Technology and Health Care 24 (2016) S435–S442
DOI 10.3233/THC-161166
IOS Press

Research on medical image encryption in telemedicine systems

Yin Dai[a,b,*], Huanzhen Wang[a], Zixia Zhou[c] and Ziyi Jin[d]
[a]*Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang, Liaoning, China*
[b]*China Medical University, Shenyang, Liaoning, China*
[c]*Department of Electronic Engineering, Fudan University, Shanghai, China*
[d]*Department of Biomedical Engineering, Zhejiang University, Hangzhou, Zhejiang, China*

Abstract. Recently, advances in computers and high-speed communication tools have led to enhancements in remote medical consultation research. Laws in some localities require hospitals to encrypt patient information (including images of the patient) before transferring the data over a network. Therefore, developing suitable encryption algorithms is quite important for modern medicine. This paper demonstrates a digital image encryption algorithm based on chaotic mapping, which uses the no-period and no-convergence properties of a chaotic sequence to create image chaos and pixel averaging. Then, the chaotic sequence is used to encrypt the image, thereby improving data security. With this method, the security of data and images can be improved.

Keywords: Digital image, chaotic sequence, image encryption

1. Introduction

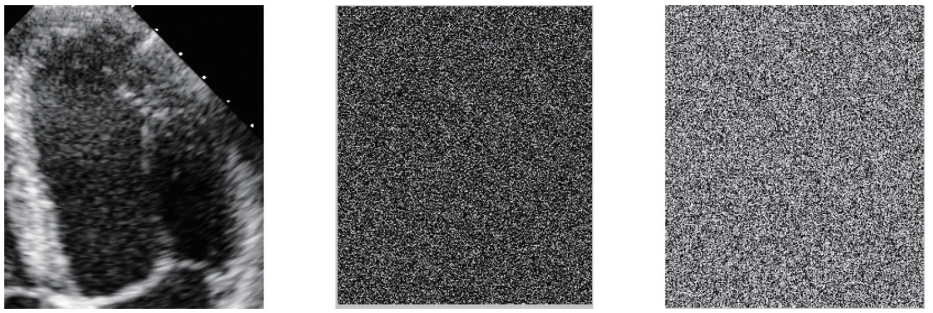
Telemedicine includes remote medical imaging, remote diagnosis, and consultation, such as remote nursing. This technology has been developed globally for about 40 years, but it has only recently been studied in China, where it has faced obstacles due to laws requiring encrypted image data [1,2]. This paper puts forward a new algorithm that combines traditional image encryption and image hiding with chaos theory. This technique can encrypt an image, and then extract the original image from the encrypted image. This technique could advance Telemedicine in China by providing a reliable method of sharing encrypted images.

2. The Traditional digital image encryption algorithm

2.1. Logistic chaotic sequence

Due to the wide application of chaos theory, the chaotic sequence has become a focal point in digital encryption. The traditional algorithm uses confusion and diffusion; confusion relocates pixels, and diffusion changes pixels. The basic formula of logistic chaotic mapping is $x_{n+1} = \mu(1 - x_n)$, $\mu \in (0, 1)$,

*Corresponding author: Yin Dai, Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang, Liaoning, China. E-mail: daiyin@bmie.neu.edu.cn.



(a) plain-image (b) cipher-image after confusion (c) cipher-image after diffusion

Fig. 1. The result of traditional image encryption.

$x_n \in (0, 1)$). The logistic chaotic sequence has sensitivity to the initial value. Changing the initial value produces a totally different output. Thus, this algorithm can ensure that the key to solve the encrypted image is unique.

2.2. The traditional encryption algorithm steps [3,4]

Step 1: The plain-image is a matrix of $M \times N$. The logistic mapping generates a chaotic sequence L and selects $M \times N$ numbers to form the chaotic sequence $L = [l_1, l_2, l_3 \ldots l_{M\times N}]$, which is used for image encryption; then, the numbers are arranged in order. Then, the sequence $H = [h_1, h_2, h_3 \ldots h_{M\times N}]$ is obtained with the values listed in order. Then, the plain-image is transformed into a one-dimensional array. The plain-image relocates its pixel locations according to sequence H to produce the chaotic image C.

