Novel Medical Image Cryptogram Technology Based on Segmentation and DNA Encoding

Hongwei Xie
Taiyuan University of Technology
Yuzhou Zhang
Taiyuan University of Technology
Hao Zhang (zhangh545@126.com)
Taiyuan University of Technology https://orcid.org/0000-0003-4281-1461
Zhenyu Li
Taiyuan University of Technology

Research Article

Keywords: 4-D hyperchaotic system, image segmentation, ROI, DNA encoding, medical image encryption

Posted Date: July 22nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-727980/v1

Novel medical image cryptogram technology based on segmentation and DNA encoding

Xie Hong-wei[1], Zhang Yu-zhou[1], Zhang Hao*[2], Li Zhen-yu[2]

(1 College of Software, Taiyuan University of Technology, Jinzhong 030600, China)

(2 College of Information and Computer, Taiyuan University of Technology, Jinzhong 030600, China)

Abstract: This paper proposes a novel medical image encryption method based on fast and robust fuzzy C-means clustering image segmentation method and deoxyribonucleic acid encoding. Firstly, the plain medical image is split to interested pixels and uninterested pixels, respectively. Then, the uninterested 0-value pixels are abandoned to reduce the pixels in encryption. Secondly, for the interested pixels, some low-value pixels are also discarded by image segmentation to further reduce the encryption time. Thirdly, a 4-dimensional hyperchaotic system is utilized to process the main pixels of medical image with deoxyribonucleic acid encoding. Finally, lossless encryption and fast encryption are done for different purposes and security analysis shows that the encryption method is robust and secure to resist various attacks.

Keywords: 4-D hyperchaotic system, image segmentation, ROI, DNA encoding, medical image encryption

1. Introduction

Medical image, as an important basis diagnostic basis, contains many important personal information of patients. Medical images (MRI, CT, X-rays) with large data storage, redundancy and high pixel correlation are easily tampered or attacked. Besides, with the rapid growth of the number of medical images, the security of transmission and storage is an important issue. Encryption is an effective and widely used method to protect image information.

The chaotic system is known as a pseudo-random generator, due to its various features such as high sensitivity to initial states, pseudo-randomness, ergodicity, and non-periodicity [1-3]. In the past few decades, many classical chaotic systems have been proposed for the encryption of medical images, such as Chen system, Tent map and Logistic map [4,5]. With the deepening research on chaotic system, many new multidimensional chaotic systems have been applied to medical images encryption. For example, Iqbal proposes an RGB (color image) encryption algorithm based on

*Corresponding author. E-mail: zhangh545@126.com

dynamic three-dimensional scrambled image (D3DSI), 5D multi-wing hyperchaotic system and deoxyribonucleic acid (DNA) calculation [6].

Since the ground-breaking work on DNA computing conducted and reported by Adleman [7]. DNA computing has attracted attention of researchers worldwide, due to its superior characteristics of large concurrency, mass storage and low energy consumption [8]. DNA coding theory is used in the field of image information security by Zhang et al [9]. Meanwhile, the DNA-based encryption method has caught attention because of its excellent performance on confusion and diffusion [10-12]. Piecewise linear chaotic map (PWLCM) is used to generate the key image, and DNA rules is used to encode the key image by E-SM et al. [13]. Folifack propose a cryptosystem based on a chaotic Jerk system and DNA encoding proposed in the article for image encryption [14]. The combination of DNA and chaos has aroused interest among scholars in image encryption [15-17].

Recently, some medical image encryption algorithms are proposed. Jeevitha proposes the discrete wavelet transform (DWT) block-based scrambling and the edge maps for medical image encryption [18]. A new medical image encryption system is proposed using a linear feedback shift register (LFSR) based on a special nonlinear filter function [19]. White and gray areas in the medical image reflect the features of image. These areas can help doctors to diagnose. Moreover, the black area occupies parts of the area in the medical image. Some existing medical image encryption schemes has taken this feature into account. Khashan et al presents a lightweight selective encryption scheme to encrypt the edge maps of medical images [20]. Although this method encrypts a small number of pixels, most areas can still obtain some medical information.

The traditional methods have the limitations of high time consumption and serial execution of programs. In order to overcome these problems, this paper proposes an image encryption algorithm based on image segmentation. The main contributions of the proposed technology are as follows: (1) Discarding the clustering pixels with lowest values in the region of interest (ROI) to reduce the number of encrypted pixels. (2) Using doctor-patient information and medical image information as input values of SHA256 to enhance plaintext correlation. (3) The 4-D hyperchaotic system and DNA encoding is used to encrypt the selected pixels.

The rest of this paper is as follows: In section 2, the preliminaries of the proposed scheme are described in detail. Section 3 introduces the encryption and decryption schemes. Section 4 gives

experimental results and analysis of medical images. Moreover, performance evaluations and comparisons with other articles are provided. Finally, a brief conclusion is made in section 5.

