Multimedia Tools and Applications (2022) 81:11415–11440
https://doi.org/10.1007/s11042-022-12266-8

Medical images lossless recovery based on POB number system and image compression

Qingdan Li[1] · Yao Fu[1] · Zehui Zhang[1] · Abdul Joseph Fofanah[2] · Tiegang Gao[1]

Received: 24 March 2021 / Revised: 8 December 2021 / Accepted: 14 January 2022 /
Published online: 17 February 2022

Abstract

To protect the information integrity of the medical images, this paper proposes a secure lossless recovery scheme for medical images based on image block compression and permutation ordered binary (POB) number system, which includes two parts: share generation, and lossless recovery. In the shares generation stage, the region of interest (ROI) of the original medical image and the image block compression coding algorithm JPEG-LS, are firstly adopted to generate the compressed data, which can use limited storage space to place the data repeatedly. Then, after separating the bit-plane, the compressed data are executed by data reorganization and data encryption respectively on the high-plane and the low-plane. Finally, two authentication bits are extracted by 8-bit pixel of two planes to be inserted into the pixel itself, and then the 10-bit pixel is converted into an 8-bit POB value to produce two shares of *ShareH* and *ShareL*, respectively. In the lossless recovery stage, data of placing repeatedly can restore the original image. At the same time, three attacks are carried in the two shares, which contain *content cropping*, *content exchange*, and *text addition*. Some comparisons with other schemes present that the proposed scheme implements a better performance under some criteria. Theoretical analysis and experimental results demonstrate that the original image can be recovered losslessly even if two shares are tampered at the ration more than 50%.

✉ Tiegang Gao
gaotiegang@nankai.edu.cn

Qingdan Li
lqd18812745024@163.com

Yao Fu
FuYao_TJ@163.com

Zehui Zhang
zhangtianxia918@163.com

Abdul Joseph Fofanah
abduljoseph.fofanah@gmail.com

[1] College of Software, Nankai University, Tianjin 300350, China

[2] Milton Margai University of Education and Technology, Freetown, Sierra Leone

Keywords Lossless recovery · Permutation ordered binary (POB) number system · Block-wise compression · Image processing

1 Introduction

With the development of the internet and multimedia technologies, the transmission, acquisition and processing of digital images have become easier. However, the security of digital images is an important issue. Especially, medical image as a kind of digital image, which contain more information and each piece of information is very critical. For example, a damaged medical image may affect a doctor's diagnosis and endanger the patient's life. Therefore, there are many images encryption algorithms [23, 25, 26] and image steganography [27, 28] are proposed to ensure the security of images. In addition, to prevent the integrity of the image from being tampered with after encryption, the image recovery scheme has become a research hotspot.

The image watermarking algorithm is an effective method to recovery images information [3, 5, 7, 9–13, 15–20, 22, 29, 31–33]. The scheme [13] proposed a reversible watermarking algorithm based on a tamper localization mechanism, which allows selective rejection of distorted cover image regions in case of authentication failure. The advantage of the algorithm is a high resolution of tampering detection and results in minimal rejection of no tampered pixels. Additionally, Tai et al. [17] adopted the pseudocode for detection and smoothing technology for an effective self-embedding watermarking scheme. Wang et al. [22] proposed an image self-recovery with a watermark self-embedding algorithm in the hierarchical detection and recovery manner. However, the shortcoming of these reversible watermarking schemes is that they cannot guarantee the accurate restoration ability and tampering position performance of the original image at the same time.

Image compression algorithms can adopt limited storage space to save a larger amount of image data, which can effectively reduce the images data size of the same quality. Therefore, some watermarking schemes based on compression are proposed [1, 3, 5, 15]. The scheme [3] presented an intelligent model based on reversible watermarking techniques. The model was combined with compression, expansion, integer wavelet transforms (IWT), and genetic programming to find the best wavelet coefficients in the embedding process. Additionally, the scheme [5] presented a semi-fragile watermarking method with additional image recovery capabilities, which enhances security by correlating the embedded watermark with the approximate sub-wavelet transform. What's more, the lossless compression algorithm and the low-pass version of BCH coding were introduced to improve the capability of image recovery. Similarly, N. Sasikaladevi et al. [15] used a lightweight model named SNAP (SeNsitive image Authentication Protection) to minimize storage space by compression without any loss of data and speed up the encryption process without compromising security. However, the scheme of the technique failed to take the fastidiousness of medical images into account.

The medical image recovery scheme needs to pay more attention to the recovery effect which should try to be lossless recovery. Tampering with medical images might lead to wrong diagnosis, treatments, and could endanger the life of the patients. Medical images are divided into two categories: the regions of interest (ROI) and the regions of non-interest (RONI). Regarding ROI, it has a significant effect on diagnosis, while RONI has little effect. Concerning the regional features of medical images and the complex texture of ROI, Gao et al. [7] proposed a scheme to achieve the contrast enhancement of ROI without distortion. Zhang et al.

[32] proposed a robust watermarking algorithm based on ROI and IWT to authenticate and recover from the distorted medical images. The algorithm can precisely locate the distorted areas of an image and effectively recover the original ROI on the basis of verifying the reliability of the image. Moreover, the scheme [9] presented a tampering detection and recovery watermarking method based on ROI, which embeds the ROI bit information into the LSB of RONI. Essentially, the bit information will be extracted for authentication in the recovery process. The above schemes have achieved some excellent results in the tampering location and recovery. However, the shortcoming of these solutions is that they cannot guarantee the lossless restoration of the original image when the tampered area is large.

Recently, some related lossless recovery solutions have been proposed [10–12, 16, 18–20, 29, 31, 33]. Zhou et al. [33] proposed a novel lossless medical image encryption scheme, which adopts the method of game theory with optimized ROI parameters and hidden ROI position. Li et al. [10] proposed a scheme for protecting medical image key regions, which uses the quick response code and reversible data hiding technology. Additionally, Shi et al. [16] developed an algorithm for reversible medical image watermarking-based regions. Although the above methods have high privacy protection and integrity authentication capabilities, they cannot achieve the balance of high tampering and high recovery.

Secret sharing [11, 31] provides a method to divide a secret into two or more shares. Only by combining these shares can the original secret data being leaked. Yan et al. [31] proposed a visual secret image sharing threshold scheme, which adopts the random grids and Boolean operations method. Li et al. [11] proposed a new lossless secret sharing method of image steganography, which can recover the original secret image and cover image lossless to some extent.

Additionally, the Permutation Ordered Binary (POB) digital system has better performance in image reconstruction. At present, the use of secret sharing and POB for tampering detection and recovery has attracted the attention of researchers [12, 18–20, 29]. The work [19] presented by introducing an image encryption scheme based on the permutation ordered binary (POB) number system. Specifically, the image information was distributed in a complete random share and can be stored in a cloud data center. Moreover, the proposed scheme achieved authentication at the pixel level. What's more, if any tampering was made on the cloud server, the scheme could accurately identify the tampered pixel by the authentication bit. The proposed scheme [18] can not only detect and restore tampering areas at the pixel level but also use the characteristics of the POB number system to minimize the overhead bandwidth transmission. Singh et al. [20] and Xiang et al. [29], presented a secure image tampering detection and self-recovery scheme using the POB number system over the cloud server. Medical images were divided into several shares, which can generate the watermark by using SVD. Liu et al. [12] used image tampering detection and lossless recovery with the POB number system to conduct neighborhood refinement and watermark refinement. Experimental results indicated that the scheme achieved a better performance under certain criteria. However, the scheme has some challenges in recovering the large-scale tampering in the two shares. The method of the two-level comparison and the two-level refinement is complicated comprehensively.

To address the above drawbacks, this paper proposes a medical image lossless recovery scheme based on the POB number system and block compression. The scheme firstly extracts the ROI of the original image, divides ROI into 8×8 non-overlapping blocks by using the JPEG-LS image coding algorithm to perform block compression, and then combines the compressed data by all non-overlapping blocks. Executing the separate operation of the complete compressed data is to generate two planes. Consequently, the data reorganization

and the data scramble are conducted on the high plane, and the low plane, respectively. Meanwhile, the data has been placed repeatedly until the size of the original image, and then used encryption algorithm in each plane. Furthermore, two shares are generated using two authentication bits of each 10-bit pixel and POB algorithm. Theoretical analysis and experimental results show that the scheme can be recovered losslessly of the original images when two shares are subjected to different tampering attacks.

Apparently, the main contributions of this scheme are summarized as follows:

1) The characteristics of the POB number system and the two authentication bits make the detection of tampering area accurate. Furthermore, data placed repeatedly can realize lossless recovery of the original image. Experiments results show that the original image can be recovered losslessly when the two shares are not tampering.
2) Through some security performance analysis, the safety performance of the proposed scheme is verified, such as keyspace analysis, statistical analysis, differential analysis and Peak Signal-to-Noise Ratio (PSNR) analysis. In this work, the original image can be recovered losslessly through the method of one comparison and one refinement, which can demonstrate the effectiveness of medical images' lossless recovery.
3) Compared with state-of-the-art schemes, our contributions are that the original image can be recovered losslessly with a large number of tampering areas in the two shares. That is, the original image can be recovered losslessly even if two shares are tampered at the ration more than 50%.

The rest of this paper is organized as follows. Section 2 describes the basic theories of the scheme. In Section 3, the processes of shares generation, and lossless recovery are described in detail. Section 4 shows the experimental results and discussions. Finally, this paper is concluded in Section 5.

