Cyclic-Shift Chaotic Medical Image Encryption Algorithm Based on Plain Text Key-Stream

Yin Dai 1,2,* , Huanzhen Wang1 and Haoran Sun1

1 *Sino-Dutch Biomedical and Information Engineering School*, Northeastern University, Shenyang, Liaoning, China
2 China Medical University, Shenyang, Liaoning, China

*Corresponding author: daiyin@bmie.neu.edu.cn

***Abstract* -- With the growing popularity of the Internet and the fast expanding to a variety of medical equipment, medical imaging technology has become increasingly sophisticated, especially the telemedicine is increasing rapidly. Therefore, in the process of transmission and storage of medical image, it is very important to encrypt it. However, compared with ordinary images, medical images contain patient information, which means more data, more rich content and the ability to resist tampering and anti-cutting requires higher. Traditional image chaotic encryption algorithm encrypts the image with preset key value, which leads to a high correlation and a relatively low sensitivity to the secret key. Therefore, the traditional image encryption algorithm cannot meet the needs of the medical image. In this regard, a cyclic shift-Chaotic Medical Image Encryption Algorithm Based on plain text key-stream is proposed. According to an established rules to obtain the required encryption of the plain text key-stream of medical image and then use this key to do Scrambling operation by using cyclic shift and Diffusion operation by using skew tent mapping, to ensure that the encryption process is closely related to medical image. The experimental results show that this algorithm has certain advantages in the statistical performance, the sensitivity and the anti-attack ability of the algorithm.**

Keywords -- Plain Text Key-stream; Cyclic Shift; Skew Tent Map; Chaotic System.

I. INTRODUCTION

Digital Imaging and Communications in Medicine (DICOM) [1] is the criterion of medical image transmission, which specifies the transmission, storage and display of digital medical image in the computer network. The medical image is fine and has generous amount of information. As a result, the common image encryption algorithm will no longer apply. There are ordinary encryption algorithm based on the Chaos Theory and the Information Entropy. The encrypted image, nevertheless, has periodicity, the contour is obvious, and the anti-tamper ability is not strong.

The sensitivity of chaotic system to initial conditions is very high, a slight change in the initial conditions can lead to great differences, which are very suitable for plaintext scrambling. Chaotic systems are random and sensitivity to initial value, and have the characteristic of broadband power spectrum density of noise these cryptography characteristic can be applied to medical image encryption system. [2]

The scholars in the field of image information security design a lot of image encryption algorithm based on chaotic system to realize the information security of the public channel. Chaotic encryption is one of the hottest topics in the field of information science and nonlinear science. The application of chaotic system in image encryption has become an important research subject in the field of image information security. In the literature [3], based on a 3D Affine Transformation and chaos, proposed a new encryption algorithm realized in the space domain. The algorithm of large key space can resist exhaustive attack. Besides, the mapping relation between plaintext and ciphertext is complex, which can effectively resist the chosen-plaintext attack. Although the proposed algorithm improves the sensitivity of the plaintext in the literature [4], unfortunately, the improved encryption scheme has yet to resist the attack of the chosen-plaintext. Literature [5] proposed a chaotic medical image encryption algorithm based on bit plane decomposition, the results demonstrate that, it is better than single mapping in three aspects: pixel correlation analysis, differential attack and information entropy.

II. CHAOTIC ENCRYPYION ALGORITHM

Image encryption algorithm is designed to get a good security and encryption speed, while resistance to known / chosen-plaintext attacks, and ciphertext image damage. The basic principle of image encryption is to make each pixel of the image fully scrambling and diffusion.

A. Cyclic shift algorithm of matrix

Because scrambling process needs to deal with all pixels in the image matrix, when the image size is large, the speed is slow, which means another scrambling methods are urgently needed. Taking into account that the

speed of cyclic shift is fast, if the scrambling algorithm is designed properly, it will help to improve the encryption efficiency.