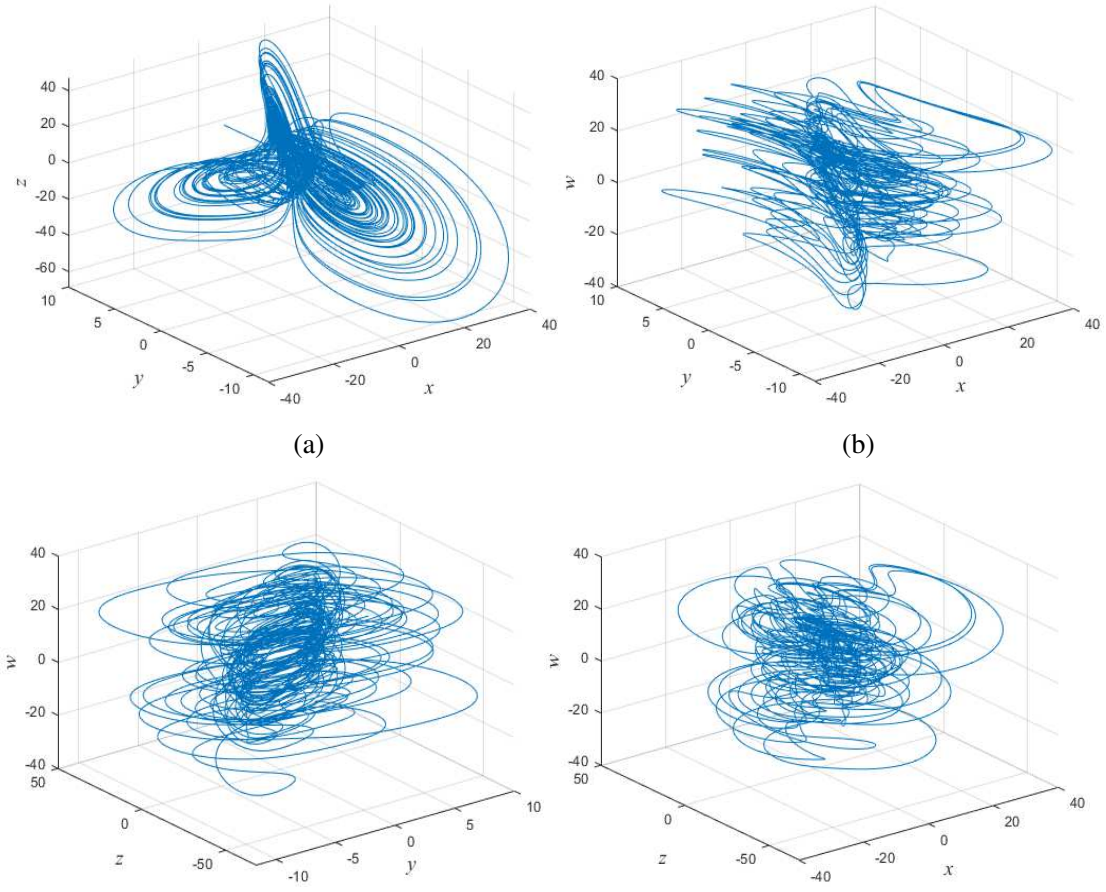
2. Hyperchaotic system and DNA encoding

2. 1 Hyperchaotic systems model and performance analysis

In this paper, an improved 4-D hyperchaotic system [21] is utilized. The multiple-wing hyperchaotic system reflects the difference of system states. And the different states of the attractor can generate different keys. Thus, the hyperchaotic system has better security. The model of the system is shown in Equation (1):

$$\begin{cases} \dot{x} = -ax + yz \\ \dot{y} = xz - y^3 + w \\ \dot{z} = -bxy + cz + w \\ \dot{w} = y - dz \end{cases}, \tag{1}$$

where a, b, c and d are the system parameters and x_1, x_2, x_3, x_4 are the initial values of the hyperchaotic system. When a =5, b =6.5, c=7, d=4 and x_1=2, x_2=8, x_3=4.5, x_4=6, the system has a typical four-winged hyperchaotic attractor, as shown in Fig. 1.

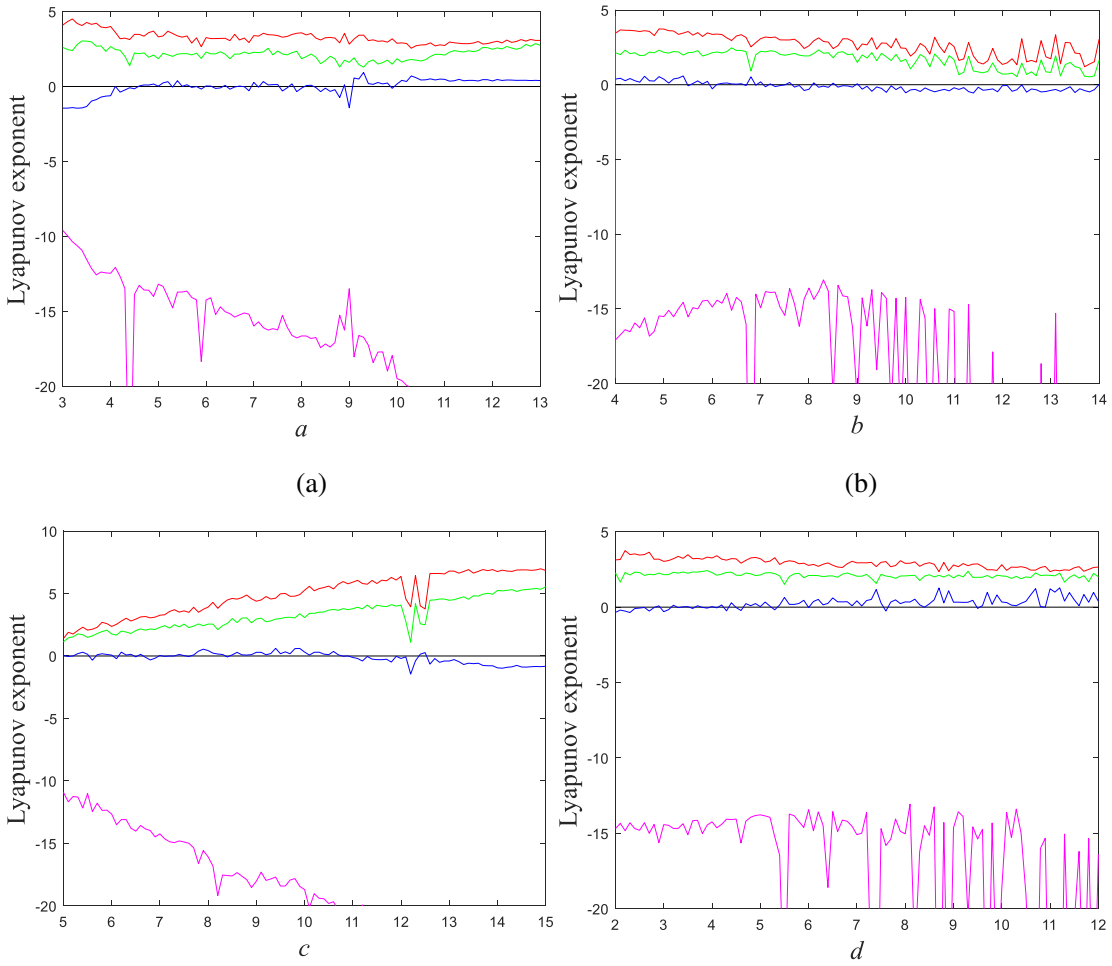


(a) (b)

(c) (d)

Fig.1 Phase diagrams of the system: (a) *x*-*y*-*z* plane, (b) *x*-*y*-*w* plane, (c) *y*-*z*-*w* plane, (d) *x*-*z*-*w* plane

Lyapunov exponent is an evaluation indicator whether a system is chaotic or not. When b =6.5, c=7, d=4 and x_1 =2, x_2 =8, x_3 =4.5, x_4 =6, the Lyapunov exponent (LE) changes with parameter a , as shown in Fig. 2 (a).



(a) (b)

(c) (d)

Fig.2 Lyapunov exponents of the system: (a) variable *a*-LE, (b) variable *b*-LE, (c) variable *c*-LE, (d) variable *d*-LE

Lyapunov exponent is an evaluation indicator whether a system is chaotic or not. As seen from the Fig. 2 (a), it is shown that when parameter a in the range (3, 13), system is hyperchaotic. Similarly, the LE changes with parameter b , c and d are shown in Fig. 2 (b), Fig. 2 (c) and Fig. 2 (d) when b, c and d change. It is obvious that there are two positive Lyapunov exponents, the proposed chaotic system is a hyperchaotic system.

