Medical image encryption scheme based on self-verification matrix

Zhenlong Man\textsuperscript{1,2} | Jinqing Li\textsuperscript{1,2} | Xiaoqiang Di\textsuperscript{1,2,3}

\textsuperscript{1} School of Computer Science and Technology, CUST, Changchun University of Science and Technology, Changchun City, Jilin Province, Changchun City 130022, China (Email: 765001821@qq.com)

\textsuperscript{2} Province Key Laboratory of Network and Information Security, CUST, Changchun University of Science and Technology, Changchun City, Jilin Province, Changchun City 130022, China

\textsuperscript{3} Information Center, CUST, Changchun University of Science and Technology, Changchun City, Jilin Province, Changchun City 130022, China

Abstract

To mitigate the shortcomings of existing medical image encryption algorithms, including a lack of anti-tampering methods and security, this report presents an anti-tampering encryption algorithm for medical images that is based on a self-verification matrix. First, chaotic coordinates generated by chaos are used to traverse all pixels in a plain image to generate a two-dimensional matrix (a self-verification matrix) with positioning information. The accurate location of illegally altered image pixels can be detected using the self-verification matrix. To improve the security of the self-authentication matrix, DNA coding is also applied to the self-authentication matrix, and the plain image is also diffused statically to destroy the pixel distribution. Next, the scrambled image and self-verification matrix are mixed and cross-scrambled. Finally, the fused image is diffused dynamically to improve the security of the encrypted image. Experimental simulation and performance analysis show that the algorithm achieves good encryption effectiveness, provides strong anti-tampering capabilities, and can accurately locate at least 4 pixels.

1 INTRODUCTION

In modern hospitals, digital medical images play an increasingly important role in the diagnosis and treatment of diseases, and have thus attracted increasing attention [1, 2]. In recent years, medical image security has gradually become a research hotspot [3] and typically involves the following aspects: confidentiality (only authorized individuals can access patient data), integrity (proving that medical information has not been modified) and authentication (involving identity recognition; two communication participants should identify each other) [4, 5]. Encryption and watermarking technology are typically used to provide security and integrity authentication for medical images. Encryption typically confuses the visual effect of medical images, and watermarking can unconsciously insert authentication information so that unauthorized users cannot access the hospital information system [6, 7].

For many years, various encryption algorithms have been widely used to provide security for digital images [8–13]. Image encryption can provide protection for image information, thus ensuring the confidentiality and security of the image [14]. Image encryption is typically divided into two stages. In the scrambling stage, changing the position of image pixels will cause visual confusion. In the diffusion stage, the influence of a single plain-image pixel or key is diffused into more cipher images by changing the value of the image pixel to conceal the relationship between the statistical characteristics of the cipher image and plain image. However, once the image is decrypted, the image is no longer protected [15–17]. Although current medical image encryption algorithms play strong roles in protecting the security of medical images, the security level of medical images is still limited because medical images may involve the privacy of many patients, some of which are confidential and sensitive [18]. In [19], a medical image encryption...
algorithm based on the Goldreich–Goldwasser–Halevi encryption scheme was studied. That algorithm can ensure security while maintaining low algorithm complexity. However, that algorithm cannot resist ciphertext attacks and can only be improved by filling before encryption. In [20], the security and integrity of the enhanced Rivest cipher algorithm based on chaos in medical images were studied. In [21], a medical image encryption algorithm using high-speed scrambling and pixel adaptive diffusion was proposed, but a cipher image was found to be completely recoverable with the chosen plaintext attack. However, the diffusion ability of the Rivest cipher is poor, and the performance of encrypted images in resisting various attacks is poor. To solve some of the shortcomings of existing medical image encryption algorithms, researchers have proposed many strong encryption algorithms according to the characteristics of medical images [22–29]. In [22], an improved encryption scheme was proposed for [21] that uses the enhanced version of the original algorithm to perform non-linear operations on the image. The experimental results and security analysis show that the improved encryption algorithm can resist the selected plain-image attack and retain the advantages of the original algorithm. In [30], according to the characteristics of the frequency domain and spatial domain, a DICOM image encryption algorithm based on the fusion of the frequency domain chaotic attractor and spatial domain DNA sequence based on integer wavelet transform (IWT) were proposed. That algorithm exhibits strong robustness and the ability to resist statistical and differential attacks. In [18], an asymmetric medical image encryption scheme was proposed with an iris for medical image encryption to improve the security of the encryption scheme. Second, asymmetric optical encryption technology was combined with three-dimensional Lorenz chaos technology to improve the key space and solve the linear problem based on double random phase coding. In [31], Ma et al. proposed a novel reversible data hiding (RDH) scheme for medical images based on block classification and code division multiplexing (CDM) in the frequency domain. This scheme provides high visual quality and a large data embedding capacity for medical images. Although a variety of encryption schemes have been developed to protect medical images, most schemes address the security of medical images, and few schemes can verify the integrity of medical images and preventing tampering [32].

