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.

© 2017 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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
(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

\[
\begin{align*}
    x_{k+1} &= \mu x_k (1 - x_k) \\
    y_{k+1} &= \sin(\arcsin y_k^l)
\end{align*}
\]

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

\[
\begin{align*}
    X_1 &= a(X_2 - X_1) + X_2X_3X_4 \\
    X_2 &= b(X_1 + X_2) - X_1X_2X_4 \\
    X_3 &= -cX_3 + X_3X_4X_5 \\
    X_4 &= -dX_4 + X_1X_2X_3
\end{align*}
\]

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:

\[
\delta(t) = f(X_m, X_n) = k_0X_m \times k_0X_n
\]

where \(k_0\) and \(k_0\) 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

\[
k_n = \left(\text{round}(|\delta(t)| \times 4) \mod 4\right)
\]

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):

\[
k = \text{mod} (\text{sum} 256) / 255
\]

Step3. The initial values of the logistic-sine mapping system are \(x_0\) and \(y_0\). The new initial values \(x_0\) and \(y_0\) for the chaotic system are solved.

Step4. Two sequences \([x_k, y_k]^T \ k = 1, 2,\ldots, m \times n\) 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

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

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
include A1 (upper right corner), A2 (bottom right corner), A3 (lower left corner) and A4 (upper left corner). Although the gray value of the pixels in sub-blocks of an image changes, this algorithm has merely one type of encryption sequences. The change in the pixels of each sub-block fails to affect the pixels of last sub-block.

If the plain-text images are conducted the processing of 2-by-2 sub-blocks as shown in Fig. 2, there are 12 types of encryption sequences theoretically. To guarantee the encryption speed, the encryption algorithm in this research selects four types as the encryption sequences of single block as follows.

The first type: A1 (upper right corner) → A2 (bottom right corner) → A3 (lower left corner) → A4 (upper left corner).

The second type: A3 (lower left corner) → A2 (bottom right corner) → A1 (upper right corner) → A4 (upper left corner).

Specific pixel value diffusion process is as follows:

Step1. The scrambled image A is conducted 2-by-2 sub-block processing and then key is input to produce key stream k.

Step2. Four types of encryption sequences are selected. If k[i] = 0, the first type of encryption sequence is chosen; if k[i] = 1, the second type of encryption sequence is chosen; if k[i] = 2, the third type of encryption sequence is chosen; if k[i] = 3, the fourth type of encryption sequence is chosen. After completing an encryption sequence, next encryption sequence chosen can solve the shortfall that the diffusion shortage of the encryption sequences for single sub-block of original algorithm.

Step3. encryption sequences are selected to calculate the XOR operation for the pixel gray values of a sub-block. Through conversion processing, the value calculated is used as the initial value of the hyper-chaotic system to produce key sub-stream k1. The following encryption methods are selected to encrypt next sub-block.

If k1[i] = 0, the diffusion encryption is conducted on the part from upper left corner to the bottom right corner of an image. If k1[i] = 1, the diffusion encryption is performed on the part from bottom right corner to upper left corner of an image. If k1[i] = 2, the diffusion
encryption is conducted on the part from upper right corner to lower left corner of an image. If \( k1[i] = 3 \), the diffusion encryption is carried out on the part from lower left corner to upper right corner of an image.

Step 4. Encryption sequences are chosen again to encrypt the matrices of sub-blocks, until the diffusion encryption of all sub-blocks is fulfilled.

4. Experimental results

In this research, a typical picture was used as the original image with the size of 256-by-256 pixels. The image was carried out simulating experiments using Matlab7.0 platform to achieve the encrypted image, as illustrated in Fig. 3. For the analysis of the histogram of gray value, the pixel points of original image is unevenly distributed, as shown in Fig. 4(a); while the pixel points of the encrypted image tends to be distributed uniformly, as indicated in Fig. 4(b). The gray information of the original image can be effectively concealed. However, the histogram of cipher text fails to present the statistics feature of the original image.

5. Performance analysis

5.1. Key sensitivity analysis

To analysis the sensitivity of encrypted images to key, different key combinations are used to decipher encrypted images by only slightly changing the initial values of the logistic-sine chaotic system and setting other control parameters and initial values being constant. Decryption fails when the initial values \( (x_0 \text{ and } y_0) \) of the system both present a deviation of \( 10^{-13} \). As shown in Fig. 5, any slight deviation of deciphering keys cannot acquire the information of original images, proving that this algorithm exhibits a great sensitivity to key.

5.2. Key space analysis

To prevent exhaustive attack, encryption schemes have to be endowed with key space as great as possible. For the encryption algorithm in permutation stage, the logistic-sine mapping encryption system is adopted with two control parameters - two initial values, and auxiliary keys. Meanwhile, the length of key stream in diffusion stage is 128 bits, and four types selections are available for both main key streams and sub-streams. If the precision of each parameter in computer lives up to \( 10^{-16} \), key space is \( 10^{64} \times 4^{256} \), suggesting a large key space. Therefore, there is only little probability of success by using exhaustive attack to encrypt images.

