Complex & Intelligent Systems (2023) 9:1653–1670
https://doi.org/10.1007/s40747-022-00881-9

ORIGINAL ARTICLE

Secure medical image sharing for smart healthcare system based on cellular neural network

Conghuan Ye[1,2] · **Cong Chen**[3]

Received: 9 March 2022 / Accepted: 20 September 2022 / Published online: 2 October 2022

Abstract
The smart healthcare system (SHCS) facilitates the healthcare process with the widespread use of medical data through the internet of medical things (IoMT). Widespread use of medical data, especially medical images can also lead to privacy issues. Traditional encryption algorithms can address some problems; however, they cannot deter the redistribution of decrypted content. To prevent the decrypted content from being used illegally, the paper proposes a combination scheme of encryption and fingerprinting based on the game of life (GOL) and singular value decomposition (SVD) with the purpose of protecting medical images. First, medical images are performed with discrete wavelet transform (DWT). Second, the highest coefficients bit planes of the approximation component are selected to confuse with GOL. Third, the other bit planes and other detail components are chosen to embed fingerprints. Finally, all subbands are diffused with SVD computing. The proposed privacy protection scheme, as far as we know, is the first privacy protection scheme for the SHCS using GOL and SVD based on a chaotic cellular neural network (CNN). The proposed scheme can provide double-level privacy protection for the SHCS. The experimental results and discussion verify it is effective for the privacy protection of the SHCS.

Keywords Chaotic neural network · Electronic medical records · Medical image encryption · Joint encryption and fingerprinting · DWT_SVD domain

Introduction

The SHCS is a component of an IoMT, which is often used for healthcare online. A number of benefits can be achieved with the SHCS. Electronic medical records (EMRs), especially medical images, will have a more important role in the SHCS, which can provide medical records of patients directly. Electronic medical information sharing has made medical images important in the SHCS. In the meantime, in the SHCS, it is necessary to provide secure medical service for patients.

✉ Conghuan Ye
ychzzw@163.com

Cong Chen
p2pgrid@gmail.com

[1] School of Information and Communication Engineering, Hubei University of Economics, Wuhan, Hubei, China

[2] School of Computer and Information Science, Hubei Engineering University, Xiaogan, Hubei, China

[3] School of Computer, Wuhan University, Wuhan, Hubei, China

The SHCS mainly manages electronic health information of people. There are mainly text health information and medical images of people [1,2]. With the rapid development of the IoMT, the distribution of medical images in the SHCS is inevitable. However, imperative does not mean that it is easy to obtain wide applications. In the SHCS, many medical images are produced, stored, and distributed through the IoMT. Healthcare applications offer distinctive challenges for the SHCS such as secret information gaining and sensitive data sharing. In this case, privacy concerns will prevail.

Medical images which are shared over the IoMT will cause the same privacy exposure threat as other content distribution networks. Concerning about privacy disclosure may limit the wide use of the SHCS. Therefore, sharing of EMRs in the SHCS must provide privacy protection for people. In this paper, we mainly focus on medical image security. Sharing medical images between doctors via the IoMT poses serious security challenges for privacy protection [3–5]. Thus, comprehensive techniques for medical image security are necessary for the SHCS [6,7].

For medical image protection, traditional encryption techniques should not be adopted [8]. The conventional encryp-

tion method such as Rivest–Shamir–Adlema (RSA) is not suitable for medical image encryption because of the integral features of the medical images, which refer to large data size, bulk data capacity, local structure, and local correlation. Those conventional encryption techniques encrypt all content of medical image. They can protect privacy of medical image. However, they not only require much computation time but also mainly concern the confidentiality aspect of the records. No unauthorized party should have read access to them.

Another popular method is selective encryption, which trades off security for computational complexity. Selective encryption only encrypts part important content of medical images. In this case, the medical images are transformed into the frequency domain from the spatial domain. Unfortunately, all medical image encryption schemes only protect image content in the communication/storage stage. If some medical experts decrypt the encrypted content, the medical image can be processed by the experts willy-nilly. The medical image will not be protected once it is decrypted. Some experts may distribute the decrypted medical image to others. In this case, even if the redistributed medical image is found, it is still not possible for the SHCS to find who illegally distributed the medical image to others. Undoubtedly, in the SHCS, safeguarding privacy of medical image is still in its infancy.

The usage of decrypted medical data should be monitored forever. Medical data should be protected even if it is decrypted. Watermarking schemes were proposed for protection of decrypted content in [9–12]. Encryption is only for secure communication. If the decrypted content is redistributed by an authorized user after the communication stage, the security of the SHCS will be threatened, and the privacy of medical images will be exposed. However watermarking can control the plain medical image application. Although the illegal use of medical images can be controlled by digital watermarking, the above two technologies can not solve the security and privacy issue of the SHCS alone. Joint encryption and watermarking algorithms for medical image protection schemes are proposed in [13–15]. But watermarking cannot identify who illegally distributed the decrypted medical image. Digital fingerprinting can trace one who shared the decrypted medical image with others. Therefore, the combination of encryption and fingerprinting can provide privacy protection for medical images in the SHCS forever.

Kundur et al. [16] put forward a joint fingerprinting and encrypted content decryption architecture for a better balance between security and application. But the architecture did not apply to medical image security. The authors [17] proposed a specific unicast and multicast scheme with digital fingerprinting based on the tree structure Haar wavelet transform.

For medical image encryption, chaotic maps are applied very widely. GOL of cellular automata (CA) system can also show chaotic characteristics as chaotic maps. GOL is based on some very simple rules with low compute complexity. The chaotic characteristics can make GOL is a good choice for image encryption [18]. In the meantime, the low compute complex can meet fast secure requirements in the SHCS. SVD is a nonsymmetrical decomposition, and the reversible property of SVD is not only convenient for watermark embedding and extracting, but also possible for diffusion. Secure medical image sharing in the SHCS is becoming more and more urgent for remote healthcare applications. It is important to design a privacy protection method for secure sharing of medical data, which can provide mobile, resource-constrained clients with personalized medical service with privacy protection. In fact, current joint watermarking and encryption methods for the SHCS have to face new challenges on content fingerprint and user fingerprint embedding and fast personalized secure medical service providing.

Targeting at above challenges faced, we first proposed a scalable combination scheme of encryption and fingerprinting to meet the fast request of image protection in the SHCS. DWT can help low the security algorithm time. In the DWT domain, both scrambling and diffusion can change coefficients value for diffusion, in this case, scrambling based on GOL in bit level of coefficients along with diffusion can improve the encryption effect. The paper will research lightweight joint encryption and dual fingerprints embedding in the DWT domain. First, we explore fingerprinting based on the original medical data, and the keys are produced from the original medical image too. Second, GOL is used to confuse the coefficients in the highest m bit plane of lower resolution approximation (LL) subband. Third, low bit planes of LL subband, horizontal (HL) subband, and vertical (LH) subband are used to embed fingerprints. Finally, LL subband, HL subband, LH subband, and diagonal (HH) subband are diffused with chaotic neural networks by SVD computing.

Joint encryption and fingerprinting (JEF) can provide two-level protection for medical images. For the field of SHCS security and privacy, digital fingerprinting can be regarded as the second level protection mechanism for medical image when the encrypted medical image is decrypted.

To achieve two-level protection for medical images, two different methods can be applied. The first is embedding user fingerprints into medical images when the encrypted medical image is decrypted. The second method conducts fingerprinting and encryption together, its encryption could be full encryption or selective encryption. To the former, all content is encrypted, this full encryption can provide the highest security for medical data; as for the latter, only the most important content is chosen to be encrypted. For example, the high-

est bit planes of an image in the spatial and DWT domain. The SHCS links to some resource-constrained devices with the IoMT. It is important achieve a balance of provision of the actual security and privacy protection and meeting fast requirements in the SHCS. In fact, it is no easy task to strike a balance between the two aspects. These problems are not deeply considered in existing work too. Undoubtedly, safeguarding privacy in the SHCS is very challenging. Understanding the inherent security of the SHCS may play a useful role in medical image forensics. To address these issues, we present a novel self-adapting joint fingerprinting and double encryption method based on CNN in the DWT domain for medical image security persistently. In the proposed scheme, the highest m bit planes of the LL subband are selected to encrypt. Other bit planes, HL and LH subbands are used to embed dual fingerprints, according to the specific needs, all subbands can be chosen for secondary encryption for higher security.

The proposed scheme can provide a scalable JEF scheme in the DWT domain to balance the security requirements and time complexity. The research will not only make up for the deficiency of joint encryption and watermarking for medical data sharing, but also provide double-level security protection. The proposed privacy protection algorithm is very simple, fast, secure, and can be realized easily. It is very appropriate for selective encryption according to the requirements of different medical settings. Selective encryption is a technique which only encrypts a portion of an important content, which is the most crucial part for visualization. For example, perform the DWT transform on an image, the important information is mainly concentrated in the approximate subband, other subbands only include the detail information. Only through detail information, the original image will not be perceived or perceived clearly. With the proposed scheme, a fast secure medical image sharing system can be well-designed. As far as we know, the proposed scheme is the first medical image protection technology in the DWT domain using GOL and SVD based on CNN for the SHCS security and privacy protection. The remainder is as follows. The basic theory is introduced in the next section. In the subsequent section, we discuss the medical image protection scheme, and the detailed experimental results and discussion are presented in the following section. The conclusion is in the final section.

