Novel medical image cryptogram technology based on segmentation and DNA encoding

Hong-wei Xie¹ · Yu-zhou Zhang¹ · Hao Zhang² · Zhen-yu Li²

Received: 9 August 2021 / Revised: 22 April 2022 / Accepted: 31 January 2023 / Published online: 17 February 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
This paper proposes a novel medical image cryptogram technology based on a fast and robust fuzzy C-means clustering image segmentation method and deoxyribonucleic acid encoding. In our method, first, the medical image is divided into background areas and regions of interest utilizing fuzzy C-means clustering image segmentation, which increases the encryption efficiency by about 60% when the background area is discarded. Second, some low-value pixels are also discarded in regions of interest to further reduce the encryption time. Third, a 4-dimensional hyperchaotic system has been improved. Furthermore, the hyperchaotic system and deoxyribonucleic acid encoding are utilized to encrypt the medical image. Finally, lossless encryption and fast encryption are done for different purposes. The experimental results demonstrate that the proposed algorithm has appealing encryption performance and the histogram and scatter graphs are governed by approximately uniform distribution. The NPCR and UACI of plaintext sensitivity and the key sensitivity are close to 99.6094% and 33.4635% respectively, which cause robustness against noise and clipping attacks.

Keywords 4-D hyperchaotic system · Image segmentation · Regions of interest (ROI) · Deoxyribonucleic acid (DNA) encoding · Medical image encryption

1 Introduction

With the development of communication technology and mobile Internet, people are used to transmitting and sharing information on the Internet. Digital image, as the important data carrier, is widely used in enterprises, personal information, medical and military fields. How to ensure the safe transmission of information and prevent hackers from stealing are serious and
urgent challenges [25]. Medical imagery, as the important basis for diagnosis, contains a lot of important personal information about patients. Medical images (MRI, CT, X-rays) with large data storage, redundancy, and high pixel correlation are easily tampered with 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. In recent years, many scholars have proposed some concepts based on semi-tensor product theory [21], fractal sorting matrix [30], and chaos theory [23, 26], which are widely used in image encryption. Wang et al. proposed an image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network [22]. Xian et al. proposed a fractal sorting matrix and its application to chaotic image encryption [29].

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 [17, 18, 24]. In the past few decades, many classical chaotic systems have been proposed for the encryption of medical images, such as the Chen system, Tent map and Logistic map [7, 9]. With the deepening research on chaotic systems, many new multidimensional chaotic systems have been applied to medical images encryption. For example, Iqbal proposed an RGB (color image) encryption algorithm based on a dynamic three-dimensional scrambled image (D3DSI), 5D multi-wing hyperchaotic system and deoxyribonucleic acid (DNA) calculation [10].

Since the groundbreaking work on DNA computing was conducted and reported by Adleman [1]. DNA computing has attracted the attention of researchers worldwide, due to its superior characteristics of large concurrency, mass storage and low energy consumption [3]. DNA coding theory was used in the field of image information security by Zhang et al. [15]. Meanwhile, the DNA-based encryption method has caught attention because of its excellent performance on confusion and diffusion [2, 8, 13]. Piecewise linear chaotic map (PWLCM) was used to generate the key image, and DNA rules were used to encode the key image by E-SM et al. [19]. Folifack proposed a cryptosystem based on a chaotic Jerk system and DNA encoding proposed in the article for image encryption [6]. The combination of DNA and chaos has aroused interest among scholars in image encryption [20, 27, 28].

