A Novel Image Encryption Algorithm Using Two Chaotic Maps for Medical Application

G.A. Sathishkumar[1,*], K. Bhoopathybagan[2], N. Sriraam[3], SP. Venkatachalam[4], and R. Vignesh[5]

[1] Assistant Professor, Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Sriperumbudur -602108
sathish@svce.ac.in
[2] Professor and HEAD, Department of Electronics, Madras Institute of Technology, Chrompet, Chennai-600044
kbb@mail.yahoo.com
[3] Center for Biomedical Informatics and Signal Processing, Department of Biomedical Engineering SSN College of Engineering, Chennai 603110
[4,5] Final year student, Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Sriperumbudur -602108

Abstract. The advancement of information technology has provided the possibility of transmitting and retrieving medical information in a better manner in the recent years. The secured medical image transmission will help in maintaining the confidentiality of information. Such security measures are highly essential for multi media data transfer from the local place to the specialist location at the remote place. This paper devoted to provide a secured medical image encryption technique using duo chaos based circular mapping. The given original images are divided into blocks and zigzag scanning is performed .To encrypt the image, chaos based circular shift mapping procedure and scrambling based on cryptography technique are adopted. The efficiency of the proposed scheme is evaluated in terms of statistical measures such as cross correlation and peak signal –to noise ratio (PSNR). It is found that the proposed image encryption scheme yields better results, which, can be suitably tested for real time problems.

Keywords: chaotic mapping, image encryption, logistic map, Bernoulli map, scrambling, medical and tele-radiology.

1 Introduction

Secured communication [12-15],[19-22] plays a vital role in ensuring multimedia content protection which is of primary importance to military and medical applications. Although the conventional cryptography techniques introduce various data encryption schemes, (DES).The scope for better encryption scheme is still to be explored.

* Corresponding author.

N. Meghanathan et al. (Eds.): CCSIT 2011, Part III, CCIS 133, pp. 290–299, 2011.

Recently non-linear chaotic dynamic systems have drawn special attention in providing valuable security measures. This is due to the fact that the basic ideology of chaotic system matches with the fundamentals of cryptography. This paper discusses a novel chaotic mapping technique for the generation of secured key for transmission and retrieval of medical data for medical applications. The security is assured and maintained in the sense that the proposed technique adopts the combination of position permutation and value transformation DES techniques.

In recent years, the advancement of information technology in biomedicine has provided the possibility of transmitting and retrieving medical information in a better manner. For medical applications, secured medical image transmission will help in maintaining the confidentiality of information. Such security measures are highly essential for data transfer from the local place to the specialist location at the remote place. To fulfil such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties. Due to the tight relationship between chaos theory [5] and cryptography, chaotic cryptography has gain importance in designing image and video encryption schemes. This paper discusses a novel chaotic mapping technique for the generation of secret key for transmission and retrieval of medical data for medical applications. The security is assured and maintained in the sense that the proposed technique adopts the combination of both position permutation and value transformation.

2 Chaos and Cryptography

The recent research activities in the field of non-linear dynamics and especially on systems with complex (chaotic) behaviour [5][11] have showed potential applications in various fields including healthcare. The special characteristics ,such as sensitivity to initial conditions ,randomness, probability and ergodicity makes chaos mapping as a potential candidate to analyze security issues.

2.1 Choatic Maps

The chaos streams are generated by using various chaotic maps. In this paper, 1 D chaotic map is used to produce the chaotic sequence and used to control the encryption process. In this paper, 1D chaotic map is used to produce the two chaotic sequences and to control the encryption process. Among the various maps, logistic map and Bernoulli map are used specifically for generation of chaotic key. Interested readers refer [6].

3 The Proposed Image Security System

The proposed encryption algorithm belongs to the category of the combination of value transformation and position permutation. We first define two bit-circulation functions with two parameters in each function. One is used to control the shift direction and another is used to control the shifted bit-number on the data transformation. In this paper, two different types of scanning methods are used and their performances are analyzed. The images are treated as a 1D array by performing Raster scanning and Zigzag scanning [23, 24].