To overcome this limitation, many researchers have proposed digital watermarking to provide security for medical images by authenticating original images, their ownership and other security requirements [33]. In [34], a new color image watermarking replacement scheme based on a Fourier transform was proposed. Two variants of the scheme were applied and achieved good imperceptibility. In [35], a new image watermarking scheme based on singular value decomposition (SVD) and chaotic mapping was proposed to enable the algorithm to achieve a good balance between robustness and imperceptibility. In [36], Xu et al. proposed a QR-based digital watermarking scheme to enhance robustness to the shear attack. In addition, that method was found to yield superior performance compared to other methods in terms of invisibility, robustness, and embedding payload.

Watermarking also has some drawbacks [37]. For example, watermarking can only detect whether the image has been tampered with but cannot locate the exact location of the tampering. In addition, watermarking will not hide the image information itself; once the watermarking is deleted, the image will no longer be protected [38]. To overcome the limitation of only encrypting or watermarking methods, a tamper-proof encryption algorithm for medical images based on a self-verification matrix is proposed. The algorithm uses random chaotic coordinates to record the pixel position information of the plain image and obtains the self-verification matrix related to plaintext. In addition to anti-tampering, it can also effectively resist known plaintext attacks and selected plaintext attacks, and improve system robustness. Then, the statistical features in the self-verification matrix information are also hidden by DNA coding, and a new image is obtained by fusing the self-verification matrix with the plain image. To ensure the security of the encrypted image, the new image is cross-scrambled, and dynamic diffusion is performed to obtain the final cipher image. To describe the proposed scheme’s reliability, performance analysis (e.g. information entropy, histogram and key sensitivity) and anti-attack detection (e.g. differential attack, noise attack and clipping attack) are performed. Comprehensive experimental results show that the method achieves strong anti-tampering capabilities and anti-attack capabilities.

The remainder of this paper is organized as follows. The fractional Chen hyperchaotic system, 4D hyperchaotic system and DNA code are introduced in Section 3, Section 4 introduces the image encryption algorithm, and Section 5 analyzes the performance of the algorithm. The last section summarizes the paper.

## 2 Related work

### 2.1 The fractional Chen hyperchaotic system model is described as [39]

\[
\begin{align*}
\frac{d\alpha}{d\tau} y_1 &= a(y_2 - y_1) + y_4, \\
\frac{d\alpha}{d\tau} y_2 &= by_1 - y_1 y_3 + \gamma_2, \\
\frac{d\alpha}{d\tau} y_3 &= y_1 y_2 - cy_3, \\
\frac{d\alpha}{d\tau} y_4 &= y_2 y_3 + \gamma_4.
\end{align*}
\]

When \(a = 35, b = 3, c = 12, d = 7\) and \(\epsilon = 0.58\), the system has two positive Lyapunov exponents of \(\lambda_1 = 0.567\) and \(\lambda_2 = 0.126\); thus the system is hyperchaotic. The prediction time of hyperchaotic systems is typically shorter than that of chaotic systems; thus the security of hyperchaotic systems is higher. Its partial chaotic attractors are shown in Figure 1.
2.2 The state equations of the 4D hyperchaotic system are as follows [40]

\[
\begin{align*}
\dot{x}_1 &= \delta_1 (x_2 - x_1), \\
\dot{x}_2 &= \delta_2 x_1 + \delta_3 x_2 - x_1 x_3 + x_4, \\
\dot{x}_3 &= x_2^2 - \delta_4 x_3, \\
\dot{x}_4 &= -\delta_5 x_1,
\end{align*}
\]

where \(\delta_1, \delta_2, \delta_3, \delta_4, \delta_5\) are the system control parameters. When \(\delta_1 = 27.5, \delta_2 = 3, \delta_3 = 19.3, \delta_4 = 2.9, \delta_5 = 3\), system (2) exhibits chaotic behaviour. The Lyapunov exponents are \(\lambda_1 = 1.6170, \lambda_2 = 0.1123, \lambda_3 = 0, \lambda_4 = -12.8245\). There are two Lyapunov exponents whose values are greater than zero; thus, system is hyperchaotic. Chaotic attractors of system are shown in Figure 2.

### 2.3 Coding and decoding of DNA

DNA is composed of nucleotides. The nitrogen-containing bases of nucleotides are A (adenine), C (cytosine), G (guanine), and T (thymine). A and T complement each other, and G and C complement each other. Because 0 and 1 are complementary in the binary system, 00 and 11 are complementary, and 01 and 10 are complementary [41]. Using 00, 01, 10 and 11 to code for A, C, G and T, there are 24 coding rules. However, only eight coding rules satisfy the Watson–Crick rule[42], as shown in Table 1. DNA decoding rules are contrary to DNA coding rules.