Suppose matrix I as:

$$I = \begin{bmatrix} a & b & c & d & e \\ f & g & h & i & j \\ k & l & m & n & o \\ p & q & r & s & t \\ u & v & w & x & y \end{bmatrix} \quad (1)$$

Set one-dimension array A1 = [0 1 2 3 4] and A2 = [1 3 2 0 4], then row cyclic-shift matrix A1 and column cyclic-shift matrix A2 in MATLAB:

$$I_{A_1} = \begin{bmatrix} a & b & c & d & e \\ g & h & i & j & f \\ m & n & o & k & l \\ s & t & p & q & r \\ y & u & v & w & x \end{bmatrix} \quad (2)$$

$$I_{A_2} = \begin{bmatrix} u & l & r & d & j \\ a & q & w & i & o \\ f & v & c & n & t \\ k & b & h & s & y \\ p & g & m & x & e \end{bmatrix} \quad (3)$$

Every row and column of the matrix should be designed to meet the best scrambling effect and have the greatest resistance to truncated differential attack and penetration attack. In order to improve the encryption strength, the design of the row and column offset is chosen as a random cyclic shift that based on the numerical values of the elements in the secret one-dimensional array.

B. Skew Tent Map

The tent map is described as equation (4):

$$F(x) = \begin{cases} x/p & x \in [0, p] \\ (1-x)/(1-p) & x \in (p, 1] \end{cases} \quad (4)$$

X ∈ [0, 1] is the system state variable, p ∈ (0, 1)is control parameters. For arbitrary p ∈ (0, 1), this piecewise linear mapping (1) corresponds to a positive Lyapunov exponent of discrete dynamical system, so this map is chaotic.

All（x_0, p）can be used as the key of the encryption algorithm.

Fig. (1). and Fig. (2). shows the chaotic behaviour of the skew tent map (1), in which x0=0.27, p=0.4. Skew tent map has great chaotic properties, such as the sensitivity of the system parameters and initial value, pseudo randomness, ergodicity, etc., and its computational complexity is low, especially suitable for the design of image encryption algorithm. For i＝0 to M×N-1, execute the following Step 1-3.

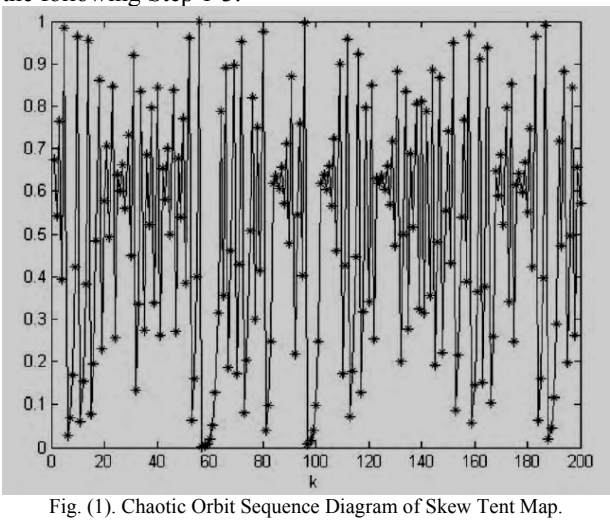


Fig. (1). Chaotic Orbit Sequence Diagram of Skew Tent Map.

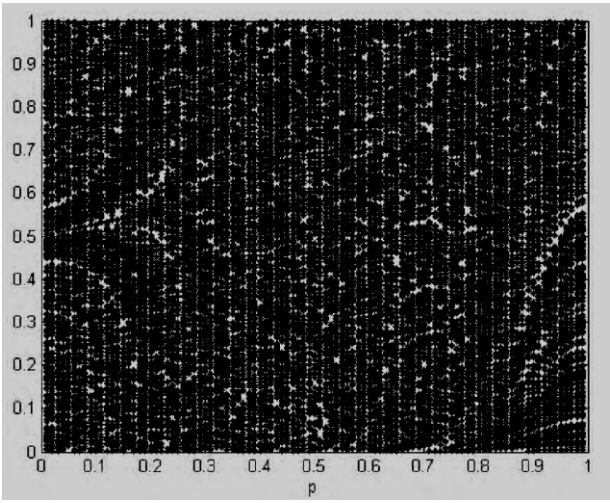


Fig. (2). Bifurcation Diagrams of Skew Tent Map

Step 1 A 8 bit pseudo random integer di is obtained according to the formula (5).

$$d_i = mod(floor(x \times 2^{48}), 256) \quad (5)$$

where x is the value of the current state of the skew tent map, the function floor(z) returns a largest integer that is less than or equal to Z, the mod(z, 256) Represent Modular Arithmetic, return the remainder of z divided by 256.