To test the randomness of the bit sequence, NIST SP800-22 tests is conducted. In the NIST SP800-22, 15 test methods are given. Each test evaluates one or a set of p-values. If every p-value is greater than or equal to 0.01, then it is shown that the chaotic system has randomness. Specific test values are shown in the table:

Table 1 NIST Test Suite Results of 4-D hyperchaotic system

NIST Statistical Tests	P-Value of (x)	P-Value of (y)	P-Value of (z)	P-Value of (w)	Result
The Frequency (Monobit) Test	0.19498	0.66284	0.92511	0.03771	Pass
Frequency Test within a Block	0.93703	0.73329	0.74338	0.13624	Pass
The Runs Test	0.30978	0.96346	0.21203	0.78126	Pass
Test for the Longest-Run-of-Ones in a Block	0.74989	0.48294	0.67172	0.68721	Pass
The Binary Matrix Rank Test	0.03247	0.01577	0.44117	0.01414	Pass
The Discrete Fourier Transform (Spectral) Test	0.93063	0.93063	0.41649	0.50449	Pass
The Non-overlapping Template Matching Test	0.37222	0.55613	0.94155	0.65460	Pass
The overlapping Template Matching Test	0.20390	0.57517	0.07149	0.81598	Pass
Maurer's "Universal Statistical" Test	0.69569	0.96674	0.94620	0.71093	Pass
The Linear Complexity Test	0.20077	0.75245	0.50350	0.51942	Pass
The Serial Test-1	0.02199	0.25521	0.35433	0.05141	Pass
The Serial Test-2	0.04886	0.08443	0.53013	0.73234	Pass
The Approximate Entropy Test	0.91793	0.16072	0.21158	0.37036	Pass
The Cumulative Sums (Cusums) Test-Forward	0.99962	0.36690	0.95376	1.00000	Pass
The Cumulative Sums (Cusums) Test-Reverse	1.00000	0.55789	0.88983	0.94312	Pass
The Random Excursions Test	0.07703	0.04735	0.48465	0.09880	Pass
The Random Excursions Variant Test	0.02747	0.06885	0.12066	0.04482	Pass

2. 2 DNA encoding

A DNA sequence includes four nucleic acid bases (adenine (A), thymine (T), cytosine (C), guanine (G)). C and G are complementary and T and A are complementary. Because 0 and 1 are complementary in the binary, 00 and 11 are complementary. Thus, 01 and 10 are also complementary. There are 8 coding schemes. As shown in Table 2.

Table 2 DNA encoding rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

This paper uses DNA encoding to encrypt medical image. Firstly, the medical images are converted to 8-bit grayscale images. Each pixel can be represented as a DNA sequence. A DNA

sequence contains four nucleic acid bases. For example, if the first pixel value of a grayscale image is 173, then it is converted to a binary sequence (10101101). Using the DNA encoding rule 1, we can obtain the DNA sequence CCTG. Similarly, using DNA encoding rule 1 to decode the same DNA sequence, we can obtain a binary sequence 10101101. If we use DNA encoding rule 2 to decode the same DNA sequence, we will get a wrong binary sequence 01011110.

Table 3 shows the encoding rules of the DNA^{+} operation. The base in the first row is added to the base in the first column, and the result is intersection of their row and column.

Table 3 The DNA^{+} operation

+	A	C	T	G
A	T	G	A	C
T	A	C	T	G
C	G	T	C	A
G	C	A	G	T

Table 4 shows the encoding rules of the DNA^{-} operation. The base in the first row is subtracted from the base in the first column, and result is intersection of their row and column.

Table 4 The DNA^{-} operation

-	A	C	T	G
A	T	G	A	C
T	A	C	T	G
C	G	T	C	A
G	C	A	G	T

In this work, DNA^{+} and DNA^{-} operations are used to merge the key with the plain image. For example, consider two different DNA sequences, CTAG and ACGT, and the DNA^{+} operation result is GCCG.

3. Image encryption and decryption schemes

3. 1 Initial key generation

The medical image cryptography system based on fast and robust fuzzy C-means clustering (FRFCM) [22], DNA encoding and 4-D hyperchaotic system. It includes four stages: initial values generation of chaotic system, key streams generation, scrambling and diffusing. The initial keys generation steps of chaotic system are as follows:

Step 1: The parameters of the chaotic system are used as a fixed password, and the plaintext information (*PI*) of 64-bit sequence value is composed of the doctor-patient information and the

device information in the medical image. Plaintext information as the input value for *SHA256*, as shown in Equation (2) and (3):

$$pi = uint8\left(mod\left(abs\left(PI\right),256\right)\right) \tag{2}$$

$$K\left(k_1,k_2,k_3\mathrm{L}\ k_{64}\right) = SHA256(pi) \tag{3}$$

Step 2: After converting *K* into a decimal sequence, add each of the adjacent bits from left to right. Lead to get a 32-bit decimal sequence *KK* ($kk_1,kk_2,kk_3\mathrm{L}\ kk_{32}$) as shown in Equation (4):

$$KK\left(kk_1,kk_2\mathrm{L}\ kk_{32}\right) = K\left(kk_1 = k_1 + k_2, kk_2 = k_3 + k_4\mathrm{L}\ kk_{32} = k_{63} + k_{64}\right) \tag{4}$$

Step 3: After kk_1 and kk_{32} are discarded, the XOR and modulo operation are performed from left to right every six adjacent bits. And we get a five-digit decimal sequence *KX* （ kx_1,kx_2,kx_3,kx_4,kx_5 ）, as shown in Equation (5):

$$\begin{cases} KX\left(kx_1,kx_2\mathrm{L}\ kx_4\right) = \mathrm{mod}\left(KK\left(kk_2 \oplus kk_3\mathrm{L}\ kk_{7,}\mathrm{L}\ kk_{26} \oplus kk_{27}\mathrm{L}\ kk_{31}\right),256\right) \\ KX\left(kx_5\right) = \mathrm{mod}\left(KK\left(kk_{26} \oplus kk_{27}\mathrm{L}\ kk_{31}\right),8\right)+1 \end{cases} \tag{5}$$

3. 2 Encryption and decryption schemes

After the initial values of chaotic sequences are generated, the steps of chaotic sequences generation, image segmentation, scrambling and diffusion are carried out. Fig.3 shows the medical image encryption process.

