Self-Adaptive based Medical Image Encryption using Multiple Chaotic Systems

Sudheesh K.V., PhD
Dept. of ECE, Vidyavardhaka College of Engineering, Mysuru

Sushmitha B.C.
Dept. of ECE, Jnana Vikas Institute of Technology, Bidadi

Chethan R.
Dept. of EEE, G Madegowda Institute of Technology, Mandya

Ganesh Kumar M.T.
Dept. of ECE, G Madegowda Institute of Technology, Mandya

Kiran
Dept. of ECE, Vidyavardhaka College of Engineering, Mysuru

ABSTRACT
With the advent of medical imaging tools and telemedicine technology, the transmission of patient data over the Internet has reduced distance barriers in healthcare delivery. To ensure patient privacy, data is encrypted while being transmitted over an insecure network.In order to overcome the problem of traditional techniques, a self-adaptive image encryption techniques based on multiple maps has been developed. Initially, plain image dependent multiple secret keys are generated for multiple maps. Input image is permuted by N umber of rounds using Arnold cat map. Value of N determined by the secret key. During diffusion process, a random image is generated with the help of 2D Logistic-Sine-Coupling Map (2DLSCM) with another secret key. Finally encrypted image obtained by performing bitwise XOR operation between permuted image and random image. Advantage of proposed multiple chaotic image encryption that incorporates two chaotic maps, Arnold's Cat Map and 2D Logistic Sine Coupling Map (2DLSCM), to improve the randomness and security of encrypted images. It also analyses the performance and security of the scheme and compares it to other known chaotic image encryption schemes.

General Terms
Security, Medical images

Keywords
Encryption, Arnold's Cat Map,2D Logistic-Sine-Coupling Map(2D-LSCM), Permutation, Diffusion

1. INTRODUCTION
Telemedicine had its roots in the 1960s and expanded into several areas of the medical system and domain, including dermatology, cardiology, and neurology. This offers several benefits to the community, including better, faster diagnosis, and significant reductions in patient consultation and treatment costs. For proper care and treatment, a variety of diagnostic information about the patient, from cardiovascular measurements to X-ray and ultrasonography results, is collected and sent to doctors and patients. Health is of paramount importance to everyone. The rapid development of medical imaging technologies such as computed tomography (CT), ultrasound, and magnetic resonance imaging (MRI) has revolutionized the effective and accurate treatment of patients. A security system is required to protect medical images from unauthorized access. Technologies such as watermarking, steganography, and encryption can play an important role in providing the necessary security measures as needed. To protect the privacy of patients and the ethics of physicians, this information should be made available only to authorized personnel. However, this diagnostic data is typically sent over a public network, increasing the risk of data leakage to unauthorized units or attackers. Therefore, it is necessary to ensure proper security for the data stored and transmitted.

2. LITERATURE REVIEW
Extensive research has been done over the last few decades on aspects of secure image transmission and retrieval. Many schemes have been proposed to protect medical images by using chaos maps in the pixel scramble and diffusion phases [1-4]. B AbdElAtty [5] proposed a Sbox based on a Logistic Chebyshev card and a pseudo-random number generator for image encryption. By performing a 1D combined chaos map, the author generated a key image K to perform an XOR operation on the original image. However, this scheme has a lower UACI value than the proposed image encryption method. Many schemes of spatial permutations using high-dimensional chaos maps have been proposed to achieve high correlation in cryptographic images [6-9].These schemes guarantee randomization during encryption, but their fixed private keys make them the target of classical attacks. To achieve a safe and efficient key stream,Xingyuan W. et al. [10] proposed an image encryption algorithm based on LL compound chaos and zigzag conversion. Here, the advanced zigzag transformation and Lu system are used together to scramble the input image and the composite chaos system is used in the diffusion stage. Global entropy measurements are minimized because the sensitivity of the image depends on the local pixels. In addition, many encryption methods based on one-time key [11–13] have been introduced to ensure resistance to cryptanalysis attacks.Mohamed Boussif [14] presented an adaptive block key for encrypting medical images. Hua Z et al. [15] proposed fast pixel shuffle and adaptive radiation-based medical image encryption by inserting random data into the image for the shuffle process. The lossless process is very tedious as it can result in data loss during the image compression phase.

3. METHODS USED IN THE PROPOSED WORK

The following methods are used for permutation and diffusion process of proposed medical image encryption.

