Received March 23, 2022, accepted April 20, 2022, date of publication April 25, 2022, date of current version June 6, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3170030

A Novel Hybrid Reversible-Zero Watermarking Scheme to Protect Medical Image

ZHEN DAI[1], CHUNYAN LIAN[1], ZHUOHAO HE[2], HUAILONG JIANG[1], AND YIFAN WANG[3]
[1]School of Software, Hunan Vocational College of Science and Technology, Changsha 410118, China
[2]School of Computer Science and Engineering, Central South University, Changsha 410083, China
[3]Department of Computer Science, Loughborough University, Loughborough LE11 3TU, U.K.

Corresponding author: Yifan Wang (y.wang6@lboro.ac.uk)

This work was supported in part by the Natural Science Foundation of Hunan Province under Grant 2021JJ60048.

ABSTRACT The verification of copyright and authenticity for medical images is critical in telemedical applications. Watermarking is a key technique for protecting medical images and can be mainly divided into three categories: region of interest (ROI) lossless watermarking, reversible watermarking and zero-watermarking. However, ROI lossless watermarking causes biases on diagnosis. Reversible watermarking can hardly provide a continuous verification function and may face verification disputes after image recovering. Zero-watermarking requires third-party storage which may cause additional security problems. To address these issues, a hybrid reversible-zero watermarking (HRZW) is proposed in this paper to effectively combine the complementary advantages of reversible watermarking and zero-watermarking. In our scheme, a novel hybrid structure is designed including a zero-watermarking component and a reversible watermarking component. In the first component, ownership share is generated by mapping nearest neighbor grayscale residual (NNGR) based features and watermark information. In the second component, the generated ownership share is embedded reversibly based on Slantlet Transform, Singular Value Decomposition and Quantization Index Modulation (SLT-SVD-QIM). Experimental results demonstrate that our proposed scheme not only yields remarkable watermarking imperceptibility, distinguishability and robustness, but also provides continuous verification function without any dispute or third-party storage, which outperforms existing watermarking schemes for medical images.

INDEX TERMS Authenticity, copyright protection, medical images, NNGR based feature, reversible-zero hybrid watermarking, SLT-SVD-QIM.

I. INTRODUCTION

The verification of copyright and authenticity for medical images has become a very important issue in telemedical applications. On the one hand, the collection of medical images requires a large amount of manpower and material resources, which indicates that the illegal use of medical images will cause huge losses to medical institutions. On the other hand, the use of medical images forged by attackers for diagnosis or scientific research may lead to invalidate scientific research results, diagnostic errors or even endanger the lives of patients.

Different from protecting traditional images, the protection for medical images needs to ensure the lossless and distinguishability of medical images besides the robustness requirement. Because any modification on medical images may lead to unwanted diagnostic risks, the lossless of their content should be guaranteed to avoid biased diagnosis. In addition, the excellent distinguishability of different medical images is also required to avoid misclassification of protected images with non-protected ones because medical images from different persons in the same modality share similar visual structures. Last but not least, robustness is certainly required to ensure the reliability of the verification of copyright and authenticity under malicious attacks.

Digital watermarking is a typical technique for protecting copyright and authenticity [1]–[5]. There are three main categories of watermarking schemes for protecting medical images, which are the Region of Interest (ROI) lossless watermarking, reversible watermarking and zero watermarking.

ROI lossless watermarking schemes [6]–[11] divide the medical image into ROI and the region of no interest (RONI)

The associate editor coordinating the review of this manuscript and approving it for publication was Qingli Li.

in the spatial domain and embed the watermark into medical images while keeping their ROI regions lossless. However, in these schemes, RONI cannot be restored losslessly, thus still leading to negative impacts on the diagnosis. Furthermore, the segmentation of ROI and RONI may cause additional security risks because all the information embedded in RONI can be easily destroyed by replacing the whole RONI simply.

Reversible watermarking schemes [12]–[19] ensure that the medical images can be recovered losslessly after extracting the watermark, which avoids distortions of RONI. However, these schemes still have one major disadvantage. The association between the watermark information and the carrier images has no more existed after the image recovering, which means the reversible watermarking schemes can only provide a one-time verification and may face unwanted disputes.

Zero-watermarking schemes [20]–[27] do not modify the original images but generate and store the ownership shares of medical images, which indicates the associations between the image features and the watermark information, for medical image protection. Because these associations (ownership shares) are well kept during the whole protection process, zero-watermarking can provide continuous protection of medical images and avoid any possible dispute. However, there are still some main disadvantages of zero-watermarking: 1) the ownership shares require third-party storage, which brings additional security risks; 2) it is difficult for zero-watermarking schemes to accurately identify the ownership share of a specific image among a large number of images without additional retrieval functions; 3) the features of similar images are possible to be the same, which may cause inaccurate (false positive) verification.