Recently, some medical image encryption algorithms have been proposed. Jeevitha proposed the discrete wavelet transform (DWT) block-based scrambling and the edge maps for medical image encryption [11]. A new medical image encryption system was proposed by using a linear feedback shift register (LFSR) based on a special nonlinear filter function [5]. White and gray areas in the medical image reflect the features of the 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 have taken this feature into account. Khashan et al. presented a lightweight selective encryption scheme to encrypt the edge maps of medical images [12]. 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. 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 the lowest values in the region of interest (ROI) can reduce the number of the encrypted pixels. (2) Using doctor-patient information and medical image information as input values of SHA256 can enhance plaintext correlation. (3) The 4-D hyperchaotic system and DNA encoding is used to encrypt the selected pixels.
The remainder of the paper is as follows: Section 2 provides a detailed description of the proposed scheme’s preliminaries. Section 3 introduces the encryption and decryption schemes. Section 4 presents the experimental results. Section 5 introduces the performance and security analysis while Section 6 provides challenges our method against current techniques. Finally, Section 7 concludes this work.

2 Hyperchaotic system and DNA encoding

2.1 Hyperchaotic systems model and performance analysis

This paper improves a 4-D hyperchaotic system [31]. The multiple-wing hyperchaotic system reflects the difference in 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 Eq. (1):

\[
\begin{align*}
\dot{x} &= -ax + yz \\
\dot{y} &= xz - y^3 + w \\
\dot{z} &= -bxy + cz + w \\
\dot{w} &= y - dz
\end{align*}
\]

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
where \( a, b, c, \) and \( d > 0 \), and in this work, we set their values to 5, 6.5, 7 and 4, respectively. When \( x_1 = 2, y_1 = 8, z_1 = 4.5, \) and \( w_1 = 6, \) the system has a typical four-winged hyperchaotic attractor. The system’s attractor is illustrated in Fig. 1.

The Lyapunov exponent is an evaluation indicator of whether a system is chaotic or not. When \( b = 6.5, c = 7, d = 4 \) and \( x_1 = 2, y_1 = 8, z_1 = 4.5, w_1 = 6, \) the Lyapunov exponent (LE) changes with parameter \( a, \) as shown in Fig. 2 (a).

According to Fig. 2 (a), when \( a \in (3, 13), \) the system is in a hyperchaotic state. Similarly, the change of LE with parameters \( b, c \) and \( d \) are illustrated in Fig. 2 (b), Fig. 2 (c) and Fig. 2 (d), revealing two positive Lyapunov exponents, and the proposed system is hyperchaotic.

The NIST SP800-22 test can detect the randomness of chaotic sequences with 15 test methods. Each test produces one or a set of P Values and if each P Value is greater than or equal to 0.01, the chaotic system has randomness. The system’s test results are reported in Table 1, highlighting that all test data are greater than 0.01. Hence the chaotic sequence has good randomness, and it is suitable for encrypting images.
2.2 DNA encoding

A DNA sequence contains 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, so 01 and 10 are also complementary. There are 8 coding schemes. As shown in Table 2.

This paper uses DNA encoding to encrypt the medical image. First, medical images are converted into 8-bit grayscale images. Each pixel may be depicted as a DNA sequence. For example, if the value of the first pixel of a grayscale image is 173, it is converted to a binary sequence (10101101). By using DNA coding rule 1, we can obtain the CCTG DNA sequence. Similarly, using DNA coding rule 1 to decode the same DNA sequence, we can achieve a 10101101 binary sequence. If we use the DNA coding rule 2 to decode the same DNA sequence, we will get the wrong binary sequence 01011110.

### 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    |

### 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 |

### Table 3 The DNA+ operation

|   | A | T | G | A | C |
|---|---|---|---|---|---|
| A | T | G | A | C |
| T | A | C | T | G |
| C | G | T | C | A |
| G | C | A | G | T |
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 the intersection of their row and column.

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 the result is the intersection of their row and column.

In this work, DNA+ and DNA− operations are used to merge the key with the plain image. For example, taking two different DNA sequences CTAG and ACGT into consideration, the DNA+ operation result is GCCG.

