A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images

XIYAO LIU[1], JIETING LOU[1], HUI FANG[2], YAN CHEN[3], PINGBO OUYANG[4], YIFAN WANG[1], BEIJI ZOU[1], LEI WANG[1]*

[1]School of Computer Science and Engineering, Central South University, Changsha, 410083, China
[2]Computer Science Department, Loughborough University, Loughborough, UK
[3]School of Medicine, University of Nottingham, Nottingham, UK
[4]Second Xiangya Hospital of Central South University, Central South University, Changsha, 410083, China

Corresponding author: Lei Wang (e-mail: wanglei@csu.edu.cn)

This research is supported by the National Natural Science Foundation of China (61602527, 61573380, 61772555), Natural Science Foundation of Hunan Province (2017JJ3416, 2018JJ2548), China Postdoctoral Science Foundation (2017M612585) and State Scholarship Fund offered by China Scholarship Council (201806375002).

ABSTRACT It is of great importance in telemedicine to protect authenticity and integrity of medical images. They are mainly addressed by two technologies, which are region of interest (ROI) lossless watermarking and reversible watermarking. However, the former causes biases on diagnosis by distorting region of none interest (RONI) and introduces security risks by segmenting image spatially for watermark embedding. The latter fails to provide reliable recovery function for the tampered areas when protecting image integrity. To address these issues, a novel robust reversible watermarking scheme is proposed in this paper. In our scheme, a reversible watermarking method is designed based on recursive dither modulation (RDM) to avoid biases on diagnosis. In addition, RDM is combined with Slantlet transform and singular value decomposition to provide a reliable solution for protecting image authenticity. Moreover, ROI and RONI are divided for watermark generation to design an effective recovery function under limited embedding capacity. Finally, watermarks are embedded into whole medical images to avoid the risks caused by segmenting image spatially. Experimental results demonstrate that our proposed lossless scheme not only has remarkable imperceptibility and sufficient robustness, but also provides reliable authentication, tamper detection, localization and recovery functions, which outperforms existing schemes for protecting medical images.

INDEX TERMS Robust reversible watermarking, authenticity, integrity, medical image

I. INTRODUCTION

Telemedicine is a potential way to provide more convenient medical services for patients in near future [1]-[3]. However, medical images transmitted through network in telemedicine applications can be easily tampered and forged, which increases the risks of misdiagnosis. Therefore, the image authenticity and integrity have become two crucial security factors in telemedicine applications [4]-[6]. Authenticity guarantees that medical images are not forged from the attackers and belong to the correct medical institutes or patients [7]-[9]. Integrity means that medical images have not been modified by non-authorized people [10]-[12]. The schemes designed to protect the authenticity and integrity of medical images are required to ensure that these images are distortion free. Otherwise, the image distortions may lead to misdiagnosis and even endanger patients' lives.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

Existing watermarking schemes used for verifying authenticity and integrity of medical images can be classified into two main categories, which are region of interest (ROI) lossless watermarking schemes [13]-[21] and reversible watermarking schemes [22]-[29]:

ROI lossless watermarking schemes divide medical images into ROI, which is considered as the most important part for medical diagnosis, and region of none interests (RONI) in spatial domain. Tamper detection, localization and recovery information of ROI are generated as the watermarks. These watermarks are embedded into ROI reversibly or RONI irreversibly. In this manner, the integrity of ROI is well protected with necessary localization and recovery functions for the tampered areas of attacked ROI. However, RONI cannot be restored losslessly in these schemes, and thus there are still negative impacts on diagnosis although the ROI is distortion free. Furthermore, the segmentation of ROI and RONI in spatial domain for watermark embedding incurs extra security risks because it is easy to destroy all the information embedded in RONI by simply replacing the RONI spatially.

Reversible watermarking schemes can restore medical images losslessly and avoid the security risks caused by spatial segmentation of the ROI and RONI for watermark embedding. However, due to the limited embedding capacity of reversible watermarking, they do not embed tamper recovery information into medical images and thus cannot provide any recover function for the tampered areas of attacked medical images.

In this paper, a novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images is proposed to solve the above-mentioned issues. There are four phases in our scheme: 1) watermark generation phase; 2) watermark embedding phase; 3) watermark extraction phase; and 4) security verification phase.

In the first phase, authenticity data and integrity data are generated. Our authenticity data is hash values of a hospital logo and our integrity data includes tamper detection, localization, and recovery information. In specific, the tamper detection information is generated by using hash function of a whole medical image. The tamper localization information is generated by calculating Cyclic Redundancy Check (CRC) of each ROI block. And the tamper recovery information is generated by using integer wavelet transform (IWT) coefficients of ROI with block truncation coding (BTC). In the second phase, all the watermarks are embedded into the medical image using Slantlet transform (SLT), singular value decomposition (SVD) and recursive dither modulation (RDM) to ensure the watermarking robustness. In the third phase, an inverse process of watermark embedding is performed to extract the watermarks. After all the watermarks are extracted, the medical image is restored losslessly based on the RDM function. The final phase verifies the authenticity and integrity of medical images and recovers their tampered areas of ROI if they are attacked.

To our best knowledge, it is the first watermarking scheme which divides ROI and RONI for watermark generation but not for watermark embedding. The differences between our proposed scheme and other existing schemes are illustrated in Figure 1. Furthermore, the key contributions of our proposed watermarking scheme are summarized as follows:

1) A SLT-SVD and RDM based reversible watermarking method is designed, which ensures sufficient watermark robustness and can restore both ROI and RONI losslessly.

2) ROI and RONI are divided for the generation of tamper localization and recovery information to provide an effective recovery function for the tampered ROI under limited embedding capacity, which cannot be achieved by existing reversible watermarking schemes.

3) IWT and BTC are used to generate tamper recovery information of ROI. The use of these methods offers a remarkable trade-off between visual quality of the recovered ROI and its required embedding capacity.

4) Watermarks are embedded into the whole medical images without dividing ROI and RONI. In this manner, the security risks caused by the segmentation of the ROI and the RONI in spatial domain for watermark embedding are avoided, which outperforms existing ROI-lossless watermarking schemes.

Experiments have been implemented on 200 medical images including 40 Computed Tomography (CT) images, 40 magnetic resonance images (MRI), 40 Ultrasound images, 40 X-ray images and 40 fundus images. The results demonstrate that our proposed scheme not only ensures remarkable watermarking imperceptibility and robustness but also provides reliable authentication, tamper detection, localization and recovery for medical images.

The rest of paper is organized as follows: the related works are discussed in Section II. Our proposed watermarking scheme is described in detail in Section III. Experiment results and discussions are presented in Section IV. Finally, conclusions of this paper are presented in Section V.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

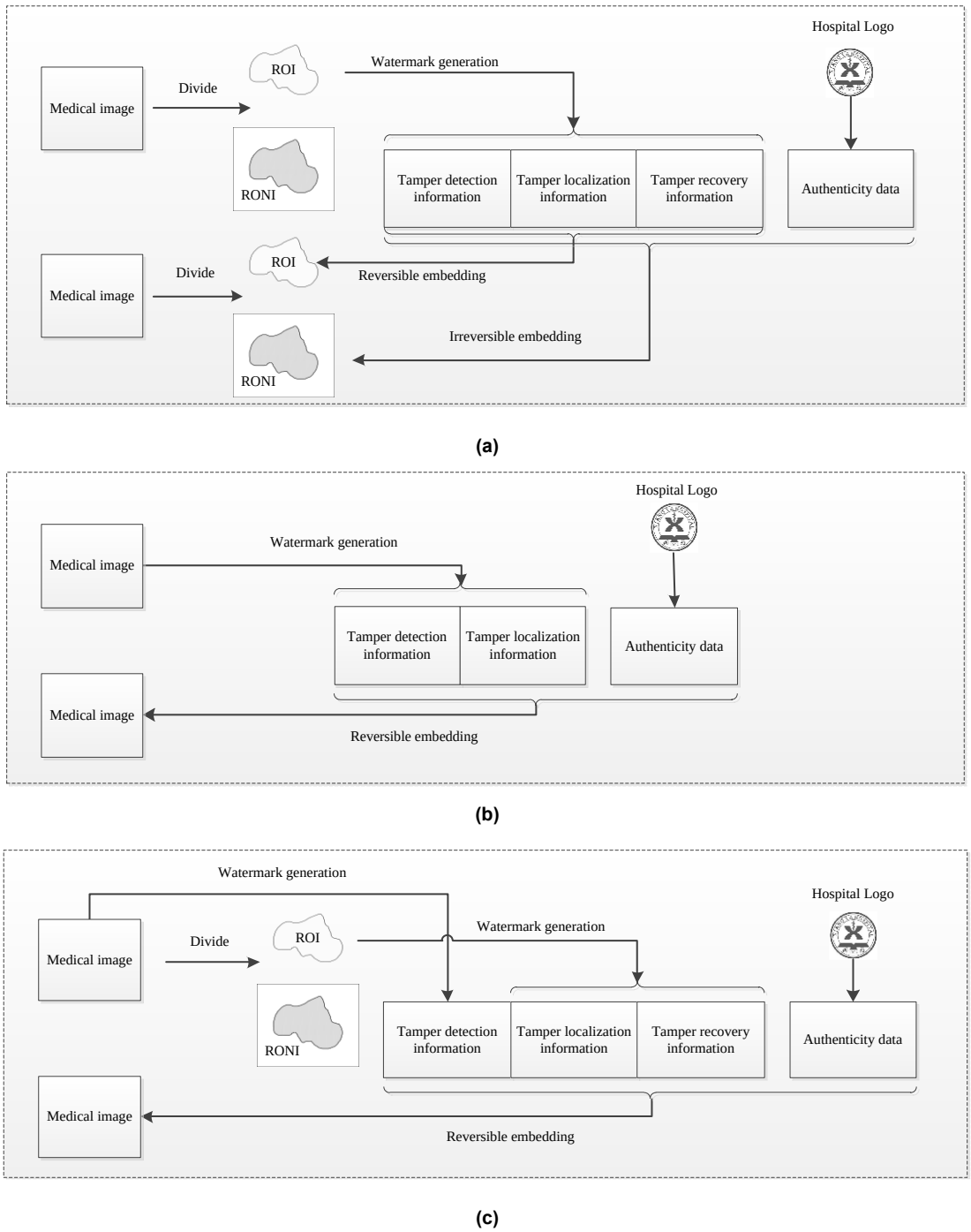

FIGURE 1. **Differences between our proposed watermarking scheme and other existing watermarking schemes. (a) ROI-lossless watermarking scheme, (b) reversible watermarking scheme, (c) our proposed watermarking scheme**