Step 2 Calculate the value of the current pixel of image encryption by current pixel value of scrambling image and a pixel value of the image before encrypted. The calculation formula is as follows:

$$A_i = mod(c_{i-1} + d_i, 256) \quad (5)$$

$$c_i = p_i' \oplus A_i \quad (6)$$

where $\oplus$ is XOR bitwise operations, ci is the output of current pixel value of the encrypted image, the initial value c_{-1} can be set to a constant (also can be regarded as the key).

Formula (7) is the inverse process of (5) - (6), which can be used for decryption:

$$p'_t = c_t \oplus mod(c_{t-1} + d_t, 256) \quad (7)$$

Step 3 Calculate k_i according to the formula (8):

$$k_t = 1 + mod(c_t, 4) \quad (8)$$

Then iterated skew tent map (1) k_i times to generate new state values x.

The decryption process is Similar to encryption. Using equation (7) instead of (5) - (6) in step 6, to obtain the scrambling image p', and then implement the inverse process of the replacement, finally get plain image P.

III. ACQUISITION ABOUT PLAIN TEXT KEY STREAM

Distinguish the medical image that demanded encryption, according to the rich contains of the medical image information and different abundance level of the information. For all kinds of medical images, the images of the human brain contain the most complex information, upper body is the second, low body is the last. Define the regional coefficient on the basis of the complexity, as showed in the Fig. (3). , different location of the human body has different regional coefficient. Description: If the location of the medical image involved cross regions, then choose the maximum coefficient of the regions.

Step 1 Read in the medical image that needed encryption, and get the gray level matrix Q, assuming the size of Q is M × N, then calculate the sum of gray values of the matrix Q, and denoted as S.

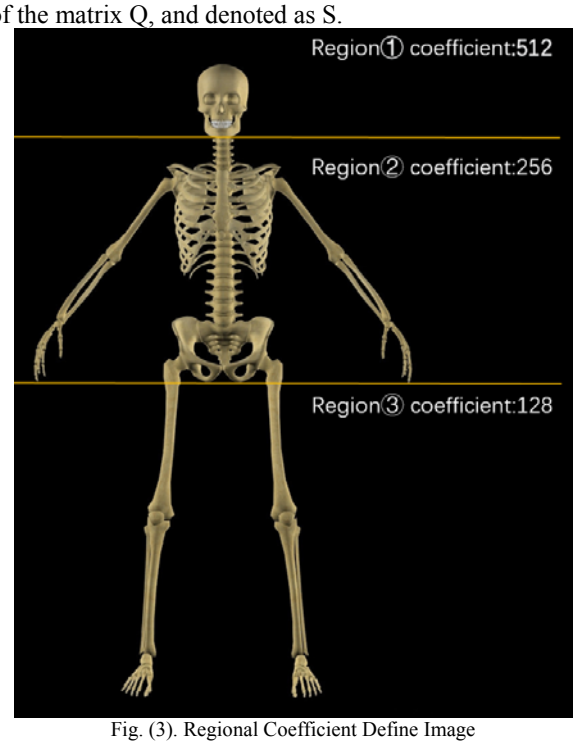


Fig. (3). Regional Coefficient Define Image

Step 2 According to the location that the medical image shot, get the corresponding area coefficient, denoted as L. (if the area is across region, take the largest factor)

Step 3 Obtain the plaintext key-stream as X, X is the remainder of S divided by L. Denote X as a three digits number ABC. (X∈(0, 512), A,B,C∈(0, 9)).