Step 2: The key sequence in the diffusion process can be determined by Eq. (1). The sequence turns decimals into integers in the equation.

$$L'(i) = mod(round(10000 \times L'(i)), 256) \tag{1}$$

Step 3: The final cipher-image can be determined by the operation of XOR, as shown in Eq. (2).

$$D(i) = L'(i) \oplus C(i), \tag{2}$$

Step 4: Output the cipher-image, as shown in Fig. 1.

3. The image hiding algorithm based on image transfer

In this paper, the image is encrypted into a carrier image in accordance with the hiding method to obtain the cipher-image [5]. This enhances the effect of image hiding and hinders unauthorized decryption [6,7].

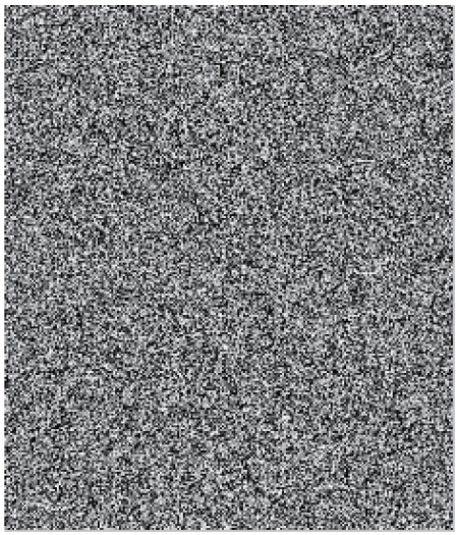


Fig. 2. Cipher-image after improved confusion.

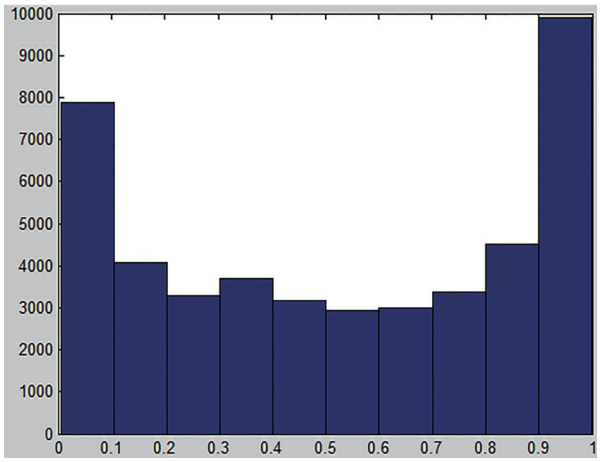


Fig. 3. Chaos sequence's sequence diagram.

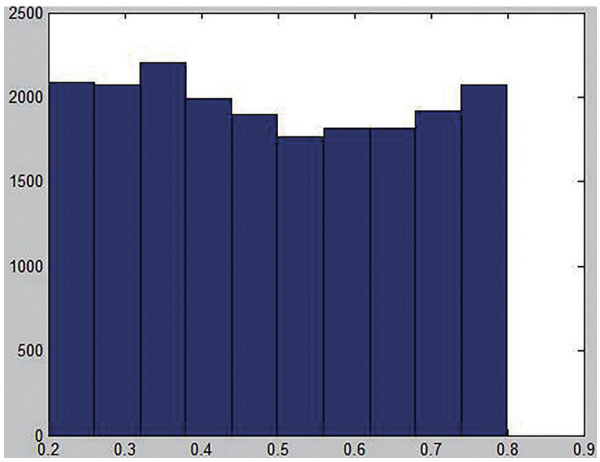


Fig. 4. Sequence diagram after cutting off.

3.1. Image encryption process improvement

Step 1: Set the original image as the matrix A with a size of $M \times N$. According to the principles of traditional algorithms, the confusion process begins with the first point. In the improved algorithm, setting a unique confusion starting point can increase security. In this way, the starting point also becomes part of the secret key encryption, which greatly improves key security. The original image is then changed into a one-dimensional array B; the values in sequence B are rearranged in accordance with the arrangement in sequence L. Then, the output image is moved into a matrix with a size of $M \times N$. Figure 2 shows the chaotic image.

Step 2: The image histogram does not change during the confusion process. It cannot effectively resist the statistical attack. The diffusion process should be used to average the pixel distribution.