2 Preliminaries

In this section, we introduce some preliminaries about the JPEG-LS image compression, POB number system and image encryption.

2.1 JPEG-LS image compression

JPEG-LS is a lossless or near-lossless compression standard for the continuous-tone image proposed by the International Standards Organization ISO/IEC JTC1 [6, 8]. It is based on the low complexity of the lossless compression for images (LOCO-I) algorithm [6] and the contextual statistical model, which depends on a pixel prediction. Therefore, it has been widely used for image compression and image security [4, 14]. The more detailed description of JPEG-LS can be found in [8].

2.2 POB number system

In 2009, Sreekumar and Sundar [21] proposed the POB number system POB (n, r), where n represents the number of bits and r represents the number of 1 s in a string. Moreover, n and r are non-negative integral parameters, where nr. In this number system, all the values P(A) are

in the range 0, 1,. . ., $\binom{n}{r}-1$, and A is a binary string with r which can be represented as $A=a_{j-1}a_{j-2}...a_0$.

Each digit a_j of the binary string A_j is related to its position value j, where $v_j=\sum_{j=0}^{n-1} a_j$. Then, the POB value of P(A) can be obtained as follows:

$$\mathrm{P(A)} = \sum_{\mathrm{j=0}}^{\mathrm{n-1}} \mathrm{a_j} \binom{\mathrm{j}}{\mathrm{v_j}} \tag{1}$$

The representation of the POB (n, r) number is unique when the POB value is given. Thus, the POB numbers in binary form can be converted into the corresponding POB values and the POB values can be also converted into the corresponding POB numbers in binary. Since each pixel of the image is embedded in two authentication bits, the 10 bits POB (10, r) strings can be converted into 8 bits decimal equivalent POB values, which can range from 0 to 251. Using the POB number system, the 10 bits of each pixel are transformed into an 8-bit number. For example, 1,011,001,100 is a POB (10, 5) number, which transforms into a POB value of 186. On the contrary, a POB value of 87 is a POB (10, 5) number 0101110001.

2.3 Image encryption

In this stage, we can adopt all kinds of secure encryption algorithm. Referring to the refs [2, 24, 30], the Arnold scrambling algorithm and bi-direction diffusion algorithm based on modulo addition are used for encryption, and the key of image encryption is generated by the hyper-chaos Lorenz system.

2.3.1 Hyper-chaos Lorenz System

The initial value and parameter of the chaotic system are extremely sensitive, non-periodical, and long-term evolutionary orbit unpredictability, which corresponds to sensitivity, ciphertext, and plaintext sensitivity of the key in the image encryption system. Therefore, the chaotic system can be used to generate the key in the image encryption and image decryption system.

A four-dimensional hyper-chaos system is used to generate a pseudo-random sequence, and the Runge-Kutta method [24] is adopted to solve the following equations:

$$\begin{cases} \dot{x} = a(y-x) + w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + rw \end{cases} \tag{2}$$

where, x, y, z, and w are state variables; a, b, c, and r are system parameters. The number , as the mean of the value of the plaintext pixel, is used to update the initial values (x_0, y_0, z_0, w_0) and system parameters (a, b, c, r) of the hyper-chaos Lorenz system. When a=10, b=8/3, c=28,

-1.52≤r≤-0.06, the system represents a hyper-chaos state. When the r=-1, the four Lyapunov exponents of the formula (2) are $\lambda_1 = 0.3381$, $\lambda_2 = 0.1586$, $\lambda_3 = 0$, λ_4=-15.1752 in sequence. Meanwhile, the hyper-chaos system exhibits hyper-chaos behavior, and its phase diagram is shown in Fig. 1.

2.3.2 Arnold scrambling

Arnold pseudo-random matrix scrambling is a commonly applied algorithm in scrambling algorithms [2]. Original image P is expanded into a one-dimensional row vector, denoted as A. The Arnold matrix transforms the coordinate position $(1, j)$ in vector A to the new coordinate position (p, q). As shown in the formula (3):

$$\begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} 1 \\ j \end{bmatrix} \tag{3}$$

That is p=1+aj and q=b+(ab+1)j. Without considering the role of p and regarding ab+1 as a new random number a [30], the formula (3) can finally denote as q=b+aj. The Arnold scrambling algorithm is simulated and verified by Matlab, which shows that the efficiency of image encryption and image decryption.

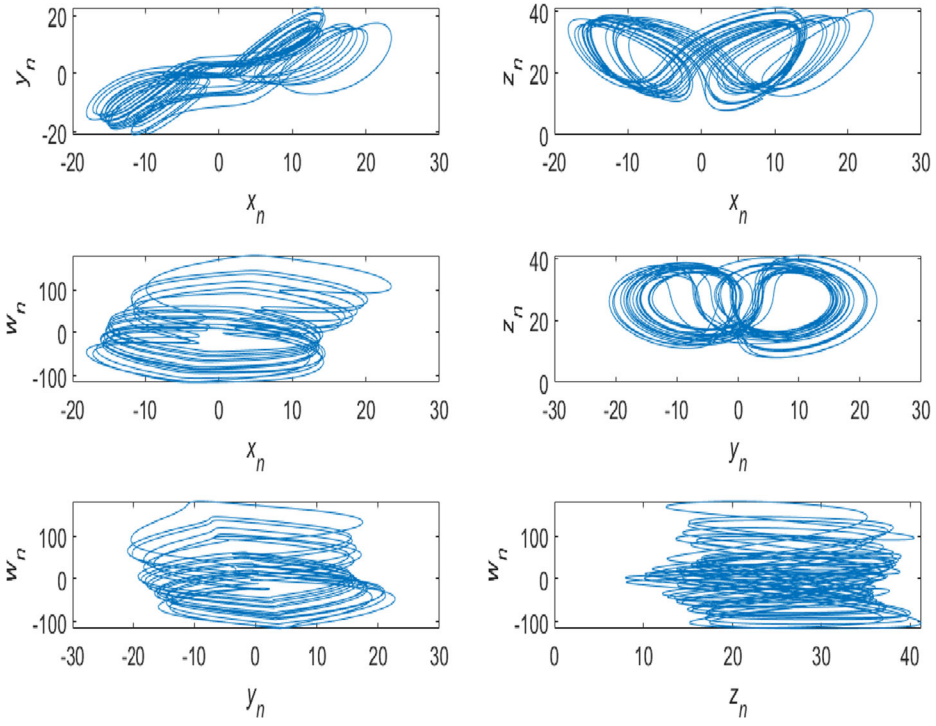


Fig. 1 Phase diagram of the hyper-chaos Lorenz system

2.3.3 Bi-direction diffusion based on modulo addition

The diffusion algorithm can diffuse the information of each pixel in the original image to the encrypted image. As shown in the formula (4) and (5), C represents the encrypted image, P represents the original image, and S represents the corresponding diffusion key in the bi-direction diffusion algorithm based on modulo addition.

Forward algorithm and its inverse algorithm formula:

$$\begin{aligned} C_i &= (C_{i-1} + S_i + P_i) \bmod 256 \\ P_i &= (2 \times 256 + C_i - C_{i-1} - S_i) \bmod 256 \end{aligned} \tag{4}$$

Inverse algorithm and its inverse algorithm formula:

$$\begin{aligned} C_i &= (C_{i+1} + S_i + P_i) \ \ 256 \\ P_i &= (2 \times 256 + C_i - C_{i+1} - S_i) \ \ 256 \end{aligned} \tag{5}$$

The bi-direction diffusion algorithm based on modulo addition is simulated and verified by Matlab, which shows that the pixel information of the original image is completely hidden by the pixels of the ciphertext image.

3 The proposed scheme

In this section, the detail of the proposed scheme is presented. Figure 2 depicts the basic flowchart of the proposed scheme, which includes two parts: share generation, and lossless recovery. To implement lossless recovery of the image, two shares are generated based on the POB number system and block compression. When the two shares are tampering, the method of two authentication bits and the repeated data can restore the data of the original image.

3.1 Generation of shares

The two shares involve some detailed steps to generate, which include ROI extraction, block-wise compression, bit-plane separation, data reorganization, image encryption, authentication bits embedded, and POB number system. Figure 3 shows the detail as follows.

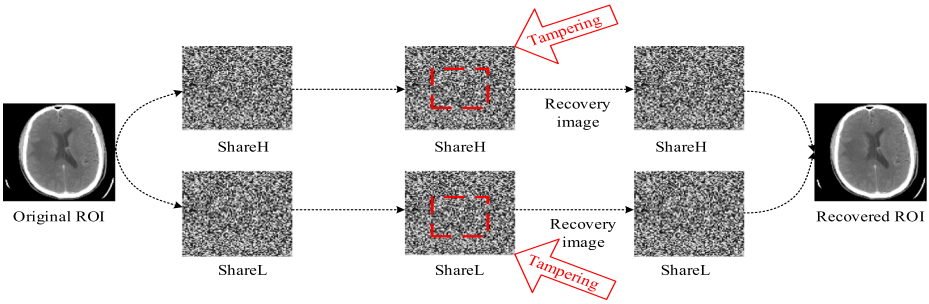


Fig. 2 The overall flowchart of the proposed scheme

3.1.1 ROI extraction and block-wise compression

In the proposed scheme, the ROI is firstly extracted from the original medical image by hand. Then the ROI is divided into some 8 × 8 non-overlapping blocks and the JPEG-LS algorithm is adopted to compress for each block. The compression algorithm can save the amount of compressed data in each small block for recovery. By compressing the ROI, substantial redundancies space could be obtained. Finally, the compressed data of each small block are connected as C, where the length is n. When n is odd, the n+1 can replace n to make separate data conveniently.