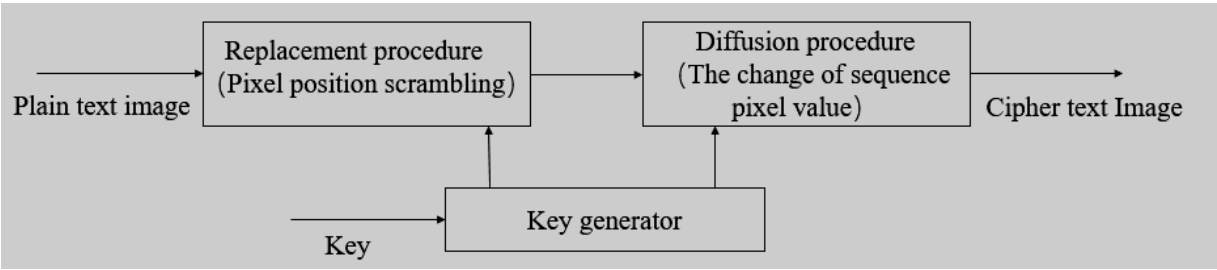


Fig. (4). the Traditional Structure of Displacement-Diffusion Process

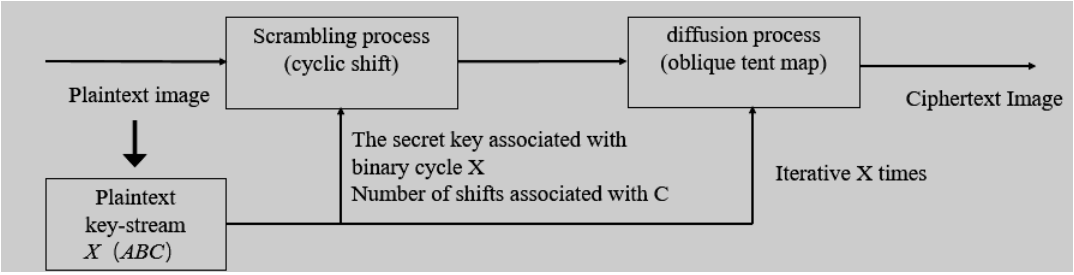


Fig. (5). the Structure of the Process in this Paper

A. The designs and analysis of image encryption algorithm in this paper

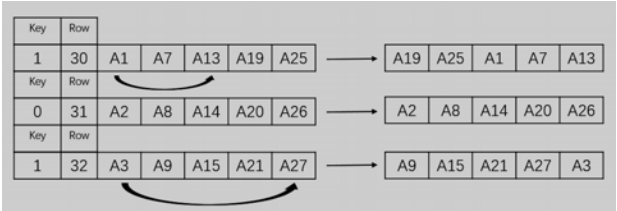
The displacement-diffusion process of the traditional image encryption algorithm based on chaos is shown in Fig. (4). In most of the algorithm suffered cracked has such a feature that the replacement process and diffusion process is independent of each other, the key-stream of the replacement has nothing to do with the plaintext image, and the key stream of diffusion process associated with the image, nevertheless the design of diffusion function has safety defects, thus the known plaintext attacks and chosen-plaintext attacks can be succeed.

In this paper, the displacement-diffusion process based on chaotic encryption algorithm of the cyclic shift of the secret key stream is shown in Fig. (5). The key X (ABC) got from the plaintext image, the scrambling process using cyclic shift algorithm, the circular key is correlated with X, the number of shifts is related to C; skew tent map algorithm is used in the diffusion process, which the number of iterations is correlated with X. Analysis of the algorithm comprehensively, compared with the traditional algorithm this algorithm is more secure.

Firstly, implement the Step1-3 in chapter 2 with the image to get the plain text key-stream X. The encryption algorithm designed in this paper is as follows:

Step 1 Calculate plaintext key stream X into a binary number, in order to generate a secret key. Then implement cyclic shift operation based on the secret key, which also used to control image transformation process.

Step 2 Transform the row of the original image: Suppose the bit that the secret key corresponding to is 1, then shift the line to the right cyclically, the shift number is equal to the row number minus (1+C) (for example: line 7, C= 2, means move the point to the right for 4 bits); if the bit value of the key is 0, the position of the corresponding line remains unchanged, as shown in Fig. (6). Then alter the column of the original image: Suppose the bit that the secret key corresponding to is 1, then shift the column downward cyclically, the shift number is equal to the column number minus (1+C) (for example: column 8, C= 2, means move the point downward for 5 bits); if the bit value of the key is 0, the position of the corresponding column remains unchanged.