### 3 Image encryption and decryption schemes

#### 3.1 Initial key generation

The medical image cryptography system is based on fast and robust fuzzy C-means clustering (FRFCM) [14], DNA encoding and a 4-D hyperchaotic system. It consists of four stages: initial value generation, keystream generation, scrambling and diffusion. The initial value generation steps of a 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 the 64-bit sequence value is composed of the doctor-patient information and the device information in the medical image. Plain text information as the input value for the SHA256, is shown in Eqs. (2) and (3):

\[
pi = \text{uint8}(\text{mod}(\text{abs}(\text{PI}), 256))
\]  
\[K(k_1, k_2, k_3 \cdots k_{64}) = \text{SHA256}(pi)
\]

**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 \(KK(kk_1, kk_2, kk_3 \cdots kk_{32})\) as shown in Eq. (4):

\[KK(kk_1, kk_2 \cdots kk_{32}) = K(kk_1 = k_1 + k_2, kk_2 = k_3 + k_4 \cdots kk_{32} = k_{63} + k_{64})
\]
Step 3: After $kk_1$ and $kk_{32}$ are discarded, the XOR and modulo operation is 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 Eq. (5):

$$\begin{align*}
KX(kx_1, kx_2 \cdots kx_4) &= \text{mod}(KK(kk_2 \oplus kk_3 \cdots kk_{26} \oplus kk_{27} \cdots kk_{31}), 256) \\
KX(kx_5) &= \text{mod}(KK(kk_{26} \oplus kk_{27} \cdots kk_{31}), 8) + 1
\end{align*}$$

(5)

### 3.2 Encryption and decryption schemes

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

Step 1: The original medical image is segmented by the FRFCM algorithm [28], and different segmentation regions are extracted from the segmented image (model 1, model 2, ..., model n). Moreover, segmentation regions are multiplied by the

![Encryption flow chart](image-url)
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 we obtain the pixel sequences \((t_{q_1}, t_{q_2}, ..., t_{q_n-1})\). \(t_{q_1}, t_{q_2}, ..., t_{q_n-1}\) have a length of \(l_1, l_2, ..., l_n - 1\), respectively.

Step 2: Initial values \((k_{x_1}, k_{x_2}, k_{x_3}, k_{x_4})\) of the chaotic system generate four chaotic sequences \((s_1, s_2, s_3, s_4)\) of length \(L\) \((L = l_1 + l_2 + ... + l_n - 1)\). \(s_1\) and \(s_2\) are used to scramble \(t_{qa}\) and \(t_{qb}\) respectively. \(s_3\) and \(s_4\) are used during diffusion.

\(\beta_i = \text{mod} (\text{floor}((\alpha_i + 100) \times 10^{10}), l_i) + 1\)  \(\text{(6)}\)

where \(i = 1, 2, ..., n-1\). \(\beta_i\) is used for confounding \(t_{qb}\). The confusion formulas are as \(\text{swap}(t_{q_i}(j), t_{q_i}(\alpha_i(j)))\), where \(j = 1, 2, ..., l_i\). The sequence \(W\) is obtained by joining sub-sequences in turn.

Step 3: we divide \(s_1\) into \(\alpha_c\) and \(s_2\) into \(\alpha_d\) and we process them according to the following Equation: \((c = 1, 2, ..., \frac{n}{2}, \frac{n}{2}; d = \frac{n+1}{2}, ..., n + 1)\)

\(C_1 = \text{DNA encode}(W, k_{x_5})\)  \(\text{(7)}\)

where \(k_{x_5}\) is the DNA encoding rules. \(C_1\) is a DNA sequence containing the information about \(W\). For chaotic sequences \(s_3\) and \(s_4\), \(S_1\) and \(S_2\) are obtained according to the above encoding method. \(\text{DNA encode}\) is calculated in Table 2. Diffusion of \(C_1\) is carried out according to the following Equation:

\(\begin{align*}
E_1(1) &= \text{DNA}^+(S_1(1), C_1(1), 'A') \\
E_1(i) &= (E_1(i-1) + C_1(i) + S_1(i))
\end{align*}\)  \(\text{(8)}\)

where \(i = 2, 3, ..., 4L\). \(E_1\) is the diffused sequence. \(\text{DNA}^+\) is calculated in Table 3. Diffusion of \(C_2\) is carried out according to the following Equation:

\(\begin{align*}
E_2(4L) &= \text{DNA}^+(S_2(4L), E_1(4L), 'A') \\
E_2(i) &= (E_2(i+1) + E_1(i) + S_2(i))
\end{align*}\)  \(\text{(9)}\)

where \(i = 4L-1, ..., 2, 1\). \(E_2\) is the diffused sequence. The sequence is performed according to the following Equation:

\(E_3 = \text{DNA decode}(E_2(i), 4L, k_{x_5})\)  \(\text{(10)}\)

where \(E_3\) is the final decoded sequence. \(\text{DNA decode}\) is calculated in 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 a 0 value to get the encrypted image.
The 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 Simulation

All encryption and decryption experiments are performed in MATLAB R2018b on a Intel(R) Core (TM) i5-6500 CPU @ 3.20 GHz and 8GB RAM platform. We chose some medical images from the MedPix dataset to validate the proposed encryption method. The medical images are named as sample_1 (s1), sample_2 (s2), sample_3 (s3), sample_4 (s4) with Fig. 4 illustrating the sample images. Figure 5 shows the lossless encrypted images (ENI), and the decrypted images (DEI).

The lossless encryption is a method of encrypting all pixels except zero value pixels. Thus, lossless encryption time is long. To overcome this problem, a fast encryption technology is proposed. Figure 6 shows the fast encrypted images (ENI) and the decrypted images (DEI). As shown in Fig. 6, fast encryption has fewer encrypted pixels than lossless encryption, so the black area occupies half the image. The encryption time is shorter and the decrypted image has no effect on the diagnostic.

5 Performance and security analyses

5.1 Key space analysis

The size of the key space represents the algorithm’s ability to resist brute force attacks. The greater the scope of the key space is, the stronger the security of the image encryption will be. In this paper, the secret keys include the generated hash values (K1) based on the doctor-patient information and SHA-256 hash function and the internal clustering key (K2) set by the user. In addition, the secret keys also include the initial conditions a, b, c, d, x0, y0, z0 and w0 of the 4-D hyperchaotic system, as well as some auxiliary keys such as DNA coding rules (K3), and DNA manipulation (K4). The key space can reach $2^{256} \times 2^8 \times 2^5 \times 2^4 = 2^{273}$, which is much larger than the required $2^{100}$. The encryption system has sufficient key space. As a result, the proposed encryption algorithm is capable of withstanding brute force attacks.

![Fig. 4 The sample images: (a) s1 image, (b) s2 image, (c) s3 image, (d) s4 image](image-url)
5.2 Histogram analysis

The histogram represents the pixel value distribution, and the histogram variance quantitatively evaluates the image uniformity. Moreover, the smaller the variance of the encrypted image, the more uniform the distribution. Variance is measured as:

$$\text{Variance} = \frac{1}{256} \sum_{i=0}^{255} \sum_{j=0}^{255} \frac{1}{2} \times (v_i - v_j)^2$$

Fig. 5 Lossless encryption results: (a) s1_ENI, (b) s2_ENI, (c) s3_ENI, (d) s4_ENI; (e) s1_DEI, (f) s2_DEI, (g) s3_DEI, (h) s4_DEI

Fig. 6 Fast encryption results: (a) s1_ENI, (b) s2_ENI, (c) s3_ENI, (d) s4_ENI; (e) s1_DEI, (f) s2_DEI, (g) s3_DEI, (h) s4_DEI
where \( v_i \) and \( v_j \) are the pixel numbers, \( i \) is the gray value of the plain image and \( j \) is the gray value of the encrypted image. The variances of the plain and encrypted images are reported in Table 5, highlighting that the variance of the encrypted image is less than 293.24, indicating that the frequency distribution of the encrypted pixels is nearly uniform.