### 3 TAMPER-PROOF ENCRYPTION/DECRYPTION SCHEME

To protect the confidentiality and integrity of medical images, and to check whether medical images have been tampered with illegally, a chaotic medical image encryption algorithm based on the self-verification matrix is designed to prevent tampering. Its structure is shown in Figure 3. The proposed scheme is deployed at the ends of Alice and Bob, where Alice is the sender of information and the encryption end, and Bob is the receiver of information and the legitimate decryption end. Eric is an attacker, that illegally tamper with the information.

#### 3.1 Encryption/decryption algorithm

The proposed algorithm consists of a self-verification matrix generation stage, a DNA coding encryption stage, a decussate scrambling stage, and a dynamical diffusion stage. This encryption flowchart is shown in Figure 4.

Step 1: We assume that plain-image \(P\) is an \(M \times N\) grey medical image.

Step 2: Iterate the fractional Chen hyperchaotic system (1) \(M \times N\) times. The results \(y_1, y_2, y_3, y_4\) are mapped to integer sequences \(C\)\(\bar{x}_1\), \(C\)\(\bar{x}_2\), \(C\)\(\bar{x}_3\) and \(C\)\(\bar{x}_4\):

\[
C_{\bar{x}_i} = \begin{cases} 
\text{ceil} (\text{mod} (y_i \times 10^{10}), N), & i = 1, 2, 4, \\
\text{ceil} (\text{mod} (y_i \times 10^{10}), M), & i = 3.
\end{cases}
\]

### TABLE 1 DNA coding rules

| Coding rules | A | T | G | C |
|--------------|---|---|---|---|
| 1            | 11| 00| 10| 01|
| 2            | 11| 00| 01| 01|
| 3            | 00| 11| 10| 01|
| 4            | 00| 11| 01| 10|
| 5            | 01| 10| 11| 00|
| 6            | 01| 10| 00| 11|
| 7            | 10| 01| 11| 00|
| 8            | 10| 01| 00| 11|
Step 3: The elements of sequence $CS_1, CS_2$ and $CS_4$ in Equation (3) are transformed into three hyperchaotic matrices $CM, CM1$ and $CM2$, whose sizes are $M \times N$, respectively.

$$
\begin{align*}
CM &= \text{reshape}(CS_1, M, N), \\
CM1 &= \text{reshape}(CS_2, M, N), \\
CM2 &= \text{reshape}(CS_4, M, N).
\end{align*}
$$

Step 4: We eliminate the repetitive elements in the integer sequences $CS_1, CS_2, CS_3$, and $CS_4$, and then obtain the hyperchaotic coordinate pairs $(Q_x, Q_y)$ and $(Q_z, Q_w)$:

$$
\begin{align*}
Q_x &= \text{ismember}(Q, CS_1), \\
Q_y &= \text{ismember}(Q, CS_2), \\
Q_z &= \text{ismember}(Q, CS_3), \\
Q_w &= \text{ismember}(Q, CS_4),
\end{align*}
$$

where $\text{ismember}()$ is the function to eliminate the repetitive elements in the sequence.

Step 5: The self-verification matrix $W$ is computed using the coordinate pair $(Q_x, Q_y)$ and hyperchaotic matrix $CM$, as described in Equation (7):

$$
W(i, j) = \text{bitxor}(P(i, j) - P(Q_x(i), Q_y(j))),
$$

where $P(i, j)$ is the pixel value at position $(i, j)$; $P(Q_x(i), Q_y(j))$ is the pixel value at position $(Q_x(i), Q_y(j))$ in plain-image $P$; and $\text{bitxor}()$ represents a bitwise XOR operation. In short, the self-verification matrix is composed of the pixel differences of two positions in the plain image.

Step 6: Concurrently, the plain-image $P$ is statically scrambled and diffused by the DNA coding encryption method as follows: First, the pixel values in the plain-image $P$ are converted into 8 bits binary. Second, according to the DNA coding rules, to obtain the DNA coding image $DNA_P$. Then the hyperchaotic coordinate pair $(Q_z, Q_w)$, shown in Equation (6), is used for position information to scramble $DNA_P$. Finally, the scrambling
result is diffused with the hyperchaotic matrix \(CM1\). The DNA coding encryption image \(DNAE\) is thus obtained:

\[
DNAE = \text{bitxor}(DNA_1(Q_x, Q_y), CM1). \tag{8}
\]

The DNA coding encryption process is shown in Figure 5.