As shown in Fig. 4, by comparing to the original medical image, the number of pixels in the extracted ROI are reduced by half. For example, if the size of a medical image is 512 × 512, the number of pixels is 262,144. After extracting ROI, there are about 131,072 pixels. Then, the pixels are about 67,325 after compressing ROI. To acquire the 512 × 512 image, each data needs to at least appear (262,144/67,325)=3 times.

3.1.2 Bit-plane separation and data reorganization

In order to improve the tampering rate for the image, the separation of bit-plane is adopted to form two shares. Firstly, the compressed data C of the length n is divided into two 4-bit planes. The upper four bits and the lower four bits of each data are extracted to form two planes, which are called *High4plane* and *Low4plane*, respectively. In each plane, the new 8-bit data are produced by combining the first 4 numbers with the next 4 numbers. Then, the data are reduced by one time, and the two new 8-bit planes are called *High8plane* and *Low8plane*, respectively.

$$\begin{aligned} \text{High}8\text{plane(i)} &= 16 \times \text{High}4\text{plane(i)} + \text{High}4\text{plane(i} + 1) \\ \text{Low}8\text{plane(i)} &= 16 \times \text{Low}4\text{plane(i)} + \text{Low}4\text{plane(i} + 1) \end{aligned} \tag{6}$$

If the compressed data C is regarded as a matrix with the size of $n \times 8$, the reorganized data of *High8plane* and *Low8plane* can be expressed as shown in Fig. 5, respectively. From Fig. 5, the process of reorganization data can be obtained. Finally, the reorganized data could be

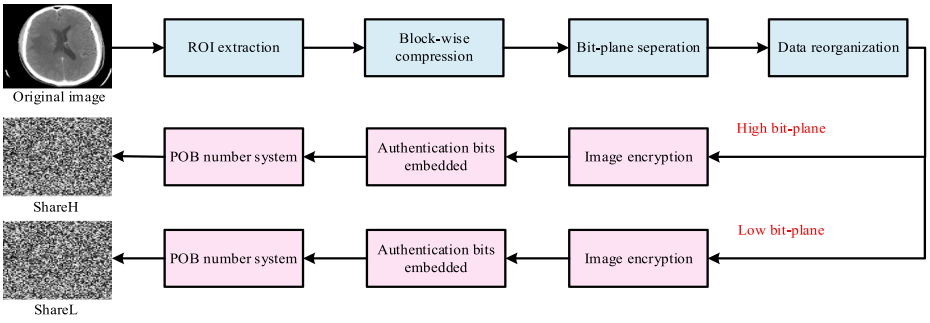


Fig. 3 The flowchart of shares generation

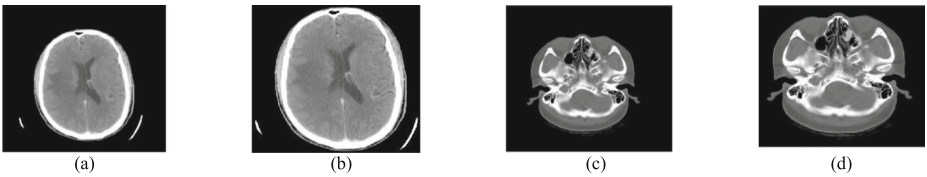


Fig. 4 The ROI of the original image. (**a**) (**c**) Original image (**b**) (**d**) Extracted ROI

converted into 8-bit data with a length of n/2, which names *High8plane* and *Low8plane* respectively.

3.1.3 Image encryption

Step 1: Two planes of reorganized data are scrambled by using the Arnold scrambling algorithm, and the key is generated by the hyper-chaos system.
Step 2: Each plane of data with a length of n/2 is placed repeatedly into the same size as the original image. That is, if the size of the original image is 512 × 512, the bit-plane data are placed repeatedly until the data fills the entire image size of 512 × 512. The specific repeated times could be found in Fig. 16.

Step 3: A bi-direction diffusion algorithm based on modulo addition operation is adopted to diffuse the above data of two planes, and the key is generated by the hyper-chaos system. Thus, two encrypted shares with the size of the original image are generated.

3.1.4 Embed authentication bits and POB number system

Primarily, two authentication bits are extracted from every 8-bit pixel of two encrypted shares. The first bit is labeled as the number of 1 s in the high four bits of the pixel, and when the odd number is 1, the even number is 0. The other bit is labeled as the number of 1 s in the low four bits of the pixel, and when the odd number is 1, the even number is 0. Subsequently, the two authentication bits are attached to the back of the 8-bit pixel, and finally, the 10-bit pixel is converted to an 8-bit POB value. The two shares of *ShareH* and *ShareL* are generated based on block-wise compression and the POB number system, respectively.

As shown in Fig. 6, for example, the decimal number 211 in the bit plane is 11,010,011, the upper 4 bits are 1101, and the lower 4 bits are 0011. Moreover, the number of 1 s in the upper

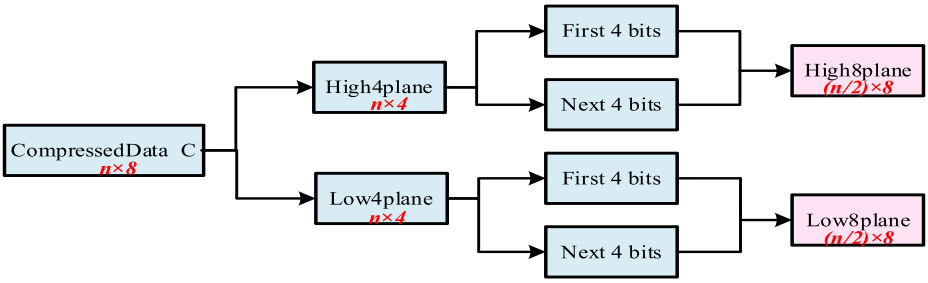


Fig. 5 The way of data reorganization

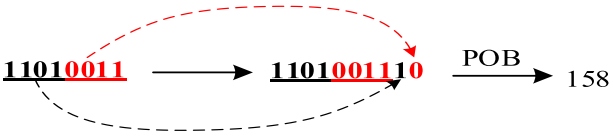


Fig. 6 The example for authentication bits embedding

4 bits is 3, and the number of 1 s in the lower 4 bits is 2. Therefore, by adding two authentication bits of 10, the pixel is 1,101,001,110, which could convert into a POB value of 158.

3.2 Lossless recovery

To protect the information of the medical image, it's necessary to conduct the method of lossless recovery. The flowchart of lossless recovery is illustrated in Fig. 7.

The three most common tampering attacks for images include *content cropping*, *content exchange*, and *text addition*, which are more misleading to modify the image content. The rest of the modification methods, such as blurring, compression, enhancement, scaling, filtering, etc., which fail to modify the content of the image. Most of them are post-processing operations to cover the traces of image tampering, which is less harmful. Thus, this paper applies three common tampering operations: *content cropping*, *content exchange*, and *text addition*.

3.2.1 POBN algorithm and extract authentication bits

The two shares of *ShareH* and *ShareL*, are generated based on the POB number system in the end. Therefore, it is significate to initialize the use of the inverse POB algorithm to recover the 10-bit number. The details are given in Algorithm 1, which is called POBN. Then, the two authentication bits are extracted to save in the array. After removing the two authentication bits from the 10-bit number, the 10-bit data could become 8-bit data.

ALGORITHM 1: [POBN: Generate POB number corresponding to the given POB value]

Input: n, r, and v, where $r \le n$ and $0 \le v \le \binom{n}{r} - 1$.

Output: The POB number $A = a_{j-1}\, a_{j-2} \ldots a_0$.

1. Let $j = n$ and $temp = v$.
2. **for** $k = r$ down to 1 do:
3. **repeat** {
4. $j = j - 1$;
5. $p = \binom{j}{k}$;
6. **if** ($temp \ge p$)
7. $temp = temp - p$;
8. $a_j = 1$;
9. **else** $a_j = 0$;
10. } **until** ($a_j = 1$) ;
11. **if** ($j > 0$)
12. **for** $k = j - 1$ down to 0 do:
13. $a_k = 0$;
14. **end**
15. **return** A.