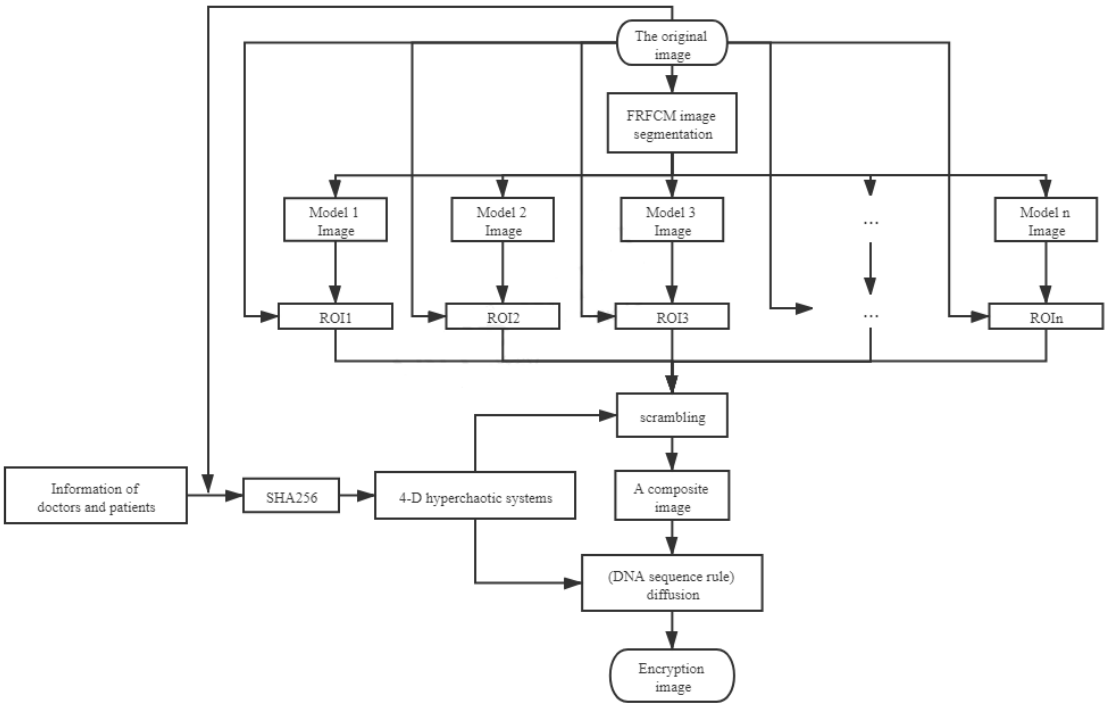


Fig.3 Encryption flow chart

Step 1: The original medical image is segmented by FRFCM algorithm [22], different segmentation regions are extracted from the segmented image (model 1, model 2, …, model n). Moreover, segmentation regions multiplied by the original image to obtain regions of interest (ROI). ROI can be further divided into ROI 1, ROI 2, ..., ROI n. The n is odd. The ROI 1 with the smallest pixel value is discarded. The non-zero pixels in the remaining ROI were obtained respectively. And getting the pixel sequences $tq_1, tq_2, \ldots, tq_{n-1}$. The lengths of these sequences are $l_1, l_2, \ldots, l_{n-1}$ respectively.

Step 2: Initial values（kx_1, kx_2, kx_3, kx_4） of the chaotic system generates four chaotic sequences (s_1, s_2, s_3, s_4) of length L ($L = l_1 + l_2 + \ldots l_{n-1}$). s_1 and s_2 are used to scramble tq_a and tq_b respectively. s_3 and s_4 are used during diffusion. $a = 1, 2, ..., \frac{n-1}{2}$, $b = \frac{n+1}{2}, ..., n+1$.

Step 3: Divide s_1 into α_c , divide s_2 into α_d and process it according to the following Equation (6) ($c = 1, 2, ..., \frac{n-1}{2}$, $d = \frac{n+1}{2}, ..., n+1$):

$$\beta_i = mod\left(floor\left(\left(\alpha_i + 100 \right) \times 10^{10} \right), l_i \right) + 1, \tag{6}$$

where *i*=1, 2, …, n-1. β_i is used for scrambling tq_i . The scrambling formulas are as $swap(tq_i(j), tq_i(\alpha_i(j)))$, where $j = 1, 2, \ldots, l_i$. After scrambling process, Sequence W is obtained by joining subsequences in turn.

Step 4: After the scrambling operation, the sequence W is encoding by DNA as following Equation (7):

$$C_1 = DNAencode\left(W, kx_5 \right), \tag{7}$$

where kx_5 is DNA encoding rule. C_1 is a DNA sequence containing the information of W . For chaotic sequences s_3 and s_4 , S_1 and S_2 are obtained according to the above encoding method. *DNAencode* is calculated with reference to Table 2. Diffusion of C_1 is carried out according to the following Equation (8):

$$\begin{cases} E_1(1) = DNA^+(S_1(1), C_1(1), 'A') \\ E_1(i) = \left(E_1(i-1) + C_1(i) + S_1(i)\right) \end{cases}, \tag{8}$$

where $i = 2, 3, \ldots, 4L$. E_1 is the diffused sequence. DNA^+ is calculated with reference to Table 3. Diffusion of C_2 is carried out according to the following Equation (9):

$$\begin{cases} E_2(4L) = DNA^+(S_2(4L), E_1(4L), 'A') \\ E_2(i) = \left(E_2(i+1) + E_1(i) + S_2(i)\right) \end{cases}, \tag{9}$$

where $i = 4L\text{-}1, \ldots, 2, 1$. E_2 is the diffused sequence. Sequence E_2 is performed according to the following Equation (10):

$$E_3 = DNAdecode\left(E_2(i), 4L, kx_5\right), \tag{10}$$

where E_3 is the final decoded sequence. $DNAdecode$ is calculated with reference to Table 2.

Step 5: After converting E_3 into a decimal sequence, E_3 are placed in the encrypted images. The remaining pixels are supplemented with 0 value to get the encrypted image.

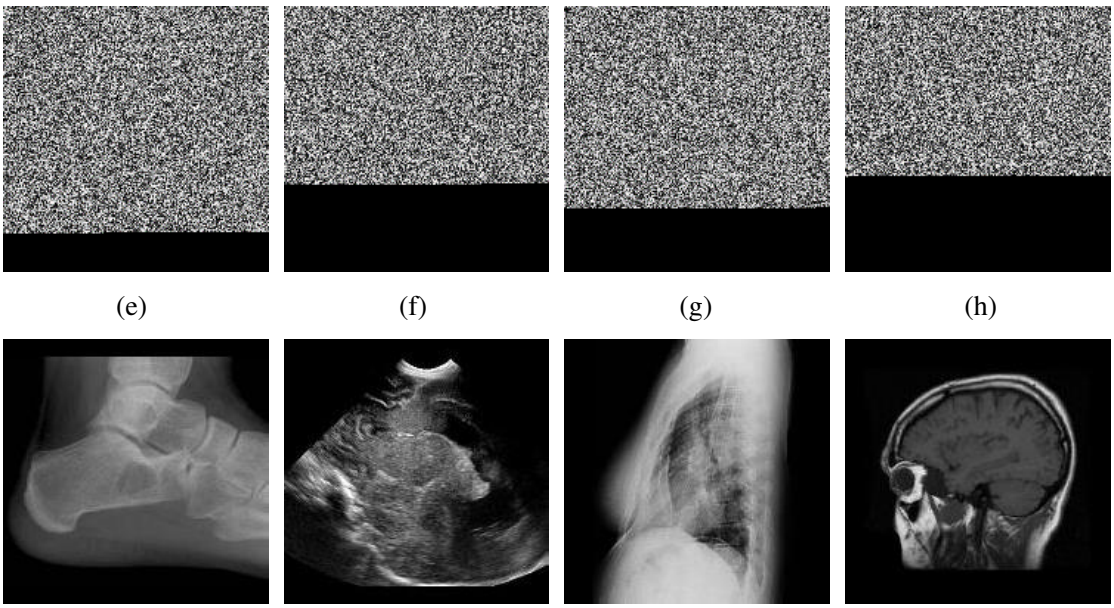
Decryption operation will be carried out in reverse, and the decrypted images will be obtained by putting the decrypted pixels back to the plain index position.