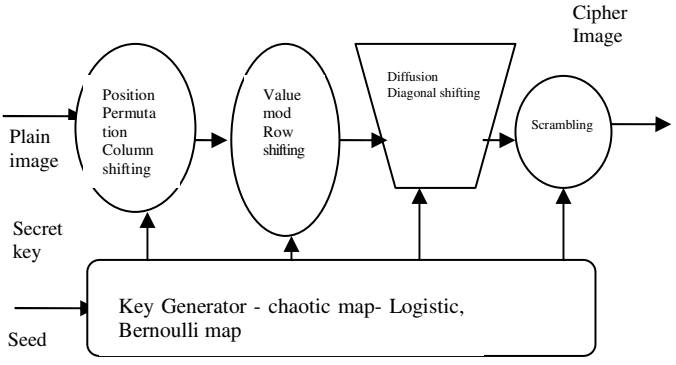

Fig. 1. Proposed Chaos based image cryptosystem

Figure 1 shows the typical schematic of the proposed method. The scanned arrays are divided into various sub blocks. Then for each sub block, position permutation and value transformation are performed and finally scramble to produce the cipher image. The sub key is generated by applying the suitable chaotic maps. Based on the initial conditions, the generated chaotic map are allowed to iterate through various orbits of chaotic maps. Hence, for each sub block various chaotic sequence patterns are applied which further increases the efficiency of the key to be determined by the brute force attack.Then, based on the chaotic system, binary sequence is generated to control the bit-circulation functions for performing the successive data transformation on the input data. Eight 8-bit data elements are regarded as a set and fed into an 8×8 binary matrix. In the successive transformation on each diagonal elements by using these two functions, we randomly determine the two parameters used in the functions according to the generated chaotic binary sequence such that the signal could be transformed into completely disorderly data.

In demonstrating the correct functionality of the proposed signal security system, we have performed the simulation on the proposed scheme. The following steps carried out for the implementation of proposed chaos based mapping technique. Interested readers refer [14] the some definitions and parameters used in this paper.

Algorithm

Step1: Covert 2-D image into 1-D array and then performs a) Raster scanning and b) Zigzag scanning.

Step2: Consider a block size of 8 x 8 and convert them in to binary values.

Step3: Sub key size is 20 bits, it is extracted from the chaos maps of Bernoulli map. The Secret key is SEED, which are the initial conditions of the each map. Based on the initial conditions the chaotic maps are allowed to iterate through various orbits. Then, based on the chaotic system, binary sequence generated to control the bit-circulation functions for performing the successive data transformation on the input data. Given pair of f and f', the combination of p, q, r, t, u and s resulting in the transformation pair may be non-unique which is the secret key.

Step4: Convert the chaotic sub key in to binary values of 20 bits.

Step5: Each 8x 8-sub block of image pixel values circularly shifted by chaos sequence generated from maps.
Step6: The Circular shifting of Diagonal as follows
Definition for Circular Shifting of Diagonal pixels:
The Mapping [14,23] $ROLR_k^{t,u}$ & $ROD_k^{t,u}$ $f \rightarrow f'$ is defined to rotate each pixel at the position (x,y) in the image such that k^{th} diagonal of f $0 \le f \le$, u bits in the up direction if t equals 1 or u bits in the down direction if t equals 0.

In different combinations of p, q, r, t, u and s, the composite mapping

$$(\sum_{j=0}^{7} ROLR_j^{q,s}) \cdot (\sum_{i=0}^{7} ROLR_i^{p,r}) \cdot (\sum_{k=0}^{13} ROLR_k^{t,u}) \qquad (1)$$

Possesses the following three desirable features:

A binary matrix f be transformed into quite different matrixes and different matrixes can be transformed into the same matrix. Given a transformation of pair f and f' the combinations of p, q, r and s resulting in the transformation pair may be non-unique.