The histogram of the normal (HPI) and encrypted (HENI) images is illustrated in Fig. 7. It indicates that the histogram of ordinary images has apparent peaks and valleys, which also reveals the image’s information. The histogram of the encrypted image is flat, and therefore it can resist statistical analysis attacks.

5.3 Correlation analysis

The correlation of adjacent pixels is an important index to evaluate a cryptosystem’s quality. The correlation coefficient (Corr) of two adjacent pixels is obtained from Eq. (12):

\[
\text{Corr}(x_1, x_2) = \frac{\text{Cov}(x_1, x_2)}{\sqrt{D(x_1)} \times \sqrt{D(x_2)}}
\]

\[
\text{Cov}(x_1, x_2) = \frac{1}{n} \times \sum_{i=1}^{n} (x_i - E(x_1))(x_i - E(x_2))
\]

\[
D(x_1) = \frac{1}{n} \times (x_i - E(x_1))^2
\]

\[
E(x_1) = \frac{1}{n} \times \sum_{i=1}^{n} x_i
\]

where \( x_1 \) and \( x_2 \) represent the two neighboring pixel values, \( n \) is the number of pixels, and \( E(x_1) \) and \( D(x_1) \) represent the expectation and variance, respectively. The correlation coefficients of the plain and the encrypted images are depicted in Table 6.

The latter figure shows that the plane image has correlation coefficients close to one in all directions, presenting a solid correlation. However, the correlation coefficient of the encrypted image is close to zero in all directions. Note that after the image is encrypted, the correlation is destroyed. The s3 correlation scatters diagram in the horizontal (H), vertical (V), positive diagonal (P), and negative diagonal (N) directions are illustrated in Fig. 8, highlighting that the pixels of the planar image are distributed near the diagonal. In contrast, the pixels of the encrypted image (EN) can be evenly distributed. Therefore, our method can resist statistical attacks.

5.4 Information entropy

Information entropy is an indicator evaluating the randomness and unpredictability of information. Information entropy is defined as:

| Image       | Variance          |          |
|-------------|--------------------|----------|
|             | Plain image | Encrypted image |  
| sample_1    | $4.6 \times 10^3$ | 285.04   |
| sample_2    | $1.5 \times 10^3$ | 251.20   |
| sample_3    | $1.4 \times 10^3$ | 250.24   |
| sample_4    | $8.2 \times 10^3$ | 257.92   |
Fig. 7 Histogram of plain and encrypted images: (a) s1_HPI, (b) s2_HPI, (c) s3_HPI, (d) s4_HPI; (e) s1_HENI, (f) s2_HENI, (g) s3_HENI, (h) s4_HENI
\[ H(x) = - \sum_{i=0}^{N} p(x_i) \log_2 p(x_i) \] (13)

where \( p(x_i) \) is the appearance probability of the symbol \( x_i \), and \( N \) is the total number of \( x_i \). The entropy of the plain and encrypted images is presented in Table 7, showing that the plain images have entropies less than 7.6. However, the entropies of the encrypted images are close to the theoretical value of 8. Therefore, the encrypted image has high randomness, and it is challenging for the attacker to obtain valid information from the encrypted images.

### 5.5 Differential attack

The slight change of pixels and keys affects the encrypted image, and thus, the encrypted images may be hacked by a differential attack. The performance of the encryption scheme for resisting differential attacks can be evaluated by the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) values. These metrics have the following mathematical expressions:

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

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

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

where \( C_1 \) and \( C_2 \) are the first and the second encrypted images and \( w \) and \( h \) are the width and height of plain image \( C \), respectively. Here, \( 2^8 \) represents the number of gray levels. The \( NPCR \) and \( UACI \) results are reported in Table 8.

From Table 8, the \( NPCR \) and \( UACI \) results of encrypted images are close to the theoretical value of 99.6094\% (\( NPCR \)) and 33.4635\% (\( UACI \)), respectively. Hence, the suggested method has high plaintext sensitivity and can resist differential attacks.