II. RELATED WORK

A. ROI-LOSSLESS WATERMARKING

ROI-lossless watermarking schemes divide medical images into ROI and RONI in spatial domain for watermarks generation and embedding. Tjokorda et al. [13] propose a ROI-lossless watermarking scheme, in which the least significant bits (LSB) of ROI pixels are replaced by tamper detection information, tamper localization information and tamper recovery information. The original LSBs of ROI pixels are compressed by run length encoding (RLE) and then embedded into RONI by replacing two LSBs of RONI pixels to ensure the reversibility of ROI. Liew et al. [14] propose another ROI-lossless watermarking scheme, in

which CRC of each ROI block and JPEG compression of ROI are embedded into LSBs of RONI for tamper localization and tamper recovery. Eswaraiah et al. [15] propose LSB-based watermarking scheme, in which hash value of ROI and original ROI LSBs are compressed by using RLE and embedded into LSBs of ROI for tamper detection. The parity bit of mean values of ROI blocks and mean values of ROI blocks are embedded into LSBs of RONI for tamper localization and tamper recovery. Kim et al. [16] keep ROI undistorted and embed tamper localization information and tamper recovery information of ROI into RONI by using homogeneity analysis and histogram shifting. Priya et al. [17] propose a LSB-based watermarking scheme, in which hash values of each ROI block and compression of ROI are embedded into LSBs of RONI for tamper localization and tamper recovery. All these watermarking schemes embed watermarks into the spatial domain of ROI or RONI fragilely. Therefore, the embedded watermarks are destroyed when medical images are attacked. It leads to a failure of tamper localization and recovery for the tampered areas of images. To address this issue, frequency domain-based ROI-lossless watermarking schemes are proposed. Maheshkar et al. [18] propose a frequency domain ROI-lossless watermarking scheme, in which tamper detection information and localization information are embedded into ROI by replacing two LSBs of each pixel. The original ROI LSBs as recovery information is embedded into RONI along with hospital logo and electronic patient record (EPR) by using IWT-SVD hybrid transform. Alhaj et al. [19] propose another frequency domain watermarking scheme, in which LSBs of ROI are replaced by fragile watermark to detect tamper. Three watermarks, hospital logo, EPR and original ROI LSBs, are embedded into RONI by using discrete wavelet transform (DWT) and SVD. Compared with the spatial domain ROI-lossless watermarking schemes, the frequency domain ROI-lossless watermarking schemes provide stronger robustness against attacks.

However, none of the above-mentioned ROI-lossless watermarking schemes can restore RONI losslessly, which increases the risks on the diagnosis. In addition, medical images are divided into ROI and RONI in spatial domain for watermark embedding in these schemes, which introducing additional security risks because all the information embedded in RONI can be destroyed easily by simply replacing the RONI spatially.

B. REVERSIBLE WATERMARKING

To address the issues of ROI-lossless watermarking schemes, reversible watermarking schemes are proposed. Reversible watermarking schemes do not divide medical images into ROI and RONI for watermark generation and watermark embedding. Thodi et al. [22] propose a fragile reversible watermarking scheme, in which watermarks are embedded based on prediction-error expansion. Gouenou et al. [23] apply histogram shifting modulation on prediction-errors to make use of the local specificities of the image for higher watermark capacity and image quality. In addition, they design a classification process to select the part of image which can be watermarked. Luo et al. [24] propose an interpolation-error based watermarking scheme to improve the quality of watermarked images. Zhang et al. [25] generate watermark based on quantized discrete cosine transform (DCT) coefficients of each block and then embed it into LSBs of corresponding block to detect and locate tamper. Although the scheme [25] can locate tampered blocks, the located blocks cannot be recovered. Ishtiaq et al. [26] propose a prediction-error expansion based watermarking scheme, in which a hybrid predictor is used to enhance the prediction efficiency and the adaptive embedding is used to improve embedding capacity. Feng et al. [27] use wavelet histogram shifting for reversible embedding. In addition, Logistic mapping, Torus mapping and CRC are used to improve the security of the watermark. These fragile reversible watermarking schemes can protect integrity of medical images effectively and restore medical images losslessly. However, when medical images are attacked, the embedded watermarks are destroyed and cannot be extracted correctly to protect authenticity of medical images. To address this issue, robust reversible watermarking schemes are proposed. Lei et al. [28] propose an IWT-SVD based watermarking scheme, in which SVD is performed on the low frequency coefficients of wavelet transform. The first singular value is then selected and one watermark bit is embedded into it by using RDM. Thabit et al. [29] propose a SLT-based watermarking scheme, in which one watermark bit is embedded by modifying the difference between the mean values of low-high frequency sub-bands and those of high-low frequency sub-bands in SLT domain. Compared with fragile reversible watermarking schemes, robust reversible watermarking schemes provide stronger robustness to resist attacks.

However, none of the above-mentioned

reversible watermarking schemes embed tamper recovery information into medical images to provide any recovery function for the tampered areas of the attacked medical images because their embedding capacity is limited.

III. PROPOSED SCHEME

Our proposed robust reversible watermarking scheme provides an effective and simultaneous solution for verifying authenticity and integrity of medical images. In our proposed scheme, the authenticity data is generated from the hash values of a hospital logo. ROI and RONI are divided for generation of integrity data to satisfy the limitation of watermark embedding capacity. Hash function of a whole medical image is used to generate tamper detection information. To locate the tampered areas of ROI, ROI is divided into 16×16 non-overlapping blocks and CRC is adopted on every block for generating tamper localization information of ROI. A method based on IWT coefficients is used to generate tamper recovery information of ROI [20]. In addition, BTC is adopted to further reduce the size of tamper recovery information of ROI. Authenticity data, tamper detection information of the medical image, tamper localization and recovery information of ROI are embedded into the whole medical image. As shown in Figure 2, our proposed reversible watermarking scheme has four phases: watermark generation phase, watermark embedding phase, watermark extraction phase and security verification phase. The detailed processes of each phase are described below.

A. WATERMARK GENERATION PHASE

In this phase, the generated watermarks consist of authenticity data and integrity data. Authenticity data is hash values of a hospital logo. And integrity data includes tamper detection information of the whole medical image, tamper localization and recovery information of ROI. The processes of watermarks generation phase are shown in Figure 3 and described below.

1) GENERATION OF AUTHENTICITY DATA

Because the possibility that hash functions of different messages are the same is closed to 0, the hash function is applied to generate authenticity data as shown in Eq. (1).

$$A = f(L) \tag{1}$$

where $f(\bullet)$ is SHA-1 hash function, L is a hospital logo, A is the 160-bit authenticity data.

2) GENERATION OF TAMPER DETECTION INFORMATION

Due to the same reason with that for generation of authenticity data, the hash function is also applied to generate tamper detection information as shown in Eq. (2).

$$D = f(M) \tag{2}$$

where $f(\bullet)$ is SHA-1 hash function, M is a medical image, D is a 160-bit tamper detection information of the medical image.

3) GENERATION OF TAMPER LOCALIZATION INFORMATION

In this paper, CRC-16 [30] is applied to generate tamper localization information of ROI instead of using hash functions. The steps of generation of tamper localization information are as follows:

Step 1: Normalize the ROI selected by clinicians, as shown in Figure 4. In addition, the coordinates of normalized ROI are saved as side information.

Step 2: Divide normalized ROI into 16×16 non-overlapping blocks.

Step 3: Select a fixed polynomial generator $G(x) = x^{16}+x^{15}+x^2+1$, which can be converted to a binary digital "1100000000000101".

Step 4: Convert each pixel of a block to 8-bit binary numbers and rearrange them to a vector.

Step 5: Append 16 0's to the end of this vector.

Step 6: Divide the vector by the polynomial generator based on the binary division to obtain the 16-bit remainder as CRC of a block for tamper localization. An example of the process of CRC is shown as follows:

FIGURE 2. The four different phases of our proposed watermarking scheme

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

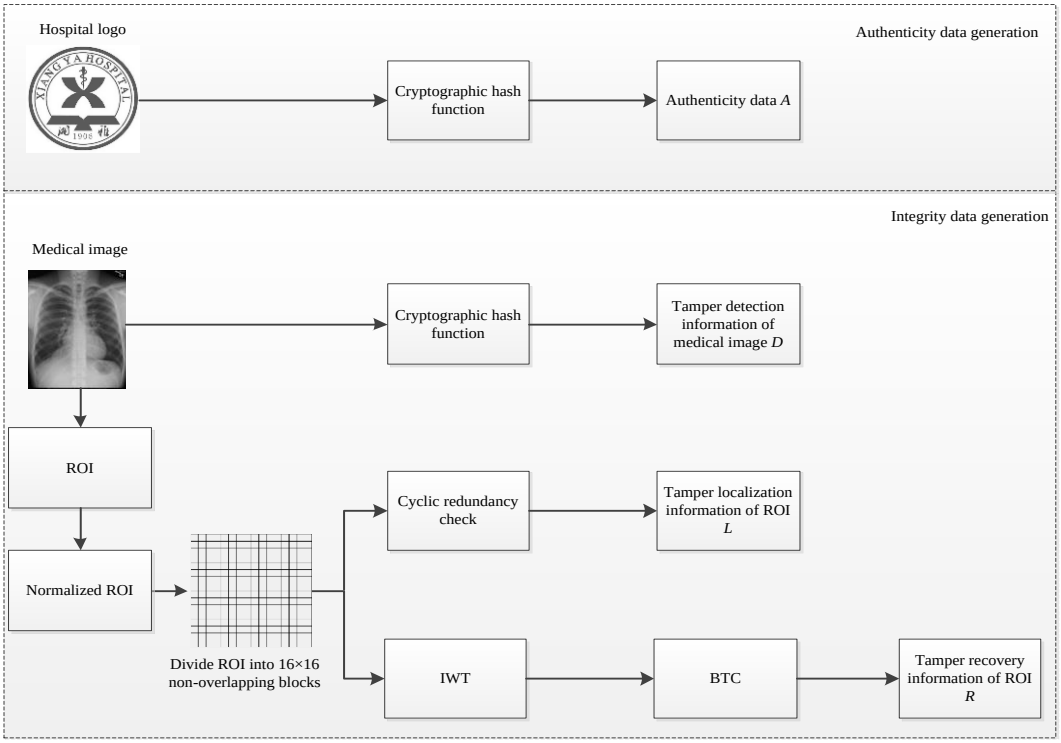

FIGURE 3. **The process of watermark generation phase**

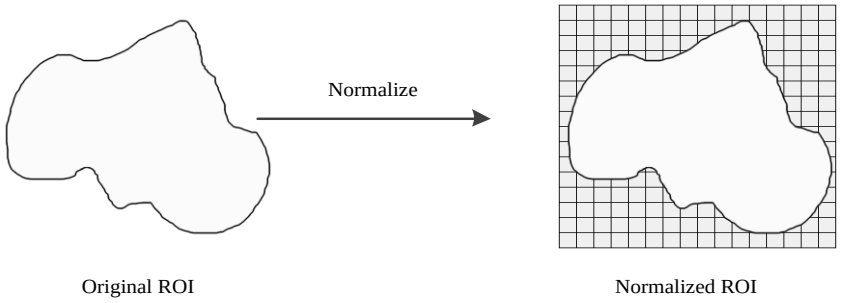

FIGURE 4. **The normalization of ROI**

Assume that the information is a 7-bit binary string "1100111". Add 16 0's to the end of "1100111" to obtain information "11001110000000000000000". Then, the information is divided by fixed polynomial generator "1100000000000101" to obtain 16-bit remainder "1000000101010001".