Key	Row	The image before sequence reset					The image after sequence reset				
1	30	A1	A7	A13	A19	A25	A19	A25	A1	A7	A13
0	31	A2	A8	A14	A20	A26	A2	A8	A14	A20	A26
1	32	A3	A9	A15	A21	A27	A9	A15	A21	A27	A3
1	33	A4	A10	A16	A22	A28	A4	A10	A16	A22	A28
0	34	A5	A11	A17	A23	A29	A5	A11	A17	A23	A29
1	35	A6	A12	A18	A24	A30	A24	A30	A6	A12	A18

Fig. (6). Row Conversion Processing

Step 3 Setting the initial value of a skew tent map is y0=0.371 and the control parameters is p1=0.467. And iterative X times based on the skew tent map (1). For i=0 to M×N-1, implement step 1-3 of diffusion process in chapter 1.2, and changed the state variable x to y. The initial value of C-1 is set to 159 for the encryption algorithm in this paper.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Application of the algorithm

Choose three medical images to test the encryption algorithm. The test results are showed in Fig. (7). Through the contrast can be seen that, there has been an "avalanche" phenomenon after the encryption, the plaintext information is well hidden, and it cannot provide a way to find the information of plaintext from the encrypted image, such as tissue contour and skeletal contour. In addition, there is no periodicity of the encrypted image.