3.1 2-Dimensional logistic sine coupling map (2D-LSCM)

2DLSCM Chaos Map is a combination of 2D Logistic Chaos Map and Sign Map. Logistic maps are used to show the time course of population rate as a function of initial population and growth rate. The equation for the two-dimensional logistic map is given by (1).

$$\begin{cases} x_{i+1} = \sin\left(\pi(4\theta x_i(1-x_i) + (1-\theta)\sin(\pi y_i))\right); \\ y_{i+1=} \sin\left(\pi(4\theta y_i(1-y_i) + (1-\theta)\sin(\pi x_{i+1}))\right), \ldots (1) \end{cases}$$

Where θ is the control parameter, having an interval of [0,1].

3.2 Arnold's cat map

Arnold's cat map is used to repeatedly shift the pixels of a square image to exponentially increase the randomness of the image. For n × n images, the original image is returned after iterating over 3n + 1 shifts. The Arnold's cat map of the n × n image is given by equation (2).

$$\begin{bmatrix} s' \\ r' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} s \\ r \end{bmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Arnold's cat cards only work with square images, so non-square images are entered to provide the best square image for your operation. (s, r) and (s', r') denotes original image coordinates and shuffled coordinates respectively. Where p and q are positive integers.

4 PROPOSED WORK

Figure shows block diagram of Block diagram of self-adaptive image encryption system. Proposed method mainly consists of three process namely Secret key generation, permutation and diffusion operation.

4.1 Secret key generation

To ensure the unpredictability and sensitivity of the proposed quantum cryptosystem, the proposed framework incorporated a dynamic seeding mechanism (initial conditions) associated with a single image. As the proposed system incorporates two chaotic maps, the secret key for encryption and decryption is composed of two parts. The first part is the secret key for Arnold's cat map, and the second part is for the 2D-LSCM map.

Plain image I of size N*N divided into four equal blocks B1, B2, B3 and B4 of size (N/2)*(N/2). N value for period of Arnold cat map determined by following equation number (3). Initial values X0, Y0 for 2D-LSCM map is given by equation 5 and 6.

$$N = \sum \frac{B1(i,j)^2}{B1(i,j)} \quad mod\ N \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$N = \sum \frac{B2(i,j)^2}{B2(i,j)} \quad mod\ 1 \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$N = \sum \frac{B3(i,j)^2}{B3(i,j)} \quad mod\ 1 \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

4.2 Permutation using Arnold's Cat map

Permutation is used in an image encryption scheme to displace or shuffle the adjacent pixels to reduce any correlation between them that may affect the encrypted images' security. According to equation 2, random positions are obtained for changing the position of every pixel in the original image. To improve the security, N number of round performed in the permutation process.

4.3 Diffusion using 2D Logistic Sine Coupling Map (2DLSCM)

X and Y sequence generated using equation (4) and (5). Then Convert the X and Y sequence into integer sequence with the upper bound of 256 and rearrange into key image of original image size. Finally bitwise XOR operation performed between permuted image key images to produce encrypted image.

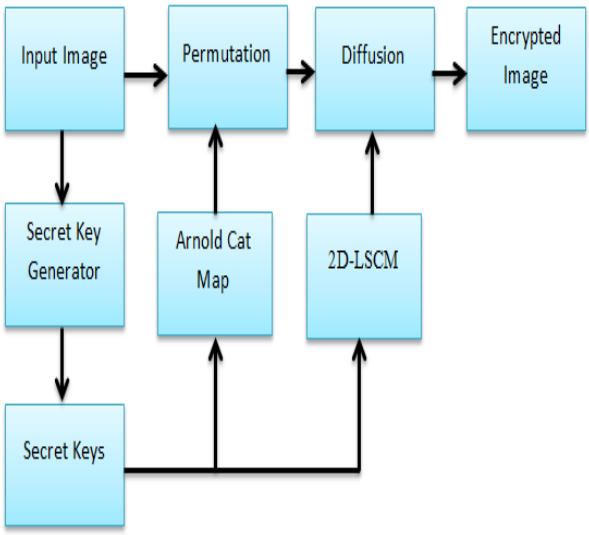

Figure 1: Block diagram of self-adaptive image encryption system

5 PERFORMANCE ANALYSIS OF PROPOSED SCHEME

Different parameters should be evaluated to analysis the performance of proposed scheme. The following parameters are involved as follows.

a. Entropy Analysis

Entropy is a measure of degree of randomness in the encryption system. The entropy is calculated using the formula [16]:

$$H(S) = \sum_{i=0}^{2^M-1} P(si) \log_2 \frac{1}{P(si)} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Where $P(s_i)$ represents the probability of occurrence of the i^{th}gray level in an image. Ideal value of entropy is 8 for a random image. If it is less, the chance of predictability is more. Table 1 shows entropy of somesample images and their corresponding cipher images.

b. Mean Square Error (MSE)

Generally MSE is analyzed between plain image and cipher image by taking mean of squared difference between them. More value of MSE leads to higher encryption and more noise

in the plain image. Mathematical equation for MSE [16] given by.