Basic theory of the proposed scheme

DWT transformation

DWT transform can decompose an image into four parts, LL subband, HL subband, LH subband, and HH subband. LL subband is the approximation component, and the other three subbands are detailed components. For an image's L-level DWT decomposition, Eq. (1) shows the transform process.

$$\begin{aligned} G_{LL}(N) &=< M \bullet LL_N > \\ G_{LH}(N) &=< M \bullet LH_i >, i = 1, ..., N \\ G_{HL}(N) &=< M \bullet HL_i >, i = 1, ..., N \\ G_{HH}(N) &=< M \bullet HH_i >, i = 1, ..., N \end{aligned} \tag{1}$$

M is the image to transform, and LL_i, LH_i, HL_i and HH_i are subbands. The following equation shows how the decomposed image could be recovered:

$$\begin{aligned} M = G_{LL}LL_N + \sum_{i=1}^{N} G_{LH}(i)LH_i + \sum_{i=1}^{N} G_{HL}(i)HL_i \\ + \sum_{i=1}^{N} G_{HH}(i)HH_i \quad i = 1, ..., N. \end{aligned} \tag{2}$$

SVD

SVD of a matrix is an important matrix decomposition in linear algebra [19]. SVD can be used to divide eigenvalues of matrices with arbitrary shapes. Most matrices in the real application scenario are not likely to be square matrices, which are data matrices with unequal number of rows and columns. It can express a more complex matrix by the multiplication of several simpler submatrices. These simpler matrices describe the important properties of the matrices. The SVD process is also an extension of similar diagonalization decomposition (also known as eigenvalue decomposition, EVD) in linear algebra. SVD is a method with obvious physical meaning, it has wide application value. The general mathematical form of SVD is as follows:

$$\begin{aligned} A &= USV^T \\ &= \begin{bmatrix} U(1,1) & U(1,2) & \cdots & U(1,M) \\ U(2,1) & U(2,2) & \cdots & U(2,M) \\ \vdots & \vdots & \ddots & \vdots \\ U(M,1) & U(M,2) & \cdots & U(M,M) \end{bmatrix} \\ &\times \begin{bmatrix} S(1,1) & 0 & \cdots & 0 \\ 0 & S(2,2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & S(M,N) \end{bmatrix} \\ &\times \begin{bmatrix} V(1,1) & V(1,2) & \cdots & V(1,N) \\ V(2,1) & V(2,2) & \cdots & V(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ V(N,1) & V(N,2) & \cdots & V(N,N) \end{bmatrix}^T, \end{aligned} \tag{3}$$

where S is called a singular value matrix. It is a $m \times n$ rectangular diagonal matrix composed of nonnegative diagonal

real elements, which are arranged in descending order. All elements in the matrix S are zero, except for the elements on the main diagonal, and each element on the main diagonal is called a singular value. S_r is a diagonal matrix in $\mathbf{R}^{r\times r}$.

$$S = \begin{bmatrix} S_t & 0 \\ 0 & 0 \end{bmatrix}, S_t = diag(S(1,1), S(2,2), ..., S(t,t)), \quad (4)$$

where $S(1,1) \geq S(2,2) \geq ... \geq S(t,t)$. On the other hand, U is an orthogonal matrix of order M, V is an orthogonal matrix of order N. Then, The two matrices satisfy:

$$I_M = U^T U = UU^T \quad (5)$$

$$I_N = V^T V = VV^T. \quad (6)$$

Secure hash algorithm (SHA)-3

A cryptographic hash function is one way compression mapping function, which can map any length of message to a fixed length. It can be used for authenticated encryption and pseudo-random number generation. Usually, a cryptographic hash function has the sensitivity property of the input message. However, the collisions of the Message-Digest algorithm (MD5) have been found [20,21]. Wang Xiaoyun later proved that SHA-1 can be cracked theoretically [22]. Therefore, with higher security requirements, MD5 and SHA-1 should be avoided in certain domains.

SHA-3, also known as Keccak, is a widely used cryptographic hash function [23]. It is more secure than previous cryptographic hash functions such as MD5, SHA-1, and SHA-2 [24]. The design of SHA-3 was based on permutation functions. For any type message as input, SHA-3 function can generate different length hash values through computing the given message. They have fixed 224, 256, 384, and 512-bit hash values. In this paper, 256-bit hash value will be as output in the proposed algorithm. The hash value can ensure the integrity and consistency of information transmission. In addition, SHA-3 is very sensitive to the input message. Even if there is only a tiny bit change between two input sequences, the returned hash value will be totally different. The time performance of the SHA-3 function is superior because of its bit-level operations. Because it has fast computation capability and is very sensitive to original input content, it will be used to design keys of medical image encryption in this paper.

Chaotic systems

Even the simplest chaotic systems can demonstrate ergodicity and pseudo-randomness. Image encryption and video encryption usually choose chaotic systems recently, because the chaotic system has some attractive characteristics, for example, sensitivity of input original values, control parameters, and pseudo-randomness. Same as chaotic systems, the hyperchaotic CNN system can also show the above attractive characteristic for image encryption. With the pseudo-randomness, the CNN system can be used for medical image encryption in this paper with the generated pseudo-random data matrix.

2D Hénon-Sine map (2D-HSM), which was proposed in [25], can show chaotic behavior. The mathematical equation is as follows:

$$\begin{cases} x_{n+1} = (1 - a\sin^2(x_n) + y_n) \bmod 1 \\ y_{n+1} = bx_n \bmod 1 \end{cases} \quad (7)$$

where controls parameters $a \in (-\infty, +\infty)$ and $b \in (-\infty, +\infty)$. Once the initial values $x_0 \in (0, 1)$ and $y_0 \in (0, 1)$, 2D-HSM can evolve into a chaotic state. Furthermore, 2D-HSM shows possessed better ergodicity and randomness, and more complex chaotic trajectories compared to Sine map and Hénon map.

The hyperchaotic CNN system can show chaotic and pseudo-randomness characteristics under certain conditions, so the hyperchaotic CNN system can be used to image encryption for secure image transmission [26]. Because the network model of the CNN system is fully connected, the output signal of each cell unit can be fed back to itself with the help of other units. The hyperchaotic CNN model is shown as follows:

$$\begin{cases} \dot{y}_1 = -y_3 - y_4 \\ \dot{y}_2 = 2y_2 + y_3 \\ \dot{y}_3 = 14y_1 - 14y_2 \\ \dot{y}_4 = 100y_1 - 100y_4 + 200p_4 \\ \dot{y}_5 = 18y_2 + y_1 - y_5 \\ \dot{y}_6 = 4y_5 - 4y_6 + 100y_2 \\ q_4 = 0.5(|y_4 + 1| - |y_4 - 1|), \end{cases} \quad (8)$$

where the initial value $y_i \in (0, 1)$, $i = 1, 2, 3, 4, 5, 6$.

CA

CA is controlled by rules that determine how the state of a cell changes over time [27,28]. In the early 1980s, Stephen wolfram identified four types of behavior, each more interesting than the previous one. The cells are arranged in a lattice (which can be regarded as a one-dimensional array), and there are two cells near each cell. The lattice can be finite, infinite, or ring mounted. Each cell still has two states: 0 and 1. The rule of determining the next state of a cell is based on its two adjacent cells, that is, a group of three cells determines the next value of the intermediate cell. The evolution rule of CA is local. When updating the state of a given cell, we only need to know the state of its adjacent cell. When a cell state

is updated, the spatial domain to be searched is called the neighbor of the cell.

GOL is (2-D) CA, which consists of an $M \times N$ panel of lattices, which are called cells. Each cell has two states—survival or death. Each cell interacts with the surrounding eight cells centered on itself. Given a panel containing $m \times n$ lattices. Each cell has an initial state: 1 is live cell, or 0 is dead cell. Each cell and its eight adjacent cells (horizontal, vertical, diagonal) follow the following four survival laws:

(1) When the current cell is living and the number of living cells around is less than 2 (excluding 2), the cell becomes dead.
(2) When there are two or three living cells around the cell, the cell remains intact.
(3) When there are more than three living cells around, the cell becomes dead.
(4) When the current cell is dead, there are three live cells around, the cell becomes live.

To maintain the two-dimensional lattice with infinite extension, the upper and lower boundaries are linked, so do the left and right boundaries.

Main contribution of the proposed scheme

The proposed medical image sharing scheme is mainly to solve privacy issues in the SHCS. The main advantages are:

(1) The proposed security and privacy protection algorithm offers a discussion of how to use a combination of fingerprinting and two-layer encryption in the DWT domain for medical image sharing.
(2) The proposed scheme is content self-adaptively. The keys are produced based on the singular value of the original image.
(3) The algorithm can provide technology for two-layer encryption and fingerprinting for continuous protection.
(4) The proposed scheme can provide fast secure sharing requirements for medical image transmission in the SHCS.
(5) A secure and controllable medical image sharing system can be designed for the SHCS with the proposed technologies.

Proposed medical image privacy protection scheme

In this section, the proposed medical image privacy protection algorithm will be introduced. The authors first describe the double encryption scheme with GOL confusion and SVD diffusion based on the chaotic neural network, and then present dual fingerprints embedding and detection. Fidelity methods are preferred in the medical image in the SHCS based on the IoMT. The watermarking schemes used in the SHCS should concern the visual quality. Because both double encryption and fingerprint-embedding processes are performed in the DWT domain, the fingerprinted medical images should not be changed visually. For medical image encryption, a novel combination of encryption and fingerprinting framework is designed as shown in Fig. 1. For a medical image, we compute the DWT coefficients directly from the original image. Then, we encrypt the highest M bit planes of low-frequency subband and embed fingerprints into low bit planes of the LL subband, and middle-frequency (LH and HL) subbands. At last, diffusion encryption will be performed according to the security request for improving the encryption effect.

Secure and controllable medical image sharing becomes more and more urgent in the SHCS, which distributes medical data to doctors with privacy protection. Thus, three security properties of the SHCS should be provided, such as information confidentiality, image verification and pirate tracing. Medical image encryption can provide information confidentiality. After encryption, the plain image will be like a random noise signal for secure distribution. The protected medical image must not be estimated to get the original image data from the protected content computationally complex without the key. While image verification can be provided by fingerprinting, and traitor tracing can be achieved by unique fingerprint information. However, medical image encryption algorithms provide no protection once it is decrypted, where an untrustworthy doctor may redistribute his/her medical image to a third without permission of the owner.

Therefore, the combination of encryption and digital fingerprinting can provide continuous protection for medical images in the SHCS. In this case, image encryption and digital fingerprinting are regarded as an "a priori" and an "a posteriori" privacy protection method respectively. Therefore, how to combine encryption and fingerprinting for addressing privacy issues in the SHCS is crucial. First, an original image is decomposed by the DWT. Fingerprints are embedded into a singular value vector of the coefficients in LL, HL, and LH subbands. Second, the approximation coefficient is selected to permute with 2D-HSM. Third, the permuted contents are encrypted using SVD. Finally, the encrypted fingerprinted contents are distributed to potential users.