Key sensitivity is as important as plaintext sensitivity. From Table 9, the \( NPCR \) and \( UACI \) results of encrypted images are close to the theoretical value of 99.6094\% (\( NPCR \)) and
Fig. 8 Correlation plot: (a) s3_H, (b) s3_V, (c) s3_P, (d) s3_N; (e) s3_EN_H, (f) s3_EN_V, (g) s3_EN_P, (h) s3_EN_N
5.6 Noise attack and clipping attack

Encrypted images may be attacked during their transmission over public channels. Such attacks result in changes and loss of data, with commonly used attacks involving salt and pepper noise attack (SPNA), speckle noise attack (SNA) and clipping attack (CA). To evaluate the robustness of the encryption method, we added two different types of attacks to the encrypted (EN) image (ENI), and the corresponding decrypted image (DEI) is presented in Fig. 9.

Under different attack types, the decrypted image is understandable, and the decrypted image does not affect the diagnosis. Thus, the developed method has strong robustness against SPNA and CA attacks. To evaluate the robustness of encryption and watermarking methods, we employ the peak signal-to-noise ratio (PSNR), mean square error (MSE) and structural similarity (SSIM) metrics, defined as follows:

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

where $w$ and $h$ represent the width and height of the image, and MSE is the mean square error.

### 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         |

### Table 8: NPCR and UACI results (plaintext sensitivity)

| 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 |

### Table 9: NPCR and UACI results (key sensitivity)

| Encrypted image | NPCR(%) | UACI(%) |
|-----------------|---------|---------|
| sample_1        | 99.5157 | 33.4333 |
| sample_2        | 99.5837 | 33.3432 |
| sample_3        | 99.6155 | 33.3684 |
| sample_4        | 99.5599 | 33.5153 |
\[ \text{MSE} = \frac{1}{w \times h} \sum_{i=0}^{w-1} \sum_{j=0}^{h-1} [P_{i,j} - C_{i,j}]^2, \]  

\[ \text{SSIM} = \frac{(2\mu_P\mu_C + l_1)(2\sigma_{PC} + l_2)}{\left(\mu_P^2 + \mu_C^2 + l_1\right)\left(\mu_P^2 + \mu_C^2 + l_2\right)}, \]  

Fig. 9  SPNA (0.01) and CA (25% of side length) results: (a) s1_ENI_SPNA, (b) s2_ENI_SPNA, (c) s3_ENI_SPNA, (d) s4_ENI_SPNA; (e) s1_DEI_SPNA, (f) s2_DEI_SPNA, (g) s3_DEI_SPNA, (h) s4_DEI_SPNA; (i) s1_ENI_CA, (j) s2_ENI_CA, (k) s3_ENI_CA, (l) s4_ENI_CA; (m) s1_DEI_CA, (n) s2_DEI_CA, (o) s3_DEI_CA, (p) s4_DEI_CA
where, $P_{i,j}$ is the plain image pixel or original watermark image pixel, $C_{i,j}$ is decrypted image pixel or the extracted watermark image pixel, $\mu_P$ and $\mu_C$ are the average pixel value of images $P$ and $C$, respectively, $\sigma_P$ and $\sigma_C$ denote the variance of $P$ and $C$, $\sigma_{PC}$ is the covariance between $P$ and $C$, and $l_1$ and $l_2$ are constants. Information is attacked in transit. Figure 10 shows the $PSNR$ and $SSIM$ results of decrypted images under $SNA(2 \times 10^{-6})$.

In Fig. 10, faster encryption $PSNR$ is greater than lossless encryption, and faster encryption $SSIM$ is similar to lossless encryption $SSIM$. It demonstrates that fast encryption can not only withstand SNA, but also improve encryption efficiency. Table 10 shows the $PSNR$ and $SSIM$ results of decrypted images under SPNA.

From Table 10, 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 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 11 provides the $PSNR$ and $SSIM$ results for the decrypted images under the CA.