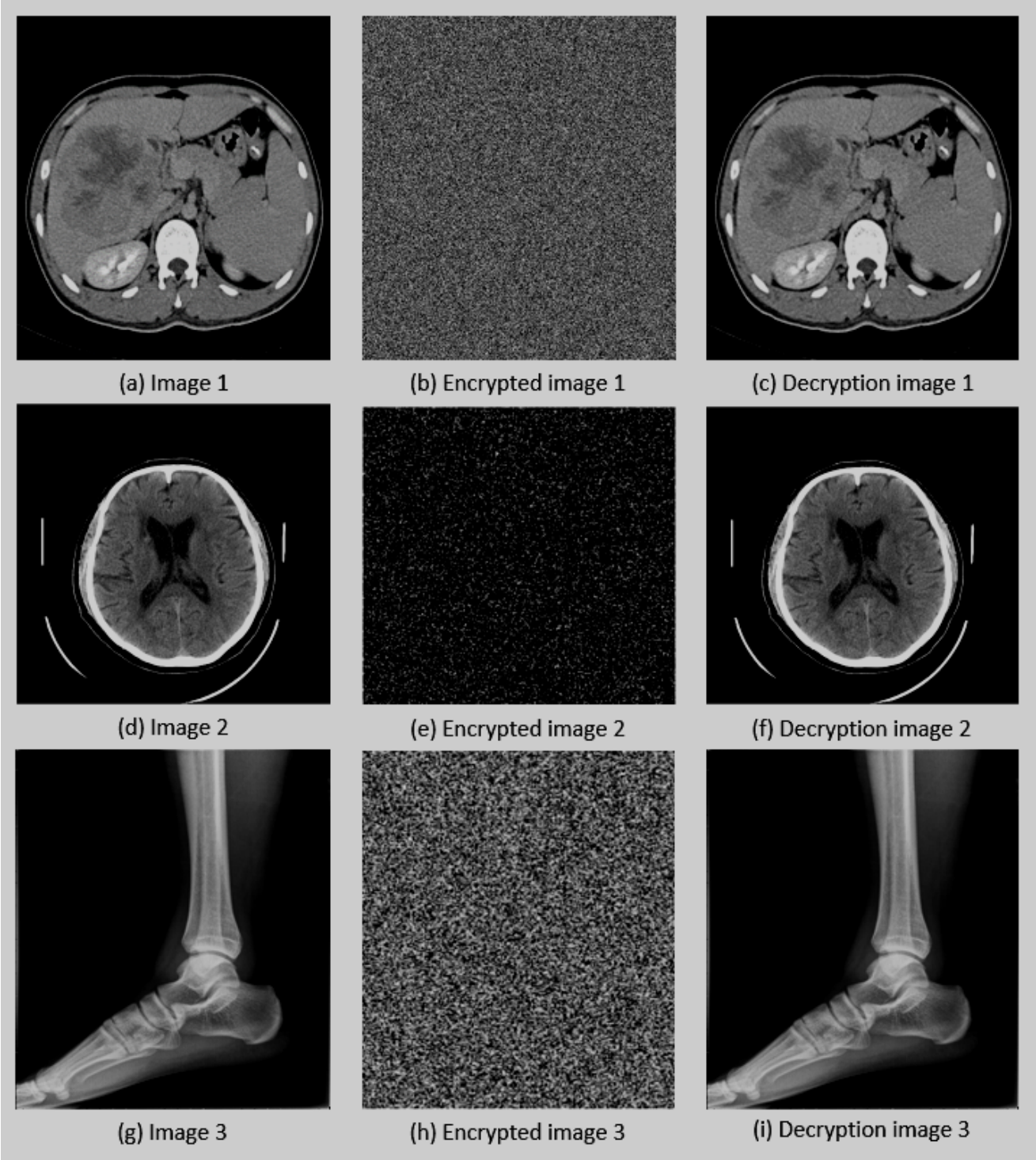


Fig. (7). Image 1-3 and their Encryption and Decryption Images

B. Tests of Algorithm

This section will carry out a series of tests to verify the effectiveness and feasibility of the algorithm. Experimental environment is the Intel i5, 2.7GHz, size of the hard disk is 500G PC. Experimental platform is the MTLAB version of 2014a. Test image is the medical image 1.

B1. The histogram of the image

According to the results, the algorithm can effectively reflect the ability of the hiding image information ability of the encryption algorithm. In order to describe the characteristics more clearly, analyzing and improving the performance of image encryption algorithm, the histograms of the images are showed as Fig. (8). given by MATLAB. The horizontal coordinates of the histogram represent the gray value of the image and the vertical coordinates represent the density distribution.

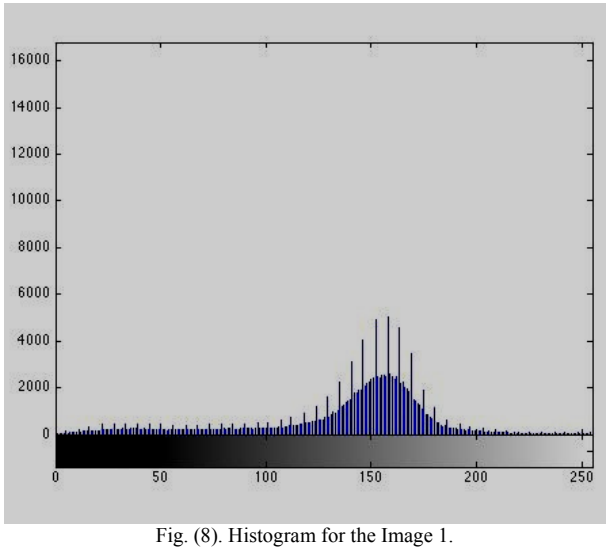


Fig. (8). Histogram for the Image 1.

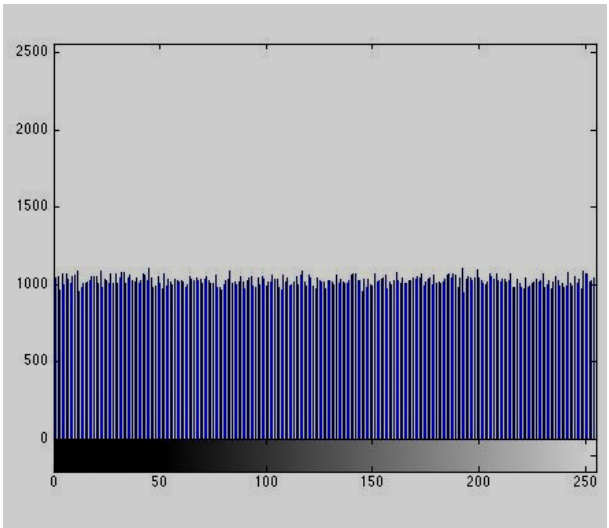


Fig. (9). Histogram of the Image 1 after the Encryption Algorithm of This Paper

From Fig. (8). the histogram distribution of original image is not uniform. There are many magnitude of pixel points distributed on 0-255, and there is a peak about 3000 when the gray value is 160.

According to the Fig. (9). , The distribution of gray value has been improved significantly with the algorithm of this paper, the pixel points all in about 1000 distribute evenly on 0-255, and there is no obvious peak. It can be seen that the gray value of the image has been improved obviously based on the algorithm of this paper, which shows that the information of the plaintext is hidden well.