In summary, reversible watermarking and zero-watermarking are more suitable for protecting medical images than ROI lossless watermarking. On the one hand, they can ensure the lossless of medical images to avoid biased diagnosis which cannot be achieved by ROI lossless watermarking. On the other hand, they do not need to divide medical images into ROIs and RONIs, and thus avoid the risks caused by the spatial division of ROI in ROI lossless watermarking. The comparison of the three watermarking methods is shown in Table 1.

More importantly, the advantages of reversible watermarking and zero-watermarking are fortunately complementary. The first one does not need additional storage while the second one makes use of the associations between the image features and the watermark information, thus confirming continuous verification without dispute.

To make use of these complementary advantages of reversible watermarking and zero-watermarking, we propose a hybrid reversible-zero watermarking (HRZW) in our paper by designing a novel hybrid structure including a zero-watermarking component and a reversible watermarking component. In the first component, ownership share is generated through exclusive OR (XOR) mapping of features and watermark information, where features are extracted based on nearest neighbor grayscale residuals (NNGR). In the second component, we design a reversible watermarking based on Slantlet Transform (SLT), Quantization Index Modulation (QIM) and Singular Value Decomposition (SVD) to embed the generated ownership shares into the corresponding image. Our contributions are highlighted as follows:

1) A novel lossless watermark architecture named HRZW is proposed, which effectively combines the advantages of both reversible watermark schemes and zero-watermark schemes. To our best knowledge, it is the first scheme to fuse zero-watermarking and reversible watermarking. Our method is a watermarking for verifying copyright and authenticity of medical images, as it is robust against some malicious attacks such as filtering, noise and clipping attacks.

2) A zero-watermarking component is designed to generate the ownership shares, which indicates the associations between the image characteristics and the watermark information and thus can be used for continuous verification without verification dispute even after the medical image is restored.

3) A reversible watermarking component is designed to embed the generated ownership shares reversibly. In this manner, the ownership share of a specific image can be extracted from its watermarked image accurately without the storage requirements of a third party. In addition, the false-positive rate of verification will be reduced, because the possibility of extracting the accurate ownership share from a similar but unwatermarked image is close to 0.

4) SLT-SVD-QIM-based watermarking and NNGR-based feature extraction are deployed to guarantee the lossless, distinguishability and robustness of our proposed HRZW.

5) Experiments implemented on 200 medical images have demonstrated that our proposed HRZW outperforms the state-of-the-art reversible watermarking and zero-watermarking schemes for medical image protection.

The rest of the paper is organized as follows. Related work is introduced in Section II. Our proposed watermarking scheme is described in detail in Section III. The experimental results are provided and analyzed in Section IV. Finally, the paper is concluded in Section V.

II. RELATED WORK

Existing watermarking schemes to verify copyright and authenticity of the medical image can be classified into three main categories, which are the region of interest (ROI) lossless watermarking schemes, reversible watermarking schemes and zero-watermarking schemes. The related works of these three categories are described as follows.

A. ROI LOSSLESS WATERMARKING SCHEME

In the ROI lossless watermarking scheme, medical images are divided into regions of interest (ROI) and regions of no interest (RONI). Tjokorda *et al.* [6] embed the information by modifying the least significant bits (LSB) of the pixels in ROI. Lee *et al.* [7] embed the bit-plane value of the

TABLE 1. Comparison of different types of watermarking algorithms.

	ROI lossless watermarking	Reversible watermarking	Zero-watermarking
Characteristics	Divide medical images into ROI and RONI and embed the watermark into ROI.	The medical images can be recovered losslessly after extracting the watermark.	Extract features to generate ownership shares which for copyright authentication.
Advantages	Keeping their ROI regions lossless.	Avoiding distortions of RONI.	No modification of the original image.
Disadvantages	1. RONI cannot be restored losslessly. 2. Risk of splitting ROI and RONI.	1. One-time verification.	1. Third party storage required. 2. Additional retrievals are required. 3. False Positive Problem.

Discrete Wavelet Transform (DWT) coefficient in the ROI into the adjacent RONI of the medical image. Parah *et al.* [8] propose a robust watermarking scheme by modifying the Discrete Cosine Transform (DCT) coefficients of ROI to embed the watermark. Priya *et al.* [9] embed the watermark information into the LSBs of RONI. Alhaj *et al.* [10] propose a watermarking scheme by modifying the LSB of the ROI after DWT and SVD, while the LSBs of the ROI are embedded into RONI. Maheshkar *et al.* [11] propose another ROI lossless scheme, in which the hospital logo and electronic medical record (EPR) are embedded in RONI by using the IWT-SVD hybrid transform.