Since f is an 8×8 matrix, the result of circulating diagonal is h bits and of circulating it (kmod8) bits in the same direction. The r and s are assumed to be in the ranges of $0 \le r \le 7$ and $0 \le s \le 7$.
Step7: Perform the encryption based on the chaotic sequence key values, which is obtained from the orbits of chaos maps iteration.
Step8: Chaos Theory Based Image Scrambling [16] Transformation
For a Gray scale image I of size M x N pixels, we can have an arbitrary chaotic iteration $x_{n+1} = f(1 - x(n)) where x_i \in R$ to generate a chaotic sequence of real numbers. The initial value X_i is the secret key. The following scheme is applied to scramble and unscramble cipher image I.
Step8.1. Let an initial value X_i that is associated to the secret key. Let t = 1.
Step8.2. Iterate from 0 to N - 1 times with the chaotic iteration 8.1, get the sequence of real numbers $\{X_1, X_2, \ldots, X_N\}$.
Step8.3. Arrange the chaotic sequence $\{X_1, X_2, \ldots, X_N\}$ in descending order , to get the sorted sequence $\{X`_1, X`_2, \ldots, X`_N\}$.
Step8.4. Determine the set of scrambling address codes $\{t_1, t_2, \ldots, t_N\}$, where $t_i \in \{1, 2, ..., N\}$. t_i is the new subscript of X_i in the sorted sequence $\{X`_1, X`_2, \ldots, X`_N\}$.
Step8.5. Permute the k^{th} column of the cipher image I with permuting address code $\{t_1, t_2, \ldots, t_N\}$,namely, replace the t_i^{th} row pixel with the i^{th} row pixel for i from 1 to N.
Step8.6. If $k = M$, end of iteration. Otherwise, let $X_I = X_N$,and $k = k+1$. Repeat the 8.2 to 8.5, to produce double encrypted cipher image data value in 1D form.
Step10: Transform the cipher image 1-Dimension to 2-Dimension.
Step11: Transmit the chaotic sub key via secure channel using public key algorithms.
Step12: Decrypt the cipher image using the same chaotic sub key and SEED.
Step13: Finally, performance analysis is carried out by doing correlation, histogram, loss and PSNR of the original, encrypted and decrypted image.

4 Experimental Results

An image size of 256 * 256 (example: X Ray of Chest, knee and human head etc.,) is considered as plain image and is performed with chaotic map with orbit key. The most direct method to decide the disorderly degree of the encrypted image is by the sense of sight. On the other hand, the correlation coefficient can provide the quantitative measure on the randomness of the encrypted images. General images typically have a higher degree of randomness associated with both the natural random nature of the underlying structure and the random noise superimposed on the image. In order to apply the parameters α and β must be determined according to Step 1. The selection of α and β should follow the empirical law. Based on the experimental experience, general combinations of α and β can always result in very disorderly results. In the simulation, α = 2 and β = 2 are adopted in Step 1. The initial conditions of chaotic maps used are, f(x)=0.5 for Bernoulli map . The offset values for producing various orbits are chosen to be very less than the initial conditions. The visual inspection of Fig. 2 shows the possibility of applying the algorithm successfully in both encryption and decryption. In addition, it reveals its effectiveness in hiding the information contained in them.