B2. The correlation between the image pixels

The correlation between adjacent pixels in the original image is very high. In order to destroy the statistical attacks, the correlation of the neighboring pixels must be reduced. Therefor select 2500 pixels from the test image randomly, to analyze the correlation between the pixels of three directions: horizontal, vertical and diagonal. Table 4-1 analyze the pixel correlation of skew tent map encryption algorithm.

TABLE 1. CORRELATION BETWEEN THE IMAGE PIXELS OF THE ALGORITHM IN THIS ARTICLE

Pixel Correlation	Plain Image	Ciphertext Image
Horizontal	0.988760	-0.001546
Vertical	0.986192	0.001719
Diagonal	0.986195	0.003527

As can be seen from the data in the table, the pixel correlation of the plaintext image is very high, which is close to 1. And the correlation is decreased to about 0.0015 after encryption. The correlation of the image pixels is greatly reduced after encryption.

The pixel correlation can also be given in the form of graphs. Selected 2500 pixels randomly to test. Fig. (10). represents the horizontal direction, that the horizontal axis is the gray value of (x, y) the vertical axis is the gray value of(x+1, y).

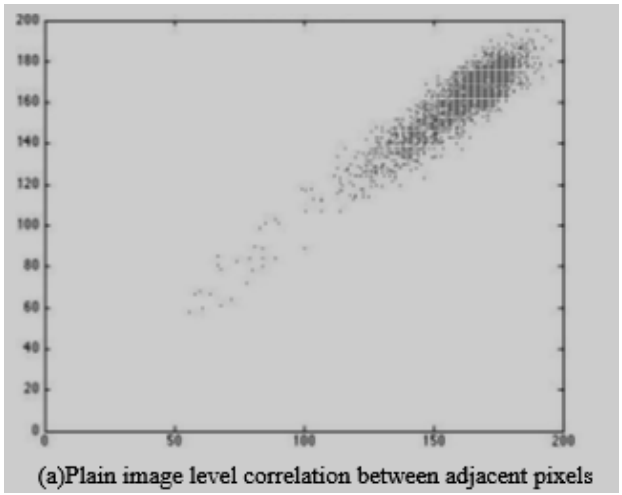


Fig. (10). The Correlation of Level Pixels

Figure 10 continues on next page

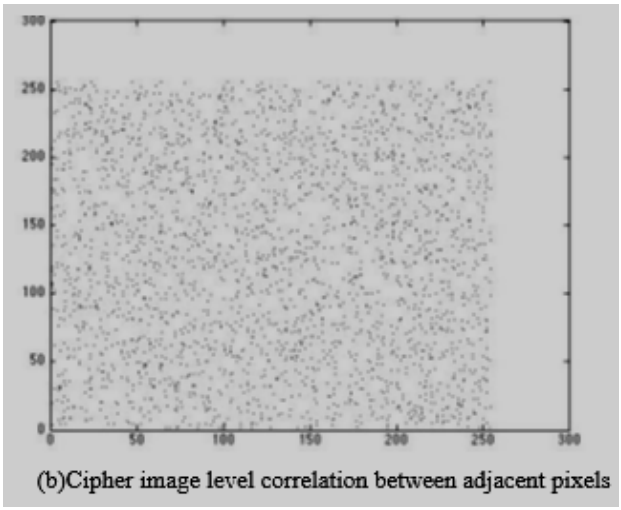


Fig. (10). The Correlation of Level Pixels

The horizontal axis is the gray value of (x, y), the vertical axis is the gray value of (x, y+1). The correlation of adjacent pixels in the plaintext image is "clustered" together, while the correlation of adjacent pixels in the same position of the encrypted image is reduced, and the distribution is uniform.

Fig. (12). is the diagonal direction. The horizontal axis is the gray value of (x, y), the vertical axis is the gray value of (x+1, y+1).