Repeat steps 3-6 until CRCs of all blocks have been calculated and combine all CRCs to obtain tamper localization information of ROI which is denoted as L.

4) GENERATION OF TAMPER RECOVERY INFORMATION

A trade-off is needed between the quality of recovered ROI and data size of tamper recovery information because of the limitation of watermark embedding capacity. We notice that the approximation coefficients matrix of IWT, which is much smaller than original image, still includes the major information of image due to the characteristics of multi-scale resolution of IWT. Therefore, this matrix is used for generating tamper recovery information of ROI in our scheme. In addition, BTC [31], which has not much impact on the quality of recovered ROI, is applied to further reduce the data size of recovery information. In our scheme, the approximation coefficient matrix is divided into 4×4 non-overlapping blocks for BTC to obtain a remarkable trade-off between required embedding capacity and quality of the recovered medical image. The detailed steps of tamper recovery information generation are as follows:

Step 1: Apply IWT on ROI I_m and obtain Approximation (CA), Horizontal (CH), Vertical

(*CV*) and Diagonal (*CD*) coefficient matrices.

Step 2: Divide *CA* into 4×4 non-overlapping blocks and apply BTC on each block to obtain a series of triples of binary matrix *B*, reconstructive level *u*1 and *u*2, as shown in algorithm 1.

Algorithm 1 The encoding of BTC

Input: medical block *I*

Output: Binary matrix *B*, reconstructive level *u*1, and reconstructive level *u*2.

1: *u*=mean2(*I*)
2: *row*=size(*I*,1), *col*=size(*I*,2)
3: *B*=zeros(*row*, *col*)
4: *sum*1=0,*sum*2=0,*q*1=0,*q*2=0
5: for *i*=1:*row*
6: for *j*=1:*col*
7: if *I*(*i*, *j*) < *u*
8: *sum*1=*sum*1+*I*(*i*, *j*), *q*1=*q*1+1
9: else
10: *sum*2=*sum*2+*I*(i, j), *q*2=*q*2+1, *B*(*i*, *j*)=1
11: end
12: end
13:end
14: *u*1=round(*sum*1/*q*1), *u*2=round(*sum*2/*q*2)

Step 3: Convert *u*1 and *u*2 to 8-bit binary numbers respectively and then save these numbers in *b*1 and *b*2.

Step 4: Rearrange *B* to a vector and combine this vector and *b*1, *b*2 to obtain tamper recovery information of ROI *R*.

B. WATERMARK EMBEDDING PHASE

SLT [32], an equivalent representation of DWT, obtains a better trade-off between time-localization and smoothness characteristics than DWT and thus can provide a better trade-off between imperceptibility and robustness for watermark applications [33], [34]. Therefore, in our proposed watermarking scheme, SLT is used for watermark embedding. Moreover, SVD is utilized and the most significant value of singular values matrix *S* is selected for watermark embedding. The utilization of SVD further enhances the watermarking robustness because this value is invariant to various attacks. Furthermore, inspired by [28], RDM-based function is applied to embed watermarks, which can restore the medical image losslessly. In this phase, watermarks are embedded without dividing the medical image into ROI and RONI to avoid security risks caused by spatially image dividing, which is different from ROI-lossless watermarking schemes. The process of watermark embedding phase is shown in Figure 5 and described as follows:

Step 1: Design a preprocessing function to avoid overflows and underflows, which may occur after embedding watermark. Bit "0" and "1" are embedded separately into each medical image block to obtain two different watermarked images by using our proposed scheme. The maximum value of possible distortion caused by watermark embedding, donated as *T*, is calculated based on these two watermarked images and the original image.

Step 2: Divide the whole medical image into 8×8 non-overlapping blocks.

Step 3: Assign a unique number to each block in a zigzag order. Randomly pick a secret key *k* and use Eq. (3) to obtain scrambled map for watermark embedding *Y*. In this manner, the security level of watermark embedding is enhanced.

$$Y_i = \left[\left(k \times X_i \right) \bmod N_b \right] + 1 \tag{3}$$

where *X* is the zigzag ordering map for blocks, *Y* is the scrambled map for watermark embedding, N_b is the total number of blocks. i, $k \in [1, N_b]$. k should be a prime number and N_b should not be divided by k.

The Y_i^{th} bit of watermark information is embedded into the X_i^{th} block. An example of the zigzag ordering map for blocks and its scrambled map for watermark embedding when secret key k=3 is shown in Figure 6.

Step 4: Apply SLT on each block to obtain SLT coefficient matrix *TB* by using Eq. (4).

$$TB = MBM^T \tag{4}$$

where *TB* is the SLT coefficient matrix, *M* is an 8×8 Slantlet matrix. Note that the sizes of *TB*, *B* and *M* are the same.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

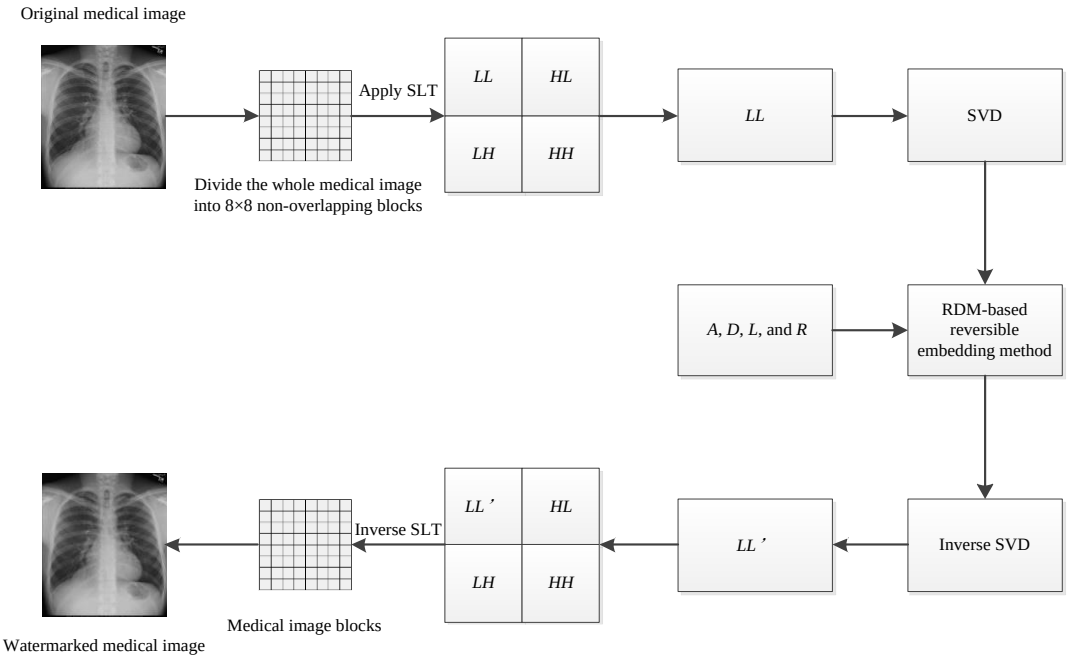

FIGURE 5. **The process of watermark embedding phase**

1	2	6	7
3	5	8	13
4	9	12	14
10	11	15	16

(a)

4	7	3	6
10	16	9	8
13	12	5	11
15	2	14	1

(b)

FIGURE 6. **An example of scrambling process, (a) zigzag ordering map for blocks, (b) scrambled map for watermark embedding**

Step 5: Divide *TB* into four sub-bands (*LL*, *HL*, *LH* and *HH*).

Step 6: Apply SVD to sub-bands *LL* by using Eq. (5).

$$LL = USV^T \tag{5}$$

where U and V are orthogonal matrices, S is a singular values matrix.

Step 7: Embed one watermark bit into singular values matrix S by adjusting $S(1,1)$ coefficient using RDM-based reversible embedding method as shown in algorithm 2. On one hand, $S'(1,1)$ and P should be in the same jitter interval as shown in Eq. (6) to ensure watermark can be extracted correctly. Therefore, the value of G should be smaller than $\Delta/2$. On the other hand, for the RDM based watermarking, the distortion E caused by watermark embedding will not be larger than Δ and the G will not be larger than 1. As a result, Δ should be larger than 2 to make sure that the watermark can be extracted correctly.

$$floor(P/\Delta) = floor(S'(1,1)/\Delta) \tag{6}$$

where the $floor(\bullet)$ is rounding toward negative infinity.

Algorithm 2 RDM-based reversible embedding method

Input: S matrix and quantization step Δ

Output: Watermarked singular values matrix S'

1: n=floor(S(1,1)/Δ)

2: if w=1 then

3: $m=n+1-\text{mod}(n,2)$

4: else

5: $m=n+1-\text{mod}(n+1,2)$

6: end

7: $P=m\times\Delta+\Delta/2$

8: $E= P-S(1,1)$

9: $G= E/\Delta$

10: $S'(1,1)=P+G$

Step 8: Apply inverse SVD on U, V and watermarked S' to obtain sub-band LL' by using Eq. (7).

$$LL' = US'V^T \tag{7}$$

where LL' is watermarked LL, S' is watermarked S.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

Step 9: Apply inverse SLT on sub-bands *HL*, *LH*, *HH* and *LL'* by using Eq. (8).

$$B^{'} = M^{T}\begin{bmatrix} LL^{'} & HL \\ LH & HH \end{bmatrix}M \tag{8}$$

where $B^{'}$ is watermarked medical image block.

Repeat steps 4 to 9 until all the watermark bits are embedded to obtain watermarked medical image.

In order to solve the overflow and underflow problems, the pixels of watermarked image are adjusted by using Eq. (9). As the same with [29], the coordinates of modified pixels are saved as side information. The maximum watermark distortion *T*, secret key *k*, coordinates of normalized ROI and shifted pixels are sent with the modified watermarked image to the receiver side.

$$I_m(i,j) = \begin{cases} I^{'}(i,j)+T & if\ \ I^{'}(i,j) < 0 \\ I^{'}(i,j) & if\ \ 0 \le I^{'}(i,j) \le 255 \\ I^{'}(i,j)-T & if\ \ I^{'}(i,j) > 255 \end{cases} \tag{9}$$

where *I'* is a watermarked image before pixel adjustment, (i, j) are the coordinates of pixels in image, and I_m is a modified watermarked image.

C. WATERMARK EXTRACTION PHASE

Extracting watermarks from the watermarked medical image is just the inverse process of embedding watermarks into the medical image. The process of extracting watermark phase is shown in Figure 7 and described as follows:

Step 1: Find the locations of shifted pixels and recover them to their original values based on the side information, as shown in Eq. (10).

$$I^{'}(i,j) = \begin{cases} I_m(i,j)-T & if\ \ I_m(i,j) < T \\ I_m(i,j)+T & if\ \ I_m(i,j) > 255-T \end{cases} \tag{10}$$

where $I'(i, j)$ is the original watermarked image pixel, $I_m(i, j)$ is the modified watermarked image pixel, and (i, j) are the coordinates of pixels in image.