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2 \dots\dots\dots\dots\dots\dots\dots (7)$$

c. Peak Signal to Noise Ratio (PSNR)

Peak signal-to noise ratio which is always opposite to Mean Square Error (MSE). Cipher image quality generally measured by PSNR quantity. For good security of image, more MSE and Less PSNR. Mathematically PSNR is given as below [16].

$$PSNR = 10\log_{10}\frac{255}{MSE} \dots\dots\dots\dots\dots\dots\dots\dots\dots (8)$$

d. UACI and NPCR

To check the sensitivity of proposed encryption technique with respect to secret key and plain image, they are two tests: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) [17]. The equation to calculate UACI is Eq. 9.

$$UACI = \frac{1}{N}\left[\sum_{i,j}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \dots\dots\dots\dots\dots\dots\dots\dots (9)$$

Where, m represents number of rows, n indicates number of column, I(p,q) and E(p,q) are the original and cipher image respectively. NPCR can be calculated by Eq. 8

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN}X100\% \dots\dots\dots\dots\dots\dots\dots\dots (10)$$

Where, m represents number of rows, n indicates number of column and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, \quad otherwise \end{cases} \dots\dots\dots\dots\dots\dots\dots (11)$$

where I(i,j) and E(i,j) are the original and cipher image respectively.

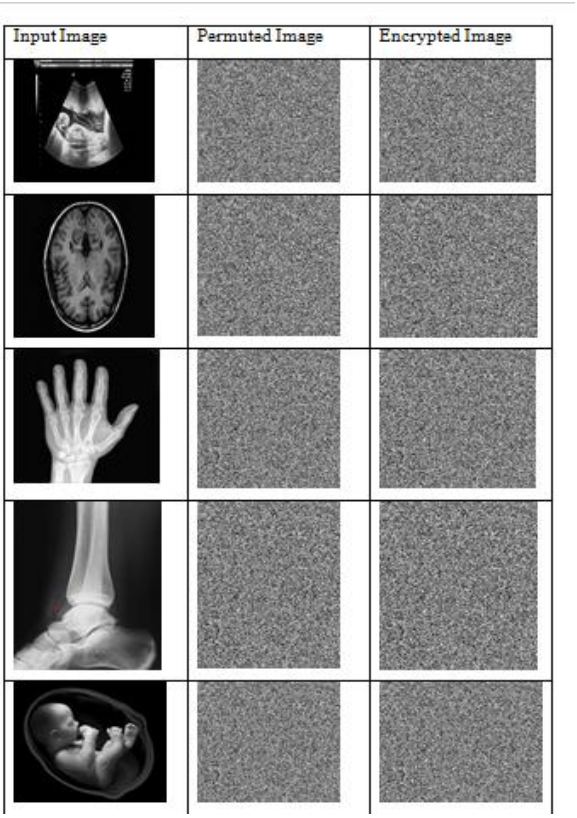

Figure 2: Original images, permuted images and encrypted images of proposed system

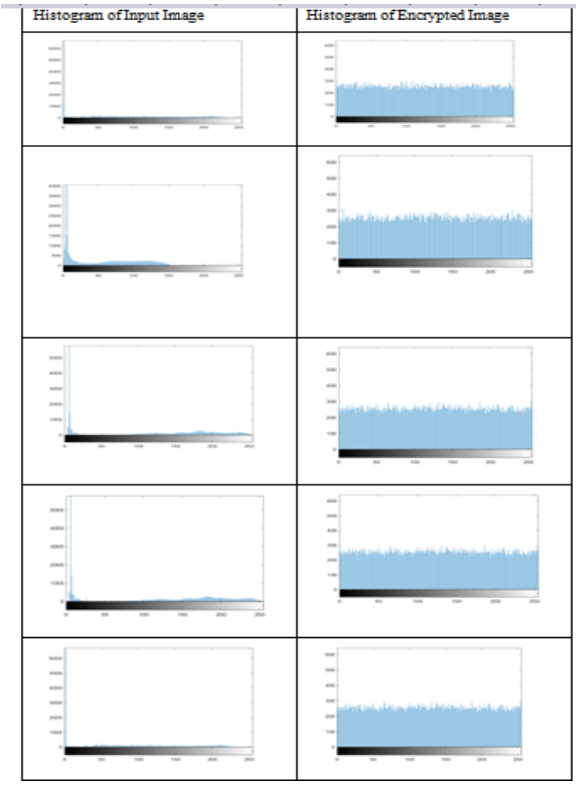

Figure 3: Histogram of original images, permuted images and encrypted images of proposed system