4. Experiments for Simulation

4. 1 Results of encryption

All the experiments are performed in MATLAB R2018b to compute the encryption and decryption method in computer with Intel(R) Core (TM) i5-6500 CPU @ 3.20 GHz, 8GB RAM. To validate the encryption method, some medical images are chosen from MedPix and named as sample_1, sample_2, sample_3, sample_4. Fig.4 shows the sample images, the lossless encrypted images, and the decrypted images.

(a) (b) (c) (d)

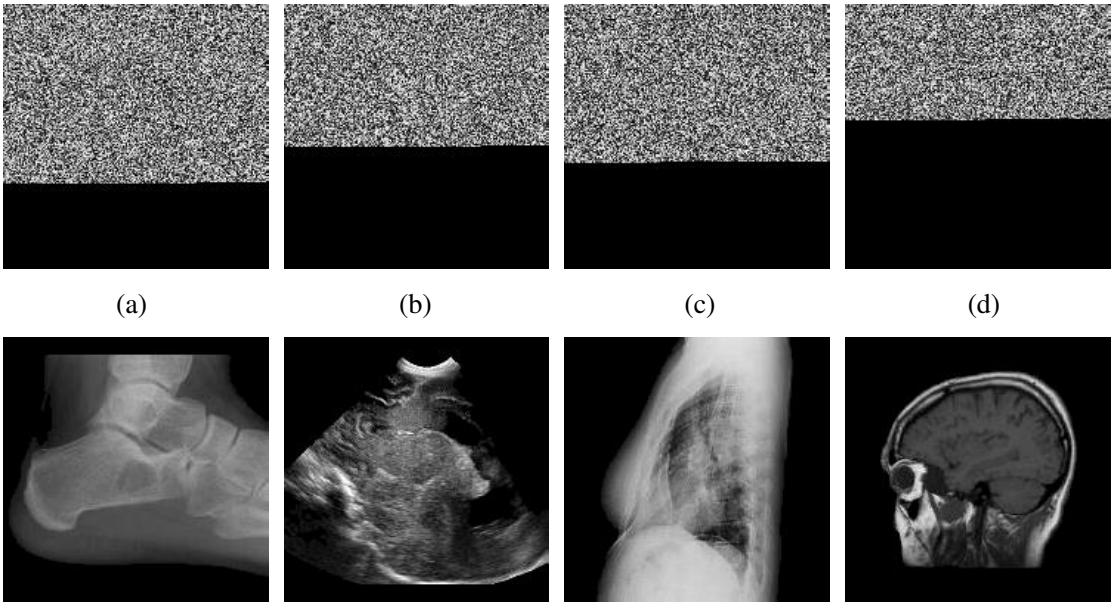


(e) (f) (g) (h)

(i) (j) (k) (l)

Fig.4 Lossless encryption results: (a) sample_1 image, (b) sample_2 image, (c) sample_3 image, (d) sample_4 image; (e) sample_1 encrypted image, (f) sample_2 encrypted image, (g) sample_3 encrypted image, (h) sample_4 encrypted image; (i) sample_1 decrypted image, (j) sample_2 decrypted image, (k) sample_3 decrypted image, (l) sample_4 decrypted image

The lossless encryption is a method of encrypting all pixels except 0-value pixels. Thus, lossless encryption time is long. In order to overcome this problem, a fast encryption technology is proposed. Fig.5 shows the fast encrypted images and the decrypted images.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig.5 Fast encryption results: (a) sample_1 encrypted image, (b) sample_2 encrypted image, (c) sample_3 encrypted image, (d) sample_4 encrypted image; (e) sample_1 decrypted image, (f) sample_2 decrypted image, (g) sample_3 decrypted image, (h) sample_4 decrypted image

From Fig.5, the fast encryption has fewer encrypted pixels than lossless encryption, so the black area occupies half of the image. The encryption time is shorter and decrypted image doesn't affect the diagnosis.

4. 2 Histogram analysis

Histogram represents the distribution of pixel values. The variance of histogram is used to quantitatively evaluate the uniformity of the image. It is worth noting that the smaller the variance value of the encrypted image is, the higher the randomness is. Variance is measured using following Equation (11):

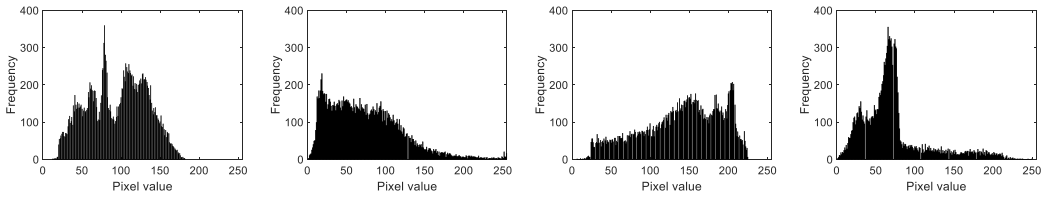
$$Variance = \frac{1}{256}\sum_{i=0}^{255}\sum_{j=0}^{255}\frac{1}{2}\times\left(v_i - v_j\right)^2, \tag{11}$$

where v_i and v_j are the number of pixels, i is gray value of plain image and j is gray value of encrypted image. Variances of plain and encrypted images are presented in Table 5.

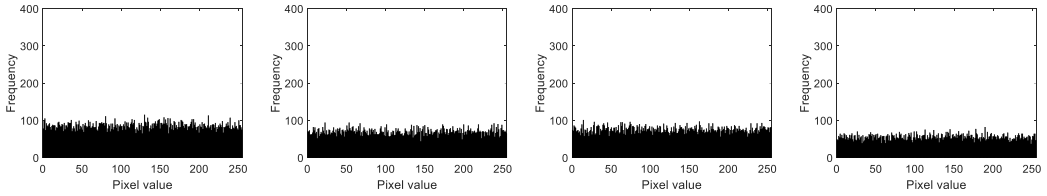
Table 5 Variance of histogram results

Image	Variance	
	Plain image	Encrypted image
sample_1	4.6×10^3	285.04
sample_2	1.5×10^3	251.20
sample_3	1.4×10^3	250.24
sample_4	8.2×10^3	257.92

Obviously, encrypted images have lower variances. Variances of encrypted images are less than the theoretical value 293.24, and it means that the frequency distribution of encrypted pixels is approximately uniform. Histograms of plain and encrypted images are shown in Fig.6.



(a) (b) (c) (d)



(e) (f) (g) (h)

Fig.6 Histogram of plain and encrypted images: (a) histogram of sample_1 image, (b) histogram of sample_2 image, (c) histogram of sample_3 image, (d) histogram of sample_4 image;(e) histogram of sample_1 encrypted image, (f) histogram of sample_2 encrypted image, (g) histogram of sample_3 encrypted image, (h) histogram of sample_4 encrypted image

From Fig.6, there is no similarity between the histograms of plain and encrypted images. Histograms of plain images have many peak-valleys, and these features will leak image information. Histogram of encrypted images is flat. It can resist statistical analysis attacks.