Step 2: Divide the whole watermarked medical image into 8×8 non-overlapping blocks.

Step 3: According to the secret key *k*, obtain random embedding sequence *Y* as shown in Eq. (3).

Step 4: Apply SLT on each block to obtain SLT coefficient matrix *TB* by using Eq. (4).

Step 5: Divide *TB'* into four sub-bands (*LL'*, *HL*, *LH* and *HH*).

Step 6: Apply SVD on sub-band *LL'* to obtain singular values matrix *S'* by using Eq. (5).

Step 7: Extract watermark bit *w* from singular values matrix *S'* by using Eq. (11).

$$w = \mathrm{mod}(\mathit{floor}\left(S^{'}(1,1)/\Delta\right), 2) \tag{11}$$

where the *floor*(•) is rounding toward negative infinity.

Step 8: Restore the original singular values matrix by using RDM-based reversible method as shown in algorithm 3. Because *S'* (1,1) and *P* are in the same jitter interval as shown in Eq. (6), *P'* is equal to *P*. As a result, *E'* is equal to *E* and *S*(1,1) can be restored by using this algorithm.

Step 9: Apply inverse SVD and inverse SLT to obtain the restored medical image block.

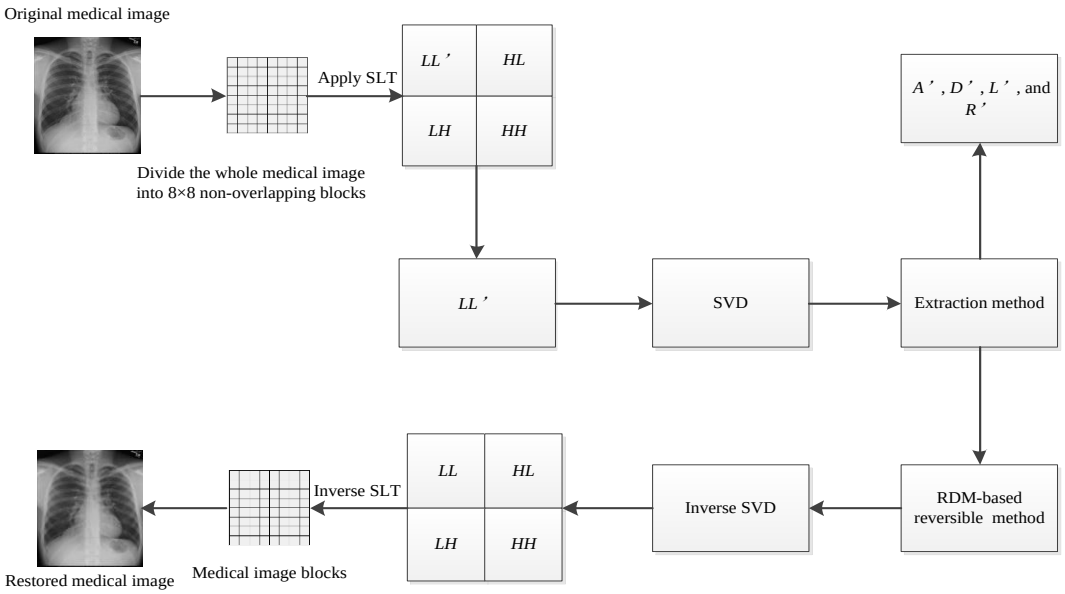

FIGURE 7. **The process of watermark extraction phase**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

Algorithm 3 RDM-based reversible method

Input: S' matrix, and quantization step Δ

Output: Restored singular values matrix S

1: n'=floor(S' (1,1)/Δ)

2: P'=n'×Δ+Δ/2

3: G'= S' (1,1)-P'

4: E'= G'×Δ

5: S(1,1)=P'-E'

Repeat steps 4 to 9 until all the watermark bits are extracted to obtain restored medical image. Reconstruct watermarks to obtain authenticity data A', tamper detection information of ROI D', tamper localization information of ROI L', and tamper recovery information of ROI R'.

D. SECURITY VERIFICATION PHASE

Security verification consists of the verification of authenticity and integrity. The former guarantees that medical images are from right source. The latter ensures that medical images have not been modified when they are transferred through networks. The processes of security verification and tamper recovery are shown in Figure 8 and Figure 9 and described as follows:

Step 1: Apply hash function on the hospital logo to obtain authenticity data A.

Step 2: Compare A with A' to ensure authenticity of a medical image. If the authenticity of the medical image is confirmed, run the next step of integrity verification. Otherwise, the medical image is considered as a forged image and our proposed scheme is finished.

Step 3: Apply hash function on the restored medical image to obtain tamper detection information D.

Step 4: Compare D with D' to verify the integrity of the medical image. If no distortions are detected, our proposed scheme is finished. Otherwise, continue to run steps 5-13.

Step 5: Obtain the coordinates of normalized ROI from the side information and divide the normalized ROI from the restored medical image.

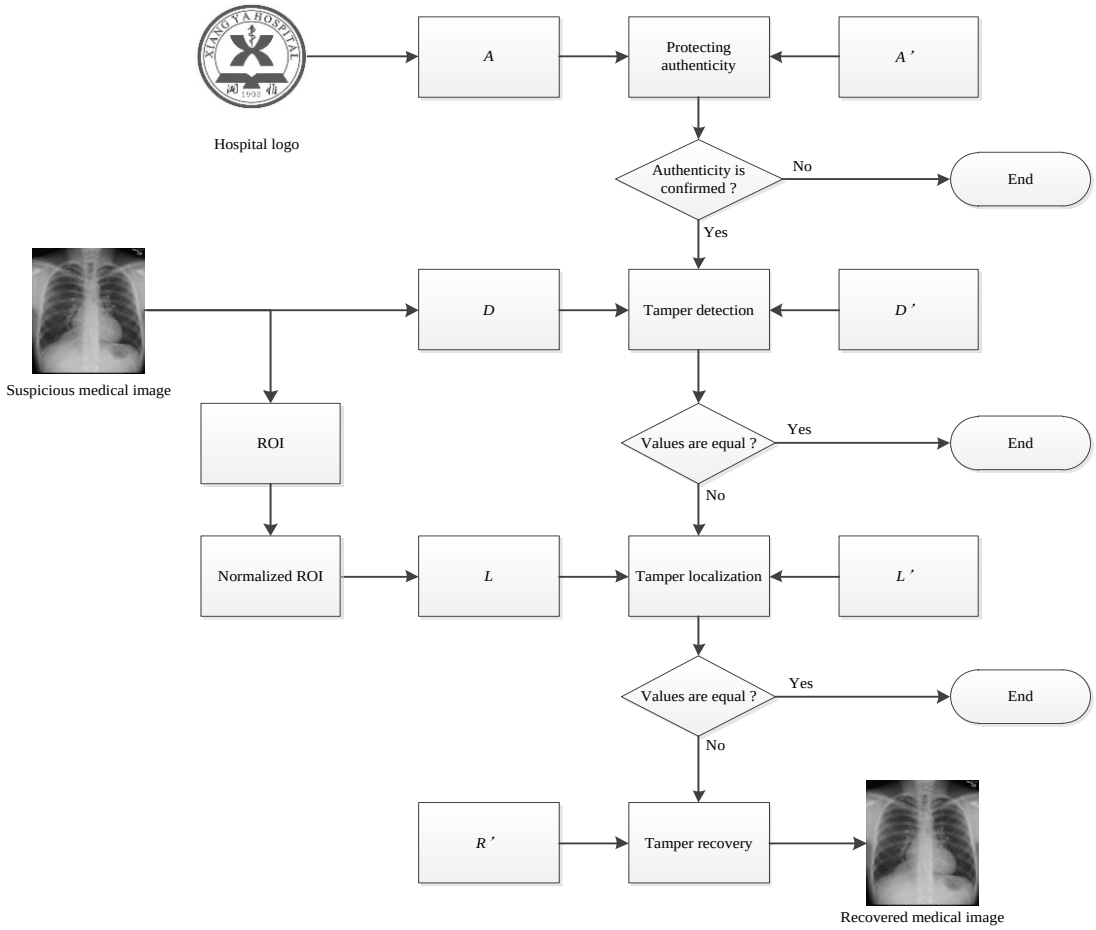

FIGURE 8. The process of security verification phase

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

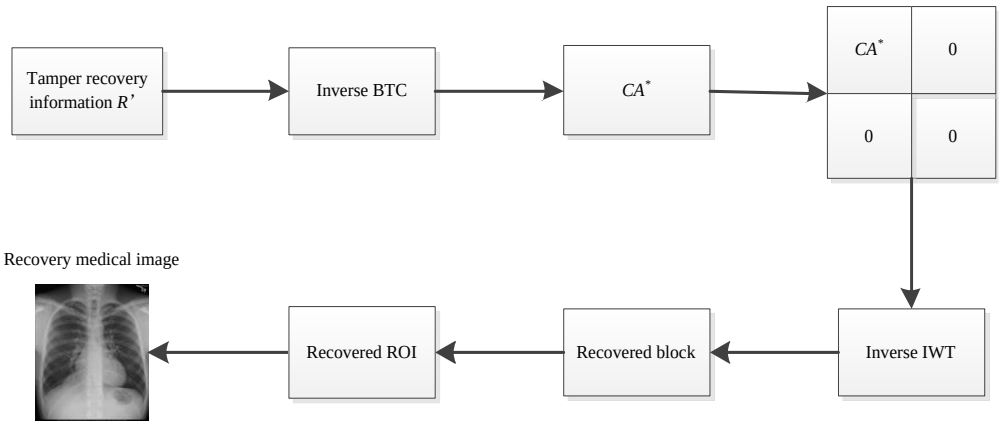

FIGURE 9. **The process of tamper recovery**

Step 6: Divide normalized ROI of the restored medical image into 16×16 non-overlapping blocks. Apply CRC on each block to obtain tamper localization information L.

Step 7: Compare L and L' to locate the tampered areas of ROI. If all these two values are equal, ROI is not distorted and our scheme is finished. Otherwise, run steps 8-13.

Step 8: Rearrange tamper recovery information of ROI R' and divide it to get bit-mapping B, 8-bit binary numbers $b1$ and 8-bit binary numbers $b2$.

Step 9: Convert $b1$ and $b2$ from binary value to decimal value and then obtain reconstructive level $u1$ and reconstructive level $u2$.

Step 10: The pixel value "0" in B is replaced by $u1$ and the pixel value "1" in B is replaced by $u2$ to obtain reconstructive approximation coefficient matrix CA^*.

Step 11: Set CH, CV and CD as zero matrices.

Step 12: Apply inverse IWT to obtain recovered blocks.