Medical image encryption and decryption algorithm

Medical image encryption based on chaotic systems can be classified into confusion-only, diffusion-only, and the joint of confusion and diffusion form. Medical image encryption with the confusion-only is advantaged because of the low

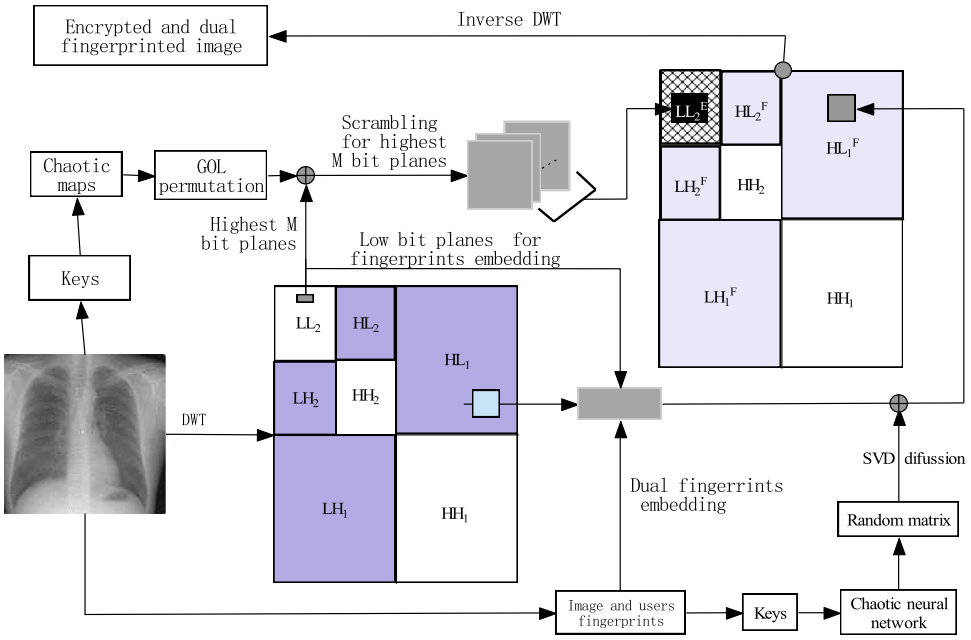

Fig. 1 The proposed privacy protection scheme

time complexity of the encryption process, but the privacy protection aspect may not be high for security. To increase the security effect, a new medical image encryption method based on the CNN system is proposed in Fig. 1. The whole two-level encryption process has two steps: confusion with GOL and diffusion using SVD based on random matrixes produced by the chaotic CNN system in the DWT domain. GOL and SVD are used for confusion and diffusion in the DWT domain one after another, and fingerprint information is embedded into the lower bit planes of LL, HL, and LH subbands of the DWT domain. According to Fig. 1, the proposed double encryption scheme is as follows:

Step 1: For an image I, perform DWT. Then four subbands can be produced. They are LL, HL, LH, and HH subbands, respectively. LL has approximation coefficients, HL, LH and HH have detailed coefficients. The second level DWT decomposition can be performed on the LL subband;

$$I \Rightarrow \{I_{LL}, I_{LH}, I_{HL}, I_{HH}\}. \tag{9}$$

Step 2: Apply SVD to LL subbands, and LH, HL, and HH subbands, i.e.,

$$A_m = U_m S_m V_m^T, (m = 1, 2, ...), \tag{10}$$

where m means one of the subbands.

Step 3: Permute the singular vector S from Step2 randomly. Use SHA-3 to the permuted vector S^P, a hash value of 256-bit V is generated. According to the order of bits, the 128-bit value is random chosen from V. The 128-bit value is segmented into eight V_1, V_2 , ... , V_8, which are 16-bit. Values x_1, x_2, x_3, x_4 x_5, x_6, y_0, z_0 and parameters a and b can be produced according to eight V_1, V_2, ... , V_8. The medical image encryption has keys which are x_1, x_2, x_3, x_4, x_5, x_6, y_0, z_0, a, and b.

$$x_1 = \frac{V_1}{2^{17}}, x_2 = \frac{V_2}{2^{17}}, x_3 = \frac{V_3}{2^{17}}, x_4 = \frac{V_4}{2^{17}} \tag{11}$$

$$x_5 = \frac{V_5}{2^{17}}, x_6 = \frac{V_6}{2^{17}}, y_0 = \frac{V_7}{2^{17}}, z_0 = \frac{V_8}{2^{17}} \tag{12}$$

$$a = \left(\frac{V_5}{2^{17}} + \frac{V_6}{2^{17}}\right)/2, b = \left(\frac{V_7}{2^{17}} + \frac{V_8}{2^{17}}\right)/2. \tag{13}$$

Step 4: Chaotic CA for scrambling. The initial matrix is generated, which is called A_0. Assume k is the iteration number. Then the scrambling matrix for confusion based on GOL is generated. Use 2D-HSM to generate two sequences $(y_1, y_2, \cdots, y_{M\times N})$ and $(z_1, z_2, \cdots, z_{M\times N})$ respectively. Then an initial matrix G^0 can be created, as the seeds of GOL. If y_i is less than the mean value of the above sequences, the initial value is 0, which represents the corresponding cell is dead, otherwise alive.

Step 5: Adjacent coefficients in the DWT domain have correlation, which can be reduced by confusing coefficients based on GOL. Perform scrambling based on a number of generations of the GOL. Then all the plain coefficients are placed into the correct position of the corresponding confusion matrix according to the mapping relationship between the plain coefficients and the encrypted coefficients.

Step 6: To protect medical image further, diffusion with SVD based on the hyperchaotic CNN system can enhance the ability to resist hack attacks. Using the hyperchaotic CNN system to generate chaotic sequences $FP_{M\times N}^{J^K} =$

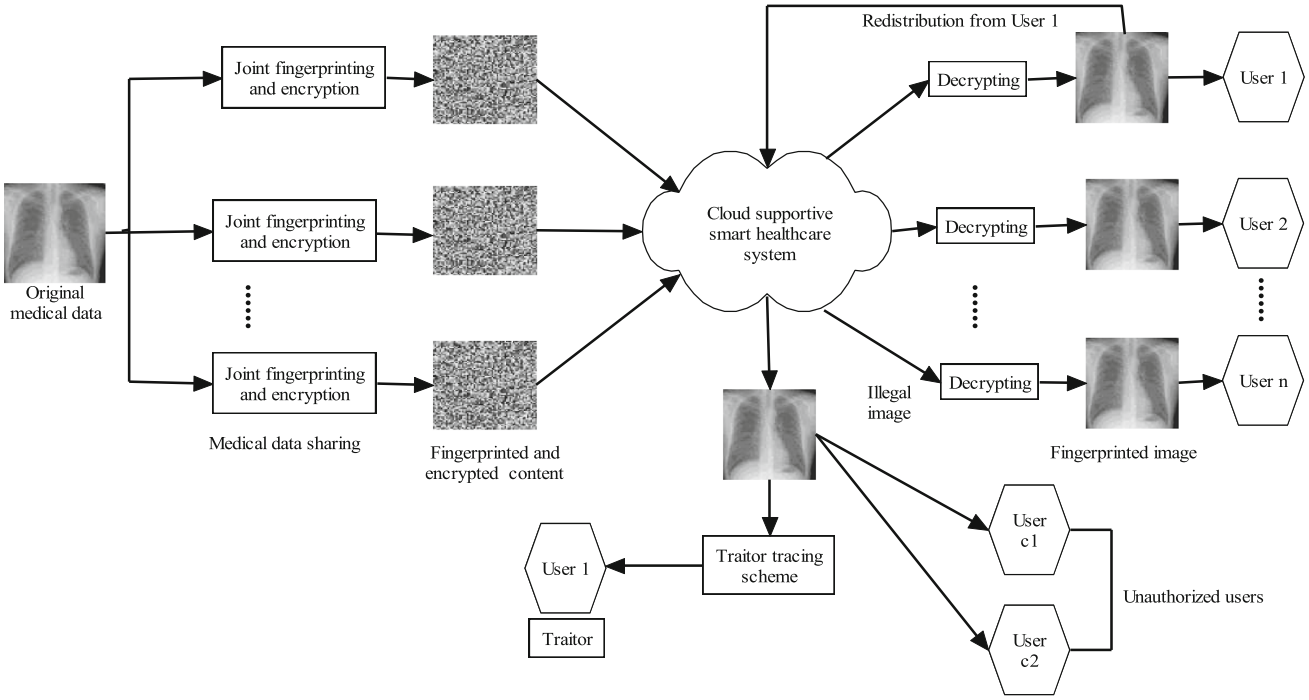

Fig. 2 Medical data sharing and traitor tracing

$\{fp_1^{J^K}, fp_2^{J^K}, ..., fp_{M\times N}^{J^K}\}$, then we can get the sequences $CP_{M\times N}^{J^K} = \{cp_1^{J^K}, cp_2^{J^K}, ..., cp_{M\times N}^{J^K}\}$ cp_i=ceiling(fp_i).

Step 7: The sequence $CP_{M\times N}^{J^K}$ is obtained from Step 6, which is shown as a $M \times N$ matrix CPK. CPK is produced randomly. With SVD of CPK, then $CPK = U_{CPK} S_{CPK} V_{CPK}^T$.

Step 8: Diffuse each subband with U_{CPK} and V_{CPK}^T, as follow:

$$I_k^E = \begin{cases} U_{CPK} I_k V_{CPK}^T, & M \le N \\ V_{CPK} I_k U_{CPK}^T, & M > N, \end{cases} \tag{14}$$

where I_k is the confused subband based on GOL, $k = \{LL, LH, HL, HH\}$.

Step 9: With fingerprints embedding into the low bit planes of the LL subband, LH subband, and HL subband, perform IDWT for the encrypted coefficients. The encrypted and fingerprinted image I^{JFE} is produced.

Encrypted medical image decryption scheme is presented as follows:

Step 1: For an encrypted and fingerprinted medical image I^{JFE}, perform the DWT decomposition. Then there is the medical image $\hat{I}_k^{JFE}$ in the DWT domain;

Step 2: Perform inverse SVD computing for diffused subbands with the following equation.

$$\tilde{I}_k^{JFE} = \begin{cases} U_{CPK}^T \hat{I}_k^{JFE} V_{CPK}, & M \le N \\ V_{CPK}^T \hat{I}_k^{JFE} U_{CPK}, & M > N \end{cases} \tag{15}$$

Step 3: According to the one-to-one map relationship between the plain matrix of LL subband and the cipher matrix, transform the confused matrix to the plain matrix;

Step 4: With inverse DWT for decrypted content, there is the medical image I^F with fingerprint information, which can trace one who redistributes the medical image to others.