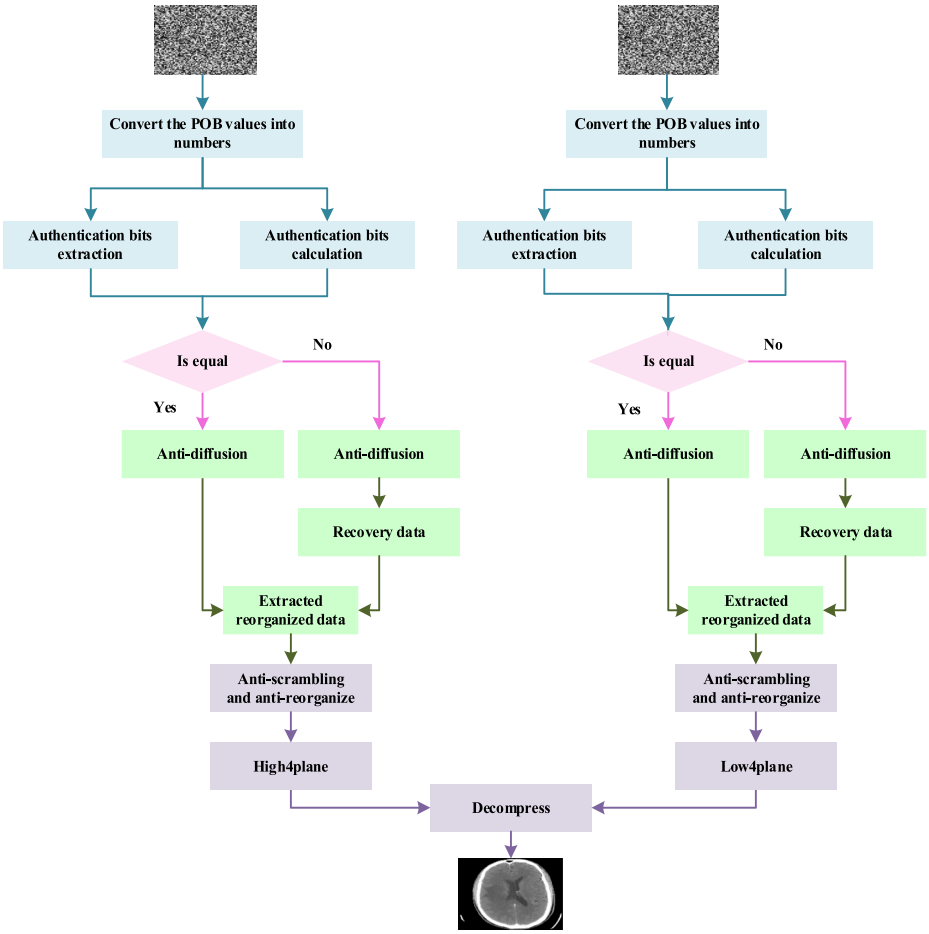


Fig. 7 The flowchart of lossless recovery

3.2.2 Data recovery and image decryption

Since the last two bits of every 10 bits in the POB number are embedded by authentication bits, two authentication bits are easily extracted from the 10 bits POB number. Meanwhile, two authentication bits are also calculated by statistical method for the number 1 s of the high 4-bit and the low 4-bit, respectively. The calculated value is labeled 1 when the number is odd, while the value is labeled 0. Compared with the two groups' values of the extracted authentication bits and calculated authentication bits, the tampering area is detected by the comparison result, which is marked by *Detect_T*. When the pixel is tampered with, the value of *Detect_T* is 0. On the contrary, the value of *Detect_T* is 1. The same operation is performed on *ShareH* and *ShareL*, respectively.

After removing the authentication bits, the anti-diffusion algorithm adopts the same key as shares generation in the image decryption process. Since the diffusion algorithm can only change the value of pixels, the position of pixels is not changed. The tampering detection array

ALGORITHM 2: [Recovery Data: recover reorganized data by data comparison and data refinement]

```
Input: High8planeD, Detect_T
Output: ReorganizedH, Detect_R
(1) High8planeD and Detect_T of ShareH, are decrypted data and tampered detection array with the size of M×N.
(2) ReorganizedH and Detect_R of ShareH, are reorganized data and recovered detection array with the size of L.
1. Read High8planeD
2. Number←floor(N×M/L) % The times of every data appear in the ShareH.
3. for i= 1 up to L do:
4. repeat {
5.   If (Detect_T(i + (Number − 1) ×L)==0) % It means the pixel is tampered.
6.   |  …
7.   |  If (Detect_T(i + L)==0) % It means the pixel is tampered.
8.   |  |  If (Detect_T(i)==0) % It means the pixel is tampered.
9.   |  |  |  Detect_R(i) ← 0 % It means that tampering cannot be recovered.
10.  |  |  |  ReorganizedH (i) ← High8planeD (i) % Extracted data.
11.  |  |  Else
12.  |  |  |  Detect_ R (i) ← 1 % It means that tampering can be recovered.
13.  |  |  |  ReorganizedH (i) ← High8planeD (i) % Extracted data.
14.  |  |  End
15.  |  Else
16.  |  |  Detect_ R (i) ← 1 % It means that tampering can be recovered.
17.  |  |  ReorganizedH (i) ← High8planeD (i + L) % Extracted data.
18.  |  End
19.  |  …
20. Else
21.  |  Detect_ R (i) ← 1 % It means that tampering can be recovered.
22.  |  ReorganizedH (i) ← High8planeD (i + (Number − 1) ×L) % Extracted data.
23. End
24.  } until (j > L);
25. End
```

of *Detect_T*, POB algorithm, and repeated data in shares generation can apply to recover the reorganized data. The reorganized data are extracted by the one-level comparison and one refinement. Some details are shown in Algorithm 2, and an array of *Detect_R* is generated to judge whether the pixel can finally be restored. Moreover, the same scramble key is used for the anti-scrambling algorithm. Two groups of reorganized data are generated for image lossless recovery.

3.2.3 Bit-plane anti-reorganization and block-wise de-compression

The same operation performs on *ShareL* and then the reorganized data of *ReorganizedL* are generated. Initially, the *ReorganizedH* data are extracted from the first-4 bits and next-4 bits to obtain the *High4plane* of the compressed data, where the data size is from n/2 to n. Then the plane from 8-bit to 4-bit, and the *High4plane* and *Low4plane* can be restored, respectively. Some details are given in Fig. 8. The compressed data are generated by combining *High4plane* and *Low4plane*. Finally, the original data of the image are recovered by block-wise de-compression of the compressed data. The ROI of the original image could be obtained and the original image could be recovered losslessly.

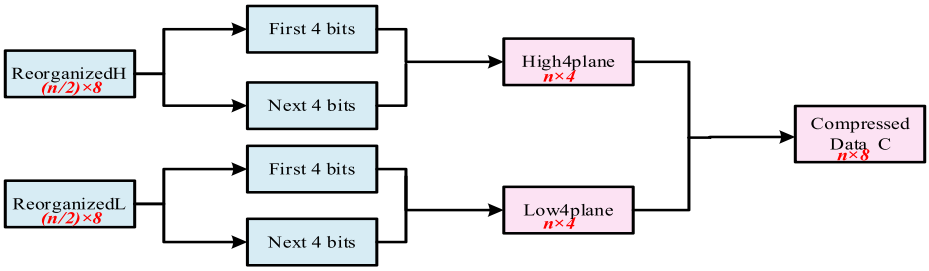


Fig. 8 The way of data anti-reorganization

4 Experimental results and analysis

The experiments are implemented on a computer with a 2.20 GHz Intel i5 processor, 8.00GB memory, and Windows 10 operating system. The Matlab R2019a is used for programming. The medical images with different formats and sizes from the Brain-CT, Chest-CT dataset and the COVID-CT dataset [32] are used for the test. Among them, the COVID-CT-Dataset has 349 CT images containing clinical findings of COVID-19 from 216 patients. Some typical images are shown in Fig. 9.

4.1 Experimental results

In the experiments, when the two shares have not been tampered with, the original ROI can be recovered without any loss of information. Figure 10 shows the lossless recovery of the original medical image with no tampering.

4.2 Security analysis

In this section, in order to evaluate the security of the proposed scheme, we analyze in terms of keyspace, pixel distribution, gray histogram, information entropy, neighboring pixel correlation, differential analysis, and peak signal-to-noise ratio (PSNR). Here, the encrypted image of *ShareH* is used for testing.

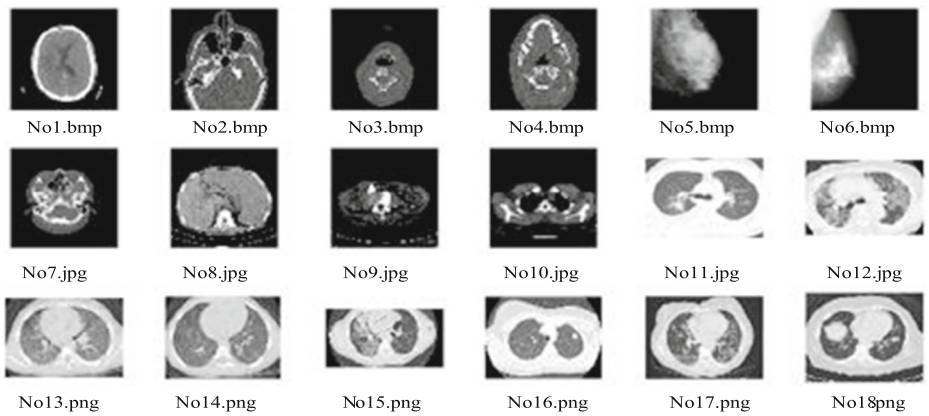


Fig. 9 The image of the proposed scheme

4.2.1 Key space analysis

Firstly, from the description of the proposed scheme, the key of scrambling algorithm is set to x_0=1.1, y_0=2.2, z_0=3.3, w_0=4.4; and the system parameters are a=10, b=8/3, c=28, r=-1. The initial value of the chaotic system are double-precision numbers, so the key spaces are $(10^{16})^4 = 2^{129}$. Secondly, the 10 bits POB (10, r) strings are converted to the POB values of decimal equivalent, which can range from 0 to $\binom{n}{r}-1$. When n is 10 and r is set to be 4, the POB values have 210 possibilities. For an image with the size of $M \times N$, the successful probability of guessing the shares is $\left(\frac{1}{210}\right)^{M \times N}$. Lastly, the diffusion algorithm has the same size of the keyspace as the scrambling algorithm. Thus, in the proposed scheme, the size of the keyspace can effectively resist brute force attacks.