Step 13: Replace tampered blocks by recovered blocks for the recovery of ROI.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. EXPERIMENTAL SETUP

In this paper, the watermark imperceptibility is first evaluated in section B. Then, the watermark robustness is evaluated in section C. the performances of tamper detection, localization and recovery functions are evaluated in section D. Finally, qualitative comparisons between our proposed scheme and other existing watermarking schemes are presented in section E. Our testing database contains 200 medical images. These medical images include 40 CT images, 40 MRI images, 40 Ultrasound images, 40 X-ray images and 40 fundus images. Examples of five different types of medical images and a 32×32 hospital logo, which is used as the authenticity data, are shown in Figure 10. The quantization step Δ should be set to a suitable value to achieve a remarkable tradeoff between watermarking robustness and imperceptibility. The watermark robustness is stronger if the quantization step Δ is larger, but the watermark imperceptibility is worse at the same time. In our paper, Δ is set to 24 empirically.

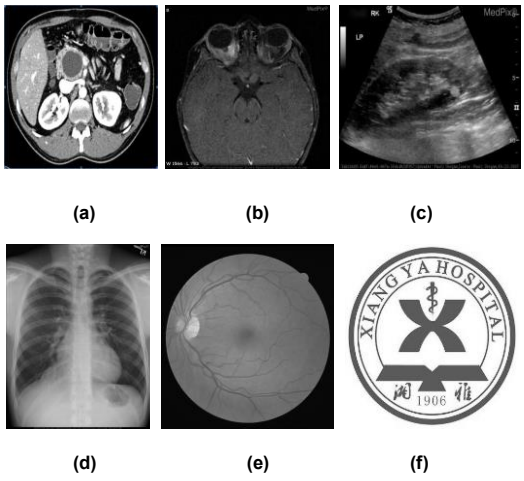

FIGURE 10. **Examples of five types of medical images and a binary hospital logo. (a) CT image, (b) MRI image, (c) Ultrasound image, (d) X-ray image, (e) fundus image, (f) hospital logo.**

B. EVALUATION OF WATERMARK IMPERCEPTIBILITY

To evaluate the imperceptibility of our proposed watermarking scheme, both subjective and objective tests are executed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

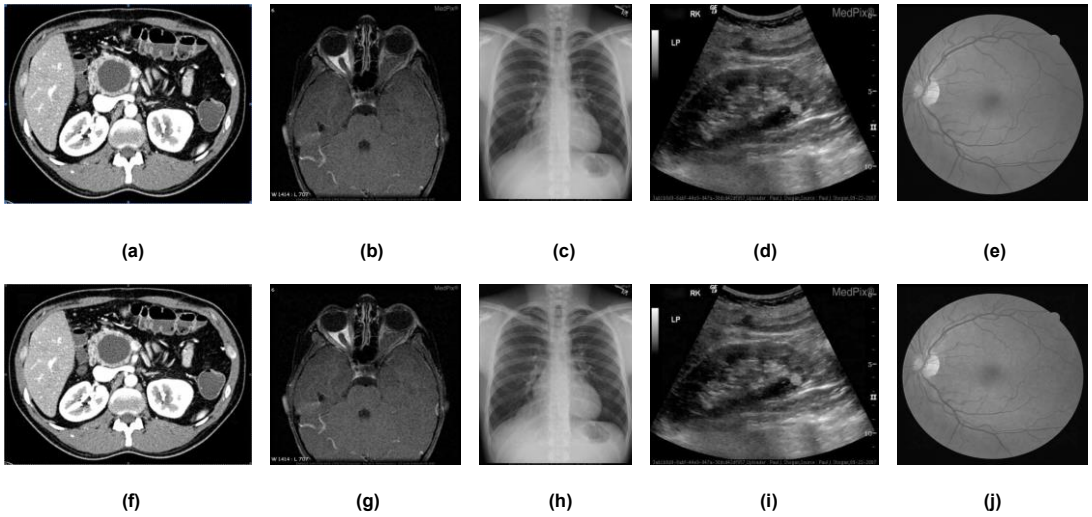

FIGURE 11. Examples of evaluating the watermarking imperceptibility. (a)-(e) original medical images, (f)-(j) watermarked medical images.

In the subjective test, examples of different medical images and corresponding watermarked images are shown in Figure 11. It is difficult to distinguish the difference between original medical images and watermarked medical images. These results demonstrate that the imperceptibility of our proposed watermarking scheme is remarkable.

In the objective test, the peak signal-to-noise ratio (*PSNR*) and structure similarity measure index (*SSIM*) between original medical images and watermarked medical images are calculated respectively to evaluate imperceptibility of our proposed watermarking scheme. The *PSNR* is calculated by using Eq. (12) and the *SSIM* is calculated by using Eq. (13).

$$PSNR = 10\log_{10}\left(\frac{255^2 \times H \times W}{\sum_{i=1}^{H}\sum_{j=1}^{W}\left(I(i,j)-I'(i,j)\right)^2}\right) \quad (12)$$

where I is a original medical image, I' is a watermarked image, H and W are the height and the width of medical images, (i, j) are coordinates of pixels in these images.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (13)$$

where μ_x, μ_y are the averages of x and y, σ^2_x, σ^2_y are the variances and σ_{xy} are covariance for x and y respectively. C_1 and C_2 are balancing constants.

PSNR and *SSIM* have ranges of [0, +∞] and [0, 1]. Two images are considered to be more similar if their *PSNR* is closer to +∞ and *SSIM* is closer to 1.

Mean *PSNR*s and mean *SSIM*s of our proposed watermarking scheme and other existing watermarking schemes [18], [20], [28], [29] are compared in Table 1. The mean PSNR of our proposed watermarking scheme is 41.2995. This value is slightly larger than those of Maheshkar et al.'s scheme [18] and Thabit et al.'s scheme [20], which are 39.7522 and 40.184. In addition, this value is comparable to those of Lei et al.'s scheme [28] and Thabit et al.'s scheme [29], which are 41.5525 and 42.8972. The mean SSIM of our proposed watermarking scheme is 0.9607. This value is the same with that of Thabit et al.'s scheme [20] and nearly equal to those of the compared watermarking schemes [18], [28], [29], which are 0.9669, 0.9660 and 0.9670. The results demonstrate that the imperceptibility of our proposed watermarking scheme is remarkable and comparable with those of state-of-art schemes. The reason of these results is the utilization of SLT transform for watermark embedding, which can provide a remarkable trade-off between imperceptibility and robustness.

TABLE 1. The mean *PSNR*s and the mean *SSIM*s of different watermarking schemes

	Proposed scheme	Maheshkar et al. [18]	Thabit et al. [20]	Lei et al. [28]	Thabit et al. [29]
PSNR	41.2995	39.7522	40.1841	41.5525	42.8972
SSIM	0.9607	0.9669	0.9607	0.9660	0.9670

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

C. EVALUATION OF WATERMARK ROBUSTNESS

To evaluate the robustness of watermarking schemes, bit error rate (*BER*) and normalized cross correlation (*NCC*) between original watermarks and extracted watermarks are calculated respectively according to Eq. (14) and Eq. (15). The value of *BER* is closer to 0 and the value of *NCC* is closer to 1, the robustness of watermarking scheme is stronger. 23 common attacks with different parameters, as shown in Table 2, are applied to test the watermarking robustness. In this section, our proposed scheme is compared with other four different existing watermarking schemes [18], [20], [28], [29] to demonstrate its superiority. The mean *BER*s and *NCC*s of authenticity data, tamper localization information, tamper recovery information of different schemes are listed in Table 3, 4 and 5, respectively.

$$BER = \frac{Number\ of\ incorrectly\ decoded\ bits}{Total\ number\ of\ bits} \quad (14)$$

$$NCC = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}\left(W_o(i,j)\times W_e(i,j)\right)}{\sum_{i=1}^{H}\sum_{j=1}^{W}W_o^2(i,j)} \quad (15)$$

where H and W are the height and the width of watermark, W_o is the original watermark, W_e is the extracted watermark, (i, j) are coordinates of pixels in these watermarks.

As shown in Table 3, all the mean *BER*s of authenticity data by using our proposed watermarking scheme are close to 0 and all the mean *NCC*s of authenticity data by using our proposed watermarking scheme are close to 1. These results demonstrate that our proposed watermarking scheme can provide reliable authenticity verification function for medical images. In addition, the average value of mean *BER*s of our proposed watermarking scheme, which is 0.0476, is smaller than those of Maheshkar et al.'s scheme [18], Thabit et al.'s scheme [20] and Lei et al.'s scheme [28], which are 0.0927, 0.0711, and 0.1003. This value is comparable to that of Thabit et al.'s scheme [29], which is 0.0365. The average value of mean *NCC*s of our proposed watermarking scheme, which is 0.9624, is larger than those of Maheshkar et al.'s scheme [18], Thabit et al.'s scheme [20] and Lei et al.'s scheme [28], which are 0.9322, 0.9362, and 0.8702. This value is comparable to that of Thabit et al.'s scheme [29], which is 0.9586. These results demonstrate that the reliability of authenticity verification function in our proposed watermarking scheme is higher than those in Maheshkar et al.'s scheme [18], Thabit et al.'s scheme [20] and Lei et al.'s scheme [28], and comparable with that in Thabit et al.'s scheme [29]. The reasons of the above phenomena are below. First, the utilization of low frequency coefficients of SLT transform, which concentrates the major energy of medical images, ensures the sufficient watermarking robustness. Second, the utilization of the largest singular value of SVD transform, which is also invariant to attacks, strengthens the watermarking robustness. Third, the utilization of RDM-based embedding method further enhances the watermarking robustness.

Especially, Thabit et al.'s scheme [20] modifies the difference between the mean values of low-high frequency sub-bands and those of high-low frequency sub-bands in SLT domain to embed authenticity data into ROI, whereas embeds tamper localization information and tamper recovery information into RONI by modifying the difference between the individual pixels of low-high frequency sub-bands and those of high-low frequency sub-bands in SLT domain. Therefore, the mean *BERs* and *NCCs* of authenticity data of this scheme are much better than those of tamper localization information and tamper recovery information, which are listed in Tables 4 and 5.

