Saudi Journal of Biological Sciences 24 (2017) 1821–1827

Contents lists available at ScienceDirect

Saudi Journal of Biological Sciences

journal homepage: www.sciencedirect.com

Original article

# Adaptive medical image encryption algorithm based on multiple chaotic mapping

Xiao Chen [a,b,*], Chun-Jie Hu [a]

[a] School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China
[b] Collaborative Innovation Center of Atmospheric Environment and Equipment Technology and Jiangsu Key Laboratory of Meteorological Observation and Information Processing, Nanjing University of Information Science and Technology, Nanjing 210044, China

ARTICLE INFO

*Article history:*
Received 13 October 2017
Revised 9 November 2017
Accepted 9 November 2017
Available online 10 November 2017

*Keywords:*
Logistic-sine mapping
Position scrambling
Image encryption
Hyper-chaotic system

ABSTRACT

Digital images are now widely used in modern clinic diagnosis. The diagnostic images with confidential information related to patients' privacy are stored and transmitted via public networks. Secured schemes to guarantee confidentiality of patients' privacy are becoming more and more vital. This paper proposes an adaptive medical image encryption algorithm based on improved chaotic mapping in order to overcome the defects of the existing chaotic image encryption algorithm. First, the algorithm used Logistic-sine chaos mapping to scramble the plain image. Then, the scrambled image was divided into 2-by-2 sub blocks. By using the hyper-chaotic system, the sub blocks were adaptively encrypted until all the sub block encryption was completed. By analyzing the key space, the information entropy, the correlation coefficient and the plaintext sensitivity of the algorithm, experimental results show that the proposed algorithm overcomes the shortcoming of lack of diffusion in single direction encryption. It could effectively resist all kinds of attacks and has better security and robustness.

## 1. Introduction

Images are now widely used in modern clinic diagnosis. The diagnostic images with confidential information related to patients' privacy are stored and transmitted via public networks (Cao et al., 2016; Al-Haj et al., 2017). With the rapid development of the internet and new communication technologies, sharing of information such as image information and position information (Chen and Zou, 2017) has become easier and faster (Kwok and Tang, 2007). As network presents openness and sharing features, the security issues such as personal privacy, and confidential files of enterprises and military in terms of the transmission and storage of image data have been increasingly challenged. These files therefore need to be provided with encryption protection. Under such context, image encryption techniques have gotten more attentions of global scholars. Digital image can be considered as two-dimensional sequences, which is greatly larger than text files. However traditional encryption algorithms including DES, AES and RSA have some shortfalls such as long encryption time consumed and security issues, which are therefore inappropriate to the encryption of real-time image (Pareek et al., 2006; Chen et al., 2004). As the chaotic system shows features including sensitivity, pseudo-random and nonlinearity of initial values, chaotic techniques have been applied into image encryption. The image encryption technologies based on chaotic systems has been widely developed (Zhang et al., 2016; Zhang and Fang, 2015; Zhou et al., 2014; Lin and Liu, 2012; Liao et al., 2010; Xie and Ding, 2015).

Fridrich proposed a chaotic encryption technique of images based on a permutation-diffusion architecture in 1998 (Fridrich, 1998). Chaotic image encryption algorithm has been highly focused. The literature (Cao, 2010) put forwards an image encryption algorithm (IEA) based on Logistic mapping. Although this algorithm can achieve the performance of pixel location and pixel value, the key space featured with small space and poor security are difficult to effectively overcome exhaustive attacks. The study (Zhen et al., 2013) proposed an IEA based on hyper-chaotic systems, which offers a large key space and increasing security. However individual encryption algorithm of chaotic systems fails to meet the demands of modern image encryption. A literature

* Corresponding author at: School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China.
*E-mail address:* chenxiao@nuist.edu.cn (X. Chen).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.sjbs.2017.11.023

(Ye and Zhou, 2014) put forwards an encryption algorithm of segmented images based on a chaotic sequence. It used a diffusion function to replace typical operation of permutation and diffusion to achieve encryption effect finally. However; this algorithm has poor robustness and encrypted images are likely to be affected by noises. A study (Deng et al., 2011) proposed an IEA on the basis of adaptive partitioning. This algorithm has only one encrypted direction of sub-blocks and adopts low-dimensional chaotic mapping with deficient diffusion.

This research proposes an adaptive image encryption algorithm based on improved chaotic mapping. First, the chaotic sequences generated by Logistic-sine map were used to scramble the position, and then the adaptive image encryption was carried out by using the hyper-chaotic system on the sub blocks. Experimental results show that the algorithm has good performance of encryption and recovery, and the security is good.

## 2. Chaotic system introduction

### 2.1. Logistic-sine mapping

The mapping equation of logistic-sine composite chaotic system is written as

$$\begin{cases} x_{k+1} = \mu x_k(1 - x_k) \\ y_{k+1} = \sin(r \arcsin \sqrt{y_k}) \end{cases} \tag{1}$$

where $x_k \in (0, 1)$, $x_k$ denotes the logistic mapping status and $y_k$ is the mapping status of sine mapping. When $3.5699456 < \mu < 4$, the logistic-sine system enters into a chaotic state in the case of $r > 1$. By mapping on the sensitivity of initial value using a composite chaotic system, corresponding chaotic sequences can be generated accordingly. Through transformation processing, digital images are performed permutation based encryption.