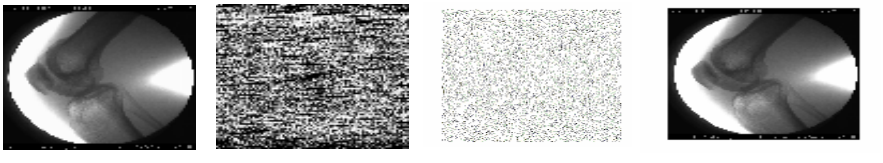

Fig. 2. (a) Original Image (b) Cipher image (c) Cipher image with Maps **&**Scrambling d) Decrypted image

To prevent the leakage of information to an opponent [10][15], it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig. 3(b). The histogram of a plain image contains large spikes. The histogram of the cipher image as shown in Fig. 3(d), is uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

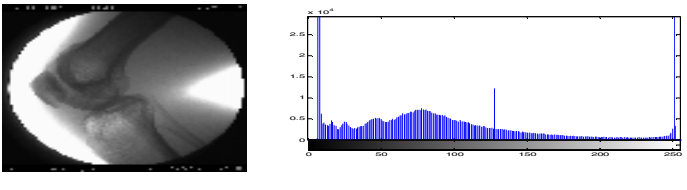

Fig. 3. a) Histogram of original image

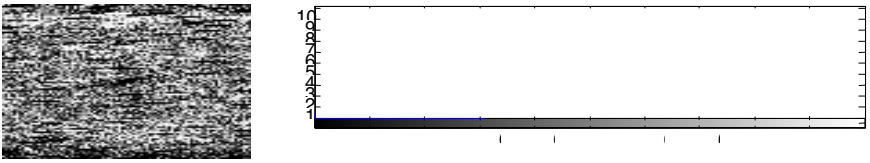

Fig. 3. b) Histogram of cipher image

In addition to the histogram analysis [16, 18, 21], we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image respectively. The procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2}$$

Fig. 4 shows the correlation distribution of two horizontally adjacent pixels in plain image and cipher image for the all image. The correlation coefficients are 0.9905 and 0.0308 respectively for both plain image and cipher image.

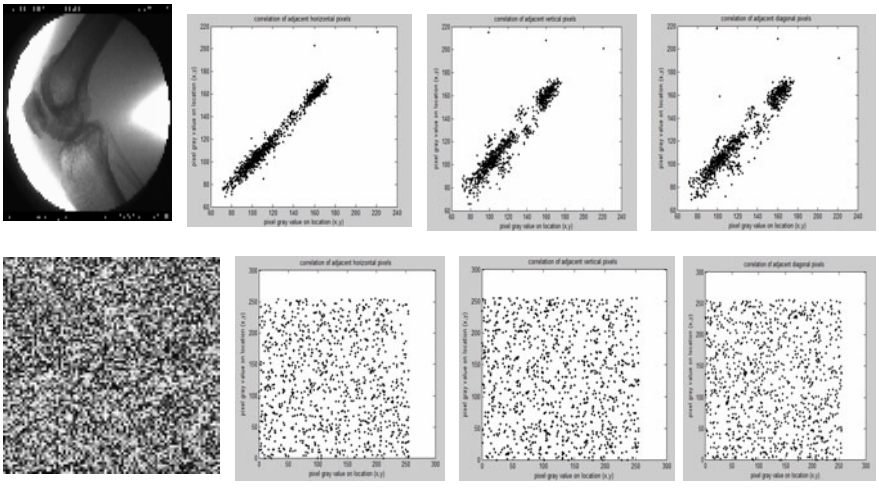

Fig. 4. Horizontal, vertical and diagonal correlation of plain and cipher image

The correlation coefficients [15, 18, and 21] of various maps are calculated and they are compared with each other. The comparison table for various plain images, various cipher images and various maps based on the correlation coefficient are given in the Tables 1-3.

Table 1. Horizontal, Vertical & Diagonal Correlation of Cipher Image

Original Image	Horizontal Correlation	Vertical correlation	Diagonal Correlation	Cipher image with Maps and scrambling
Knee	0.2254	0.4400	0.0012	-0.00070115
Chest	-0.0515	-0.0241	-0.0084	0.00010436
Human Head	0.5930	0.5759	-0.0646	-0.00094391

The correlation coefficient is found for the various directions of scanning patterns employed and the tabulated in the Table 4. The observation shows that the zigzag scanning is more efficient than the raster scanning. In addition, cipher image with multiple maps are more resistant to crypt analyst attacks.