TABLE 2. Attacks with parameters

Attack type	Parameters	Attack type	Parameters
Average filtering (AF)	Window=3×3, 5×5	Median filtering (MF)	Window=3×3, 5×5
Gaussian blurring (GB)	Window=3×3, variance=0.5, 1	Crop from image edges (CR)	5%, 10%, 20%
Gaussian noise (GN)	variance=0.0001, Mean=0.001, 0.003, 0.0005	Salt & pepper noise (SN)	Density=0.001, 0.003, 0.0005
JPEG compression (JC)	Quality=70, 80	Resizing (RS)	0.8, 1.2
JPEG2000 compression	Compression ratio=4, 8	Wiener filter (WF)	Window=3×3, 5×5

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

TABLE 3. The mean *BER*s and *NCC*s of authenticity data under various attacks

Attacks	Proposed scheme		Maheshkar et al. [18]		Thabit et al. [20]		Lei et al. [28]		Thabit et al. [29]	
	BER	*NCC*	*BER*	*NCC*	*BER*	*NCC*	*BER*	*NCC*	*BER*	*NCC*
AF (3×3)	0.0705	0.9604	0.1071	0.8868	0.0622	0.9463	0.1485	0.8132	0.0146	0.9844
AF (5×5)	0.1371	0.8978	0.2425	0.7831	0.3393	0.6953	0.2659	0.6955	0.1424	0.8543
MF(3×3)	0.0457	0.9759	0.0866	0.9115	0.0539	0.9549	0.1039	0.8557	0.0162	0.9823
MF (5×5)	0.1098	0.9215	0.2353	0.7934	0.3807	0.6538	0.2170	0.7369	0.2138	0.7793
GB (0.5)	0.0094	0.9937	0.0162	0.9797	0.0000	1.0000	0.0217	0.9780	0.0000	1.0000
GB (1)	0.0914	0.9422	0.1064	0.8733	0.0491	0.9585	0.1671	0.7963	0.0031	0.9965
CR (5%)	0.0000	1.0000	0.0361	0.9879	0.0058	0.9956	0.0526	0.9081	0.0138	0.9816
CR (10%)	0.0000	1.0000	0.0793	0.9844	0.0130	0.9836	0.1051	0.8061	0.0610	0.8980
CR (20%)	0.0644	0.9803	0.1538	0.9842	0.0424	0.9455	0.1907	0.6402	0.1558	0.7643
GN (0.001)	0.0117	0.9885	0.0722	0.9273	0.0001	0.9993	0.0578	0.9357	0.0011	0.9990
GN (0.003)	0.0721	0.9016	0.0730	0.9268	0.0009	0.9992	0.1779	0.8116	0.0012	0.9989
GN (0.005)	0.1349	0.8723	0.0733	0.9260	0.0011	0.9991	0.2072	0.7818	0.0013	0.9987
SN (0.001)	0.0282	0.9744	0.0565	0.9791	0.0242	0.9786	0.0220	0.9386	0.0051	0.9950
SN (0.003)	0.0758	0.9306	0.0691	0.9642	0.0684	0.9399	0.0611	0.9386	0.0142	0.9855
SN (0.005)	0.1246	0.8866	0.0808	0.9493	0.1013	0.9100	0.0971	0.9023	0.0240	0.9758
JC (Q=70)	0.0061	0.9939	0.1062	0.9700	0.1294	0.8806	0.0155	0.9842	0.0422	0.9851
JC (Q=80)	0.0032	0.9982	0.0940	0.9721	0.0470	0.9577	0.0048	0.9955	0.0025	0.9970
JPEG2000 (4)	0.0023	0.9993	0.0475	0.9755	0.0012	0.9988	0.0021	0.9979	0.0044	0.9961
JPEG2000 (8)	0.0133	0.9874	0.0851	0.9539	0.0227	0.9819	0.0239	0.9616	0.0401	0.9638
RS (0.8)	0.0057	0.9972	0.0265	0.9683	0.0035	0.9975	0.0255	0.9654	0.0001	0.9999
RS (1.2)	0.0010	0.9988	0.0080	0.9906	0.0001	1.0000	0.0069	0.9934	0.0000	1.0000
WF (3×3)	0.0122	0.9935	0.0787	0.9203	0.0539	0.9662	0.1000	0.8629	0.0130	0.9871
WF (5×5)	0.0757	0.9418	0.1977	0.8320	0.2347	0.7911	0.2333	0.7280	0.0704	0.9250
Average	0.0476	0.9624	0.0927	0.9322	0.0711	0.9362	0.1003	0.8702	0.0365	0.9586

As shown in Table 4, all the mean *BER*s of tamper localization information by using our proposed watermarking scheme are close to 0 and all the mean *NCC*s of tamper localization information by using our proposed watermarking scheme are close to 1. These results demonstrate that our proposed watermarking scheme can provide reliable localization function for the tampered areas of medical images, which cannot be achieved by Lei et al.'s scheme [28], and Thabit et al.'s scheme [29]. In addition, the average value of mean *BER*s of our proposed watermarking scheme, which is 0.0462, is smaller than those of Maheshkar et al.'s scheme [18] and Thabit et al.'s scheme [20], which are 0.3502, and 0.2154. The average value of mean *NCC*s of our proposed watermarking scheme, which is 0.9562, is larger than those of Maheshkar et al.'s scheme [18] and Thabit et al.'s scheme [20], which are 0.6590, and 0.7752. These results demonstrate that the reliability of tamper localization function in our proposed watermarking scheme is higher than those in Maheshkar et al.'s scheme [18], and Thabit et al.'s scheme [20]. Reasons of the results in Table 4 are the same with those in Table 3.

Especially, Maheshkar et al.'s scheme [18] replaces LSBs of ROI to embed localization information whereas embeds hospital logo and tamper recovery information into RONI by using IWT-SVD based method. Therefore, the mean *BER*s and *NCC*s of tamper localization information of this scheme are much worse than those of hospital logo and tamper recovery information as shown in Tables 3 and 5.

As shown in Table 5, all the mean *BER*s of tamper recovery information by using our proposed watermarking scheme are close to 0 and all the mean *NCC*s of tamper recovery information by using our proposed watermarking scheme are close to 1. These results demonstrate that our proposed watermarking scheme can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

provide reliable recovery function for the tampered areas of medical images, which cannot be achieved by Lei et al.'s scheme [28], and Thabit et al.'s scheme [29]. In addition, the average value of mean *BER*s of our proposed watermarking scheme, which is 0.0456, is smaller than those of Maheshkar et al.'s scheme [18] and Thabit et al.'s scheme [20], which are 0.0889, and 0.2049. The average value of mean *NCC*s of our proposed watermarking scheme, which is 0.9562, is larger than those of Maheshkar et al.'s scheme [18] and Thabit et al.'s scheme [20], which are 0.9346, and 0.7377. These results demonstrate that the reliability of tamper recovery function in our proposed watermarking scheme is higher than those in Maheshkar et al.'s scheme [18], and Thabit et al.'s scheme [20]. Reasons of the results in Table 5 are the same with those in Table 3.

D. EVALUATION OF PERFORMANCES OF TAMPER DETECTION, LOCALIZATION AND RECOVERY FUNCTIONS

In this section, erasing and copy-paste tampering process is imposed on watermarked medical images to evaluate tamper detection, localization and recovery subjectively and objectively, as the same with [18], [20].

In the subjective test, erasing and copy-paste tampering process is imposed on watermarked medical images to evaluate tamper detection, localization and recovery. As shown in Figure 12, our proposed scheme can successfully detect and locate tampered areas of ROI. In addition, it is difficult to distinguish the difference between original medical images and recovered medical images. These results demonstrate that our proposed watermarking scheme can provide remarkable tamper detection, localization and recovery functions for tampered ROI.

TABLE 4. The mean *BER*s and *NCC*s of tamper localization information under various attacks

Attacks	Proposed scheme		Maheshkar et al. [18]		Thabit et al. [20]		Lei et al. [28]		Thabit et al. [29]	
	BER	*NCC*	*BER*	*NCC*	*BER*	*NCC*	*BER*	*NCC*	*BER*	*NCC*
AF (3×3)	0.0478	0.9541	0.4957	0.5041	0.4707	0.5134	N/A	N/A	N/A	N/A
AF (5×5)	0.1422	0.8525	0.5018	0.5006	0.4852	0.5001	N/A	N/A	N/A	N/A
MF(3×3)	0.0250	0.9687	0.3295	0.6695	0.4220	0.5641	N/A	N/A	N/A	N/A
MF (5×5)	0.1038	0.8900	0.5666	0.5632	0.5349	0.5007	N/A	N/A	N/A	N/A
GB (0.5)	0.0041	0.9944	0.4413	0.5581	0.0132	0.9862	N/A	N/A	N/A	N/A
GB (1)	0.0681	0.9322	0.4969	0.5028	0.2030	0.7907	N/A	N/A	N/A	N/A
CR (5%)	0.0000	1.0000	0.0124	0.9739	0.0223	0.9661	N/A	N/A	N/A	N/A
CR (10%)	0.0000	1.0000	0.0347	0.9273	0.0549	0.9097	N/A	N/A	N/A	N/A
CR (20%)	0.0627	0.8901	0.0812	0.8320	0.1668	0.7827	N/A	N/A	N/A	N/A
GN (0.001)	0.0103	0.9948	0.4977	0.5018	0.1101	0.8843	N/A	N/A	N/A	N/A
GN (0.003)	0.0587	0.9868	0.4979	0.5017	0.1102	0.8839	N/A	N/A	N/A	N/A
GN (0.005)	0.1395	0.9329	0.4999	0.5013	0.1112	0.8830	N/A	N/A	N/A	N/A
SN (0.001)	0.0358	0.9651	0.0006	0.9994	0.0261	0.9710	N/A	N/A	N/A	N/A
SN (0.003)	0.0970	0.9031	0.0015	0.9986	0.0649	0.9303	N/A	N/A	N/A	N/A
SN (0.005)	0.1397	0.8521	0.0026	0.9973	0.0959	0.8976	N/A	N/A	N/A	N/A
JC (Q=70)	0.0057	0.9965	0.4960	0.5036	0.4130	0.5706	N/A	N/A	N/A	N/A
JC (Q=80)	0.0041	0.9975	0.4931	0.5066	0.3564	0.6293	N/A	N/A	N/A	N/A
JPEG2000 (4)	0.0015	0.9985	0.2886	0.7107	0.0682	0.9296	N/A	N/A	N/A	N/A
JPEG2000 (8)	0.0088	0.9956	0.4565	0.5433	0.2527	0.7359	N/A	N/A	N/A	N/A
RS (0.8)	0.0026	0.9973	0.4709	0.5288	0.0980	0.8994	N/A	N/A	N/A	N/A
RS (1.2)	0.0008	0.9992	0.4009	0.5988	0.0175	0.9819	N/A	N/A	N/A	N/A
WF (3×3)	0.0113	0.9868	0.4908	0.6695	0.4220	0.5697	N/A	N/A	N/A	N/A
WF (5×5)	0.0929	0.9043	0.5007	0.5632	0.4345	0.5505	N/A	N/A	N/A	N/A
Average	0.0462	0.9562	0.3502	0.6590	0.2154	0.7752	N/A	N/A	N/A	N/A

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

TABLE 5. The mean *BER*s and *NC*s of tamper recovery information under various attacks