4. 3 Correlation analysis

A good cryptographic system considers that there is a low correlation between adjacent pixels of the encrypted image. The correlation coefficient (*Corr*) of two adjacent pixels can be obtained by the following Equation (12):

$$\begin{cases} Corr\left(x_1, x_2\right) = \dfrac{Cov\left(x_1, x_2\right)}{\sqrt{D\left(x_1\right)} \times \sqrt{D\left(x_2\right)}} \\ Cov\left(x_1, x_2\right) = \dfrac{1}{n} \times \sum_{i=1}^{n} \left(x_i - E\left(x_1\right)\right)\left(x_i - E\left(x_2\right)\right) \\ D\left(x_1\right) = \dfrac{1}{n} \times \left(x_i - E\left(x_1\right)\right)^2 \\ E\left(x_1\right) = \dfrac{1}{n} \times \sum_{i=1}^{n} x_i \end{cases}, \tag{12}$$

where x_1 and x_2 represent the two neighboring pixel values, n is the number of pixels, $E\left(x_1\right)$ and $D\left(x_1\right)$ represent the expectation and variance. The correlation coefficient results of the plain image and the encrypted image are shown in Table 6.

Table 6 Results of correlation coefficients of the plain and encrypted images

Image	Plain image				Encrypted image			
	horizontal	vertical	positive diagonal	negative diagonal	horizontal	vertical	positive diagonal	negative diagonal
sample_1	0.9617	0.9239	0.9147	0.8934	0.0241	-0.0365	0.0345	-0.0358

sample_2	0.8496	0.7137	0.6914	0.6705	0.0154	-0.0311	-0.0207	-0.0270
sample_3	0.9218	0.9482	0.8646	0.9251	0.0045	0.0438	0.0337	0.0055
sample_4	0.8419	0.7496	0.6939	0.6793	-0.0054	-0.0212	-0.0797	-0.0152

The correlation coefficients of the plain images are close to 1 in all directions. It shows that the plain images have a strong correlation. However, the correlation coefficients of the encrypted images are close to 0 in all directions. The correlations of the encrypted images are broken. The sample_3 correlation scatter plots of horizontal, vertical, and diagonal directions are illustrated in Fig.7.

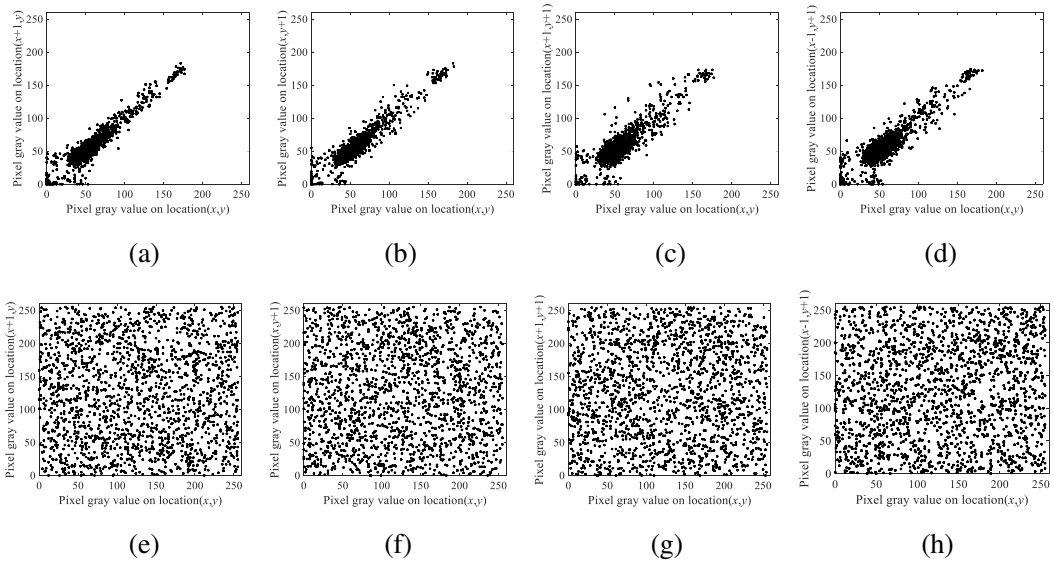


Fig.7 Correlation plot: (a) the correlation scatter plots of horizontal; (b)the correlation scatter plots of vertical; (c) the correlation scatter plots of positive diagonal; (d) the correlation scatter plots of negative diagonal; (e) the encrypted correlation scatter plots of horizontal; (f) the encrypted correlation scatter plots of vertical; (g) the encrypted correlation scatter plots of positive diagonal; (h) the encrypted correlation scatter plots of negative diagonal

From Fig.7, the pixels of plain images have a strong correlation, and they are distributed near the diagonal. The pixels of encrypted images can be fully distributed evenly. Thus, this method can successfully resist the statistical attacks.

4. 4 Information entropy

Information entropy is an indicator for evaluating the randomness and unpredictability of information. Information entropy defined as following Equation (13):

$$H(x) = -\sum_{i=0}^{N} p(x_i) \log_2 p(x_i), \tag{13}$$

where $p(x_i)$ is the probability of appearance of symbol x_i, and N is the total number of x_i. The entropy values of plain images and encrypted images are shown in Table 7.

Table 7 Information entropy results

Image	Information entropy	
	Plain image	Encrypted image
sample_1	7.10412	7.99167
sample_2	7.35563	7.98883
sample_3	7.51807	7.99060
sample_4	6.94793	7.98813

As apparent in Table 7, the entropies of the plain images are less than 7.6. However, the entropies of the encrypted images are close to theoretical value 8. Therefore, the encrypted image has a high randomness. It is difficult for the attacker to obtain valid information from the encrypted images.

4. 5 Differential attack

The slight change of pixel value of plain images can affect the encrypted image. Thus, the encrypted images may be hacked by the differential attack. The performance of the encryption scheme for resisting differential attack can be evaluated by the number of pixel change rate (*NPCR*) and the unified average changing intensity (*UACI*) values. Two indicators are measured as following Equation (14), (15) and (16):

$$NPCR = \left(\frac{\sum_{i=1}^{w} \sum_{j=1}^{h} D(i,j)}{w \times h} \right) \times 100\% , \tag{14}$$

$$UACI = \left[\frac{\sum_{i=1}^{w} \sum_{j=1}^{h} \left| C_1(i,j) - C_2(i,j) \right|}{\left(2^8 - 1\right) \times w \times h} \right] \times 100\% , \tag{15}$$

$$D(i,j) = \begin{cases} 0 & \text{when } C_1(i,j) = C_2(i,j) \\ 1 & \text{when } C_1(i,j) \neq C_2(i,j) \end{cases}, \tag{16}$$

where C_1 is the first encrypted image and C_2 is the second encrypted image, w and h are the width and height of C. Here, 2^8 represents the number of gray levels. The results of *NPCR* and *UACI* values are shown in Table 8.