Table 2. Horizontal Correlation Co - efficient for Raster Scanning and Zigzag Scanning

IMAGE	Raster Scanning	Zigzag Scanning
Knee	0.0539	-0.00139
Chest	-0.0535	-0.00590
Human Head	0.0174	-0.0023

Table 3. Correlation Co - efficient in Plain image and Cipher Image

Direction of Adjacent Pixels	Plain image	Cipher image using Bernoulli map	Cipher image with Maps and scrambling
Horizontal	0.9670	0.0781	0.00887
Vertical	0.9870	0.0785	0.00923
Diagonal	0.9692	0.0683	0.00893

Sensitivity Analysis

In differential attacks, to test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures are used: Number of Pixels Change Rate (NPCR) [12, 13, 18, 19, 21and Unified Average Changing Intensity (UACI) [12, 18, 19, 21].

For, higher security, more difference between cipher images is expected. Number of pixel change rate (NPCR) means the number of pixels changed in the cipher image when only one pixel value is changed in plain-image. The larger the NPCR is, the higher sensitivity in the plain image has and the more difficult the system's security against differential attack. Let two ciphered images, whose corresponding plain images have only one pixel difference; be denoted by CI1 and CI2.Label the grayscale values of the pixels at grid (i,j) in CI1 and CI2 by C I(i,j) and CI(i,j), respectively. Define a bipolar array D, with the same size as images CI1 and CI2. Then, Diff(i,j)is determined by CI1(i,j) and CI2(i,j), namely, if CI1(i,j) =CI2(i,j) then Diff(i,j) = 1; otherwise, Diff(i,j) = 0.

The NPCR [12, 13, 18, 19, 21] is defined as

$$NPCR = \frac{\sum_{i,j} Diff(i,j)}{W \times H} \times 100\% \quad (3)$$

Unified average changing intensity (UACI) means changing intensity of the corresponding pixels of the plain image and cipher image. The larger the UACI is, the more resistant to the differential attack the encryption scheme.

The UACI [12, 18, 19,21] is defined by:

$$UCAI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{CI1(i,j) - CI2(i,j)}{255}\right] \times 100\% \quad (4)$$

Table 4. NCPR AND UACI FOR Cipher Image

IMAGE	NPCR	UACI
Knee	99.993896	-0.000772
Chest	99.843402	-0.00546492
Human Head	98.430901	-0.00839120

PSNR [18, 21] of encrypted image and original image is computed as follows

$$PSNR = 10\log_{10} \frac{hw\left[\max_{1 \le i \le m, 1 \le j \le n} \{p'i,j\}\right]^2}{\sum_{i=1}^{h}\sum_{j=1}^{w}(pi,j - p'i,j)^2} \quad (5)$$

Where *h* and *w* are the width and height of original image, while *p*ij and *p'*ij are pixel values of encrypted image and original image respectively. In the proposed scheme, higher the visual quality of the cipher image is, the less the number of changed pixels will be, and the larger the value of PSNR will be and it is around 9.3158 for the chest image, 9.0061for the knee image and 9.2709 for the head image.

5 Conclusions and Future Scope

In this paper, a novel chaotic mapping encryption scheme for the transmission of medical images is proposed**.** To protect the medical information, Bernoulli and logistic chaos mapping has been used to generate the secret key. Statistical analysis such as correlation, PSNR, NPCR and UACI where used to evaluate the performance of the proposed scheme. It can be seen from the experimental that the chaos based encryption scheme provides better results and can be tested for real – time problems.