Fingerprint embedding algorithm

Multimedia fingerprinting can identify a traitor who uses a medical image illegally. For example, medical images are shared with others without permission. With the help of fingerprint information inside the medical image, traitor/pirate can be traced as Fig. 2 shows. Fingerprint information should be embedded into the medical image with watermarking technology. When a suspected copy is found, the SHCS can extract fingerprint information to decide who reuses the medical image illegally. The fingerprint embedding algorithm first uses SVD to hide information in the low bit planes of the LL component, LH, and HL components of the DWT domain of a medical image. In the proposed algorithm, fingerprint information is embedded into the above three components of the medical image by modifying the SVD coefficients of the low bit planes of LL component, HL subband, and LH subband using the watermarking technology. It has been proven to perform better performance than the existing watermarking methods based on SVD on security and robustness.

Step 1: The medical image to embed fingerprint information is decomposed by DWT; $I \Rightarrow \{I_{LL}, I_{LH}, I_{HL}, I_{HH}\}$

Step 2: Use SVD computing for subbands which are chosen to embed fingerprint information. $I_k \Rightarrow U_k S_k V_k^T$, where $k = \{LL_{low}, LH, HL\}$, LL_{low} represents the low bit planes of LL subband.

Step 3: Insert fingerprints into the singular value vectors of the corresponding subbands in the DWT domain of the medical image, $S_k^{F_i} = S_k + \alpha X_k^{F_i}$, where $k = \{LL_{low}, LH, HL\}$, S^{F_i} is the fingerprinted S matrix for user i, α is the scaling factor. In this step, multiplication between fingerprints matrix and α is a point multiply operation.

Step 4: Perform SVD computing for the modified coefficients of the related subbands, $I_k^F = U_k S_k^F V_k$, where $k = \{LL, LH, HL, HH\}$

Step 5: Through inverse IDWT, the modified coefficients of the related subband can transform the fingerprinted and encrypted image.

Experiment results and discussion

The effectiveness of the combination of encryption and fingerprinting scheme is demonstrated through related experimental results in this section. To show the effectiveness of privacy protection and efficiency of the proposed method, some important medical images are downloaded from the Internet as the original test images. They are 8 bit Digital Imaging and Communications in Medicine (DICOM) medical images. These 256 gray level medical images with dimensions of 512×512 pixels are tested on the proposed JEF algorithm. The medical image types include X-Ray, CT scan, MRI, and Ultrasound. Matlab platform is used to simulate the experiment. The original medical image and the corresponding encrypted medical image are shown in Fig. 3a,b respectively. The decrypted images are shown in Fig. 3c, d. Figure 3c is the decrypted image with the wrong secret key, and Fig. 3d is the correct fingerprinted image with the correct key. According to the encrypted experiment result shown in Fig. 3b, the original information of the medical image is very difficult to know. Using the wrong secret key, the plain image can not be recovered from the encrypted medical image shown in Fig. 3c. It is very obvious that the proposed combination of encryption and fingerprinting scheme can achieve a good privacy protection effect.

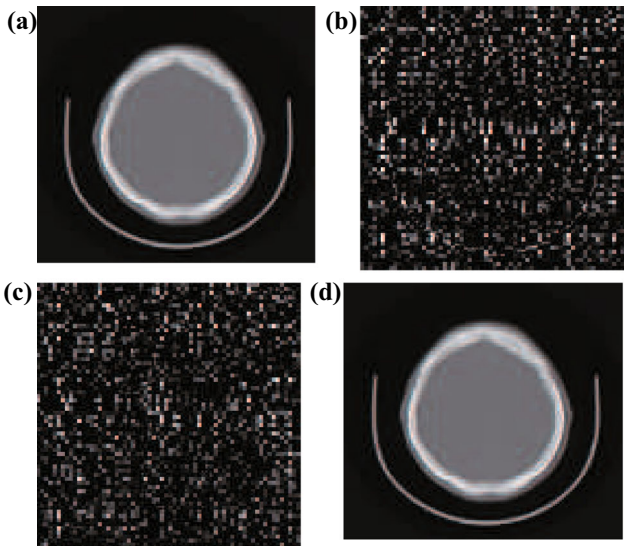

Fig. 3 Medical image encryption and decryption results: (a) Original medical image, (b) Encrypted medical image, (c) Decrypted medical image with a tiny changed initial values and control parameters, (d) Decrypted image with correct keys

Encryption and fingerprint perceptual effect

Generally, for secure medical image communication to get confidentiality, the encrypted medical image should not be intelligible. In the privacy protection scheme in this paper, the M highest bit planes of LL subband in the DWT domain are first confused by permutation through GOL. Then the fingerprint information is embedded into the low bit planes of LL subband, HL, and LH subband based on modifying singular values of the related matrices. At last, the confused and scrambled coefficients are diffused with SVD. Figure 4b shows the visual effect of the proposed combination of encryption and fingerprinting scheme. According to Fig. 4b, the visual effect of all encrypted and fingerprinted medical images is very poor. Original medical image information can not be perceptible from the encrypted images because all medical images in Fig. 4b are noise-like. With the proposed encryption algorithm, the privacy of medical images can be protected.

Fingerprint information is embedded into the wavelet coefficients of the medical image between confusion and diffusion stages. For medical images, the visual quality of fingerprinted medical images should not be changed apparently. To provide the tracing ability later, fingerprint information should not be perceptible from the decrypted fingerprinted medical images. Decrypted fingerprinted medical images are shown in Fig. 4c. From Fig. 4c, it is very clear that the fingerprint information can not be detectable, and the visual quality of decrypted fingerprinted medical images is not changed apparently.

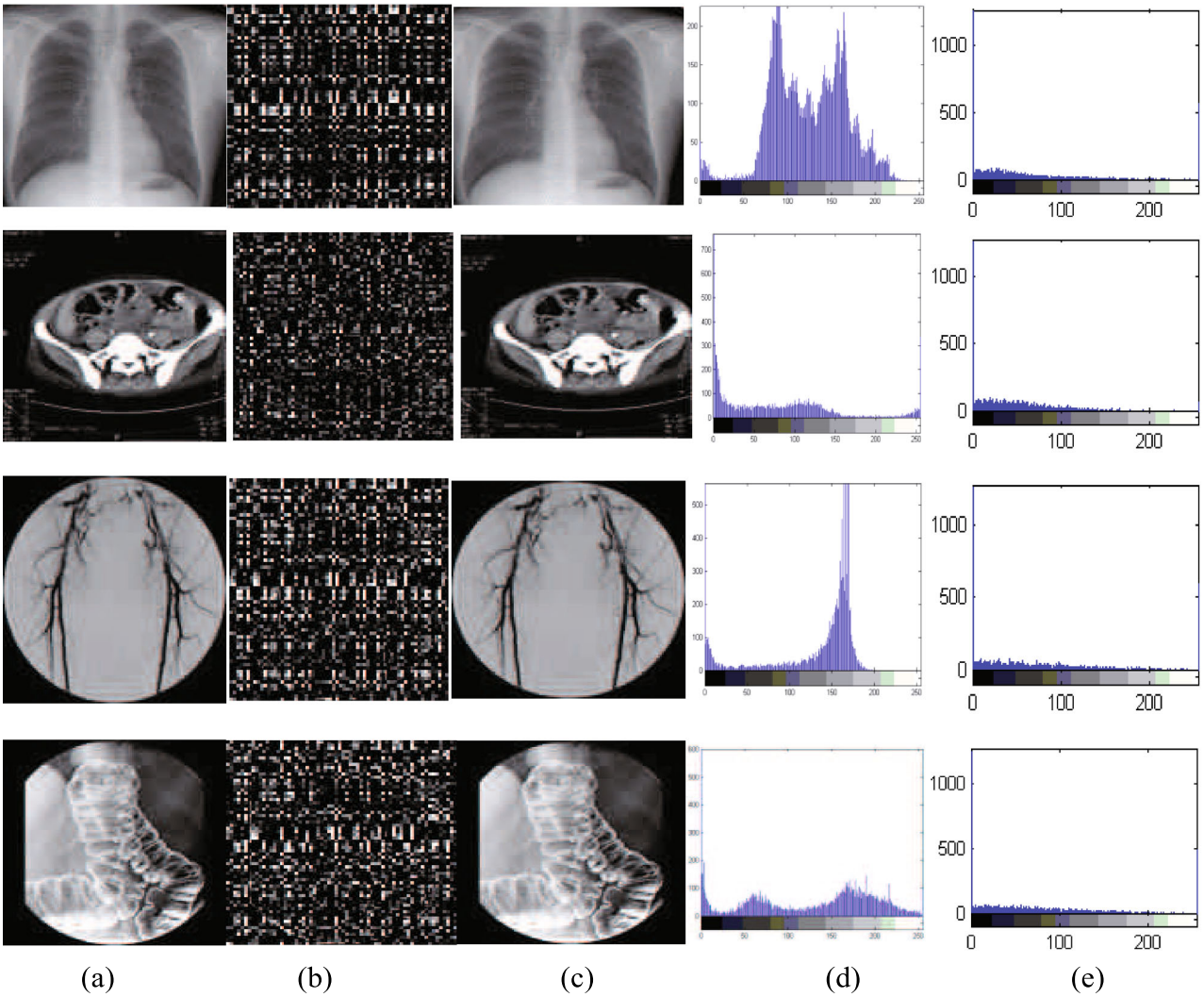

Fig. 4 Medical images encryption results: (**a**) Original medical images, (**b**) Encrypted medical images, (**c**) Decrypted and fingerprinted medical images, (**d**) Histograms of the original medical images, (**e**) Histograms of the encrypted images

Fingerprinting performance analysis

Fingerprint information is embedded into the related subbands of the DWT domain of a medical image in parallel. To realize the invisibility of fingerprint information, the fingerprint information is embedded into the low bit planes of LL subband, LH and HL subbands, the fingerprint hiding in the decrypted medical image should not reduce medical image visual quality. The visual quality of decrypted fingerprinted medical images is not changed apparently according to Fig. 4c compared to the original medical image. Fingerprint information embedding into the low bit planes of LL subband, LH and HL subbands of the DWT domain in parallel can decrease the computational complexity.