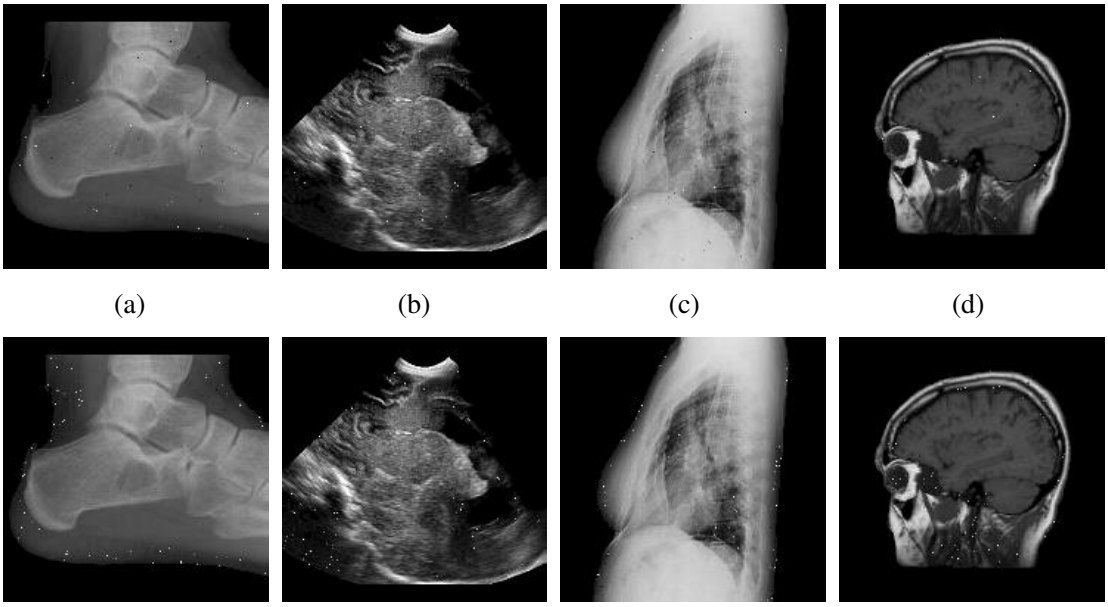
Table 8 *NPCR* and *UACI* results

Encrypted image	NPCR(%)	UACI(%)
sample_1	99.6424	33.8123
sample_2	99.5892	33.1487
sample_3	99.5489	33.1348
sample_4	99.6647	33.4478

From Table 8, the *NPCR* and *UACI* results of encrypted images are close to the theoretical value 99.6094% ($NPCR$) and 33.4635% ($UACI$), respectively. Apparently, the method has a high plaintext sensitivity, and it can resist differential attack.

4. 6 Salt and pepper noise attack and clipping attack

When the encryption image is transmitted in the public channel, we must pay attention to the transmission security. During transmission, the image may be subject to various attacks, resulting in the change and loss of the image data. There are two kinds of attacks commonly used, salt and pepper noise attack (SPNA) and clipping attack (CA). To evaluate the robustness of the encryption method, two different types of attacks are added to the encrypted images, as shown in Fig.8.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig.8 SPNA and CA results: (a) sample_1 decrypted images with SPNA intensity of 0.001, (b) sample_2 decrypted images with SPNA intensity of 0.001, (c) sample_3 decrypted images with SPNA intensity of 0.001, (d) sample_4 decrypted images with SPNA intensity of 0.001; (e) sample_1 decrypted images with CA (image of 0.25%), (f) sample_2 decrypted images with CA (image of 0.25%), (g) sample_3 decrypted images with CA (image of 0.25%), (h) sample_4 decrypted images with CA (image of 0.25%)

Under different types of attacks, the decrypted image is understandable and the decrypted image doesn't affect the diagnosis. Thus, the method has strong robustness against SPNA and CA attacks.

The quality of the decrypted image is judged by the peak signal-to-noise ratio (*PSNR*), mean square error (*MSE*) and structural similarity index (*SSIM*), which are expressed as:

$$PSNR = 1 - \log_{10}\left[w \times h\right]\frac{1}{MSE}, \tag{17}$$

$$MSE = \frac{1}{w \times h}\sum_{i=0}^{w-1}\sum_{j=0}^{h-1}\left[P_{i,j} - C_{i,j}\right]^2, \tag{18}$$

$$SSIM = \frac{\left(2\mu_P\mu_C + l_1\right)\left(2\sigma_{PC} + l_2\right)}{\left(\mu_P^2 + \mu_C^2 + l_1\right)\left(\mu_P^2 + \mu_C^2 + l_2\right)}, \tag{19}$$

where, $P_{i,j}$ is plain image pixel, $C_{i,j}$ is encrypted image pixel. μ_P and μ_C are the averages of the images *P* and *C*, respectively. σ_P and σ_C denote the variance of *P* and *C*, respectively; σ_{PC} is the covariance between *P* and *C*. l_1 and l_2 are constants. Information is attacked in transit. Table 9 show the *PSNR* and *SSIM* results of decrypted images under SPNA.

Table 9 Quality of the decrypted images after noise attacks

Attack	Image	PSNR-Fast	SSIM-Fast	PSNR-Lossless	SSIM-Lossless
SPNA(0.001)	sample_1	48.50869	0.76225	50.64033	0.94853
	sample_2	30.94532	0.80442	39.93503	0.97703
SPNA(0.005)	sample_1	34.55569	0.75507	40.87441	0.78464
	sample_2	28.67611	0.77412	37.98685	0.91548
SPNA(0.01)	sample_1	22.22182	0.51199	22.55145	0.59131
	sample_2	24.99447	0.68535	33.24152	0.79885

From Table 9, it can be seen that the *PSNR* and *SSIM* decrease when the density of SPNA increases. After decryption, the quality of the image is reduced, but the content of the image can still be clearly recognized. Moreover, the *PSNR* and *SSIM* of the lossless encryption are better than the fast encryption, because the fast encryption discards some low-value pixels. Furthermore, information is lost in transmission. CA is equal to information loss. Table 10 show the *PSNR* and *SSIM* results of decrypted images under CA.

Table 10 Quality of the decrypted images after clipping attacks

Attack （Percentage of total pixels）	Image	PSNR-Fast	SSIM-Fast	PSNR-Lossless	SSIM-Lossless
CA (0.25%)	sample_1	22.26780	0.73531	25.85807	0.87882
	sample_2	30.62287	0.77118	37.07617	0.91611
CA (1.5625%)	sample_1	14.17790	0.64625	17.54901	0.76738
	sample_2	28.60503	0.68973	30.89828	0.77836
CA (6.25%)	sample_1	11.10932	0.45444	12.71368	0.63163
	sample_2	16.27516	0.55619	19.48266	0.62211

From Table 10, it is obvious that the *PSNR* and *SSIM* also decrease when the density of CA increases. Moreover, the *PSNR* and *SSIM* of the lossless encryption are also better than the fast encryption. *SSIM* of the lossless encryption is close to the theoretical value 1. The lossless encryption can encrypt all feature pixels. Thus, the lossless encryption is more secure than the fast encryption.