From Table 11, 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 one. The lossless

![Graph](image)

*Fig. 10* SNA results: (a) s1-s4 $PSNR$ _SNA_, (b) s1-s4 $SSIM$ _SNA_
encryption can encrypt all feature pixels. As a result, lossless encryption is safer than fast encryption.

5.7 Encrypted pixel ratio

The algorithm proposed in this paper discarded some pixels that do not affect the diagnosis, to improve the encryption efficiency. Figure 11 shows the encryption pixel ratio of the sample image in the general encryption method and the proposed encryption method.

In Fig. 11, the ratio of the lossless encrypted pixels is less than 90%, and the encrypted pixel reduction ratio is small. The ratio of fast encrypted pixels is about 60%, and the encrypted pixel reduction ratio is relatively large. The reduction in the number of the encrypted pixels improves encryption efficiency without affecting the doctor’s diagnosis.
6 Comparison and discussion

Table 12 shows the performance comparison of the proposed encryption method with some of the existing encryption methods.

It can be seen from Table 12 that the proposed encryption method is superior to current encryption, and the indexes of the proposed encryption methods are closer to the theoretical values. That’s because some low-value pixels were discarded in the fast encryption and 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 chosen based on different requirements.

7 Conclusion

In this paper, the medical image encryption method based on hyperchaotic system and DNA encoding is proposed. It has several advantages as follows. First, ROI can be extracted and some important pixels can be encrypted. Thus, the encryption time is also reduced. Second, hyperchaotic system is used for medical image encryption. Third, compute resources can be saved because of the use of DNA encryption. The sequences of pixel values and chaotic sequences can be encoded and decoded at the same time. Finally, the results of the security analysis and experiments show that the proposed encryption method can withstand 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.

Based on the above advantages, the method can be applied to a safe medical system. In the future work, we intend to implement this method of hardware to improve the execution efficiency of encryption algorithms. Although the proposed scheme focuses on medical image encryption, it is not limited to this field. Further future work may explore related applications in other areas of information security.

Table 12 Performance comparison

| Methods          | Correlation | Entropy | NPCR(%) | UACI(%) | Time(s) |
|------------------|-------------|---------|---------|---------|---------|
|                  | Horizontal  |         | Vertical|         |         |
| [26]             | -0.0010     | 7.9993  | 99.60   | 33.46   | 2.46    |
| [10]             | -0.0177     | 7.9972  | 99.61   | 33.24   | 5.36    |
| [16]             | 0.0027      | 7.9891  | 99.63   | 33.44   | -       |
| [4]              | -0.0015     | 7.8231  | 99.61   | 33.15   | -       |
| [32]             | 0.0036      | 7.9992  | 99.61   | 33.42   | -       |
| Proposed-Fast    | -0.0391     | 7.9916  | 99.64   | 33.81   | 1.63    |
| Proposed- Lossless| -0.0126    | 7.9921  | 99.61   | 33.16   | 2.36    |

Funding  This research is supported by the National Natural Science Foundation of China (Nos: 61702356), National Natural Science Foundation of Shanxi Province (Nos: 201801D121143 and 20210302124050).
Declarations