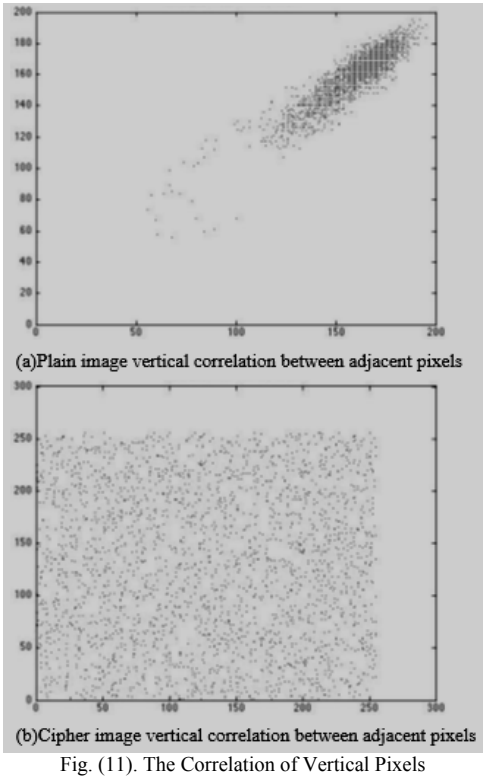


Fig. (11). The Correlation of Vertical Pixels

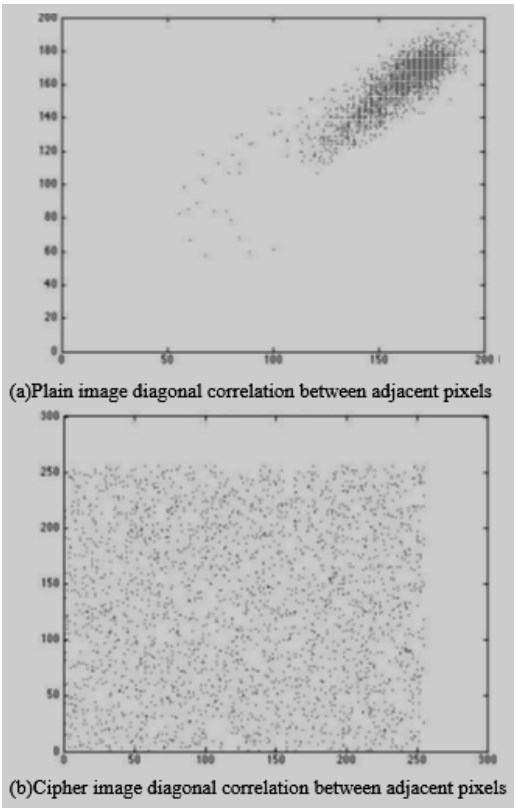


Fig. (12). The Correlation of Diagonal Pixels

Through the test of the correlation pixels, proved that the statistical information of image after encrypt is much better than the plaintext image, which means the ability to hide the text message effectively and resist attacks has been improved.

V. SUMMARY AND CONCLUSION

The improved algorithm in this paper has an innovation point and two improvements. The innovation is put forward the plain text key-stream for medical images, achieved a picture of a key with a high security. One improvement is that the cyclic shift used in the permutation process is related to the plain text key-stream, which makes the improved encryption algorithm more sensitive to the plain-text image, implements the ability to resist known plaintext and select plaintext attacks, and has a high level of scrambling the same as its speed. Another improvement is that the number of iterations used in the skew tent map diffusion process is related to the plaintext key-stream, rather than the default values in the traditional algorithm, which enhance the security of image encryption, finally the improved encryption algorithm also strong the ability to resist differential cryptanalysis attack algorithm and improved so as to enhance the of attack ability to resist.

ACKNOWLEDGMENT

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

REFERENCE

[1] Liu L P, Zhang X F. “Image encryption algorithm based on chaos and bit operation” [J]. Computer application,2013,33 (4):1070-1073.
[2] Wen C C, Wang Q, Liu X H. “New image encryption algorithm based on affine and complex chaos” [J]. Computer research and development,2013,50(2):319-324.
[3] Ye R S, Guo W H. “Image encryption algorithm based on bit plane scrambling and gray value bidirectional diffusion” [J], Journal of shantou university : Natural Science Edition, 2014, 29 (2) : 18-27.
[4] Eslami Z, Bakhshandeh A. “An improvement over an image encryption method based on total shuffling” [J].Optics Communications, 2013, 286 (1) : 51-55.
[5] Dai Yin, Huanzhen Wang, Zixia Zhou. “Research on Medical Image Encryption in Telemedicine System” [J]. Technology and Health Care , 2016, 30(4): 11-17.