The fast content distribution can be achieved, above all, the traitor can be traced with the proposed fingerprinting algorithm in the SHCS. The tracing algorithm is as follows:

Step 1: Use DWT on the suspected fingerprinted image.

$$I_k^{F*} \Rightarrow \left\{ I_{LL}^{F*}, I_{LH}^{F*}, I_{HL}^{F*}, I_{HH}^{F*} \right\} \Rightarrow \left\{ I_{LL}^{F}, I_{LH}^{F}, I_{HL}^{F}, I_{HH}^{F} \right\}. \tag{16}$$

Step 2: Use SVD computing for subbands which are embedded fingerprint information. $I_k \Rightarrow U_k S S_k V_k^T$, where $k = \{LL_{low}, LH, HL\}$.

Step 3: Minimum-distance detector is used to decide who is the traitor. Subtract the original S_k from the new SS_k for the related fingerprinted subbands, the operation is as following:

$$\hat{m} = \arg \min_{i=1,2,\ldots,N_u} \left\| SS_k - S_k^{F_i} \right\|^2, \tag{17}$$

where $k = \{LL_{low}, LH, HL\}$. The above detector decides the $\hat{m}$th user is a pirate.

Ability of resisting exhaustive attack

A good image encryption method should resist exhaustive attacks with a large key space. The medical image encryption scheme should be sensitive to a tiny change of the keys. The proposed medical image encryption includes confusion and diffusion processes. To achieve a large key space, employing chaotic CNN systems and 2D-HSM for diffusion and confusion. Both of them have the properties of parameter sensitivity and initial-value sensitivity. The key space has the keys used in two processes of confusion and diffusion. All the initial values and control parameters belong to the key space, which are the keys: initial values $x_1, x_2, x_3, x_4, x_5, x_6$, y_0, z_0, and parameters a and b. The sensitivity of the keys is considered as 10^{-16}, then the key space is $10^{16\times 10} = 10^{160}$. The total key space has a large scale to resist the brute-force attack. Figure 3b shows the decrypted fingerprinted image with the wrong key.

Statistical attack discussion

Statistical attack analysis is another important method to evaluate the effect of medical image encryption. The statistical attack includes image histogram analysis and correlation coefficient analysis. Good image encryption should have uniform histograms of different encrypted medical images. In this paper, the medical image encryption method is the selective encryption of important content in the DWT domain. For medical image encryption, if the encrypted medical images have similar encrypted histograms, which are different from the original image histograms, then the medical image encryption scheme is a good encryption method. On the other hand, the histograms of decrypted fingerprinted medical images should be similar to their corresponding original medical images.

The grey histogram analysis

The proposed medical image encryption scheme is rapid selective encryption in the DWT domain. Different from the spatial domain encryption, the encrypted histograms of encrypted medical images should be not only apparently different from the histograms of the corresponding original ones, but also the encrypted histograms of the encrypted images are fairly uniform with each other. Then the medical image encryption is said to be perfect. The histograms between the original medical images and the corresponding encrypted and fingerprinted medical images are shown in Fig. 4d, e respectively. According to the original and encrypted histograms, it is very clear that the grey values of pixels in the original medical images have mainly focused on a few values. From the encrypted histograms shown in Fig. 4e, the histograms of the encrypted medical images are similar, but these encrypted histograms are apparently not the same as the corresponding histograms of the original images. There, grey histogram analysis shows that the statistical attack is very difficult for the proposed medical image encryption scheme.

Correlation analysis

According to Fig. 5a, in the original medical image, the correlation of any adjacent pixels is really high. The correlation analysis regards that the adjacent pixels of encrypted images' correlation will be broken by a good medical image encryption scheme. The correlation of the encrypted fingerprinted medical image and the original medical image is analyzed. For medical image encryption, we will achieve the balance of encryption efficiency and encryption effect to meet the fast security request in the SHCS. The medical image encryption algorithm is said to be a good method if the correlation among adjacent pixels of the encrypted and fingerprinted medical images is decreased compared to the corresponding original medical images. To demonstrate the encrypted and fingerprinted medical images and the corresponding original medical images, 5000 pairs of adjacent pixels in the encrypted and fingerprinted medical images and the corresponding original medical images are randomly selected.

The correlation is calculated and shown in Fig. 5. Figure 5c, d shows the correlation of two adjacent pixels in the original medical image in Fig. 5a and its encrypted image in Fig. 5b. Figure 5c shows that the pixels' correlations in the original medical image. From Fig. 5, it is apparent that the correlations in Fig. 5d has decreased compared to the correlation of the corresponding original medical image in Fig. 5c. Figure 5d shows that the correlations of adjacent pixels in the encrypted image are greatly reduced.

Selective encryption discussion

In the proposed selective encryption process, it can be seen that the confusion process for the highest M bit planes in the DWT domain shown in Fig. 1. The experimental results are shown in Fig. 6. Even if selective 4×4 block permutation via GOL in the LL2 subband can get unintelligible encrypted images. Figure 6c, d show the selective medical images with single coefficient permutation in the LL2 subband and 4×4 block permutation in the LL2 subband, HL subbands, and LH subbands via GOL respectively. Just the same as Fig. 6b, all the selective encrypted medical images can not be perceptual. The encrypted results from Fig. 6b,c,d show that selective encryption in the DWT domain can meet the privacy protection requests of the SHCS.

Although single coefficient permutation in the highest m bit planes of LL subbands via GOL can achieve a better effect than 4×4 blocks permutation in the LL subband, the former

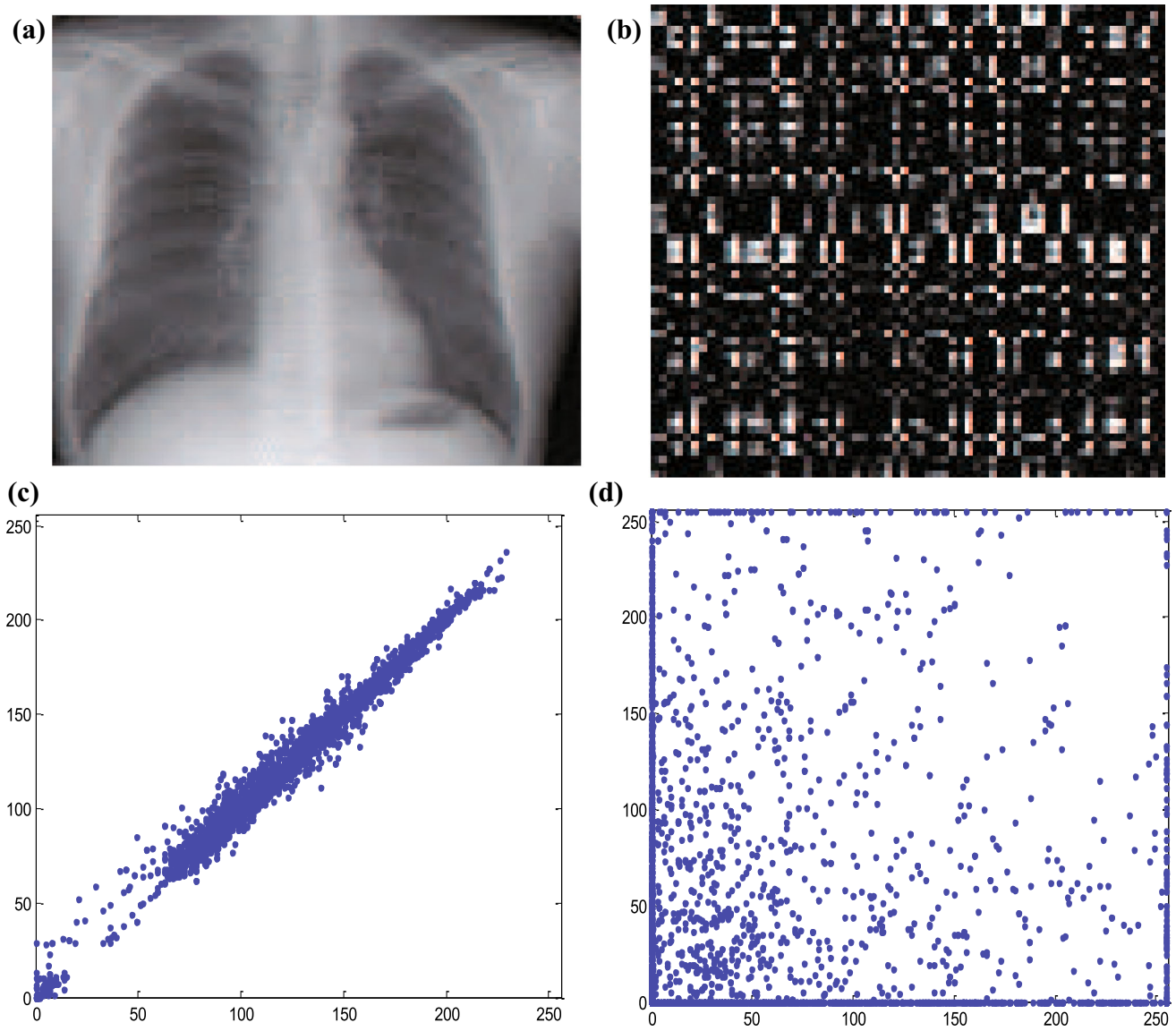

Fig. 5 Correlation analysis: (**a**) original medical image, (**b**) encrypted medical image, (**c**) the correlation of two adjacent pixels in (**a**), (**c**) the correlation of two adjacent pixels in (**b**)

will take 16 times as much as the time that the latter will take. In fact, the latter can get almost the same encryption visual effect as that of single coefficient permutation when the block size is 4×4. Furthermore, block permutation only took 1/16 time that single coefficient permutation took. Therefore, 4×4 blocks permutation can get better performance than the others in general. On the other hand, if the HL and LH subbands are selected to be permuted, the encrypted effect shown in Fig. 6d does not significantly improve in comparison with Fig. 6b. In the DWT domain, all LL, HL, and LH are encrypted and fingerprinted in parallel, so HL and LH encryption can only increase the visual security effect.

The proposed medical image encryption scheme includes confusion and diffusion. The diffusion is an inverse SVD multiply operation. If the selective confusion operation in the DWT is broken, the part decrypted medical image cannot be understood because the random matrix for diffusion-based SVD operation can make the part decrypted and fingerprinted image not intelligible.