5.3. Information entropy

As information entropy is seen as a key index for measuring the randomness of images, the more disordered, the better the entropy approximates. The calculation equation is written as

\[
H(m) = \sum_{i=1}^{2N-1} p(m_i) \log_2 \frac{1}{p(m_i)}
\]
where \( P(m_i) \) indicates that information source is the probability of the \( i \)th symbol \( m_i \).

This parameter can be employed to evaluate the uncertainty of the information containing in the images, which is the information entropy of the image. Based on Eq. (6), the information entropy of the original image was calculated to be 7.5683, while the information entropy of the encrypted images is 7.9891. Compared to the information entropy (7.7626) in the literature (Deng et al., 2011), the encryption algorithm in this research had bigger information entropy (7.7626) in the literature (Deng et al., 2011), the encryption algorithm in this work has a smaller correlation coefficient \( r \), indicating favorable diffusion performance of the algorithm (see Table 2).

5.4. Correlation coefficient analysis

Because ordinary plain text images involve a huge amount of redundancy information, there is a certain correlation between adjacent pixels. To check the correlation between plain text images and encrypted images, \( N \) couples of adjacent pixels in the horizontal, vertical and diagonal directions were randomly chosen from the plain text and encrypted images respectively. The correlation was calculated based on the following equation

\[
\begin{align*}
D(x) &= \frac{1}{n} \sum_{i=1}^{n} [x_i - E(x)]^2 \\
\text{cov}(x, y) &= \frac{1}{n} \sum_{i=1}^{n} [x_i - E(x)][y_i - E(y)] \\
r &= \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}
\end{align*}
\]

where \( n \) is the number of pixel points; \( E(x) \) and \( E(y) \) present the expectation of \( x \) and \( y \); while \( x \) and \( y \) indicate the gray values of two adjacent pixel points; \( \text{cov}(x, y) \) represents the covariance of \( x \) and \( y \) and \( r \) is a correlation coefficient of adjacent pixels.

2000 couples of adjacent pixel points were randomly selected from the vertical, horizontal and diagonal directions respectively from plain-text and encrypted images. Fig. 6 shows the distribution of the correlation among pixels along vertical, horizontal and diagonal directions in plain text and encrypted images.

As displayed in Table 1, the adjacent pixels have great correlation in original images, which approximates to 1. The adjacent pixels present small correlation in encrypted images, which is close to 0. Table 1 also lists the correlation coefficients solving using the chaotic image encryption algorithm. The results show that the algorithm in this work has a smaller correlation coefficient \( r \), indicating favorable diffusion performance of the algorithm (see Table 2).

5.5. Differential attack analysis

This purpose is intended to emphasize the diffusion property of an encryption system under consideration with respect to small changes in plain image. This is important because otherwise the encryption system would be vulnerable to chosen-plain text attack. The diffusion performance of an image of P1 encryption system is commonly measured by means of two criteria, namely, NPCR (the number of pixel change rate) and UACI (the unified average changing intensity) (Wang and Jiang, 2011). The NPCR is used to measure the percentage of different pixel numbers between two images. Let \( P_1(i, j) \) and \( P_2(i, j) \) be the \((i, j)\) pixel of two images \( P_1 \) and \( P_2 \), respectively, the NPCR can be defined as

\[
\text{NPCR} = \frac{\sum_i D(i, j)}{m \times n} \times 100\% \tag{8}
\]

where \( m \) and \( n \) are the width and \( D(i, j) \) is defined as

\[
D_{ij} = \begin{cases} 
1, & c_1(i, j) \neq c_2(i, j) \\
0, & c_1(i, j) = c_2(i, j)
\end{cases}
\]

The second criterion, UACI is used to measure the average intensity of differences between the two images. It is defined as

\[
\text{UACI} = \frac{1}{m \times n} \left[ \sum_{ij} \frac{|c_1(i, j) - c_2(i, j)|}{255} \right] \times 100\% \tag{9}
\]

The ideal expectation values of NPCR and UACI for a gray image (Deng and Zhu, 2014) are 99.6094% and 33.4635% respectively. The calculated values of NPCR and UACI in this algorithm are 99.59% and 33.42% respectively. This suggested that any small change occurring to original images would result in the obvious variation of encrypted images, showing that the algorithm presents strong sensitivity of plain text. This algorithm indicated a better robustness to differential attacks compared to the algorithms in literature (Zhang and Fang, 2015; Lin and Liu, 2012).
Fig. 6. (a and b) Horizontal correlation of plain text and cipher images, (c and d) vertical correlation of plain text and cipher images, and (e and f) diagonal correlation of plain text and cipher images.