4.2.2 Statistical analysis

(1) Pixel Distribution

Three-dimensional (3D) pixel distribution of an image as a significant characteristic in statistical analysis, can describe the distribution characteristics of image pixel values in the three-dimensional space.

The x-y plane represents pixel coordinates and the ordinate represents the value of image pixels. For an effective.

encrypted image system, the 3D pixel distribution of the encrypted image should be as evenly distributed as possible to resist statistical analysis. Figure 11 shows the experimental results that the 3D distribution of the proposed scheme can resist statistical attacks.

(2) Histogram

As a significant characteristic in statistical analysis, the image histogram describes the intensity of the gray value of an image by calculating the intensity of pixels. An effective good encrypted image system should be as flat as possible in order to resist statistical analysis. The corresponding histogram of the original image, two shares are shown in Fig. 12. It can be observed that the histogram of the proposed scheme can resist statistical attacks. However, due to a large number of pixels with 0 values in the medical image, the histogram is not flat enough.

(3) Correlation

As a meaningful visual medium, an image has a high correlation between adjacent pixels in horizontal, vertical and diagonal directions. It is important for an image encryption algorithm to break the strong pixel correlation in the encryption process. Generally, the correlation coefficient between adjacent pixels in the original image is very high, while the correlation coefficient of the encrypted image is low. This is why the encrypted image looks like a noisy image. The correlation between adjacent pixels can be calculated by the formula (10).

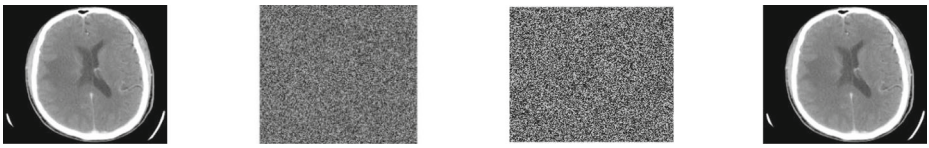


Fig. 10 Result of no tampering. (**a**) Original ROI (**b**) (**c**)POB shares (**d**) recovered ROI

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{8}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(x)) \tag{9}$$

$$\gamma_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{10}$$

where x and y represent the pixel values of two adjacent pixels, N represents the total number of selected adjacent pixel pairs.

To analyze and compare the correlation of adjacent pixels between original and encrypted images, we randomly select 4000 pairs of adjacent pixels at the horizontal, vertical, and diagonal directions of the original image and encrypted image. The correlation distribution is shown in Fig. 13, which proves that the encryption image can break the correlation of the original image. Obviously, the adjacent pixels of the original image have a strong correlation while the adjacent

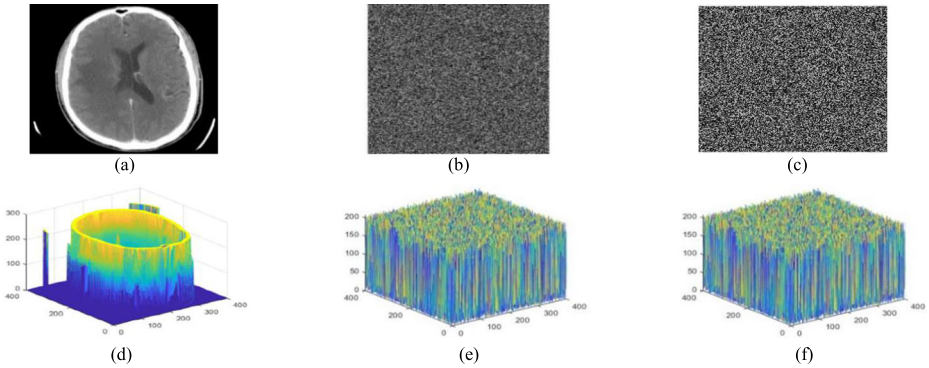


Fig. 11 Pixel distribution of the image. (**a**) Original ROI (**b**) (**c**) POB shares (**d**) pixel distribution of the original ROI (**e**) (**f**) pixel distribution of the POB shares

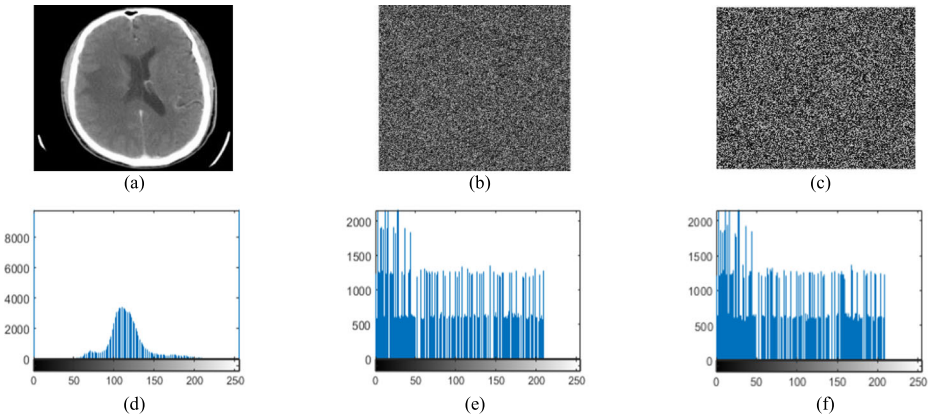


Fig. 12 Histogram of the image. (**a**) Original ROI (**b**) (**c**) POB shares (**d**) histogram of original ROI (**e**) (**f**) histogram of POB shares

pixels of the encrypted image has a low correlation. Then we calculate the adjacent pixels' correlation coefficient of the original image and encrypted image in horizontal, vertical, and diagonal directions. The results are shown in Table 1, which can clearly see that the correlation coefficients of the original images are close to 1 while the encrypted images are around 0 in all directions. This further proves that the scheme can effectively resist statistical attacks.

(4) Information Entropy

Information entropy is an efficient criterion to measure the randomness of an information source. For an effectively encrypted image with 256 Gy level, the value of information entropy should be close to 8. The definition of information entropy shows in formula (11), where β represents the information source, N represents the number of bits corresponding to β, and P(β) represents the probability of β.

$$\mathrm{H}(\beta) = \sum_{i=0}^{2^N-1} \mathrm{P}(\beta i) \log \frac{1}{\mathrm{p}(\beta i)} \tag{11}$$

Experimental results show that the value of information entropy in ROI image is 4.5214, the value of *ShareH* is 7.2195, and the value of *ShareL* is 7.2175, which can provide sufficient security to resist statistical attacks.

4.2.3 Differential analysis

Apparently, the differential attack as a chosen-plaintext attack is a classic type of attack. For an effective image encryption algorithm, any slight change in the original image should be able to make big differences between encryption images. NPCR (number of pixels change rate) and UACI (unified average changing intensity) are two common indicators to evaluate the differential attack performance of an encryption algorithm. NPCR and UACI are tested by changing the value of one pixel in the original image. In an ideal state, the NPCR is closer to 99.60% and the UACI is closer to 33.46%. After calculating the formula (12) and formula (13), the value of the proposed scheme is closer to the ideal value.

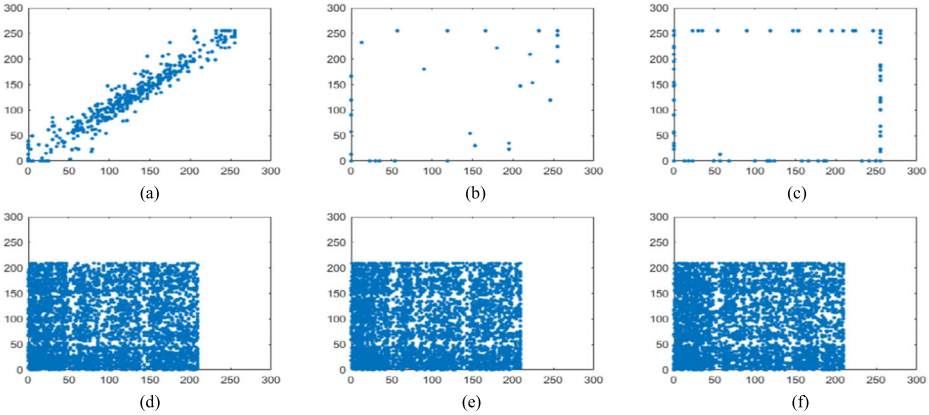


Fig. 13 Correlation of image. (**a**) Original ROI (**b**) (**c**) POB shares (**d**) correlation of original ROI (**e**) (**f**) correlation of POB shares

$$\mathrm{NPCR} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \mathrm{D}(\mathrm{i},\mathrm{j}) \times 100\% \tag{12}$$

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \frac{|\mathrm{C1}(\mathrm{i},\mathrm{j}) - \mathrm{C2}(\mathrm{i},\mathrm{j})|}{255} \times 100\% \tag{13}$$

$$D(i,j) = \{array0C1(i,j) = C2(i,j)1C1(i,j) \neq C2(i,j) \tag{14}$$

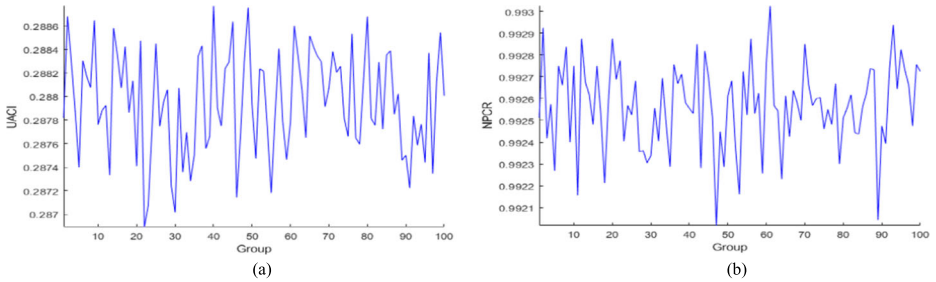
Taking account of 100 experimental data, the average value of UACI is 28.80% and NPCR is 99.26% in *ShareH*. Furthermore, the average value of UACI is 28.67% and NPCR is 99.76% in S*hareL*. Experimental results of *ShareH* are shown in Fig. 14, which shows great performance in the case of resisting differential attacks.

