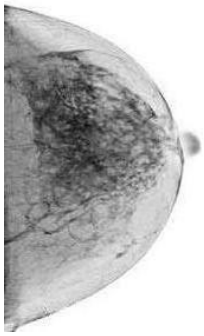

Figure.3(a) Original mammography image

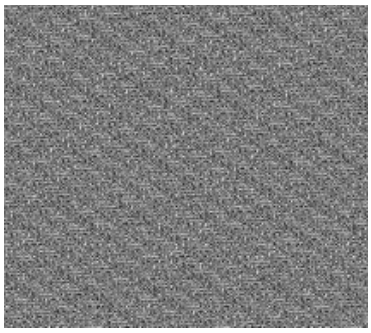

Figure.3(b) Scrambled medical image

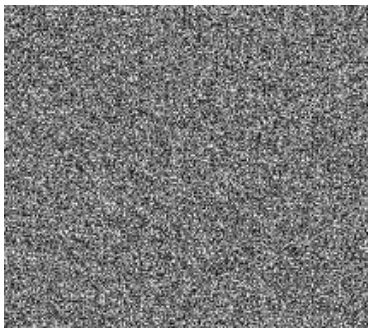

Figure.3(C) Scrambled and encrypted image

VII. CONCLUSION

In this paper, a medical 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 (of the corresponding pixels values), is proposed to achieve adequate level of security for medical 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 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.

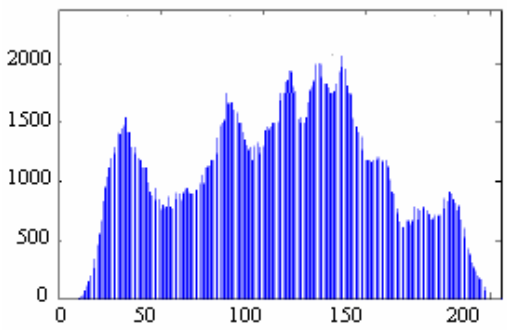

Figure4(a). Histogram of medical image in figure 3(a)

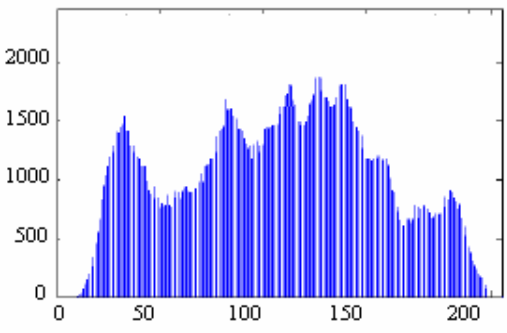

Figure4(b). Histogram of scrambled medical image in figure 3(b)

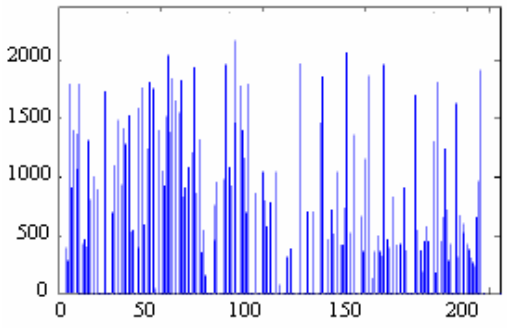

Figure4(C). Histogram of scrambled and encrypted medical image in figure 3(C)

ACKNOWLEDGMENT

The authors acknowledge helpful comments provided by the anonymous reviewers. We benefited from advices by Dr. Hossein Sameti, Dr. M. Bagheri, Dr. E. Fatemizadeh, Mr. P. Amani and critical readings by Saeed Asadi, Meisam Ashtiyani and A. Dayani. The authors are grateful to Imam Hossein University, Islamic Azad University and Tarbiat Modares University.

REFERENCES

[1] G.R. Chen and Y.B. Mao et al., A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (2004), pp. 749–7612.

[2] 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

[3] 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 (2006) 349–353

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

[5] 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

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

[7] T.-J. Chuang and J.-C. Lin, "New approach to image encryption," *J. Electronic Imaging*, vol. 7, no. 2, pp. 350–356, 1998

[8] 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

[9] 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

[10] T. B. Arthur and Y. Kan, "Magic Squares Indeed", J. the Mathematical Gazette, 108, pp. 152-156, 2001

[11] 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

[12] C. Charilaos, S. Athanassios and E. Touradj, "The JPEG2000 Still Image Coding Systems", *IEEE Trans.on Consumer Electronics* 46, pp. 1103-1127, 2000

[13] R. Matthews, "On the Derivation of a Chaotic Encryption", *Cryptologies*, XIII(1), pp. 29-49, 1989

[14] 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

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

[16] 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 2007, pp.91-98.

[17] M. Musa, E. Schaefer, and S. Wedig, "A simplified AES algorithm and its linear and differential cryptanalyses," in *Cryptologia* 27, pp.148–177, April 2003.

[18] 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.

[19] W. Stallings, Cryptography and Network Security, Third Edition, Prentice Hall 1999.

[20] D. Stinson, *Cryptography Theory and Practice*, second Edition, CRC Press, 2002.

[21] B. schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* 2nd edition, John Wiley and Sons, 1996