Step 7: The 4D hyperchaotic system (2) is used to generate the secret keys of decussate scrambling and dynamical diffusion. Iterate system (2) \(2 \times M \times N\) times. We reshape the results of iteration, \(x_1, x_2, x_3, x_4\) into four matrices:

\[
\begin{align*}
ST1 &= \text{reshape}(x_1, M, N), \\
ST2 &= \text{reshape}(x_2, M, N), \\
ST3 &= \text{reshape}(x_3, 2 \times M, N), \\
ST4 &= \text{reshape}(x_4, 2 \times M, N),
\end{align*} \tag{9}
\]

where \(ST1\) and \(ST2\) are the decussate scrambling key matrices, and \(ST3\) and \(ST4\) are the dynamical diffusion key matrices.

Step 8: The DNA coding encryption image \(DNAE\) and the self-verification matrix \(W\) are decussately scrambled. The decussate scrambling rules are given by:

\[
\begin{align*}
\lambda_1 &= DNAE(i, j), \\
DNAE(i, j) &= DNAE(Q_x(i), Q_y(j)), \\
ST1(i, j) &\leq \mu_1, \\
DNAE(Q_x(i), Q_y(j)) &= \lambda_1, \\
\lambda_2 &= DNAE(i, j), \\
DNAE(i, j) &= W(Q_x(i), Q_y(j)), \\
ST1(i, j) &> \mu_1, \\
W(Q_x(i), Q_y(j)) &= \lambda_2, \\
\lambda_3 &= W(i, j), \\
W(i, j) &= W(Q_x(i), Q_y(j)), \\
ST2(i, j) &\leq \mu_2, \\
W(Q_x(i), Q_y(j)) &= \lambda_3, \\
\lambda_4 &= W(i, j), \\
W(i, j) &= DNAE(Q_x(i), Q_y(j)), \\
ST2(i, j) &> \mu_2, \\
DNAE(Q_x(i), Q_y(j)) &= \lambda_4,
\end{align*} \tag{10}
\]

where \(\lambda_1, \lambda_2, \lambda_3, \lambda_4\) are the intermediate variable; \(i = 1, 2, 3, ..., M; j = 1, 2, 3, ..., N;\) and \(\mu_1, \mu_2\) are the decussate scrambling control thresholds.

Step 9: Up and down splice the \(W(i, j)\) and \(DNAE\) of decussate scrambling, obtain the scrambling image \(Img\). Then \(St, 3\) and \(ST4\), and then we finally obtain the cipher-image \(CImg\):

\[
\begin{align*}
MI &= \text{bitxor}(StImg, ST3), \\
CImg &= \text{bitxor}(MI, \text{bitxor}([\text{bitxor}([\text{bitxor}(\rho, ST3) + ST4), N], ST4'), N).
\end{align*} \tag{11}
\]

where \(\rho\) is the dynamic encryption control parameter, \(\rho \in \mathbb{N}\), and \(\rho \leq 2 \times M \times N\).

This algorithm is a symmetric encryption algorithm, and the decryption process is the inverse of encryption. Through the inverse operation of the dynamical diffusion and decussate scrambling, we can obtain the decrypted image and a decrypted self-verification matrix ‘\(W\)’.

## 4 EXPERIMENTAL SIMULATION AND PERFORMANCE ANALYSIS

Here, we simulate the proposed algorithm, and analyze the security of grey images and color images, including key space analysis, statistical analysis and differential attack analysis. As shown in Figure 6a-c, the plain image used for the experiment, and (d–f) the corresponding cipher image. The initial key is \(y_1 = -4, y_2 = -3, y_3 = 5, y_4 = -6, x_1 = 2.55, x_2 = 5.2, x_3 = 3.12, x_4 = 7.31, \mu_1 = 10, \mu_2 = 58\).

### 4.1 Self-verification tamper-proof method

As shown in Figure 3, Alice encrypts the plain-image \(P\) to the cipher image \(CImg\), and then sends it to the legal decryptor Bob. The attacker Eric illegally intercepts and decrypts \(CImg\), and maliciously tampers with it to obtain the tampered image \(TImg\), which is then sent to Bob. Thus, the decryption-image obtained by Bob is a tampered decrypted image \(DTImg\).

The proposed self-verification method can achieve pixel-level image tampering detection. First, a decrypted self-verification matrix \(W\) generates during the decryption process. Next, we calculate the verification matrix \(V\), as shown in Equation (12):

\[
V(i, j) = \text{bitxor}(DTImg(i, j) - DTImg(Q_x(i), Q_y(j)), CM(i, j)), \tag{12}
\]

where, \(Q_x(i), Q_y(j)\) and \(CM(i, j)\) are symmetrically computed from the fractional Chen hyperchaotic system(1), as described in Section 2.1.
The simulation results show that: (a) the 'bone' of the plain image, (b) the 'intestine' of the plain image, (c) the 'chest' of the plain image, and (d) the corresponding cipher image, (e) the corresponding cipher image, (f) the corresponding cipher image.

FIGURE 7 Detection matrix $U$

Ultimately, the decrypted self-verification matrix $W'$ is compared with the verification matrix $V'$ and then, the detection matrix $U$ is generated.