Figure 6e shows that the diffusion based on SVD operation is applied, and Fig. 6b,c,d does not use SVD operation. According to the encrypted results, it can be seen that the SVD operation can increase the encryption effect. The visual metric of the encrypted images in Fig. 6e is decreased very apparently compared to the confusion processes which do not use SVD operation. Therefore the perceptual security for privacy protection can be enhanced when the diffusion process is adopted. In this case, if a higher security level of

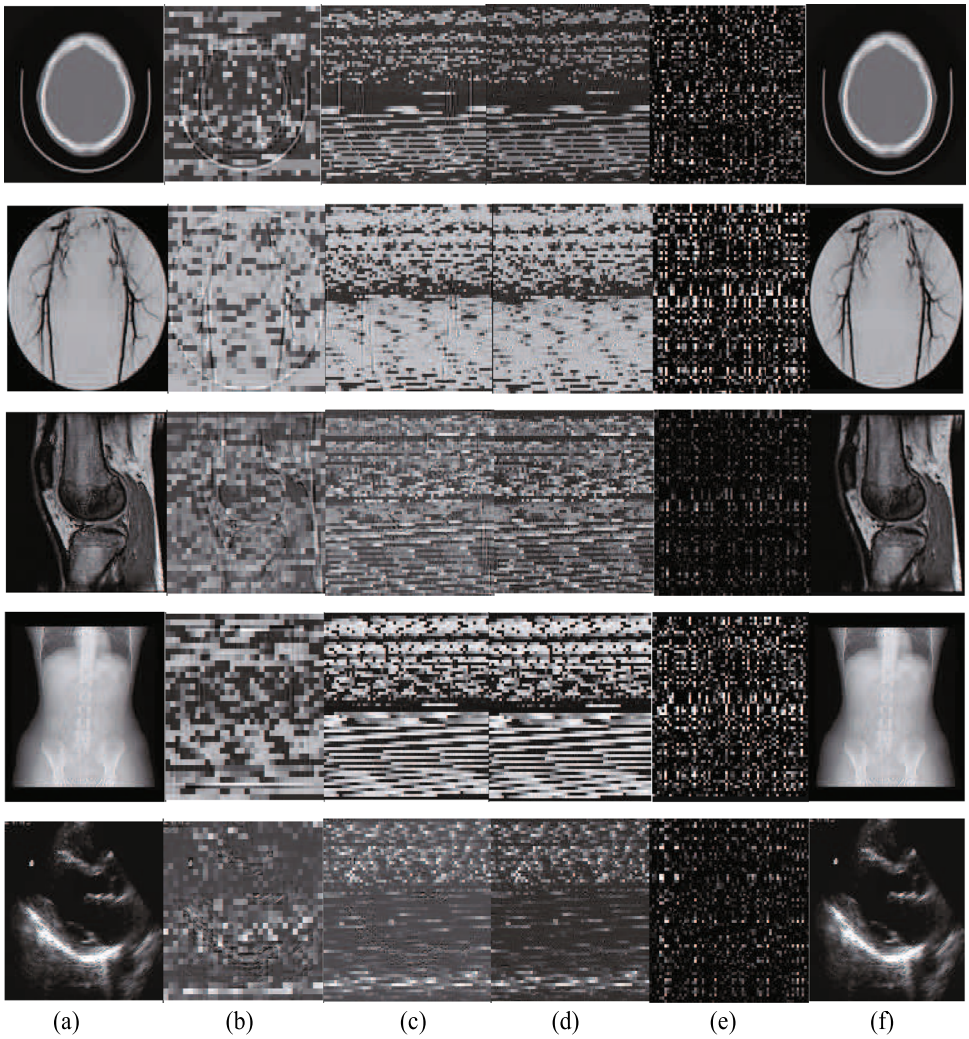

Fig. 6 Discussion of the selective encryption: (**a**) original medical images, (**b**) 4×4 blocks permutation via GOL in the LL2 subband, (**c**) images which are permutated by single coefficient permutation via GOL, (**d**) images which are permutated by 4×4 blocks permutation in the LL2 subband, HL subbands, and LH subbands, (**e**) 4×4 blocks permutation in the LL2 subband and diffusion with SVD operation, (**f**) decrypted fingerprinted images

Table 1 Entropy

ImageNo.	(a)	(b)	(c)	(d)	(e)	(f)
1	5.6297	6.6311	6.6933	6.6045	4.8610	5.6297
2	5.7949	6.6720	6.9328	6.9161	4.6363	5.7949
3	6.8947	6.9050	7.1470	7.2886	4.6704	6.8974
4	6.5635	7.1273	7.3487	7.4057	4.8778	6.5635
5	5.7715	6.4712	6.3996	6.4980	4.4484	6.7715

Table 2 PSNR

ImageNo.	(b)	(c)	(d)	(e)	(f)
1	27.2055	27.2144	27.1539	25.0105	∞
2	27.8985	27.1978	27.1213	26.4180	∞
3	29.1171	28.1715	27.5892	25.7583	∞
4	28.1527	27.8725	26.7735	26.5763	∞
5	28.9128	28.3186	26.4928	25.5527	∞

confidentiality is demanded, diffusion with SVD operation can be adopted. On the other hand, the selective encryption method via GOL without diffusion can perform on medical images, because even if the original medical images can not be told through a rough sketch without more details. For medical images in the SHCS, detailed medical information would not be revealed. The rough sketch of the encrypted and fingerprinted medical image makes the perceptual quality unacceptable. Privacy is still protected in the medical area. Therefore, selective encryption not only meets the fast request but also is very suitable for medical image encryption.

Furthermore, some different ways are used to evaluate the suggested joint encryption and fingerprinting scheme. These ways, which include information entropy, Peak Signal to Noise Ratio (PSNR), Number of Pixel Change Rate (NPCR), Unified Averaged Changed Intensity (UACI), mainly evaluate image security performance. Those images in Fig. 6 are evaluated. From top to bottom, the numbers of these images are labeled as 1, 2, 3, 4, and 5.

Table 3 NPCR and UACI experimental results

	NPCR				UACI			
	b	c	d	e	b	c	d	e
1	0.9983	0.9991	0.9982	0.9911	0.2757	0.2802	0.2529	0.2647
2	0.9903	0.9933	0.9913	0.9113	0.2205	0.2556	0.2547	0.3994
3	0.9942	0.9954	0.9955	0.9880	0.2342	0.2642	0.2451	0.2671
4	0.9978	0.9975	0.9977	0.9152	0.3132	0.3571	0.3627	0.3535
5	0.9980	0.9964	0.9951	0.9953	0.2208	0.2433	0.1898	0.1856

Table 4 Time efficiency(s)

ImageNo.	JEF	Decryption	Total
1	1.41005	0.76415	2.1742
2	1.4576	0.7656	2.2232
3	1.35945	0.78625	2.1457
4	1.43286	0.79364	2.2265
5	1.2786	0.719	1.9976

The information entropy is defined as follows:

$$H(m) = -\sum_{i=0}^{L} P(m_i) \log_2 P(m_i), \tag{18}$$

where m_i is the i th grey value for an L level grey image, $P(m_i)$ is the emergence probability of m_i , so $\sum_{i=0}^{L} P(m_i) = 1$. For an encrypted image, the value of the information entropy should be different from that of the corresponding original image. We obtained information entropy according to Table 1. According to Table 1, the information entropy of original images and their corresponding decrypted fingerprinted images is the same. Therefore, the visual metric of decrypted fingerprinted images is not decreased in comparison with that of their corresponding original images.

The PSNR is mainly used to evaluate the visual quality of an image. The PSNR is computed as follows:

$$PSNR\,(I_1, I_2) = 10log_{10}\left(\frac{\left[2^{dep}-1\right]^2}{MSE\,(I_1, I_2)}\right) \tag{19}$$

$$MSE\,(I_1, I_2) = \frac{1}{L}\sum\nolimits_{k=1}^{L}[I_1(k) - I_2(k)]^2, \tag{20}$$

where L is the number of pixels of the image I, k is the pixel number of the image. I_1 are I_2 two different images which have some relationship, and dep is its depth. Usually, dep equals 8. Then, $PSNR = 10 \times \log_{10}(255^2/MSE)$.

Table 2 lists PSNR value of images in Fig. 6 with its corresponding original images. From Table 2, (b) means the PSNR value of images in Fig. 6b with its corresponding original images in Fig. 6(a), so do (c), (d), (e), and (f). All PSNR values in Table 2(b), (c), (d), and (e) is below 30dB. And according to Fig. 6b, c, d, e, it is not accepted by the human visual system (HVS). The decrypted fingerprinted medical images and its corresponding original medical images are shown in Fig. 6f, a respectively. The PSNR value of images in Fig. 6f with the corresponding images in Fig. 6a is infinite. There is no data loss in the decrypted fingerprinted medical images with the proposed joint encryption and fingerprinting scheme.

Differential attack is mainly used to calculate the differences of the original pixel with its changes in the cipher image. Two main categories of differential attack analysis are NPCR and UACI. Through comparing the original image and its corresponding encrypted image, the difference between the original image and the encrypted image can be found out. It is called differential attack. Such difference can be measured by two criteria, namely the NPCR and UACI. They can be calculated as follows:

$$C(i,j) = \begin{cases} 0, & if\ T_1(i,j) = T_2(i,j) \\ 1, & if\ T_1(i,j) \neq T_2(i,j) \end{cases} \tag{21}$$

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\% \tag{22}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} ||T_1(i,j) - T_2(i,j)||}{M \times N \times 255} \times 100\%, \tag{23}$$

where T_1 and T_2 are two different images. M and N are the image width and height. $C(i, j)$ is a bipolar array with the same size as image T_1. $C(i, j)$ is determined using Eq. (21). For an encrypted image and its corresponding original image, NPCR measures the percentage of different pixels between them. UACI measures the average intensity of differences between them. The high NPCR values mean that the position of each pixel is dramatically randomized. And UACI values represent how many pixels in the encrypted image are changed to indistinguishable. To illustrate the performance of the proposed algorithm, Table 3 lists the NPCR and UACI results of those encrypted images with their corresponding original images shown in Fig. 6. These results demonstrates that our algorithm has a strong security ability to resist attack.