Attacks	Proposed scheme		Maheshkar et al. [18]		Thabit et al. [20]		Lei et al. [28]		Thabit et al. [29]	
	BER	*NC*	*BER*	*NC*	*BER*	*NC*	*BER*	*NC*	*BER*	*NC*
AF (3×3)	0.0397	0.9592	0.1043	0.8909	0.4240	0.4813	N/A	N/A	N/A	N/A
AF (5×5)	0.1508	0.8490	0.2377	0.7864	0.4740	0.4337	N/A	N/A	N/A	N/A
MF(3×3)	0.0254	0.9726	0.0838	0.9142	0.3734	0.5390	N/A	N/A	N/A	N/A
MF (5×5)	0.1114	0.8836	0.2300	0.7974	0.4785	0.4332	N/A	N/A	N/A	N/A
GB (0.5)	0.0044	0.9963	0.0154	0.9815	0.0163	0.9759	N/A	N/A	N/A	N/A
GB (1)	0.0607	0.9402	0.1046	0.8781	0.2202	0.7200	N/A	N/A	N/A	N/A
CR (5%)	0.0000	1.0000	0.0348	0.9874	0.0329	0.9357	N/A	N/A	N/A	N/A
CR (10%)	0.0000	1.0000	0.0759	0.9852	0.0849	0.8320	N/A	N/A	N/A	N/A
CR (20%)	0.0498	0.9183	0.1490	0.9845	0.2100	0.6919	N/A	N/A	N/A	N/A
GN (0.001)	0.0059	0.9950	0.0666	0.9327	0.1043	0.8540	N/A	N/A	N/A	N/A
GN (0.003)	0.0598	0.9860	0.0670	0.9323	0.1200	0.8538	N/A	N/A	N/A	N/A
GN (0.005)	0.1010	0.9486	0.0677	0.9315	0.1250	0.8531	N/A	N/A	N/A	N/A
SN (0.001)	0.0390	0.9599	0.0535	0.9802	0.0279	0.9584	N/A	N/A	N/A	N/A
SN (0.003)	0.1056	0.8935	0.0662	0.9651	0.0692	0.8999	N/A	N/A	N/A	N/A
SN (0.005)	0.1552	0.8373	0.0782	0.9508	0.0750	0.8498	N/A	N/A	N/A	N/A
JC (Q=70)	0.0043	0.9946	0.0974	0.9716	0.3785	0.5337	N/A	N/A	N/A	N/A
JC (Q=80)	0.0031	0.9957	0.0865	0.9732	0.3087	0.6147	N/A	N/A	N/A	N/A
JPEG2000 (4)	0.0020	0.9969	0.0452	0.9774	0.0750	0.9351	N/A	N/A	N/A	N/A
JPEG2000 (8)	0.0058	0.9941	0.0789	0.9564	0.2650	0.7258	N/A	N/A	N/A	N/A
RS (0.8)	0.0029	0.9975	0.0249	0.9705	0.1071	0.8645	N/A	N/A	N/A	N/A
RS (1.2)	0.0007	0.9992	0.0075	0.9915	0.0213	0.9704	N/A	N/A	N/A	N/A
WF (3×3)	0.0112	0.9867	0.0761	0.9233	0.4100	0.5187	N/A	N/A	N/A	N/A
WF (5×5)	0.1099	0.8873	0.1932	0.8336	0.4161	0.4927	N/A	N/A	N/A	N/A
Average	0.0456	0.9562	0.0889	0.9346	0.2049	0.7377	N/A	N/A	N/A	N/A

In the objective test, the false-positive rate P_{fpd} and the false-negative rate P_{fnd} of tamper detection under erasing and copy-paste tampering are calculated by using Eq. (16) and Eq. (17) and the results are listed in Table 6 and Table 7. P_{fpd} is a probability of considering a lossless image as a tampered one. P_{fnd} is a probability of considering a tampered image as lossless one.

$$P_{fpd} = \frac{N_{fpd}}{N_{disd}} \tag{16}$$

$$P_{fnd} = \frac{N_{fnd}}{N_{sd}} \tag{17}$$

where N_{fpd} is the number of lossless images which are considered as tampered ones, N_{disd} is the true number of lossless images, N_{fnd} is the number of tampered images which are considered as lossless ones, N_{sd} is the true number of tampered images.

The false-positive rate P_{fpl} and the false-negative rate P_{fnl} of tamper localization under erasing and copy-paste tampering are calculated by using Eq. (18) and Eq. (19) and the results are listed in Table 6 and Table 7. P_{fpl} is a probability of considering a lossless ROI block as tampered one. P_{fnl} is a probability of considering a tampered ROI block as lossless one.

$$P_{fpl} = \frac{N_{fpl}}{N_{disl}} \tag{18}$$

$$P_{fnl} = \frac{N_{fnl}}{N_{sl}} \tag{19}$$

where N_{fpl} is the number of lossless ROI blocks which are considered as tampered ones, N_{disl} is the true number of lossless ROI blocks, N_{fnl} is the number of tampered ROI blocks which are considered as lossless ones, N_{sl} is the true number of tampered ROI blocks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

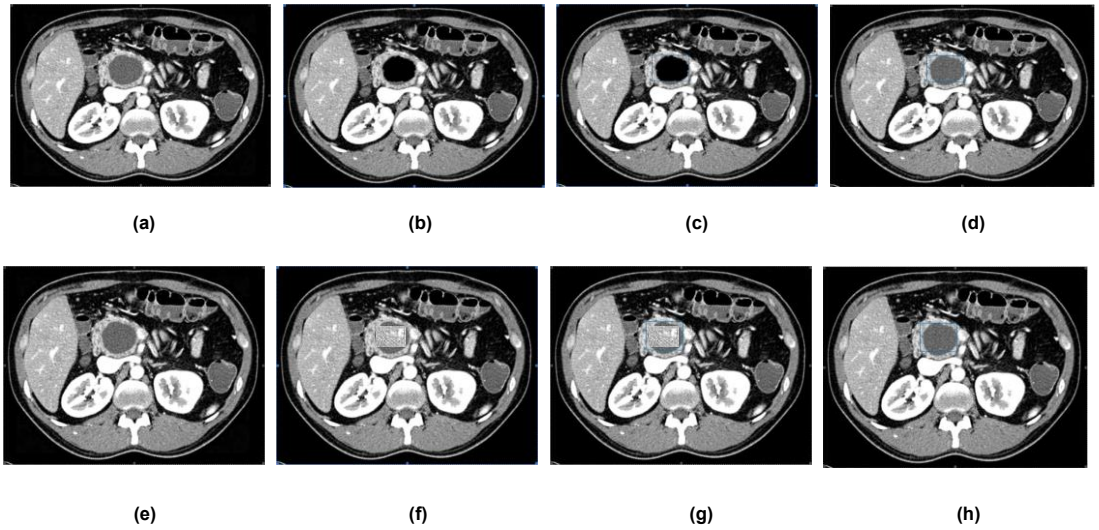

FIGURE 12. **Examples to evaluate tamper detection, localization and recovery, (a) watermarked image, (b) erase tampered image, (c) localization of tampered blocks, (d) recovery of erase tampered image, (e) watermarked image, (f) copy-paste tampered image, (g) localization of copy-paste tampered blocks, (h) recovery of copy-paste tampered image.**

TABLE 6. **The false-positive rate and false-negative rate of tamper detection and localization under erase tampering**

Ratio of tampered blocks in ROI	Tamper detection		Tamper localization	
	P_{fpd}	P_{fnd}	P_{fpl}	P_{fnl}
1 random pixel	0	0	0	0
25%	0	0	0	0
50%	0	0	0	0
75%	0	0	0	0
100%	0	0	0	0

TABLE 7. **The false-positive rate and false-negative rate of tamper detection and localization under copy-paste tampering**

Ratio of tampered blocks in ROI	Tamper detection		Tamper localization	
	P_{fpd}	P_{fnd}	P_{fpl}	P_{fnl}
1 random pixel	0	0	0	0
25%	0	0	0	0
50%	0	0	0	0
75%	0	0	0	0
100%	0	0	0	0

The mean *PSNR*s and the mean *SSIM*s between original images and recovered images are calculated to evaluate the performance of temper recovery. In our proposed watermarking scheme, the results of tamper recovery are the same when the ratios of tampered blocks in ROI under erasing and copy-paste tampering are the same. Therefore, they are listed in one same Table, which is Table 8.

As shown in Table 6, all the P_{fp}s and P_{fn}s of tamper detection and localization under erase tampering are 0. As shown in Table 7, all the P_{fp}s and P_{fn}s of tamper detection and localization under copy-paste tampering are also 0. These results demonstrate that our scheme can detect and locate any distortions on tampered areas of ROI reliably and precisely by utilizing hash functions and CRC.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

TABLE 8. The mean *PSNR*s and the mean *SSIM*s between original images and recovered images

	Ratio of tampered blocks in ROI	ROI of medical images		Tampered blocks	
		PSNR (db)	*SSIM*	*PSNR* (db)	*SSIM*
200 medical images	1 random pixel	66.8374	0.9999	55.1561	0.9990
	25%	54.1422	0.9963	46.0746	0.9618
	50%	51.4307	0.9879	47.0958	0.9772
	75%	48.7422	0.9760	46.7932	0.9788
	100%	45.3569	0.9762	45.3569	0.9762
40 CT images	1 random pixel	61.4102	0.9999	56.5655	0.9991
	25%	56.2484	0.9972	52.9370	0.9658
	50%	55.7332	0.9911	54.0775	0.9860
	75%	54.8616	0.9841	54.1120	0.9892
	100%	55.0736	0.9884	55.0736	0.9884
40 MRI images	1 random pixel	67.8338	0.9999	54.0413	0.9993
	25%	53.4147	0.9965	44.0827	0.9586
	50%	50.2549	0.9864	45.1374	0.9701
	75%	48.2119	0.9706	45.7756	0.9704
	100%	43.0274	0.9668	43.0274	0.9668
40 ultrasound images	1 random pixel	64.4322	0.9999	55.1829	0.9993
	25%	54.7881	0.9986	48.4664	0.9779
	50%	53.0997	0.9951	49.6379	0.9873
	75%	51.2322	0.9889	49.6079	0.9882
	100%	45.7199	0.9843	45.7199	0.9843
40 X-ray images	1 random pixel	65.6261	0.9990	52.2289	0.9986
	25%	50.2527	0.9908	40.9208	0.9342
	50%	47.5516	0.9738	42.1331	0.9683
	75%	42.1711	0.9531	39.7348	0.9718
	100%	38.4723	0.9683	38.4723	0.9683
40 fundus images	1 random pixel	74.8845	0.9999	57.7617	0.9993
	25%	56.0073	0.9986	43.9661	0.9723
	50%	50.5139	0.9929	44.4933	0.9745
	75%	47.2342	0.9832	44.7354	0.9742
	100%	44.4914	0.9734	44.4914	0.9734

As shown in Table 8, our proposed watermarking scheme provides remarkable recovery function for tampered areas of ROI. When modifying 1 random pixel, 25%, 50%, 75% and even 100% of ROI, the mean *PSNR*s and *SSIM*s between original ROI and recovered ROI of 200 medical images are 66.8374, 54.1422, 51.4307, 48.7422, 45.3569 and 0.9999, 0.9963, 0.9879, 0.9760, 0.9762, respectively. The mean *PSNR*s and *SSIM*s between the original blocks which have been tampered and their corresponding recovered blocks of 200 medical images are 55.1561, 46.0746, 47.0958, 46.7932, 45.3569 and 0.9990, 0.9618, 0.9772, 0.9788, 0.9762, respectively. In addition, all the mean *PSNR*s and *SSIM*s between original ROI and recovered ROI of five different types medical images are larger than 61.4102, 50.2527, 47.5516, 42.1711, 38.4723 and 0.9990, 0.9908, 0.9738, 0.9531, 0.9683, respectively. In addition, all the mean *PSNR*s and *SSIM*s between the original blocks which have been tampered and their corresponding recovered blocks of five different types medical images are larger than