The self-verification matrix is calculated by the difference between the pixel values of two random positions $(i, j)$ and $(Q_x(i), Q_y(j))$ in the image. If there are different values between the decrypted self-verification matrix $W'$ and the self-verification matrix $V'$ calculated in the decrypted image, the encrypted image been tampered with. As shown in Figure 7, the value in the self-verification matrix is derived from the difference between $P(i, j)$ and $(Q_x(i), Q_y(j))$. When $W'$ and $V'$ in the self-verification matrix are different, the two pixels have been tampered with. By comparing the values in the two self-verification matrices, we can identify the pixels that may be tampered with. Finally, the densest area of pixel aggregation is found to be the tampered location. Thus, we can accurately locate the tampered pixels that have been tampered with.

The black parts of the highlight block are the tampered parts that tamper with 4, 9 and 16 pixels in Figures 8a–c and 9a–c, respectively. We can easily find the locations of pixels that have been tampered with using the detection matrices shown in Figures 8d–f and 9d–f. Experimental results show that the proposed method effectively detects and locates pixels that have been tampered with.

4.2 Normalization analysis

In order to prove the robustness of the proposed scheme, we do a series of performance analysis and anti-attack test on the merged cipher image, and also do the color scale normalization on the self-verification matrix $W'$ and medical image DNAE before merging. It can be seen from Figure 10 that after image enhancement, neither the image nor the histogram can show any useful information, which further proves the feasibility of the scheme [44].

4.3 Information entropy

The information entropy of the image can measure the distribution of the image grey value. Image entropy $H(m)$ is defined as [43]:

$$H(m) = -\sum_{i=0}^{2^{N-1}} p(m_i) \log_2 p(m_i),$$

where $N$ is the number of $m_i$ pixels and $p(m_i)$ is the probability of $m_i$. For 256 greyscale images, the ideal information entropy of the cipher image is 8, which shows that the probability of occurrence of each grey-level pixel is equal, indicating a uniform distribution (i.e. a white noise image). Therefore, the information entropy of cipher image with high security should be near 8. Table 2 shows the results of the information entropy
FIGURE 8  'Intestine' medical image tamper-proof analysis: (a) 4 pixels that have been tampered with; (b) 9 pixels that have been tampered with; (c) 16 pixels that have been tampered with; (d) detection matrix of 4 pixels that have been tampered with; (e) detection matrix of 9 pixels that have been tampered with; (f) detection matrix of 16 pixels that have been tampered with

FIGURE 9  'Bone' medical image tamper-proof analysis: (a) 4 pixels that have been tampered with; (b) 9 pixels that have been tampered with; (c) 16 pixels that have been tampered with; (d) detection matrix of 4 pixels that have been tampered with; (e) detection matrix of 9 pixels that have been tampered with; (f) detection matrix of 16 pixels that have been tampered with

FIGURE 10  Normalization analysis: (a) self-verification matrix $W$; (b) histogram of (a); (c) color order normalization self-verification matrix $W^c$; (d) histogram of (c); (e) encrypted medical image DNAE; (f) histogram of (e); (g) medical image with color order normalization DNAE; (h) histogram of (g)

TABLE 2  Information entropy

|             | Bone    | Intestines | Chest (red component) | Chest (green component) | Chest (blue component) | [18]   | [21]   | [36]   |
|-------------|---------|------------|-----------------------|-------------------------|------------------------|--------|--------|--------|
| Information entropy | 7.9973  | 7.9973     | 7.9975                | 7.9972                  | 7.9980                 | 7.9969 | 7.9960 | 7.9971 |
4.4  Histogram analysis

The image histogram represents the intensity distribution of pixels in an image. A secure encryption system should make the histogram distribution as flat as possible because only the uniform distribution histogram has maximum entropy [44]. Figure 11 shows histograms of 'large intestine' and 'bone' plain images and cipher images. Figure 11 shows that the histogram distribution of all cipher images is relatively uniform, and the strong regularity of the plain-image pixels is not brought into the cipher image, which indicates that the attacker cannot obtain any useful statistical information from the cipher image to attack the algorithm.

4.5  Variance analysis

We use the variances of the histograms to evaluate the uniformities of the encrypted images. Variance is defined by [45]:

\[
\text{var}(\mathbf{z}) = \frac{1}{N \times M} \sum_{j=1}^{N} \sum_{i=1}^{M} (z_{ij} - \overline{z})^2,
\]  (14)

whereas \(\overline{z}\) represents the value of the histogram vector, the lower the variance of image is, the higher the uniformity. Table 3 shows the test results of different images. Compared with the plain image, the variance of the cipher image is markedly lower.