References

1. Smid, M.E., Branstad, D.K.: The data encryption standard: past and future. Proceedings of the IEEE 76(5), 550–559 (1988)
2. Yen, J.-C., Guo, J.-I.: An efficient hierarchical chaotic image encryption algorithm and its VLSI realization. IEE Proceedings—Vision, Image and Signal Processing 147(2), 167–175 (2000)

3. Kuo, C.J., Chen, M.S.: A new signal encryption technique and its attack study. In: Proc. IEEE International Carnahan Conference On Security Technology, Taipei, Taiwan, pp. 149–153 (October 1991)
4. Macq, B.M., Quisquater, J.-J.: Cryptology for digital TV broadcasting. Proceedings of the IEEE 83(6), 944–957 (1995)
5. Parker, T.S., Chua, L.O.: Chaos: a tutorial for engineers. Proceedings of the IEEE 75(8), 982–1008 (1995)
6. Wu, C.W., Rulkov, N.F.: Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications 40(10), 707–721 (1993)
7. Biham, E.: Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT 1991. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 532–534. Springer, Heidelberg (1991)
8. Yi, X., Tan, C.H., Siew, C.K.: Fast encryption for multimedia. IEEE Transactions on Consumer Electronics 47(1), 101–107 (2001)
9. Wolter, S., Matz, H., Schubert, A., Laur, R.: On the VLSI implementation of the internal data encryption algorithm IDEA. In: Proc. IEEE Int. Symp. Circuits and Systems, Seattle, Washington, USA, vol. 1, pp. 397–400 (1995)
10. Kuo, C.J., Chen, M.S.: A new signal encryption technique and its attack study. In: Proceedings of IEEE International Conference on Security Technology, Taipei. Taiwan. DD, pp. 149–153 (1991)
11. Dachselt, F., Schwarz, W.: Chaos And Cryptography IEEE Transactions On Circuits And Systems—I. Fundamental Theory And Applications 48(12) (2001)
12. Ahmed, H.E.H., Kalash, H.M., Allah, O.S.F.: An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption. Informatica 31, 121–129 (2007)
13. Pareek, N.K., Patida, V., Sud, K.K.: Image encryption using chaotic logistic map. Elsevier Image and Vision Computing 24, 926–934 (2006)
14. Chen, H.-C.: Design and Realization of a New Signal Security System for Multimedia Data Transmission. EURASIP Journal on Applied Signal Processing 2003 13, 1291–1305 (2003)
15. El-Fishawy, N., Zaid, O.M.A.: Quality of encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms. International Journal of Network Security 5(3), 241–251 (2007)
16. Xiangdong, L., Junxing, Z., Jinhai, Z., Xiqin, H.: Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation. IJCSNS International Journal of Computer Science and Network Security 8(1) (2008)
17. Wang, S., Zheng, D., Zhao, J., Tam, W.J., Speranza, F.: An Image Quality Evaluation Method Based on Digital Watermarking. Transactions Letters IEEE Transactions On Circuits And Systems For Video Technology 17(1) (2007)
18. Krishnamoorthi, R., Sheba Kezia Malarchelvi, P.D.: Selective Combinational Encryption of Gray Scale Images using Orthogonal Polynomials based Transformation. IJCSNS International Journal of Computer Science and Network Security 8(5) (May 2008)
19. Zhang, L., Liao, X., Wang, X.: An image encryption approach based on chaotic maps. Elsevier Chaos, Solitons and Fractals 24, 759–765 (2005)
20. Mao, Y., Chen, G.: Chaos-Based Image Encryption. Springer, Berlin (2003)
21. Giesl, J., Vlcek, K.: Image Encryption Based On Strange Attractor. ICGST-GVIP Journal (9) (2009), ISSN 1687-398X

22. He, X., Zhang, Q.: Image Encryption Based on Chaotic Modulation of Wavelet Coefficients. In: 2008 Congress on Image and Signal Processing, IEEE Computer Society Press, Los Alamitos (2008)
23. http://www.mathworks.com/matlabcentral/fileexchange/11362
24. http://users.ece.gatech.edu/~njayant/mmc5/sld012.htm
25. Ozturk, I.: Analysis and Comparison of Image Encryption Algorithms. Proceedings Of World Academy Of Science, Engineering And Technology 3 (2008)