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2921894, IEEE Access

TABLE 9. Qualitative comparisons with other watermarking schemes

	ROI-lossless watermarking		Reversible watermarking		Proposed scheme
	Spatial [13]-[17]	Frequency [18]-[21]	Fragile [22]-[27]	Robust [28],[29]	
Watermark robustness	Insufficient	Sufficient	Insufficient	Sufficient	Sufficient
Tamper recovery	Involved	Involved	Not involved	Not involved	Involved
Reversibility	ROI-Reversible	ROI-Reversible	Reversible	Reversible	Reversible
Watermark generation	ROI and RONI are divided	ROI and RONI are divided	ROI and RONI are not divided	ROI and RONI are not divided	ROI and RONI are divided
Watermark embedding	ROI and RONI are divided	ROI and RONI are divided	ROI and RONI are not divided	ROI and RONI are not divided	ROI and RONI are not divided

62.2289, 40.9208, 42.1331, 39.7348, 38.4723 and 0.9986, 0.9342, 0.9683, 0.9704, 0.9668, respectively. All the values of these *PSNR*s and *SSIM*s are quite large, which demonstrate that our proposed watermarking scheme provides remarkable recovery function for tampered areas of ROI. The reason of these results is that tamper recovery information of ROI is generated based on the approximation coefficient matrix of IWT, which contains the most information of ROI.

Especially, the mean *PSNR* of X-Ray images are lower than those of other images when the tamper ratios are large. The reason of this phenomenon is that X-Ray images tested in our experiment have more unstructured details comparing to the other testing images.

E. QUALITATIVE COMPARISONS

Qualitative comparisons between our proposed schemes with ROI-lossless watermarking and reversible watermarking schemes are conducted in terms of five aspects: 1) the sufficiency of watermark robustness; 2) the involvement of tamper recovery function; 3) the reversibility of medical image; 4) whether ROI and RONI are divided for watermark embedding; and 5) whether ROI and RONI are divided for watermark generation. The results are shown in Table 9. Compared with the spatial domain-based ROI-lossless watermarking schemes [13]-[17], our proposed watermarking scheme is much more robust against various attacks and thus provides more reliable verifications of image authenticity. Compared with both the spatial domain-based and the frequency domain-based ROI-lossless watermarking schemes [13]-[21], our proposed watermarking scheme restores both ROI and RONI losslessly and thus there are no negative impacts on medical diagnosis. In addition, our proposed watermarking scheme embeds watermarks without dividing medical images into ROI and RONI. In this manner, the security risks caused by the segmentation of the ROI and the RONI in spatial domain for watermark embedding are avoided, which cannot be achieved by either spatial domain-based or frequency domain-based ROI-lossless watermarking schemes. Compared with the fragile reversible watermarking [22]-[27], our proposed watermarking scheme provides stronger robustness against various attacks and thus provides more reliable verifications of image authenticity. Compared with both fragile and robust reversible watermarking schemes [22]-[29], our proposed watermarking scheme divides ROI and RONI for watermark generation and provides an effective recovery function for tampered ROI under limited embedding capacity. In this manner, the most diagnosis values of medical images are still maintained even they are attacked, which cannot be achieved by either fragile or robust reversible watermarking schemes.

V. CONCLUSION

In this paper, a novel robust reversible watermarking scheme based on SLT-SVD hybrid transform is proposed for verifying authenticity and integrity of medical images. To the best of our knowledge, it is the first watermarking scheme which ROI and RONI are divided only for watermark generation, whereas they are not divided for watermark embedding. The analytical and experimental results have demonstrated that our proposed watermarking scheme provides remarkable performances in terms of robustness, imperceptibility, authentication, tamper detection, tamper localization, and tamper recovery. Moreover, our proposed watermarking scheme has following merits compared with other existing

watermarking schemes for protecting medical images: 1) by using RDM-based reversible function for watermark embedding, both ROI and RONI can be restored losslessly, which outperforms existing ROI-lossless watermarking; 2) by using SLT-SVD hybrid transform and RDM-based embedding method, our proposed watermarking scheme provides strong robustness against various attacks, which outperforms existing spatial domain-based ROI-lossless watermarking and fragile reversible watermarking; 3) by dividing ROI and RONI and using IWT with BTC for generation of the tamper recovery information of ROI, our proposed watermarking scheme can recover the tampered areas of ROI under limited embedding capacity, which cannot be achieved by existing reversible watermarking schemes; 4) by embedding watermark into the whole medical image without dividing ROI and RONI, our proposed watermarking scheme avoids the security risks caused by spatially image dividing, which outperforms existing ROI-lossless watermarking.

Our future work will focus on how to further enhance the watermarking robustness against the rotation attacks by designing a pre-process registration step based on local features and increase the embedding capacity of reversible watermarking schemes.

REFERENCES

[1] B. Davie et al., "Bringing health-care applications to the internet," *IEEE Internet Comput.*, vol. 5, no. 3, pp. 42-48, 2001.

[2] K. Swaraja, "Medical image region based watermarking for secured telemedicine," *Multimedia Tools Appl.*, vol. 77, pp. 28249-28280, 2018.

[3] J. C. Dagadu, J. Li, "Context-based watermarking cum chaotic encryption for medical images in telemedicine applications," *Multimedia Tools Appl.*, vol. 77, no. 18, pp. 24289-24316, 2018.

[4] D. Bouslimi, G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," *Signal Process.-Image*, vol. 47, pp. 160-169, 2016.

[5] R. Patel, P. Bhatt, "A review paper on digital watermarking and its techniques," *Int. J. Comput. Appl.*, vol. 110, no. 1, pp. 10-13, 2015.

[6] R. Bakthula, S. Shivani, S. Agarwal, "Self authenticating medical X-ray images for telemedicine applications," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8375-8392, 2018.

[7] H. Nyeem, W. Boles, C. Boyd, "A review of medical image watermarking requirements for teleradiology," *J. Digit. Imaging*, vol. 26, no. 2, pp. 326-343, 2013.

[8] D. Bouslimi et al., "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images," *IEEE T. Inf. Technol. B.*, vol. 16, no. 5, pp. 891-899, 2012.

[9] A. Tashk, H. Danyali, M. A. Alavianmehr, "A modified dual watermarking scheme for digital images with tamper localization/detection and recovery capabilities," in *2012 9th International ISC Conference on Information Security and Cryptology*, 2012, pp. 60-65.

[10] G. Coatrieux et al., "A watermarking-based medical image integrity control system and an image moment signature for tampering characterization," *IEEE J. Biomed. Health*, vol. 17, no. 6, pp. 1057-1067, 2013.

[11] L. O. M. Kobayashi, S. S. Furuie, "Proposal for DICOM multiframe medical image integrity and authenticity," *J. Digit. Imaging*, vol. 22, no.1, pp. 71-83, 2009.

[12] E. Gul, S. Ozturk, "A novel hash function based fragile watermarking method for image integrity," *Multimedia Tools Appl.*, pp. 1-18, 2019.

[13] T. A. BW, F. P. Permana, "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression," in *2012 IEEE Int. Conf. Commun.*, 2012, pp. 167-171.

[14] S. C. Liew, S. W. Liew, J. M. Zain, "Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication," *J. Digit. Imaging*, vol. 26, no. 2, pp. 316-325, 2013.

[15] R. Eswaraiah, E. S. Reddy, "A fragile ROI-based medical image watermarking technique with tamper detection and recovery," *2014 Fourth International Conference on Communication Systems and Network Technologies. IEEE*, pp. 896-899, 2014.

[16] K. S. Kim et al., "Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging," *Comput. Vis. Image Und.*, vol. 115, no. 9, pp. 1308-1323, 2011.

[17] R. L. Priya, V. Sadasivam, "Protection of health

imagery by region based lossless reversible watermarking scheme," *Sci. World J.*, vol. 2015, pp. 1-15, 2015.

[18] S. Maheshkar, "Region-based hybrid medical image watermarking for secure telemedicine applications," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3617-3647, 2017.

[19] A. Al-Haj, "Secured telemedicine using region-based watermarking with tamper localization," *J. Digit. Imaging*, vol. 27, no. 6, pp. 737-750, 2014.

[20] R. Thabit, B. E. Khoo, "Medical image authentication using SLT and IWT schemes," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 309-332, 2017.

[21] A. Tareef et al., "A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding," in *proc. 36th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2014, pp. 5554-5557.

[22] D. M. Thodi, J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE T. Image Process.*, vol. 16, no. 3, pp. 721-730, 2007.

[23] G. Coatrieux et al., "Reversible watermarking based on invariant image classification and dynamic histogram shifting," *IEEE T. Inf. Foren. Sec.*, vol. 8, no. 1, pp. 111-120, 2013.

[24] L. Luo et al., "Reversible image watermarking using interpolation technique," *IEEE T. Inf. Foren. Sec.*, vol. 5, no. 1, pp. 187-193, 2010.

[25] X. Zhang et al. "Reversible fragile watermarking for locating tampered blocks in JPEG images," *Signal Process*., vol. 90, no. 12, pp. 3026-3036, 2010.

[26] M. Ishtiaq et al., "Hybrid predictor based four-phase adaptive reversible watermarking," *IEEE Access*, vol. 6, pp. 13213-13230, 2018.

[27] B. Feng et al., "A Reversible Watermark with a New Overflow Solution," *IEEE Access*, vol. 6, pp. 1-14, 2018.

[28] B. Lei et al., "Reversible watermarking scheme for medical image based on differential evolution," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3178-3188, 2014.

[29] R. Thabit, B. E. Khoo, "A new robust lossless data hiding scheme and its application to color medical images," *Digit. Signal Process.*, vol. 38, pp. 77-94, 2015.

[30] W. W. Peterson, D. T. Brown, "Cyclic codes for error detection," *Proceedings of the IRE*, vol. 49, no. 1, pp. 228-235, 1961.

[31] C. C. Chang, C. Y. Lin, Y. H. Fan, "Lossless data hiding for color images based on block truncation coding," *Pattern Recogn.*, vol. 41, no. 7, pp. 2347-2357, 2008.

[32] I. W. Selesnick, "The Slantlet Transform," *IEEE T. Signal Process.*, vol. 47, no. 5, pp. 1304-1313, 1999.

[33] I. M. Alwan, M. M. Lafta M M, "Watermarking in image using slantlet transform," *Iraqi J. Sci.*, vol. 52, no. 2, pp. 225-230, 2011.

[34] R. T. Mohammed, B. E. Khoo, "Image watermarking using slantlet transform," in *2012 IEEE Symp. Industrial Electronics Appl. (ISIEA2012)*, Sep. 2012, pp. 281-286.