4.6  Correlation analysis

Due to the characteristics of digital images, plain images typically show a certain degree of correlation between two adjacent pixels. To analyze the correlation of adjacent pixels, 4000 pairs of adjacent pixels are randomly selected from the plain image and cipher images of 'bone' and their correlation coefficients
FIGURE 12  Distribution of correlation coefficients of adjacent pixels: (a) distribution of horizontal correlation coefficients of adjacent pixels of plain images; (d) distribution of horizontal correlation coefficients of adjacent pixels of cipher images; (b) distribution of vertical correlation coefficients of adjacent pixels of plain images; (e) distribution of vertical correlation coefficients of adjacent pixels of cipher images; (c) the distribution of diagonal correlation coefficients of adjacent pixels in plain images; (f) the distribution of diagonal correlation coefficients of adjacent pixels in cipher images

are calculated by:

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

where \(x\) and \(y\) represent the grey value of two adjacent pixels, and the correlation distribution of adjacent pixels in horizontal, vertical and diagonal directions is shown in Figure 12 [10, 46, 47] reports comparative algorithms, where the adjacent pixels of plain image have a strong correlation, and adjacent pixels of cipher image have low correlation. Then, we calculated the correlation coefficients of adjacent pixels of 'intestine' and 'bone' in three directions. As shown in Table 4, the correlation coefficient of the cipher image is significantly lower and near zero, which also highlights that the proposed method can effectively resist statistical attacks.

4.7 Key sensitivity analysis

A secure cryptosystem should be sensitive to a given encryption key. A small change in the encryption key will result in a large change in the cipher image, and a small difference in the decryption key will also lead to the incorrect decryption of the image. Considering a 128 × 256 'intestine' image as an example. Figure 13a shows the plain image, and Figure 13 shows the cipher image. Figure 13c-f shows that if there is any change in the keys, even just a \(10^{-16}\) difference, we cannot correctly recover the plain image.

Table 4  Coefficient correlation analysis

|                        | Horizontal | Vertical | Diagonal |
|------------------------|------------|----------|----------|
| Cipher-image 'bone'    | -0.0033    | 0.0092   | 0.0101   |
| Cipher-image 'intestine' | 0.0047    | -0.0026  | -0.0307  |
| Cipher-image 'chest(Red)' | 0.0008    | 0.0015   | 0.0122   |
| Cipher-image 'chest(Green)' | -0.0055  | 0.0035   | 0.0089   |
| Cipher-image 'chest(Blue)' | -0.0059  | -0.0094  | 0.0315   |
| [10]                   | 0.0122     | -0.0061  | -0.0197  |
| [46]                   | 0.0056     | 0.0132   | -0.0006  |
| [47]                   | 0.0122     | 0.0059   | 0.0023   |

4.8 Peak signal-to-noise ratio

The difference between the plain image and cipher image is measured by the mean square error (MSE). MSE is defined as:

\[
MSE = \frac{\sum \sum (P(i, j) - C(i, j))^2}{T} \times 100\%,
\]

where \(T\) represents the number of pixels in a cipher image. The larger the value of \(MSE\) is, the greater the difference between the cipher image and the plain image, and the better the image encryption effect. The peak signal noise ratio (PSNR) is the ratio between the plain image and cipher image. PSNR is defined as:

\[
PSNR = 10 \log_{10} \left( \frac{P_{\text{max}}^2}{MSE} \right),
\]
where \( \text{MAX} \) is the maximum pixel value of plain image. In a good encryption algorithm, PSNR should be as low as possible, because the larger the PSNR value, the more similar the cipher image is to the original image. The MSE and PSNR values of the cipher image are shown in Table 5, and [47] reports an algorithm for comparison.

### 4.9 Differential attack

An ideal cryptosystem should ensure that any minor changes in plain images should produce large changes in cipher images. The number-of-pixels change rate (NPCR) [49] and the unified averaged changing intensity (UACI) [50] are two criteria that are used to analyze differential attacks. These metrics are defined by:

\[
\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100%,
\]

\[
\text{UACI} = \frac{1}{M \times N} \left[ \sum_{i,j} \left| C_1(i,j) - C_2(i,j) \right| \right] \times 100%,
\]

(18)

where \( C_1 \) and \( C_2 \) represent two cipher images after changing one bit in the same plain image, and \( D(i,j) \) is defined as:

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

(19)

The ideal NPCR value and UACI value of the cipher image are 99.6093% and 33.4653%, respectively [51]. 'Intestine' and 'bone' and 'chest' images are used as test images. The UACI and NPCR values of this algorithm are compared with those of other algorithms as shown in Table 6. Results show that the NPCR and UACI values of this algorithm are similar to the theoretical values and have the ability to resist differential attacks.