4.2.4 Structural Similarity Index Metrics (SSIM) Analysis

The structural similarity index metrics (SSIM) is a widely used image quality evaluation index. It is based on the assumption that the human eye will extract structured information when viewing an image, and it can better reflect the subjective feeling of the human eye. The calculation is complicated, and the general value ranges from 0 to 1. When the SSIM value of the image is larger, the image distortion is smaller.

Table 1 Correlation coefficients of horizontal, vertical, and diagonal

direction	horizontal	vertical	diagonal
Original ROI	0.9973	0.9612	0.8828
ShareH	0.0191	0.0215	0.0216
ShareL	0.0101	0.0214	0.0394



(a) (b)

Fig. 14 CNPCR and UACI of the *ShareH*

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(\sigma_{xy} + c_2\right)}{\left(\mu_x^2\mu_y^2 + c_1\right)\left(\sigma_x^2\sigma_y^2 + c_2\right)} \tag{15}$$

where x and y are two images, μ_x and μ_y represent the average of x and y respectively, σ_x and σ_y represent the variance of x and y respectively, and σ_{xy} is the covariance of x and y. And c_1, c_2 are constants to maintain the stability of the system.

Experimental results show that the value of SSIM is 0.0044 in *ShareH* and the value of SSIM is 0.056 in *ShareL*, which can prove the better performances of the proposed scheme.

4.2.5 Peak Signal-to-Noise Ratio (PSNR) analysis

The peak signal to noise ratio (PSNR) and the mean square error (MSE), are adopted to detect the difference between encrypted image and original image. Apparently, the larger PSNR between the encrypted image and the original image is, the less similar they are. The PSNR and MSE can be calculated as follow.

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} (\mathrm{P(i,j)} - \mathrm{C(i,j)})^2 \tag{16}$$

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{\mathrm{I}_{\max}^2}{\mathrm{MSE}}\right) \tag{17}$$

where $M \times N$ is the size of the image, P(i,j) is the gray value of the pixel in the original image, C(i,j) is the gray value of the pixel in the encrypted image, and $I_{\max}$ is the maximum pixel value of the original image.

Experimental results show that the value of PSNR is 7.9960 in *ShareH* and the value of PSNR is 7.9955 in *ShareL*, which can prove the better performances of the proposed scheme.

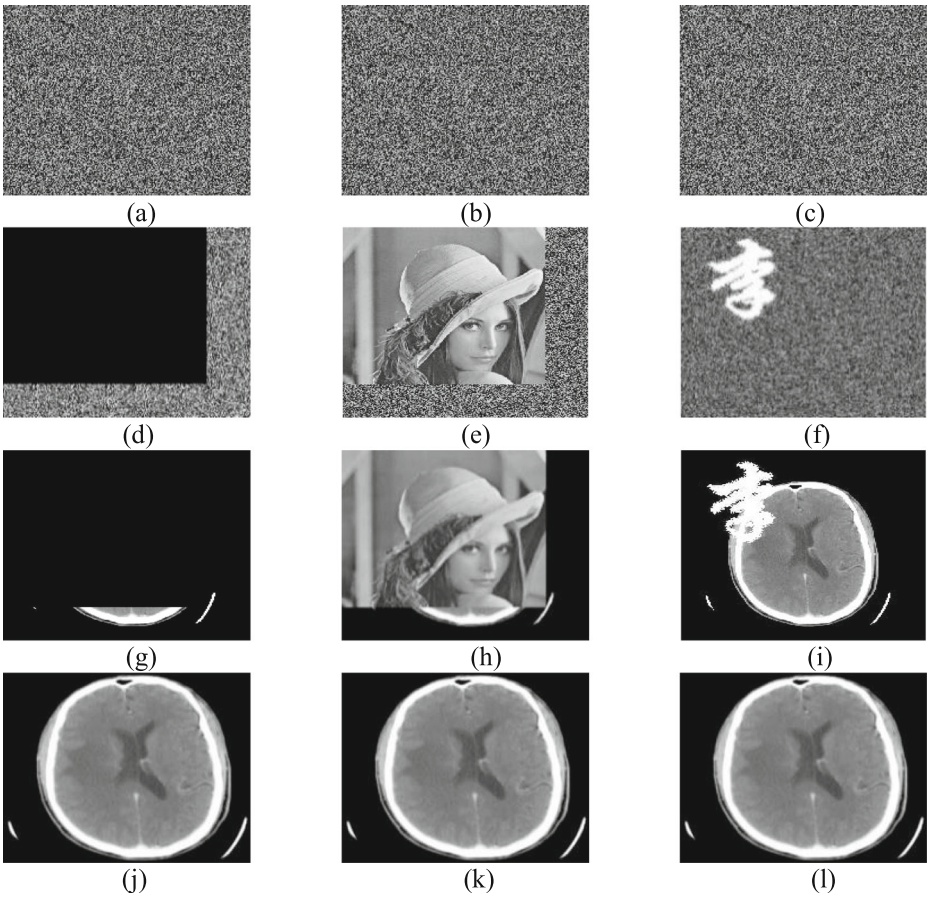


Fig. 15 Result of one share attacks. (**a**)-(**c**) the ShareL (**d**)-(**f**) the ShareH of content cropping, content exchange, and text addition. (**g**) recovered content cropping (**h**) recovered content exchange (**i**) recovered text addition (**j**)-(**l**) recovered ROI

4.3 Recovery evaluation

To verify the performance of the lossless recovery, attack tests are conducted. Firstly, the *ShareH* is conducted by three attacks. As shown in Fig. 15, the attacks contain *content*

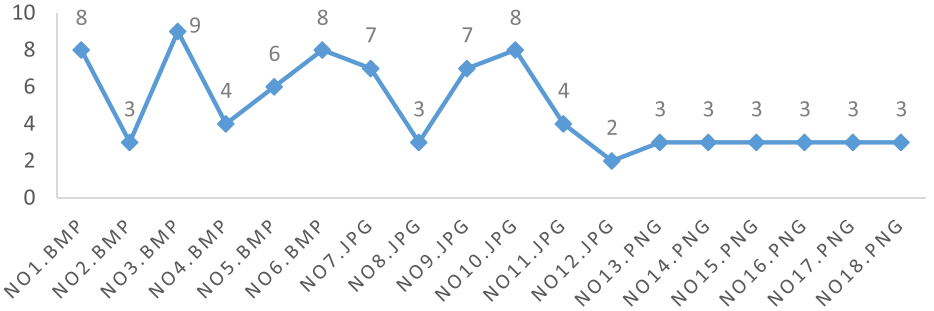


Fig. 16 Repeat times of the image data in *ShareH*

cropping, *content exchange*, and *text addition*. The first column is cropping a block with the size of 422 × 422 from the left corner; the second column is replacing a block with the size of 422 × 422 by 'Lena' content from the left corner; the third column is embedding text 'Li' with the size of 283 × 283 from the left corner. Furthermore, the experiments in the *ShareL* are obtained the same results, which shows that the ROI can be recovered losslessly when one of two shares are suffered three attacks of *content cropping*, *content exchange*, and *text addition*.

The same test is performed on 18 images with different sizes and different formats. Experimental results show that the extraction of ROI, compression algorithm, and the features of POB, make a large amount of redundant space for placing the image data. As shown in Fig. 16, the image data can be placed repeatedly average of 5 times. Thus, satisfactory restored results can be obtained by the proposed scheme.

Similarly, the three-type attacks on 18 images can be found that the tampering rate of the forward *content cropping* can reach up to 66.4%, the tampering rate of backward *content cropping* can reach up to 77.7%, the tampering rate of *content exchange* with 'Lena' also achieve to 66.4%, and the *text addition* accordingly to the corresponding image size can be restored. The results of *content cropping* are shown in Fig. 17, it can be inferred that medical images can be recovered even if the tampering rate of *content cropping* is more than 50% in the two shares.

Then, two shares have been conducted the attacks. As shown in Fig. 18, when two shares are tampered with more than 50% at the same time, the image can still be restored. The first column is the content cropping in the two shares; the second column is the content exchange in the two shares; the third column is the text addition in the two shares.

Finally, some tests are conducted with no regular tampers in the two shares. Figure 19 presents the experimental results of *content clipping* with no regular tampers in the two shares, which proves the high performance of recovery. The first row is *content cropping* with the tampered size of 422 × 422 in the two shares; the second row is *content cropping* with the tampered size of 370 × 370 in the two shares. In more detail, by conducting different kinds of attacks on 18 test images, the experiment results are summarized in Table 2. From Table 2, it can be observed that our scheme can recover the original image losslessly with varying tampering ratios of 10%, 20%, 30%, 50%, 55%.