4. 7 Performance comparison

Table 11 shows the performance comparison of the proposed encryption method with some of the existing encryption methods.

Table 11 Performance comparison

Methods	Correlation			Entropy	NPCR(%)	UACI(%)	Time(s)
	Horizontal	Vertical	Diagonal				
[6]	-0.0177	-0.0668	0.0335	7.9972	99.61	33.24	-
[23]	0.0027	-0.0026	0.0042	7.9891	99.63	33.44	-
[24]	-0.0015	0.0011	0.0032	7.8231	99.61	33.15	-
[25]	0.0036	-0.0075	0.0021	7.9992	99.61	33.42	-
[26]	0.0031	-0.0039	0.0073	7.9994	99.61	33.99	-
Proposed-Fast	-0.0391	0.0009	0.0018	7.9916	99.64	33.81	1.63
Proposed- Lossless	-0.0126	-0.0019	0.0176	7.9921	99.61	33.16	2.36

From Table 11, the proposed encryption method is better than the existing encryption methods, and the indices of the proposed method are all closer to the theoretical value. Because of some low-value pixels were discarded in the fast encryption, some unimportant information is lost. Moreover, the fast encryption is faster than the lossless encryption and some time and computing resources are saved. The corresponding encryption method can be selected according to different requirements.

5. Conclusion

In this paper, the medical image encryption method based on hyperchaos and DNA encoding is proposed. It has several advantages as follows. First, ROI images can be extracted and some

important pixels can be encrypted. It can reduce the number of encryption pixels, so that the encryption time is also reduced. Secondly, hyperchaotic sequences are used to reduce the pixel correlation. Thirdly, due to the usage of DNA encoding, computing storage resources can be saved. The sequences of pixel values and chaotic sequences can be encoding and decoding at the same time. Finally, the results of the security analysis and experiments show that the proposed encryption method can resist various attacks, such as noise attacks, clipping attacks and statistical analysis. Compared with the traditional encryption methods, the proposed medical image encryption method has achieved better results in all the tests.

Acknowledgement: This research is supported by the National Natural Science Foundation of China (Nos: 61702356, 61672124 and 61503375), National Natural Science Foundation of ShanXi Province (Nos: 201801D121143).

References

[1] C. Pak, L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Processing, 138 (2017) 129-137.

[2] R. Parvaz, M. Zarebnia, A combination chaotic system and application in color image encryption, Optics & Laser Technology, 101 (2018) 30-41.

[3] X. Wang, L. Liu, Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, Optics and Lasers in Engineering, 66 (2015) 10-18.

[4] M. Gafsi, N. Abbassi, M. A. Hajjaji, J. Malek, A. Mtibaa, Z. Pan, Improved chaos-based cryptosystem for medical image encryption and decryption, Scientific Programming, 2020 (2020) 1-22.

[5] M. A. Hajjaji, M. Dridi, A. Mtibaa, A medical image crypto-compression algorithm based on neural network and PWLCM, Multimedia Tools and Applications, 78 (2019) 14379-14396.

[6] N. Iqbal, M. Hanif, S. Abbas, M.A. Khan, Z. Ul Rehman, Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding, Journal of Information Security and Applications, 58 (2021) 102809.

[7] L. M. Adleman, Molecular computation of solutions to combinatorial problems, Science, 266 (1994) 1021–1024.

[8] X. Chai, Z. Gan, K. Yuan, Y. Chen, X. Liu, A novel image encryption scheme based on DNA sequence operations and chaotic systems, Neural Computing and Applications, 31 (2017) 219-237.

[9] X. Li, B. Wang, H. Lv, Q. Yin, Q. Zhang, X. P. Wei, Constraining DNA sequences with a triplet-bases unpaired, IEEE Transactions on Nanobioscience, 19 (2020) 299-307.

[10] X. Chai, Y. Chen, L. Broyde, A novel chaos-based image encryption algorithm using DNA sequence operations, Optics and Lasers in Engineering, 88 (2017) 197-213.

[11] R. Guesmi, M. A. B. Farah, A. Kachouri, M. Samet, A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2, Nonlinear Dynamics, 83 (2015) 1123-1136.

[12] M. Kumar, A. Iqbal, P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Processing, 125 (2016) 187-202.

[13] W. Shafai, F. Khallaf, E. S. M. Rabaie, F. E. A. Samie, Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications, Journal of Ambient Intelligence and Humanized Computing, (2021) doi: 10.1007/s12652-020-02597-5.

[14] V. R. Folifack Signing, T. Fozin Fonzin, M. Kountchou, J. Kengne, Z. T. Njitacke, Chaotic Jerk system with hump structure for text and image encryption using DNA coding, Circuits Systems and Signal Processing, (2021) doi: 10.1007/s00034-021-01665-1.

[15] X. Wu, H. Kan, J. Kurths, A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, Applied Soft Computing, 37 (2015) 24-39.

[16] X. Wang, L. Feng, H. Zhao, Fast image encryption algorithm based on parallel computing system, Information Sciences, 486 (2019) 340-358.

[17] X. Y. Wang, Y. Q. Zhang, X. M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Optics and Lasers in Engineering, 73 (2015) 53-61.

[18] S. Jeevitha, N. Amutha Prabha, Novel medical image encryption using DWT block-based scrambling and edge maps, Journal of Ambient Intelligence and Humanized Computing, 12 (2020) 3373-3388.

[19] S. Deb, B. Bhuyan, Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR, Multimedia Tools and Applications, 80 (2021) 19803-19826.

[20] O. A. Khashan, M. AlShaikh, Edge-based lightweight selective encryption scheme for digital medical images, Multimedia Tools and Applications, 79 (2020) 26369-26388.

[21] Y. J. Xian, K. R. Fu, C. B. Xu, A 4-D multi-stable hyper-chaotic system multi-wing attractors,1 (2021) 15-22.

[22] T. Lei, X. Jia, Y. Zhang, L. He, H. Meng, A. K. Nandi, Significantly fast and robust fuzzy c-means clustering algorithm based on morphological reconstruction and membership filtering, IEEE Transactions on Fuzzy Systems, 26 (2018) 3027-3041.

[23] H. Liu, A. Kadir, Y. Li, Asymmetric color pathological image encryption scheme based on complex hyper chaotic system, Optik, 127 (2016) 5812-5819.

[24] Y. Dai, H. Wang, Y. Wang, Chaotic medical image encryption algorithm based on bit-plane decomposition, 30 (2016) 1657001.

[25] X. Xue, H. Jin, D. Zhou, C. Zhou, Medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length, Front Genet, 12 (2021) 654663.

[26] S. Deb, B. Biswas, B. Bhuyan, Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field, Multimedia Tools and Applications, 78 (2019) 34901-34925.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- BIBChecklist.docx
- BIBAuthorDeclarationForm.docx