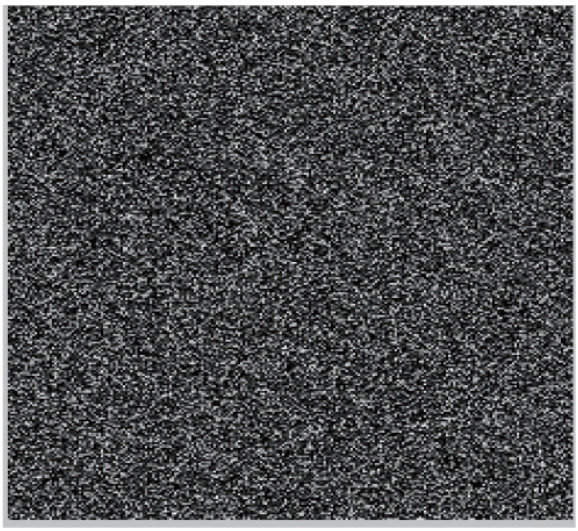


Fig. 5. Cipher-image after improved diffusion.

Equation (1) describes the method to turn the chaotic decimal sequence into integer sequence $L'(i)$. Figure 3 describes the Chaotic Sequence, it influences the randomness an d complexity. The middle uniform part can be used as a diffusion sequence to improve the encryption result, as shown in Fig. 4. Thus, multiple diffusion processes can be used, following Eqs (3–8).

$$B_1(i) = L'(i) \oplus B(i), \tag{3}$$

$$C_1(i) = B_1(i) \oplus B_1(i-1); \tag{4}$$

$$B_2(i) = C_1(i) \oplus L'(i), \tag{5}$$

$$C_2(i) = B_2(i) \oplus B_2(i-1); \tag{6}$$

$$B_n(i) = L(i) \oplus C_{n-1}(i), \tag{7}$$

$$C_n(i) = B_n(i) \oplus B_{n-1}(i-1); \tag{8}$$

In this paper, we rounded $n = 4$ to get the encryption image shown in Figs 3–5.

Step 3: Image Hiding Process.

Considering the hiding result, the pixel of the chosen carrier image is similar to the plain-image. After the hiding process, the appearance of the final image is the same as the carrier image, so it can effectively withstand unauthorized decryption. In this section, image encryption is combined with image hiding to enhance security.

Equation (9) shows the image hiding interpolation formula, where F is the carrier image, C is the plain-image, S is the final hidden image, and a is a constant parameter.

$$S(x,y) = aF(x,y) + (1-a)C(x,y); \tag{9}$$

The inverse hidden formula is:

$$C(x,y) = (S(x,y) - aF(x,y))/(1-a), a \in (0,1) \tag{10}$$

As a increases, the hidden image is more similar with the carrier image F. When a equals 1, it becomes the carrier image F. To avoid this mistake, a is replaced by a calculation formula of limits in the final

Fig. 6. Carrier image.

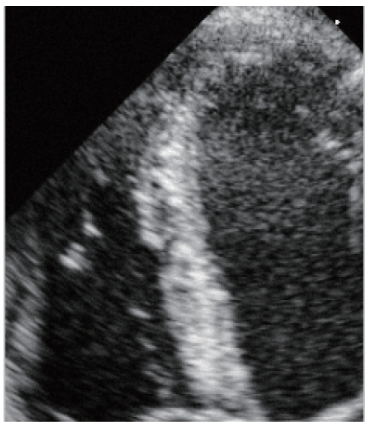


Fig. 7. Cipher-image after hiding.