### 4.10 Data loss attack

To protect the cryptosystem from data loss attacks during transmission and storage, image data with sizes of 64 \( \times \) 64, 128 \( \times \) 128 and 256 \( \times \) 128 are deleted from the cipher image to evaluate the robustness of the proposed algorithm to the data loss attack. Cropping results are shown in Figure 14a-c, and the corresponding decrypted images are shown in Figure 14d-f.
4.11 Noise attack

During real transmission and storage, noise is often added to the image. The ability to resist noise attacks is also an evaluation index to verify the robustness of the cryptosystem. In this section, salt-and-pepper noise is used to test the anti-noise attack ability [51]. Figure 15a-c show cipher image after adding 0.01, 0.05 and 0.1 salt-and-pepper noise, respectively, and Figure 15d-f are the corresponding decrypted images. Experimental results show that the decrypted image is still recognizable after adding salt-and-pepper noise, and the algorithm has good anti-noise ability.

4.12 Speed analysis

In addition to security, encryption efficiency is also important, particularly real-time Internet multimedia applications. In the proposed encryption scheme, cross-scrambling and dynamic diffusion can improve the overall encryption efficiency. Compared with other encryption schemes, Table 7, shows that the proposed algorithm exhibits advantages with regard to speed. Concurrently, due to the symmetric structure, the time costs of encryption and decryption are the same. The proposed scheme meets the definition of real-time encryption and decryption; real-time encryption can perform real-time processing of data encryption and decryption requirements in the user’s normal work, without displaying the encryption and decryption process, and does not generate temporary files. Real-time encryption and decryption technology provides users with a transparent operating experience while avoiding the process of repeated encryption and decryption of data on the storage medium, and solves the problems of complex operations and low efficiency of traditional encryption and decryption technologies. Thus, the proposed algorithm can realize support real-time communication.

5 CONCLUSION

In this study, a tamper-proof encryption scheme for medical images based on a self-verification matrix is proposed. The self-verification matrix is composed of plain-image position information that is controlled by a chaotic system. By combining DNA coding with a chaotic system, cross-scrambling and dynamic diffusion are used to ensure the security and integrity of the self-verification matrix and medical image. Finally, through security analysis and a tamper-proof test, the reliability of the proposed encryption scheme is shown to exhibit good tamper-proof capabilities and accurate positioning abilities. In future work, we plan to perform more detailed research on anti-tampering methods, particularly with regard to hiding verification information. The self-verification matrix information proposed in this paper should be combined with the plain image and encrypted together. The next step in this field of research is to integrate verification information into the cipher image, which can effectively reduce the complexity of the algorithm and improve encryption efficiency.

ACKNOWLEDGEMENTS

This work was supported in part by China’s Natural Science Foundation Project (20190201188JG) of the Science and Technology Department of Jilin Province and China’s Science and Technology Project (JJKH20181137K) for the 13th Five-Year Plan of the Education Department of Jilin Province.