### 2.2. Hyper-chaotic system

The equation of the hyper-chaotic system is described as

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1x_3x_4 \\ \dot{x}_3 = -cx_3 + x_1x_2x_4 \\ \dot{x}_4 = -dx_4 + x_1x_2x_3 \end{cases} \tag{2}$$

where a, b, c, and d are the control parameters of the system. In the case that a = 35, b = 10, c = 1, and d = 10, a fourth-order Runge-Kutta algorithm is used to solve Eq. (2) with a step of h = 0.001. Meanwhile, x1 is set as small initial value produced from key stream, while other parameters are unchanged. The four groups of discrete chaotic sequences produced by iteration are X1, X2, X3, and X4. The system attractor diagram is shown in Fig. 1.

To further improve the nonlinearity of the chaotic sequences generated in the hyper-chaotic system, the integer processing of nonlinearity is defined as:

$$\delta(t) = f(X_m, X_n) = k_aX_m \times k_bX_n \tag{3}$$

where $k_a$ and $k_b$ are integers, while $X_m$ and $X_n$ are two random sequences of four sequences produced by hyper-chaotic systems.

A real-number sequence generated by ordinary chaotic mapping systems is shown in the interval of [0, 1]. To satisfy the demands of the encryption algorithm in this research, the integer operation needs to be performed on this sequence, which is distributed in the interval of [0, 3]. The integer operation is defined as

$$k_n = (round|\delta(t)| \times 4) \text{mod } 4 \tag{4}$$

## 3. Encryption algorithm

### 3.1. Pixel position scrambling

Pixel location scrambling denotes that an image is rearranged to destroy their correlation, which makes the image become a disturbing image. The logistic-sine composite hyper-chaotic system used in this work is conducted the permutation of plain texts and images in following steps.

Step1. The images to be encrypted are converted into two dimensional matrices. The number of row and column is recorded in data arrays C1 and C2.

Step2. By calculating the sum of all pixel values in the image, auxiliary key k can be obtained based on Eq. (5);

$$k = \text{mod}(sum, 256)/255 \tag{5}$$

Step3. The initial values of the logistic-sine mapping system are $x_0$ and $y_0$. The new initial values $x\prime_0$ and $y\prime_0$ for the chaotic system are solved.

Step4. Two sequences $\{x_k, y_k|\ k = 1, 2, \ldots, m \times n\}$ are generated in n times of iteration based on Eq. (4).

Step5. The sequences $x_k$ and $y_k$ are conducted ascending ordered arrangement and the subscripts of multiple elements in the original sequences are recorded to exchange the indexes (index1 and index2) in the sequences with the row C1 and the column C2 of the image. The permutation performance is therefore achieved to acquire scrambled images.

### 3.2. Pixel value diffusion

Ordinary pixel diffusion encryption methods based on gray value mainly refer to that a pixel and its adjacent pixel in an image is conducted XOR operation. The solved results are seen as new pixel value to replace the original pixel value. The diffusion encryption approach of pixel gray value in the direction along the positive diagonal of matrix images is used and it consisted of four types.

Type 1, the diffusion encryption is conducted on the part from upper left corner to the lower right corner of an image

$$I_{x+1}(i,j) = I_x(i,j) \oplus I_{x+1}(i-1,j-1) \oplus I_{x+1}(i-1,j) \oplus I_{x+1}(i,j-1)$$

Type 2, the diffusion encryption is performed on the part from bottom right corner to the upper left corner of an image

$$I_{x+1}(i,j) = I_x(i,j) \oplus I_{x+1}(i+1,j+1) \oplus I_{x+1}(i+1,j) \oplus I_{x+1}(i,j+1)$$

Type 3, the diffusion encryption is conducted on the part from upper right corner to the lower left corner of an image

$$I_{x+1}(i,j) = I_x(i,j) \oplus I_{x+1}(i+1,j-1) \oplus I_{x+1}(i+1,j) \oplus I_{x+1}(i,j-1)$$

Type 4, the diffusion encryption is conducted on the part from lower left corner to the upper right corner of an image

$$I_{x+1}(i,j) = I_x(i,j) \oplus I_{x+1}(i-1,j+1) \oplus I_{x+1}(i-1,j) \oplus I_{x+1}(i,j+1)$$

Each key value k in the key stream after integer processing corresponds to encryption methods.

If k[i] = 0, the diffusion encryption is conducted on the part from upper left corner to the bottom right corner of an image; If k[i] = 1, the diffusion encryption is made on the part from bottom right corner to upper left corner of an image; If k[i] = 2, the diffusion encryption is carried out on the part from upper right corner to lower left corner; If k[i] = 3, the diffusion encryption is conducted on the part from lower left corner to upper right corner.

The encryption algorithm in the literature (Deng et al., 2011) firstly divided plain-text images into 2-by-2 sub-blocks and then encrypts the matrices of four sub-blocks clockwise. The matrices