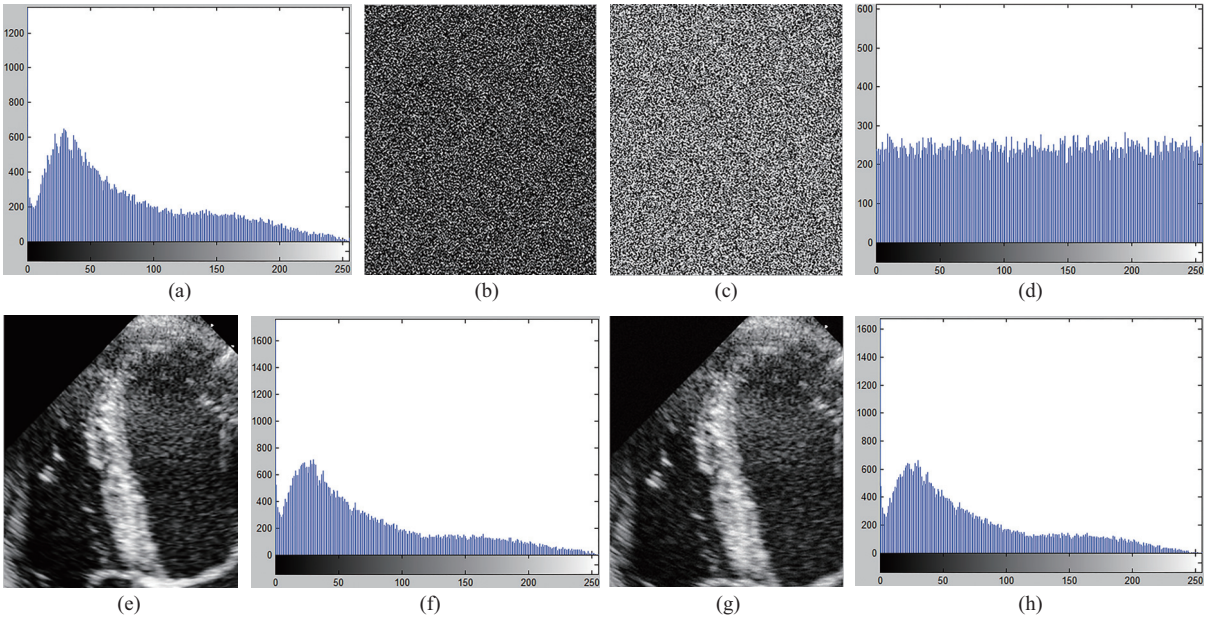


Fig. 8. The result of improved algorithm. (a) the histogram of plain-image; (b) cipher-image after improved confusion; (c) cipher-image after improved diffusion; (d) the histogram of cipher-image after improved diffusion; (e) carrier image lena; (f) the histogram of carrier image lena; (g) cipher-image after hiding; (h) the histogram of Fig. 7(g).

Eq. (11).

$$S(x,y) = \left(1 - \frac{1}{x}\right) F(x,y) + \left(1 - \left(1 - \frac{1}{x}\right)\right) C(x,y) \tag{11}$$

The inverse hidden formula is:

$$C(x,y) = \frac{S(x,y) - \left(1 - \frac{1}{x}\right) F(x,y)}{1 - \left(1 - \frac{1}{x}\right)}; (x \neq 0) \tag{12}$$

Table 1
Result analysis

Number	PSNR
Figure 1(a) and Figure 7(e)	18.3305
Figure 7(e) and Figure 7(g)	42.8684
Figure 1(a) and Figure 7(c)	17.2233

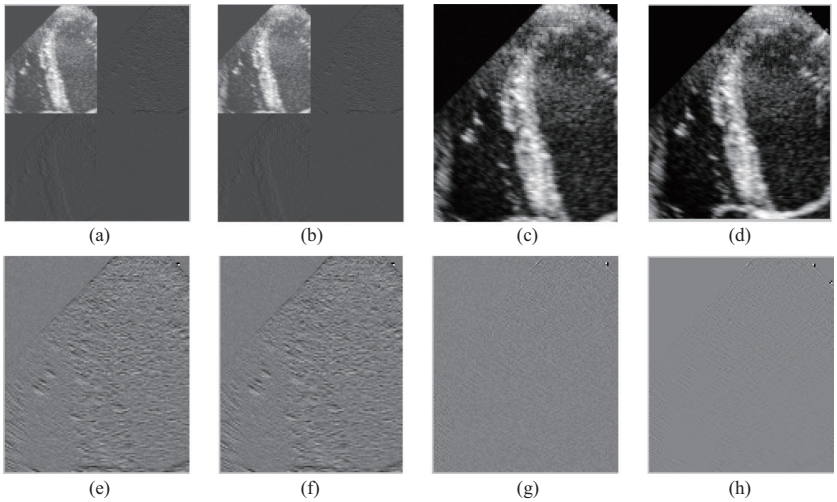


Fig. 9. The result of images after one-level wavelet decomposition. (a) one-level wavelet decomposition of image after hiding; (b) one-level wavelet decomposition of carrier image; (c) the detail component after one-level wavelet decomposition of hidden image; (d) the detail component after one-level wavelet decomposition of carrier image; (e) the horizontal component after one-level wavelet decomposition of hidden image; (f) the horizontal component after one-level wavelet decomposition of carrier image; (g) the high-frequency of component along the diagonal of hidden image after one-level decomposition; (h) the high frequency component along the diagonal of carrier image after one-level decomposition.