ORCID

Zhenlong Man https://orcid.org/0000-0003-1974-9890

REFERENCES

1. Zinger, S.: View interpolation for medical images on autostereoscopic displays. IEEE Trans. Circuits Syst. Video Technol. 22(1), 128–137 (2011)
2. Lacoste, C.: Medical-image retrieval based on knowledge-assisted text and image indexing. IEEE Trans. Circuits Syst. Video Technol. 17(7), 889–900 (2007)
3. Liu, J.: A new simple chaotic system and its application in medical image encryption. Multimedia Tools Appl. 77(17), 22787–22808 (2018)
4. Zhang, Y.: Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. 11(1), 88–95 (2015)
5. Collen, M.F., Ball, M.J.: The History of Medical Informatics in the United States. Springer, Berlin (2015)
6. Sajjad, M.: Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimedia Tools Appl. 76(3), 3519–3536 (2017)
7. Mantos, P.L., Maglogiannis, I.: Sensitive patient data hiding using a ROI reversible steganography scheme for DICOM images. J. Med. Syst. 40(6), 156 (2016)
12. Zhou, J., et al.: A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. IEEE Access 8, 122210–122228 (2020)
13. Kumar, S., et al.: Medical image encryption using fractional discrete cosine transform with chaotic function. Med. Biol. Eng. Comp. 57(11), 2517–2533 (2019)
14. Nyeem, H., et al.: A review of medical image watermarking requirements for teleradiology. J. Digit. Imag. 26(2), 326–343 (2013)
15. Memon, N.A., Gilani, S.A.M.: Watermarking of chest CT scan medical images for content authentication. Int. J. Comput. Math. 88(2), 265–280 (2011)
16. Zhou, X., Huang, H.K., Lou, S.A.: Secure method for sectional image archiving and transmission[J]/Medical Imaging 2000: PACS Design and Evaluation: Engineering and Clinical Issues. International Society for Optics and Photonics 3980, 390–399 (2000)
17. Coatrieux, G., et al.: Relevance of watermarking in medical imaging. In: Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. ITAB-ITIS 2000. Joint Meeting Third IEEE EMBS International Conference on Information Technology, IEEE (2000)
18. Wang, X.: Medical image encryption based on biometric keys and lower-upper decomposition with partial pivoting. Appl. Opt. 60(1), 24–32 (2021)
19. Sokouti, M., et al.: Medical image encryption: an application for improved padding based GGH encryption algorithm. Open Med. Inform. J. 10, 11 (2016)
20. Shahzadi, R.: Chaos based enhanced RC5 algorithm for security and integrity of clinical images in remote health monitoring. IEEE Access 7, 52858–52870 (2019)
21. Chen, Y., et al.: Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. 167, 107286 (2020)
22. Hua, Z., et al.: Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. 144, 134–144 (2018)
23. Hua, Z., Zhou, Y.: Design of image cipher using block-based scrambling and image filtering. Inf. Sci. 396, 97–113 (2017)
24. Zhou, N.: Image compression encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt. Laser Technol. 82, 121–135 (2016)
25. Prakash, M., et al.: Synchronization of Markovian jumping inertial neural networks and its applications in image encryption. Neural Netw. 83, 86–95 (2016)
26. Liu, J.: A novel fourth order chaotic system and its algorithm for medical image encryption. Multidim. Syst. Sign. Process. 30(4), 1637–1657 (2019)
27. Dagadu, J.C.: Medical image encryption scheme based on multiple chaos and DNA coding. IET Secur. 21(1), 83–90 (2019)
28. Zanin, M., Pisarchik, A.N.: Gray code permutation algorithm for high-dimensional data encryption. Inf. Sci. 270, 288–297 (2014)
29. Zhang, Y., Xiao, D.: An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun. Nonlinear Sci. Numerical Simul. 19(1), 74–82 (2014)
30. Amritharanjan, R.: A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach. Med. Biol. Eng. Comp. 58(7), 1445–1458 (2020)
31. Ma, R.: A code division multiplexing and block classification-based real-time reversible data-hiding algorithm for medical images. J. Real-Time Image Process. 16(4), 857–869 (2019)
32. Al-Haj, A.: Secured telemedicine using region-based watermarking with tamper localization. J. Digit. Imag. 27(6), 737–750 (2014)
33. Cox, I.J.: Digital watermarking, vol. 53. Springer, Berlin (2002)
34. Fares, K., et al.: A robust blind color image watermarking based on Fourier transform domain. Optik 208, 164562 (2020)
35. Zainol, Z., et al.: A new chaotic image watermarking scheme based on SVD and IWT. IEEE Access 8, 43391–43406 (2020)
36. Hsu, C.-S., Tu, S.-F.: Enhancing the robustness of image watermarking against cropping attacks with dual watermarks. Multimedia Tools Appl. 79, 11297–11323 (2019)
37. Dagadu, J.C., Li, J.: Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. Multimedia Tools Appl. 77(18), 24289–24312 (2018)
38. Bouslimi, D., Coatrieux, G.: A crypto-watermarking system for ensuring reliability control and traceability of medical images. Signal Process.: Image Commun. 47, 160–169 (2016)
39. Peng, D.: The synchronization method for fractional-order hyperchaotic systems. Phys. Lett. A 383(13), 1427–1434 (2019)
40. Hao-Xiang, W.: Nonlinear feedback control of a novel hyperchaotic system and its circuit implementation. Chin. Phys. B 19(3), 030509 (2010)
41. Wang, X.Y.: An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access 6, 23733–23746 (2018)
42. Watson, J., Crick, F.: Molecular structure of nucleic acids: A structure for deoxyribosenucleic acid. JamaAMA 269(15), 1966–1967 (1993)
43. Wu, Y., et al.: Shannon entropy based randomness measurement and test for image encryption. arXiv:1103.5520 (2011)
44. Finlayson, G., et al.: Illuminant and device invariant colour using histogram equalisation. Pattern Recognit. 38(2), 179–190 (2005)
45. Seyedzadeh, S.M., Mirzakuchaki, S.: A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Process. 92(5), 1202–1215 (2012)
46. Lima, J., et al.: Encryption of medical images based on the cosine number transform. Signal Process.: Image Commun. 35, 1–8 (2015)
47. Fu, C.: An efficient and secure medical image protection scheme based on chaotic maps. Comput. Bio. Med. 43(8), 1000–1010 (2013)
48. Mildenberger, P., et al.: Introduction to the DICOM standard. Eur. Radiol. 12(4), 920–927 (2002)
49. Ghebleh, M., et al.: An image encryption scheme based on irregularly decimated chaotic maps. Signal Process.: Image Commun. 29(5), 618–627 (2014)
50. Liu, H., et al.: Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. IET Image Process. 11(5), 324–332 (2017)
51. Ye, G.: A chaotic image encryption algorithm based on information entropy. Int. J. Bifurcation Chaos 28(01), 1850010 (2018)
52. Wang, X., et al.: An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access 6, 23733–23746 (2018)