Table 5 Comparisons of the Related Schemes

	Ours	[29]	[30]	[31]	[32]	[33]
Watermarking	Yes	Yes	Yes	No	Yes	Yes
Selective encryption	Yes	No	No	No	No	No
Tracing	Yes	No	Yes	No	Yes	Yes
Scalability	Yes	No	No	No	No	No
Communication security	Yes	Yes	Yes	Yes	Yes	Yes
Watermark domain	DWT	Spatial	Spatial	No	DWT	DWT/DCT
Encryption domain	DWT	Spatial	Spatial	Spatial	Spatial	Spatial
Encryption scheme	Chaos	RC4	RC4	BC	BC	Chaos
Total overhead	Light	Heavy	Heavy	Light	Light	Heavy

Table 6 Encryption time comparison(s)

ImageNo.	ours	[33]
1	0.8124	29.1572
2	0.8167	29.2915
3	0.8936	29.3219
4	0.9012	29.1628
5	0.8103	28.7533

Encryption and fingerprinting efficiency

In all applications of the SHCS, privacy protection efficiency of the SHCS is very important for people. The efficiency of the proposed combination of encryption and fingerprinting is evaluated. Efficiency and comparative analysis are discussed as follows. In the case of the SHCS, there are some resource-constrained devices connected to the system through the IoMT. For medical image sharing in the SHCS, if a privacy protection algorithm takes a huge amount of time to embed fingerprints into a medical image and encrypt a medical image, then the proposed algorithm can not be applied in the SHCS. Therefore, the real-time efficiency is analyzed.

In the proposed combination of encryption and fingerprinting technique, time efficiency is mainly affected by two factors, which are: 1) JEF operation, and 2) decryption process. The time that the two factors took is calculated and shown in Table 1. Both JEF operation and decryption process are performed on a Pentium(R) Dual-Core E5700 computer, and the software platform is MATLAB 9. According to Table 1, it is known that the JEF took more time than the medical image decryption operation. The total JEF process took 1.5 s or so, but the second factor only took 0.6–0.8s. So, it can be seen that the proposed combination of encryption and fingerprinting scheme is efficient. With the JEF operation, privacy protection services can be provided. The JEF algorithm is fast for the SHCS. Table 4 shows the computing time of images in Fig. 6.

Comparative analysis

Comparative analysis with the related work is presented. The considered medical image protection technique is a joint encryption/watermarking algorithm proposed by D. Bouslimi et al. [30], watermarking algorithm [29], image encryption scheme [31], dual watermarking scheme [32], and multilayer security method [33]. Both of encryption/watermarking algorithm [30] and watermarking algorithm [29] proposed a joint of RC45 stream cipher scheme and digital watermarking technology. In the proposed joint model, the illegal user can be traced by watermarked information. But the RC45 algorithm still takes a high encryption time complex concerned to the potential enormous data of medical images. On the other hand, watermarking and encryption are conducted in the spatial domain. Encryption of all spatial pixel data will make the proposed joint approach inefficient.

The proposed combination of encryption and fingerprinting algorithm can improve the aforementioned problem by incorporating selective confusion by GOL and SVD diffusion in the DWT domain. In the DWT domain, all encryption and fingerprinting operation can be performed in parallel. Furthermore, it is very clear that GOL and SVD operation is very fast and the random matrix produced by chaotic maps is very sensitive to keys. Therefore, the final random matrix will change apparently with even a slight change in the initial seed. Furthermore, the proposed diffusion encryption technique by SVD operation is perceptually efficient for higher security requests. SVD operation has another benefit, the random matrix used to diffuse is invertible. Therefore the decryption operation is very fast, and the decrypted and fingerprinted medical image can be reconstructed very conveniently. Digital fingerprinting can track who redistributes the decrypted copy compared to digital watermarking. The above comparative analysis shows the proposed combination of encryption and fingerprinting can make improvements to the existing watermarking and encryption technique for medical image security.

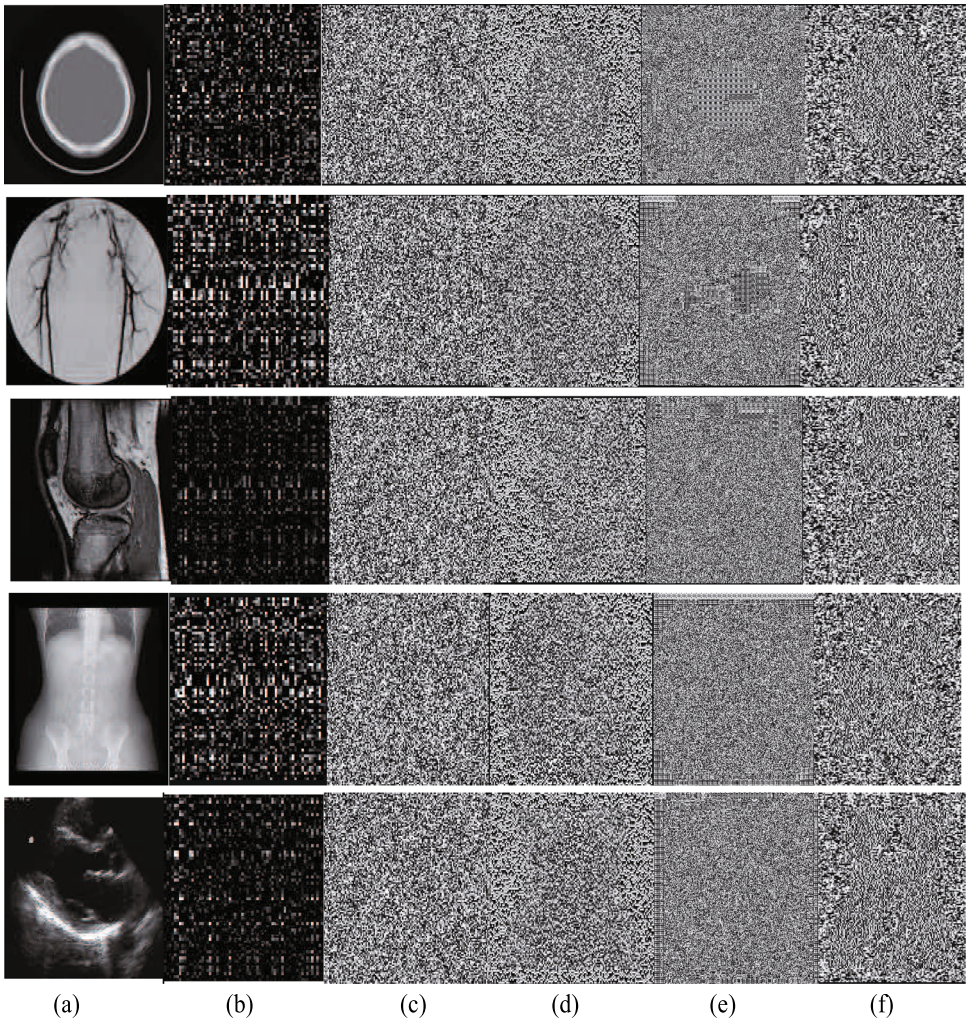

Fig. 7 Original medical images and encrypted images with different schemes

Table 5 summarizes the roles of the proposed approach and five existing medical image security schemes, i.e., watermarking algorithm [29], joint watermarking and encryption method [30], image encryption scheme [31], dual watermarking scheme [32], and multi-layer security method [33]. In Table 5, selective encryption means that only the important part, rather than the whole content, is encrypted. Rivest Cipher (RC) 4 is a stream encryption algorithm. BC is a block cipher.

As the existing schemes conducted in the spatial domain and only provided part security protection, they can not provide multilevel security and privacy protection for SHCS. With these schemes, a high comprehensive security measure is not guaranteed. For a SHCS oriented medical image sharing system, the scheme should be sensitive to scalability in a way that the fingerprinted content can be protected according to the security requirements. This can be achieved by introducing a scalable joint encryption and fingerprinting in the DWT domain. Table 6 lists the encryption time of our scheme and that of [33]. Compared to the method in [33], the proposed scheme took less time to encrypt.

The different encrypted images with different schemes are shown in Fig. 7. The Fig. 7a shows the original medical images, the Fig. 7b demonstrates the encrypted images with the proposed scheme, the Fig. 7c indicates the encrypted images with the scheme in [29], the Fig. 7d demonstrates the encrypted images using the joint watermarking and encryption method [30], the Fig. 7e shows the encrypted images with the dual watermarking scheme [32], the Fig. 7f indicates the encrypted images with the multi-layer security method [33].

The different decrypted images with different schemes are shown in Fig. 8. The Fig. 8a shows the decrypted images with the proposed scheme, the Fig. 8b indicates the decrypted images with the scheme in [29], the Fig. 8c demonstrates the decrypted images using the joint watermarking and encryption method [30], the Fig. 8d shows the decrypted images with the dual watermarking scheme [32], the Fig. 8e indicates the decrypted images with the multi-layer security method [33]. From Fig. 8, all the decrypted images loo like the orig-