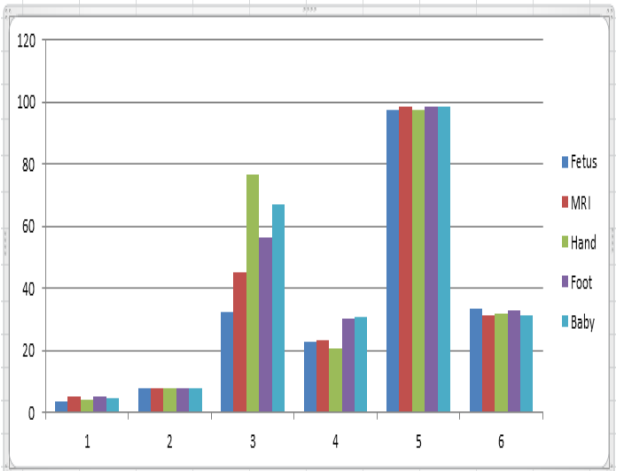

Figure 4: Graphical analysis of encryption parameters for proposed system

Image Name	Entropy_In (Bit)	Entropy_Enc (Bit)	MSE	PSNR(db)	NPCR(%)	UACI(%)
Fetus	3.5963	7.972	32.4253	22.7620	97.5804	33.4852
MRI	5.0030	7.967	45.1345	23.1984	98.6292	31.0373
Hand	4.2654	7.976	76.7731	20.4390	97.6368	31.8776
Foot	5.3264	7.974	56.5421	30.3340	98.7328	32.7076
Baby	4.4524	7.978	66.8941	30.5340	98.5378	31.3476

Figure 5: Performance parameters table for proposed ROI encrypted system

From the figure 5 we concluded that entropy values of cipher images are more than original plain image. MSE values are increases according to different image that will give the amount of encryption. NPCR and UACI values are approaches to theoretical value. Figure 4 shows that graphical representation of different parameters used in proposed encryption system. For different images different values has been obtained.

6 CONCLUSION

A self-adaptive image encryption techniques based on multiple maps has been developed. Proposed method mainly consists of three process namely Secret key generation, permutation and diffusion operation plain image dependent multiple secret keys are generated for multiple maps. we introduced a new chaos encryption scheme for Arnold`s Cat Map and 2DLSCM integrated medical imaging to achieve better security than other existing schemes This suggested approach has a wide range of applications in the field of image encryption. It can be utilized in secure visual communications because of its high level of security.

7 REFERENCES

[1] Laiphrakpam DS, Khumanthem MS. Medical image encryption based on improved elgamal encryption technique. Optik 2017;147:88–102.

[2] Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications. Commun Nonlinear SciNumer Simul 2015;24(1–3):98–116.

[3] Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A. Secure image encryption algorithm design using a novel chaos based s-box. Chaos Solitons Fractals 2017;95:92–101.

[4] Artiles JA, Chaves DP, Pimentel C. Image encryption using block cipher and chaotic sequences. Signal Process, Image Commun 2019;79:24–31.

[5] Abd-El-Atty B, Amin M, Abd-El-Latif A, Ugail H, Mehmood I. An efficient cryptosystem based on the logistic-Chebyshev map. In: 2019 13th international conference on software, knowledge, information management and applications (SKIMA). IEEE; 2019.

[6] Li Y, Wang C, Chen H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Lasers Eng 2017;90:238–46.

[7] Chen X, Hu C-J. Adaptive medical image encryption algorithm based on multiple chaotic mapping. Saudi J BiolSci 2017;24(8):1821–7.

[8] Boriga R, Dăscălescu AC, Priescu I. A new hyperchaotic map and its application in an image encryption scheme. Signal Process, Image Commun 2014;29(8):887–901.

[9] Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284(16–17):3895–903.

[10] Xingyuan W, Junjian Z, Guanghui C. An image encryption algorithm based on zigzag transform and LL compound chaotic system. Opt Laser Technol 2019;119:105581.

[11] Liu H, Wang X. Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 2010;59(10):3320–7.

[12] Dong C. Color image encryption using one-time keys and coupled chaotic systems. Signal Process Image Commun 2014;29(5):628–40.

[13] Khedr WI. A new efficient and configurable image encryption structure for secure transmission. Multimedia Tools Appl 2019;1–25.

[14] Boussif M, Aloui N, Cherif A. Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition. IET Image Process 2017;11(11):1020–6.

[15] Hua Z, Yi S, Zhou Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process 2018;144:134–44.

[16] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," International Journal of Video and Image Processing and Network Security, Vol. 12, 2012, pp. 18-31.

[17] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications, 2011, pp. 31-38.