Table 1
The correlation coefficient of adjacent pixels.

| Direction | Plain image | Cipher image | RE (Liao et al., 2010) | RE (Xie and Ding, 2015) | RE (Deng et al., 2011) | RE (Kanso and Gheblen, 2012) | RE (Teng and Wang, 2012) |
|-----------|-------------|--------------|------------------------|-------------------------|-----------------------|-------------------------------|----------------------------|
| Horizontal| 0.9568      | -0.0028      | 0.0127                 | 0.0136                  | 0.0500                | -0.2546                       | 0.0242                     |
| Vertical  | 0.9842      | 0.0171       | 0.0190                 | 0.0062                  | 0.0400                | -0.0573                       | 0.0154                     |
| Diagonal  | 0.9351      | -0.0022      | 0.0012                 | 0.0175                  | 0.0200                | -0.0024                       | 0.0024                     |
6. Conclusion

This research proposes an improved chaotic mapping image encryption algorithm. First, the algorithm used Logistic-sine chaos mapping to scramble the plain image position. Then, a hyper-chaotic system was applied in adaptive image encryption algorithm of multiple selections to overcome the diffusion shortage resulting from the single encryption sequences in traditional encryption algorithms. In permutation stage, the sequences generated by secondary key were used to perform permutation on the rows and columns of images. The algorithm can be applied in encryption transmission of images and exhibits preferable practical significance and application prospect. The experimental results confirmed that this algorithm can achieve good encryption performance and has advantages of easy operation, large key space, high security, and attack resisting performance.

Acknowledgments

This work is supported by project grants from the six talent peaks project in Jiangsu Province of China (DZXX-006), 333 high level personnel training project Jiangsu Province of China, the Natural Science Foundation of Jiangsu Province of China (BK20161536), and the Priority Academic Program Development of Jiangsu Higher Education Institutions.

References

Al-Haj, A., Mohammad, A., Amer, A., 2017. Crypto-watermarking of transmitted medical images. J. Digit. Imag. 30 (1), 26–38.

Cao, J.Q., Xiao, H.R., Lan, Z.L., 2010. Chaos encryption algorithm based on dual scrambling of pixel position and value. Comput. Eng. Appl. 46 (28), 192–195.

Cao, W.J., Zhou, Y.C., Chen, C.L.P., Xia, L.M., 2016. Medical image encryption using edge maps. Signal Process. 132, 96–105.

Chen, G., Mao, Y., Chui, C., 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solit. Fract. 21, 749–761.

Chen, X., Zou, S., 2017. Improved Wi-Fi indoor positioning based on particle swarm optimization. IEEE Sens. J. 17 (21), 7143–7148.

Deng, S.J., Huang, G.C., Chen, Z.J., 2011. Research and implement of Self adaptive image encryption algorithm based on chaos. J. Comput. Appl. 31 (6), 1502–1504.

Deng, X.H., Zhu, C.X., 2014. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit. J. Commun. 35 (3), 216–223.

Fridrich, J., 1998. Symmetric ciphers based on two dimensional chaotic maps. Int. J. Bifurcation Chaos 8 (6), 1259–1284.

Kanso, A., Ghebelen, M., 2012. A novel image encryption algorithm based on a 3D chaotic map. Commun. Nonlinear Sci. Numer. Simul. 17 (4), 2943–2959.

Kwok, H.S., Tang, W.K.S., 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solit. Fract. 32 (4), 1518–1529.

Liao, X.F., LAI, S.Y., Zhou, Q., 2010. A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process. 90 (9), 2714–2722.

Liu, R., Lin, Q.N., Zhang, C.L., 2012. A new fast algorithm for gyrator transform. Laser Technol. 36 (1), 50–53.

Pareek, N.K., Patidar, V., Sud, K.K., 2006. Image encryption using chaotic logistic map. Image Vis. Comput. 24 (9), 926–934.

Teng, L., Wang, X.Y., 2012. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt. Commun. 285 (20), 4048–4054.

Wang, J., Jiang, G.P., 2011. Cryptanalysis of a hyper chaotic image encryption algorithm and its improved version. Acta Phys. Sinica 60 (6), 83–93.

Xie, G.B., Ding, Y.M., 2015. Image encryption algorithms with variable confusion parameters based on logistic mapping. Microelectron. Comput. 32 (4), 111–115.

Ye, G., Zhou, J., 2014. A block chaotic image encryption scheme based on self-adaptive modelling. Appl. Soft Comput. 22 (5), 351–357.

Zhang, J., Hou, D., Ren, H., 2016. Image Encryption Algorithm Based on Dynamic DNA Coding and Chen’s Hyperchaotic System, Mathematical Problems in Engineering, Article ID 6408741, 11pages.

Zhang, J., Fang, D.X., 2015. Image encryption technology applied chaotic maps index and DNA coding. Comput. Eng. Des. 36 (3), 613–618.

Zhen, W., Huang, X., Li, Y.X., 2013. A novel image encryption algorithm based on the fractional order hyper chaotic Lorenz system. Chin. Phys. 22 (1), 1–7.

Zhou, Y.C., Bao, L., Chen, C.L.P., 2014. A new 1D chaotic system for image encryption. Signal Process. 97, 172–182.

| Test | Proposed | RE (Pareek et al., 2006) | RE (Zhang et al., 2016) |
|------|----------|-------------------------|-------------------------|
| NPCR/% | 99.59 | 99.70 | 88.99 |
| UACI/% | 33.42 | 28.29 | 30.21 |