As shown in the Eq. (12), x controls the result of the hiding process without increasing computational complexity. In this paper, Fig. 6 was chosen as the carrier image and Fig. 7 was chosen as the cipher-image after hiding.

4. Performance and security

A usable image encryption should be capable of hiding the plain image in the carrier image [8]. In this section, the histogram and wavelet decomposition were performed on the proposed image encryption scheme, as shown in Fig. 8.

Through the confusion, diffusion, and hiding, the plain image was hidden in the carrier image. The histograms of Figs 8(f)–(h) are similar. To distinguish the two images, this paper used secondary wavelet decomposition to decompose the high and low frequency components. This method clearly shows the differences between the two images.

Figure 9 shows the high and low frequency components after one-level wavelet decomposition. The low frequency components of one-level decomposition between the two images (Figs 9(c)–(d)) are the same. However, the two images after one-level wavelet decomposition are very different in the horizontal and diagonal directions. The low frequency components determine the main outline of the image, while the high frequency components represent the images' details.

Comparing the images shows that the outline of the hidden and carrier images are basically identical, resulting in histogram formation.

To further analyze the image hiding effect, the article introduced PSNR [9] (Peak signal-to-noise) to measure the carrier and hidden images. The PSNR equation is shown as Eq. (13).

$$PSNR = 10 \log 10 \left[\frac{M \times N \times 255^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} [B(i,j) - G(i,j)]^2} \right] \tag{13}$$

PSNR is a method for measuring image fidelity. According to Table 1, the carrier and hidden images had the highest PSNR values. This illustrates that the two images are very similar, resulting in a high degree of image hiding.

5. Conclusions

This paper combines image encryption and hiding to form a new algorithm, which could be useful for telemedicine. The algorithm sets a new starting point during confusion, which greatly expands the secret key space, adopts multiple iteration operations, and uses its own pixel values to execute XOR, which improves the average pixel value after diffusion. Finally, the encrypted image is loaded into the carrier image to further improve the security of the plain image, which compensates for the deficiency of the single encryption method. Future studies will address image encryption algorithm keys and the other relevant topics in the field of telemedicine.

Acknowledgements

This work is supported by the Education Fund of the Education Department 110 of Liaoning, China (L20150171). This work is supported by the Ministry of Education Fundamental Research 112 Project, National Seed Fund Project, China (N151904001). This work is supported by National Natural Science Foundations of China (61302013).

References

[1] Lin Qiu-hua, Yin Fu-liang, Mei Tie-min, et al. A blind source separation-based method for multiple image encryption [J]. Image and Vision Computing, 2008, 26: 788–798.
[2] Chen Gang, Zhao Xiao-yu, Li Jun-li. A self-adaptive algorithm on image encryption[J]. Journal of Software, 2005, 16(11): 1975–1982.
[3] Fu C, Chen JJ. A chaos-based digital image encryption scheme with an improved diffusion strategy. Optics Express. 2012, 20(3): 2363–2378.
[4] Zhu Zhiliang, Zhang Wei, Wong K-W, et al. A chaos-based sym-metric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011 (181): 1171–118.
[5] Acharya B, Patra SK, Panda G, Image encryption by novel cryptosystem using matrix transformation, 2008, Washington DC: IEEE Pres, 2008: 77–81.
[6] Gao Tie-gang, Chen Zeng-qiang, A new image encryption algorithm based on hyper-chaos[J], Physics letters A, 2008 (372): 394–400.
[7] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Softw. 58 (2001): 83–91.

[8] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, ImageVision. Computer. 24 (2006): 926–934.
[9] U.P. Rajendra Acharya, S. Bhat, S. Kumar, L.C. Min, Transmission and storage of medical images with patient information, Computer Biomedical. 33 (2003): 303–310.