Conflict of interest The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Adleman LM (1994) Molecular computation of solutions to combinatorial problems. Science 266:1021–1024
2. Chai X, Chen Y, Broyde L (2017) A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng 88:197–213
3. Chai X, Gan Z, Yuan K, Chen Y, Liu X (2017) A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput & Applic 31(1):219–237
4. Dai Y, Wang H, Wang Y (2016) Chaotic medical image encryption algorithm based on bit-plane decomposition. Int J Pattern Recognit Artif Intell 30(04):1657001
5. Deb S, Bhuyan B (2021) Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR. Multimed Tools Appl 80(13):19803–19826
6. Fohiffack Signing VR, Fozin Fonzin T, Kountchou M, Kengne J, Njitacke ZT (2021) Chaotic jerk system with hump structure for text and image encryption using DNA coding. Circuits, Systems, and Signal Processing 40(9):4370–4406
7. Gafsi M, Abbassi N, Hajaji MA, Malek J, Mitiba A, Pan Z (2020) Improved chaos-based cryptosystem for medical image encryption and decryption. Sci Program 2020:1–22
8. Guesmi R, Farah MAB, Kachouri A, Samet M (2015) A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. Nonlinear Dynamics 83(3):1123–1136
9. Hajaji MA, Dridi M, Mitiba A (2019) A medical image crypto-compression algorithm based on neural network and PWLCM. Multimed Tools Appl 78(11):14379–14396
10. Iqbal N, Hanif M, Abbas S, Khan MA, Rehman Z (2021) Dynamic 3D scrambled image-based RGB image encryption scheme using the hyperchaotic system and DNA encoding. Journal of Information Security and Applications 58:102809
11. Jeevitha S, Amutha Prabha N (2020) Novel medical image encryption using DWT block-based scrambling and edge maps. J Ambient Intell Humaniz Comput 12(3):3373–3388
12. Khashan OA, AIShaikh M (2020) Edge-based lightweight selective encryption scheme for digital medical images. Multimed Tools Appl 79(35-36):26369–26388
13. Kumar M, Iqbal A, Kumar P (2016) A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Process 125:187–202
14. Lei T, Jia X, Zhang Y, He L, Meng H, Nandi AK (2018) Significantly fast and robust fuzzy c-means clustering algorithm based on morphological reconstruction and membership filtering. IEEE Trans Fuzzy Syst 26(5):3027–3041
15. Li X, Wang B, Ly H, Yin Q, Zhang Q, Wei XP (2020) Constraining DNA sequences with a triplet-bases unpaired. IEEE Transactions on Nanobioscience 19(2):299–307
16. Liu H, Kadir A, Li Y (2016) Asymmetric color pathological image encryption scheme based on the complex hyper chaotic system. Optik 127(15):5812–5819
17. Pak C, Huang L (2017) A new color image encryption using a combination of the 1D chaotic map. Signal Process 138:129–137
18. Parvaz R, Zarebnya M (2018) A combination chaotic system and application in color image encryption. Opt Laser Technol 101:30–41
19. Shafai W, Khalilaf F, Rabaie ESM, Samie FEA (2021) Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J Intell Humaniz Comput 12(10):9007–9035
20. Wang X, Feng L, Zhao H (2019) Fast image encryption algorithm based on the parallel computing system. Inf Sci 486:340–358
21. Wang X, Gao S (2020) Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Inf Sci 507:16–36
22. Wang X, Gao S (2020) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci 539:195–214
23. Wang X, Liu C, Jiang D (2021) A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inf Sci 574:505–527
24. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
25. Wang X, Yang J (2021) A privacy image encryption algorithm based on piecewise coupled map lattice with multi-dynamic coupling coefficient. Inf Sci 569:217–240
26. Wang X, Zhang M (2021) An image encryption algorithm based on new chaos and diffusion values of a truth table. Inf Sci 579:128–149
27. Wang XY, Zhang YQ, Bao XM (2015) A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 73:53–61
28. Wu X, Kan H, Kurths J (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl Soft Comput 37:24–39
29. Xian Y, Wang X (2021) Fractal sorting matrix and its application on chaotic image encryption. Inf Sci 547:1154–1169
30. Xian Y, Wang X, Teng L (2021) Double parameters fractal sorting matrix and its application in image encryption. IEEE Transactions on Circuits and Systems for Video Technology. https://doi.org/10.1109/TCSVT.2021.3108767
31. Xian YJ, Fu KR, Xu CB (2021) A 4-D multi-stable hyper-chaotic system multi-wing attractors. Journal of Vibration and Shock 40(1):15–22
32. Xue X, Jin H, Zhou D, Zhou C (2021) Medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length. Front Genet 12:654663

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.