4.4 Analysis and comparisons of the proposed scheme with other schemes

To illustrate the performance of the proposed scheme, analysis and comparisons are conducted compared with other schemes, which thus shows that our proposed scheme performs better.

4.4.1 Analysis of the proposed scheme

According to our experimental results, the proposed scheme can recover the ROI of the medical image in different image sizes and formats when two shares have tampered with more than 50%. Among them, the experimental results with the theory can be discussed and analyzed. The JPEG-LS coding shows strong compression performance for medical images. Through experiments on a large number of medical images, even if the ROI is the original image itself, the image data after JPEG-LS compression reduces at least 50%. Then, the compressed data is divided into two planes and reorganized within the plane, which leads to the data decreased by 50%. Thus, even if the ROI is the original image itself, the ROI still can be recovered when the two shares are tampered with 75% in theory. However, the medical

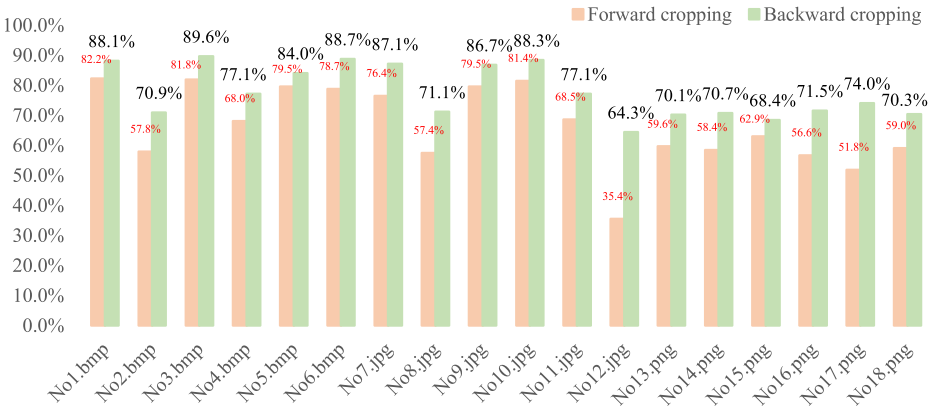


Fig. 17 Content cropping of the *ShareH*

image actually has a lot of black redundancy, its ROI will also decrease by 50% of image data. Therefore, this scheme can recover the original image when the two shares are tampered with more than 50%. Theoretical analysis and experimental results show that the proposed scheme can provide sufficient validity.

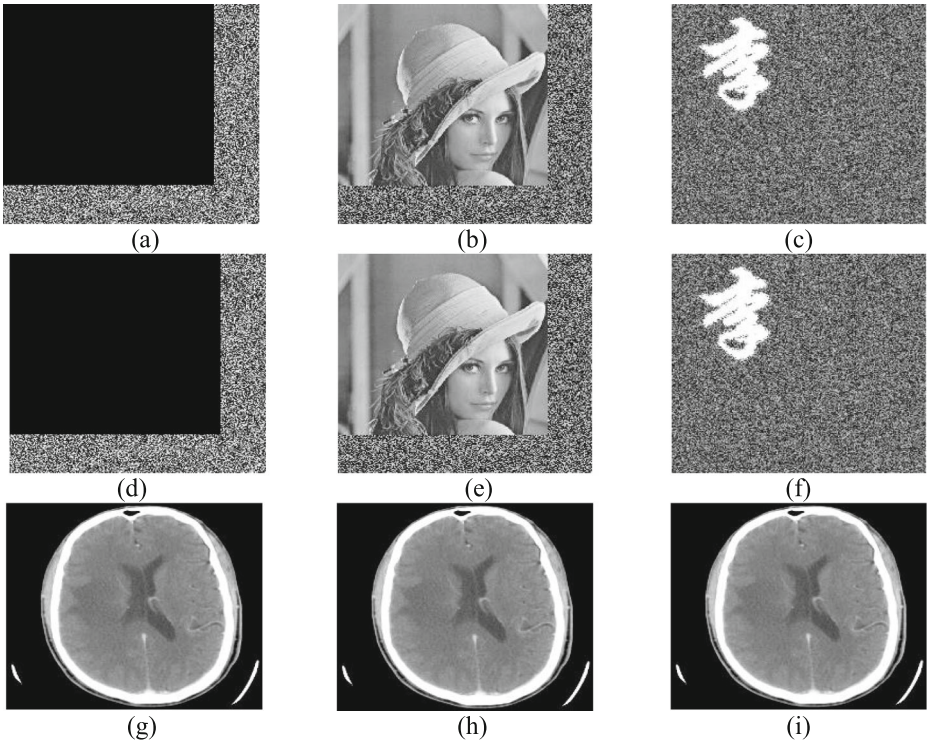


Fig. 18 Result of two shares attacks. (**a**)(**d**) content cropping (**g**) recovered ROI (**b**)(**e**) content exchange (**h**) recovered ROI (**c**) (f)text addition (**i**) recovered ROI

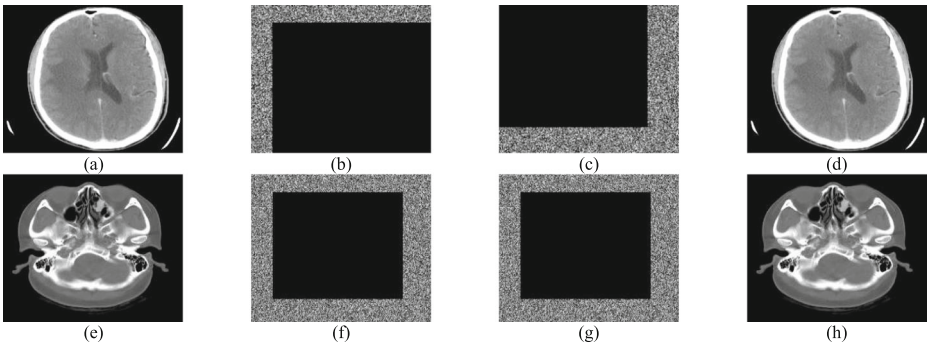


Fig. 19 Result of two shares with no regular tampers. (**a**) (**e**)original image(**b**)(**c**) (**f**)(**g**) content cropping (**d**) (**h**)recovered image

As compression and reorganization increase the space of plane, the data can be stored repeatedly. According to the same data in different locations, the compressed data are easily restored losslessly. As shown in Fig. 16, the experimental results show that the data can be placed repeat on average of 5 times.

Although it is possible to restore original images when the two shares are tampered with more than 50%, this scheme still has shortcomings. Since the data is not exchanged between the high plane and low plane during the recombination, one of the shares completely tampered with is not recovered. And when the size of medical images is too small, the original image cannot be recovered. That is because, there is challenging to compress not relevant pixels in the JPEG-LS compression algorithm. Such as the medical image of 6%3.jpg from the COVID-CT dataset, where the size of the image is 176 × 120. Through experiment, the compressed data of the original image are too large to replace repeatedly.

4.4.2 Some comparisons of the proposed scheme with other schemes

A comparative study of the proposed scheme with some existing algorithms in the encrypted domain based on various criteria are described as follows.

(1) *Structural Similarity Index Metrics (SSIM)*: The SSIM can measure the secure performance of the encrypted image. Similarly, the SSIM also can be introduced to measure the recovery performance of the original image. When the two images in SSIM are replaced with the original image and the restored image, the value of the SSIM can be used to evaluate the degree of recovery for the image.

Experimental results show that the value of SSIM between original image and

Table 2 Result of lossless recovery for original image

Tampered ratios in *ShareH*	Tampered ratios in *ShareL*	Whether the original image is recovered losslessly
10%	10%	√
20%	20%	√
30%	30%	√
50%	50%	√
55%	55%	√

Table 3 Comparison with other schemes in the one share tampered

PSNR (dB)TR	Schemes	10%	20%	30%	50%
Restored image	[17]	<∞	<∞	<∞	<∞
	[22]	<∞	<∞	<∞	<∞
	[20]	<∞	<∞	<∞	<∞
	[29]	43.37	40.12	38.24	36.17
	[12]	∞	∞	∞	∞
	Proposed	∞	∞	∞	∞

restored image is 1, which further illustrates that the proposed scheme is a lossless restoration

(2) *The Peak Signal to Noise Ratio (PSNR)*: The PSNR can measure the secure performance of the encrypted image. Similarly, the PSNR also can be introduced to measure the recovery performance of the original image. When the two images in PSNR are replaced with the original image and the restored image, the value of the PSNR can be used to evaluate the degree of the recovery for the image.

As shown in Tables 3 and 4, when one share and two shares have tampered with different tampering rates, the image of our scheme can be restored losslessly while other schemes cannot. At the same time, the scheme [32] achieved the maximum PSNR value of 51.24 in the COVID-19 dataset. The proposed method [17, 20, 22, 29] can only achieve recovery with a specific value, which cannot achieve the PSNR value of ∞. Although scheme [12] can reach ∞ when one share is tampered with, it cannot reach the target value when two shares are tampered with. All of the baselines [12, 17, 20, 22, 29] recovery methods of the image can be described in Table 5. The proposed method of the PSNR value ∞ in all cases is excellent, which proves that the scheme has better results in terms of lossless recovery. Tables 3 and 4 summarize the PSNR values with different tampered rates in one share and in two shares. Since there is no difference between the restored image and the original image, the PSNR values of our scheme are ∞ while the PSNR values of other schemes are not more than 50 (dB). Experiments exhibit that the proposed scheme has high performance in terms of restoring the tampered image compared with other schemes.