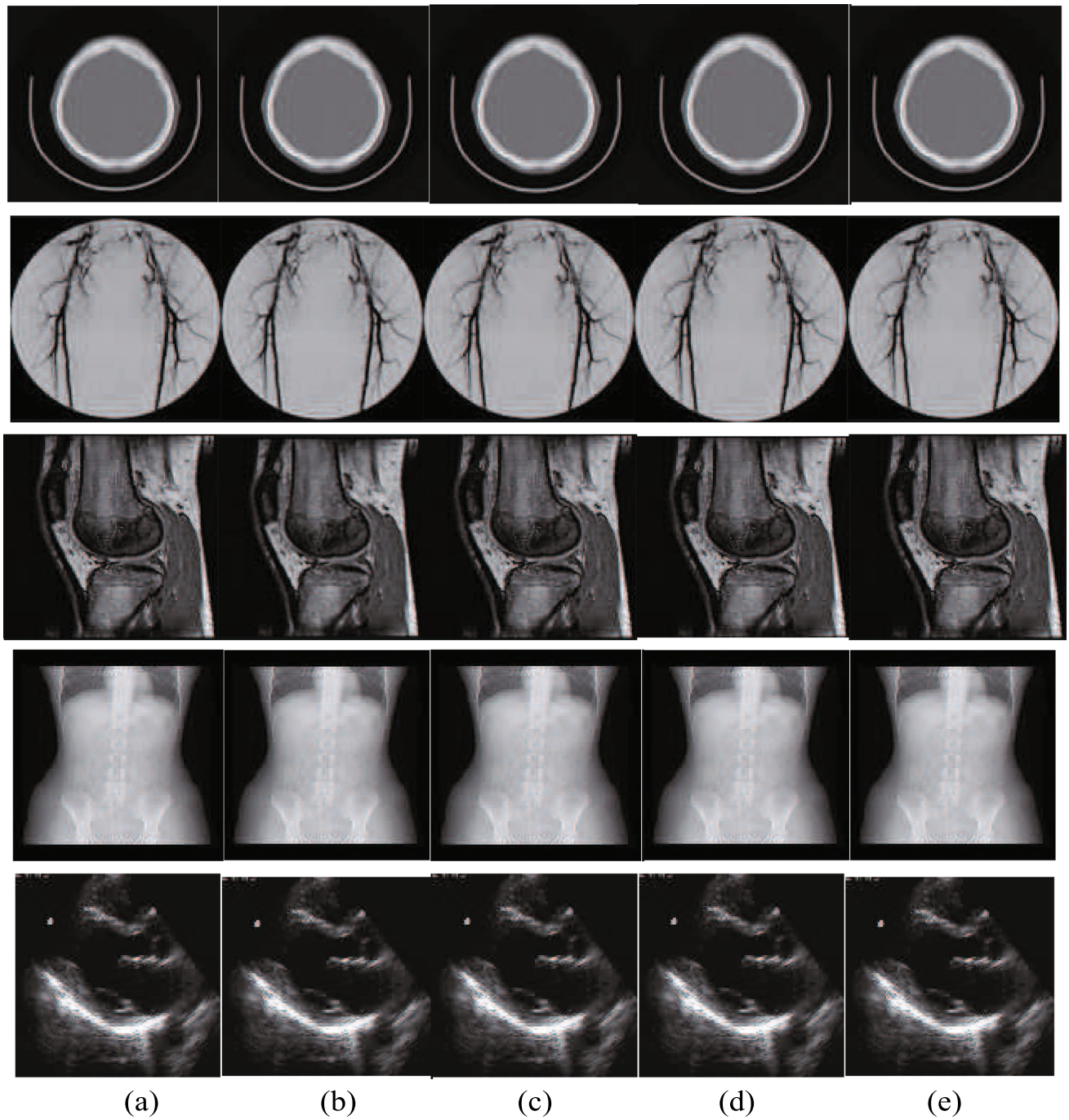

Fig. 8 Decrypted images with different schemes

inal medical images in the Fig. 6a. Their visual quality is not affected.

From Fig. 7, all the encrypted images are noise-like. The visual effect of all encrypted medical images is very poor. Original medical image information can not be perceptible from the encrypted images. With these encryption algorithms, the privacy of medical images can be protected. However, the proposed scheme is a selective encryption way,

Table 7 Quantitative measurements comparison

Average value	Ours	[29]	[30]	[32]	[33]
Entropy	4.6988	7.9885	7.9916	7.9514	7.9335
PSNR	∞	55.9318	60.2318	48.6539	36.8246
NPCR	0.9602	0.9966	0.9992	0.9962	0.9961
UACI	0.2941	0.2627	0.2705	0.2640	0.2695

only important content in the DWT domain is chosen to encrypt. In comparison with image encryption in the spatial domain, selective encryption in the DWT domain can provide advantages such as scalability, controllable security level, low time complex, parallel security computing, and watermark/fingerprint detection in the encrypted domain.

Table 7 summarizes some quantitative measurements of the proposed approach and four existing medical image security schemes, i.e., watermarking algorithm [29], joint watermarking and encryption method [30], dual watermarking scheme [32], and multi-layer security method [33]. In Table 7, information entropy, PSNR, NPCR, and UACI are demonstrated. Because the proposed scheme only chose the most coefficients to encrypt, the average information entropy and NPCR are lower than those with the encryption methods in the spatial domain. All spatial domain methods encrypt all image pixels. For all these spatial domain methods, the watermark/fingerprint must be embedded in the transform domain, and then through the inverse transform, the watermarked image is encrypted in the spatial domain. In this case, watermark detection must be in the decrypted domain. In the end, the image privacy can be disclosed for authentication or traitor tracing. In the proposed scheme, the confused content is different from the watermarked content. Therefore, watermark detection can be performed on the encrypted content. Even if the proposed scheme is a selective encryption method, the average PSNR and UACI outperform those of the existing methods in Table 7. Most important of all, the proposed scheme can meet different security level requirements in the SHCS.

Conclusion

In this paper, we proposed a combination of encryption and fingerprinting algorithms for privacy protection in the SHCS. The fingerprint information is embedded into the low bit planes of LL subband, HL subband, and LH subband in the DWT domain. The encryption includes confusion of the M highest bit planes of LL subband via GOL and diffusion with SVD operation in the DWT domain, the latter can improve the encryption effect. The two encryption algorithms are selective encryption. Only important coefficients are chosen to encrypt to meet the fast security request in the SHCS. The encrypted and fingerprinted results and discussion demonstrate that the scheme has not only a large key space to resist brute-force, and statistical attacks, but also an imperceptible visual effect of encrypted and fingerprinted images. Furthermore, the proposed combination scheme has a low time complexity compared to spatial encryption because only the important content is chosen for encryption. All encryption and fingerprinting operation can be performed in parallel. In the end, time efficiency is desirable to meet fast security requests. The proposed combination scheme is a good candidate technology applied in the SHCS for medical image security.

In the future, we will investigate and research the practical security level requirements in the SHCS, so that we can balance the security level and time complexity of the proposed method.

Acknowledgements This related work is funded by NSFC Grants 61502154 , the NSF of Hubei Province (Nos.2015CFB236), Hubei Provincial Department of Education Project(No.D20142703), and Youth Team Project of Hubei Provincial Department of Education(No.T201410).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Mohan PH (2020) Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Future Generation Comput Syst 111:213–225
2. Mohamed E, Shankar K, Lakshmanaprabu SK, Andino M, Arunkumar N, (AUG, (2020) Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Comput Appl 32(15):10979–10993
3. Yang Y, Xianghan Z, Wenzhong G, Ximeng L, Victor C, (APR, (2019) Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Inform Sci 479:567–592
4. Randhir K, Rakesh T (2021) Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. J Supercomput
5. Hathaliya Jigna J, Sudeep T (2020) An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput Commun 153:311–335
6. Wei J, Chen X, Huang X, Hu X, Susilo W (2019) Rs-habe: Revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud. IEEE Trans Dependable Secure Comput, pages 1–1
7. Dzwonkowski M, Rykaczewski R (2019) Secure quaternion feistel cipher for dicom images. IEEE Trans Image Process 28(1):371–380

8. Satendra Pal Singh and Gaurav Bhatnagar (2021) A novel biometric inspired robust security framework for medical images. IEEE Trans Knowl Data Eng 33(3):810–823
9. Balasamy K, Suganyadevi S (2020) A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. Multimedia Tools Appl
10. Rohit T, Ashish K (2020) Multi-level security of medical images based on encryption and watermarking for telemedicine applications. Multimedia Tools Appl
11. Dong X, Zhang W, Shah M, Wang B, Yu N (2020) Watermarking-based secure plaintext image protocols for storage, show, deletion and retrieval in the cloud. IEEE Trans Services Comput, pages 1–1
12. Thakur S, Singh AK, Ghrera SP (JAN 25 2021) NSCT domain-based secure multiple-watermarking technique through lightweight encryption for medical images. Concurrency Comput Practice Exp, 33(2, SI)
13. Anand A, Singh AK (2020) Joint watermarking-encryption-ecc for patient record security in wavelet domain. IEEE MultiMedia 27(3):66–75
14. Anand A, Singh AK, Lv Z, Bhatnagar G (2020) Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE MultiMedia 27(4):133–143
15. Haddad S, Coatrieux G, Moreau-Gaudry A, Cozic M (2020) Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains. IEEE Trans Inform Forensics Secur 15:2556–2569
16. Kundur D, Karthik K (2004) Video fingerprinting and encryption principles for digital rights management. Proc IEEE 92(6):918–932
17. Conghuan Y, Hefei L, Zenggang X, Fuhao Z, Cong L, Fang X (2016) Secure Social Multimedia Big Data Sharing Using Scalable JFE in the TSHWT Domain. ACM Trans Multimedia Comput Commun Appl, 12(4, S)
18. Liu Ruizhen, Tan Tieniu (2002) An svd-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 4(1):121–128
19. Liu RZ, Tan TN, (MAR, (2002) An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 4(1):121–128
20. Thompson Eric (2005) Md5 collisions and the impact on computer forensics. Digital Investigation 2(1):36–40
21. Cid Carlos (2006) Recent developments in cryptographic hash functions: security implications and future directions. Inform Secur Tech Rep 11(2):100–107
22. Wang Xiaoyun, Yu Hongbo (2005) How to break md5 and other hash functions. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pages 19–35, Berlin, Heidelberg. Springer Berlin Heidelberg
23. Jungk Bernhard, Stoettinger Marc (2016) Serialized lightweight sha-3 fpga implementations. *Microprocessors and Microsystems*, 71, NOV 2019. International Conference on Reconfigurable Computing and FPGAs (ReConFig), Cancun, MEXICO, NOV 30-DEC 02
24. Smah A (2022) Forensic hash value guidelines: Why md5 and sha1 should no longer be used and a recommendation for their replacement. 03
25. Jiahui Wu, Liao Xiaofeng, Yang Bo (2018) Image encryption using 2d hénon-sine map and dna approach. Signal Process 153:11–23
26. Wang Xingyuan Xu B, Huaguang Z (2010) A multi-ary number communication system based on hyperchaotic system of 6th-order cellular neural network. Communications in Nonlinear Science and Numerical Simulation 15(1):124–133
27. Wolfram S (2002) A new kind of science
28. Zhihua G, Xiuli C, Jitong Z, Yushu Z, Yiran C (2020) An effective image compression-encryption scheme based on compressive sensing (CS) and game of life (GOL). Neural Comput Appl 32(17):14113–14141
29. Ali A-H, Heba A-N (2021) An efficient watermarking algorithm for medical images. Multimedia Tools Appl 80(17):26021–26047
30. Bouslimi D, Coatrieux G, Cozic M, Roux C (2012) A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans Inform Technol Biomed 16(5):891–899
31. Omer K (2022) Secure medical image encryption with walsh-hadamard transform and lightweight cryptography algorithm. Med Biol Eng Comput 60(6):1585–1594
32. Anand A, Amit Kumar S (2022) Dual watermarking for security of covid-19 patient record. IEEE Trans Dependable Secure Comput, pages 1–1
33. Thakur Sriti, Singh Amit Kumar, Ghrera Satya Prakash, Elhoseny Mohamed (FEB 2019) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia Tools Appl*, 78(3):3457–3470,