Moreover, the following indicators can detect the restoration characteristics of image. By comparing with other schemes, it is found that this scheme has better performance in terms of effectiveness.

(3) *The mode of recovery (MR)*: The indicator describes the technique to restore the image.

Table 4 Comparison with other schemes in the two shares tampered

PSNR (dB)TR	Schemes	10%	20%	30%	50%
Restored image	[17]	<∞	<∞	<∞	<∞
	[22]	<∞	<∞	<∞	<∞
	[20]	<∞	<∞	<∞	<∞
	[29]	<∞	<∞	<∞	<∞
	[12]	<∞	41.23	36.31	30.23
	Proposed	∞	∞	∞	∞

Table 5 Comparison with other schemes

Criteria	*MR*	*Q*	*BA*	*LTD*	*LR*
[17]	Pseudocode for detection and smoothing	Lossy	Yes	Block	Block
[22]	Hierarchical detection and recovery	Lossy	Yes	Block	Block
[20]	POB based secret sharing	Lossless	Yes	Block	Block
[18]	POB numbers of compacted pixel values	Lossless	Yes	Pixel	Block
[29]	None	None	Yes	Pixel	Block
[12]	Two-level comparison and two refinements	Lossless	Yes	Block	Block
Proposed	One-level comparison and one refinement	Lossless	Yes	Pixel	Pixel

(4) *The quality (Q)*: It describes the quality of the restored image, which is classified as 'Lossless', 'Slightly Lossy', and 'Lossy'. If the restored image is identical to the original image, the quality is called 'Lossless'. And if the PSNR value of the restored image is near 40 (dB), which is called 'Slightly Lossy', and the rest types are called 'Lossy'.

(5) *Blind authentication (BA)*: This indicator refers to the scheme whether used the share plane information to detect the tampers.

(6) *Level of tamper detection (LTD)*: When the way of tampering detection is image, it is called 'image' level; when the way of tampering detection is block, it is called 'block' level; when the way of tampering detection is pixel, it is called 'pixel' level.

(7) *Level of recovery (LR)*: When the way of recovering is image, it is called 'image' level; when the way of recovering is block, it is called 'block' level; when the way of recovering is pixel, it is called 'pixel' level.

Table 5 presents the results of indicators in different schemes. The schemes [17, 22] cannot recover the tampered image losslessly. Among the schemes [12, 29], the way of tampering detection for image is conducted by block. Moreover, the way of recovering for image is conducted by block in the schemes [18, 20]. There are not enough precise detection and recovery, so this cannot assure the lossless recovery, while our scheme could recover the images losslessly by conducting the tampering detection and recovering of pixel. What's more, this scheme adopts an effective algorithm to achieve better performance in tampering detection and lossless recovery for the image.

Experimental results show that this scheme has better performance than other schemes. This scheme has the.

following three advantages compared with the scheme [12]:

(1) The proposed scheme can achieve lossless recovery when one of two shares are tampered with more than 50%, which is the same as the reference [12].

(2) The proposed scheme can achieve lossless recovery when two shares are tampered with more than 50%. But this can't be achieved in reference [12]. Theoretical analysis and experimental results prove that the proposed scheme has better performance in terms of effectiveness and lossless recovery.

(3) Compared with the two-level comparison and two-level refinement in reference [12], the proposed scheme only needs one-level comparison and one-level refinement to recover the original image.

5 Conclusions

In this paper, a novel lossless recovery scheme for medical images is proposed. Original medical image is divided into two shares by POB number system and blocks compression JPEG-LS coding. In addition, two authentication bits are applied during embedding to detect the tampering position of shares. The data placed repeatedly are employed to improve the quality of the image in the recovery process. Experimental results have justified that the designed scheme can effectively recovery with different modifications, which contains *content cropping*, *content exchange*, and *text addition*. Comparisons and tests are implemented to prove that the proposed scheme has better performance in terms of effectiveness and lossless recovery. The original image can be losslessly recovered even if two shares are tampered with the size more than 50%. Next, we will improve the JPEG-LS algorithm to recover the original image when the size of image is small.

Acknowledgements This work was supported by the National Science and Technology Major Project, China (Grant No. 2018YFB0204304).

Declarations

Conflict of interest The authors 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. Afjal MI, Mamun MdA, Uddin MdP (2019) Band reordering heuristics for lossless satellite image compression with 3D-CALIC and CCSDS. J Vis Commun Image Represent 59(Feb. 2019):514–526
2. Arnold VI, Avez A (1967) Problèmes Ergodiques De La Mécanique Classique. Gauthier-Villars, Paris
3. Arsalan M, Qureshi AS, Khan A (2017) Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. Appl Soft Comput 51(Feb. 2017): 168–179
4. Caldelli R, Filippini F, Barni M (2006) Joint near-lossless compression and watermarking of still images for authentication and tamper localization. Signal Process-Image Commun 21(10):890-903
5. Chamlawi R, Khan A (2010) Digital image authentication and recovery: Employing integer transform based information embedding and extraction. Inf Sci 180(Dec. 2010):24
6. Dimpal B, Pratap CN, Bhavin S (2016) Optimized lossless image compression algorithm LOCO-I for small images. In: Proceedings of the 2016 Conference on Advances in Signal Processing (CASP), 223-225
7. Gao G, Wan X, Yao S (2017) Reversible data hiding with contrast enhancement and tamper localization for medical images. Inf Sci 385(Apr. 2017):250-265
8. Jtc1/Sc29/Wg1, I (1997) Lossless and near-lossless coding of continuous tone still images (jpeg-ls). FCD 14495
9. Khor HL, Liew S-C, Jasni Mohd Z (2017) Region of interest-based tamper detection and lossless recovery watermarking scheme (ROI-DR) on ultrasound medical images. J Digit Imaging 30(3):328-349
10. Li J, Zhang Z, Li S (2020) A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology. BMC Med Inform Decis Mak 20(14):1-16
11. Li L, Abd El-Latif AA, Yan X. et al (2012) A lossless secret image sharing scheme based on steganography. 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, 1247-1250
12. Liu Y, You Z, Gao T (2020) Lossless image hierarchical recovery based on POB number system. Signal Process 167(Feb. 2020)
13. Naskar R, Chakraborty RS (2013) A generalized tamper localization approach for reversible watermarking algorithms. ACM Trans Multimed Comput Commun Appl 9(3):Article 19, 22pages

14. Sahar H et al (2017) 2017.Joint watermarking and lossless JPEG-LS compression for medical image security. IRBM 38(4):198–206
15. Sasikaladevi N, Geetha K, Mahalakshmi N et al (2019) SNAP-compressive lossless sensitive image authentication and protection scheme based on Genus-2 hyper elliptic curve. Multimed Tools Appl 78: 26163–26179
16. Shi H, Wang Y, Li (2021) Region-based reversible medical image watermarking algorithm for privacy protection and integrity authentication. Multimed Tools Appl 80(Apr. 2021):3231–3252
17. Singh D, Singh SK (2006) Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability. J Vis Commun Image Represent 38(Jul 2016):775–789
18. Singh P, Atrey PK (2019) Recovering tampered regions in encrypted video using POB number system. Signal Process-Image Commun 74(May. 2019):96-109
19. Singh P, Raman B, Agarwal N (2017) Secure cloud-based image tampering detection and localization using POB number system. ACM Trans Multimed Comput Commun Appl 13(3)
20. Singh P, Raman B, Agarwal N (2018) Toward encrypted video tampering detection and localization based on POB number system over Cloud. IEEE Trans Circuits Syst Video Technol 28(9):2116–2130
21. Sreekumar A, Sundar SB (2009) An efficient secret sharing scheme for n out of n scheme using POB-number system. Hack 1(2009)33–37
22. Tai W-L, Liao Z-J (2018) Image self-recovery with watermark self-embedding. Signal Process. Signal Process Image Commun 65(Jul. 2018):11–25
23. Wang X, Gao S (2021) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci 539(Oct. 2020):195–214
24. Wang X, Wang M (2007) Hyperchaotic Lorenz system. Acta Phys Sin 56(9):5136-5141
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(Aug. 2021):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(Nov. 2021):128–149
27. Wang C, Wang X, Xia Z et al (2019) Image description with polar harmonic Fourier moments. IEEE Trans Circuits Syst Video Technol 30,12(Dec. 2019):4440-4452
28. Wang C, Wang X, Xia Z et al (2019) Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. Inf Sci 470(Jan. 2019):109–120
29. Xiang Y, Xiao D, Wang H (2019) A Secure image tampering detection and self-recovery scheme using POB number system over cloud. Signal Process 162(Sep. 2019):282–295
30. Xu G, Wu W (2012) Arnold encryption algorithm based on pseudo-random sequence. Comput Sci 39(12): 79-82
31. Yan X, Wang S, Abd El-Latif AA (2015) Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. Multimed Tools Appl 74(Dec. 2015):3231-3252
32. Zhang X, Zhang W, Sun W (2020) A robust watermarking scheme based on roi and iwt for remote consultation of covid-19. CMC-Comput Mater Continua 64(3):1435–1452.21
33. Zhou J, Li JQ, Di XQ (2020) A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. IEEE Access 8(Jul. 2020):122210–122228