B. REVERSIBLE WATERMARKING SCHEME

The reversible watermarking scheme directly embeds and extracts watermarks without dividing the ROI and RONI. The scheme can ensure that the medical images can be losslessly recovered after watermark extraction. Thodi *et al.* [12] propose a prediction error expansion-based reversible scheme. To improve the watermarking robustness, Deng *et al.* [13] embed watermark based on Huffman coding and K-means clustering. Luo *et al.* [14] use interpolation errors for watermark embedding to improve the quality of watermarked images. Gouenou *et al.* [15] shift the histogram modulation of prediction errors, which exploits the local specificities of the image to enhance both the watermark capacity and imperceptibility. An *et al.* [16] embed watermarks in the wavelet coefficients based on shifting and clustering of statistical histograms. Lei *et al.* [17] propose a recursive dither modulation-based watermarking which embeds watermarks into the DWT-SVD coefficients of medical image. Thabit *et al.* [18] modify the relationship between the mean values of low-high and high-low frequency sub-bands of the SLT domain for watermark embedding to enhance the watermarking robustness. Liu *et al.* [19] propose a novel robust reversible watermarking scheme based on recursive dither modulation (RDM) for protecting the authenticity of medical images. In addition, they further use Cyclic Redundancy Check (CRC) and block truncation coding (BTC) for modification location and recovery. In addition, Reversible watermarking is also used for sensitive applications such as military imagery [28] and remote sensing imagery [29], [30]. For example, the lossless watermarks have being incorporated as an integrity protection mechanism into the ISSE guard [31].

C. ZERO-WATERMARKING SCHEME

In the zero-watermarking scheme, the mapping relationship between copyright information and medical image features is established and continuous verification without any dispute can be performed by using the mapping relationship and extracting image features. In addition, there is no distortion in the image content because the copyright information is not directly embedded in the medical image. Han *et al.* [20] propose a robust zero watermarking scheme that deploys 3D-DWT and Legendre Chaotic Neural Network for feature extraction. Dong *et al.* [21] design another low-frequency DCT coefficient-based zero watermarking scheme for better robustness. Seenivasagam *et al.* [22], [23] exploit Contourlet transform (CT) and deploy the first 3 and 6 Hu invariant moment sign bits in the CT-SVD domain to extract features. Fan *et al.* [24] design a zero watermarking algorithm based on Cellular Automate Transformation (CAT) for copyright protection to achieve sufficient security and robustness. In order to improve the distinguishability of features, Du *et al.* [25] propose a 2D-DCT based zero-watermarking scheme for the digital right management of fundus images for better distinguishability. Zou *et al.* [26] design a zero-watermarking scheme by using features based on the grayscale differences in the fan ring partitions to further improve the feature distinguishability. Liu *et al.* [27] extract the content-based features of medical images based on completed local binary patterns to further chance the feature robustness against rotation attacks.

III. REVERSIBLE-ZERO HYBRID WATERMARKING SCHEME

Our scheme includes two main procedures: a watermark registration phase and a watermark authentication phase as shown in Figure 1. In the first phase, we extract binarized features based on NNGR, use a logistic-logistic system based chaotic map to generate scrambled binary features, and use the scrambled binary features and watermark information to generate ownership share. Then, we embed the generated ownership share into the image reversibly based on SLT-SVD-QIM. In the watermark authentication phase, we first extract features based on NNGR, generate scrambled binary features based on LLS and use the watermarking scheme based on SLT-SVD-QIM to extract ownership share. Then, the ownership share and the binarized features are used together to generate the watermark information for authentication. In this manner, the additional security risks of using third-party storage are avoided. In addition, the false-positive rate of verification will be reduced. Last but not least, the watermark is associated with image features by using the ownership share of zero-watermarking and thus our method can still carry out continuous verification without dispute in multiple stages after the image is restored. The detailed architecture of HRZW is described as follows.

A. WATERMARK REGISTRATION

1) FEATURE EXTRACTION BASED ON NNGR

In this stage, an algorithm for feature extraction based on NNGR is applied to extract image features. As shown in Figure 2, the image is partitioned into several fan rings, and then the grayscale modifications in both radial and tangential direction of each partition are calculated to extract the feature. The detailed steps are shown in Algorithm 1.

2) LLS ENCRYPTION

An important problem with SVD-based image watermarking is false positive detection [32]. The attackers can remove any watermark by exploiting the U and V components with their own singular values without knowing the original watermark embedded in the watermarked image to assert their ownership of the watermarked image.

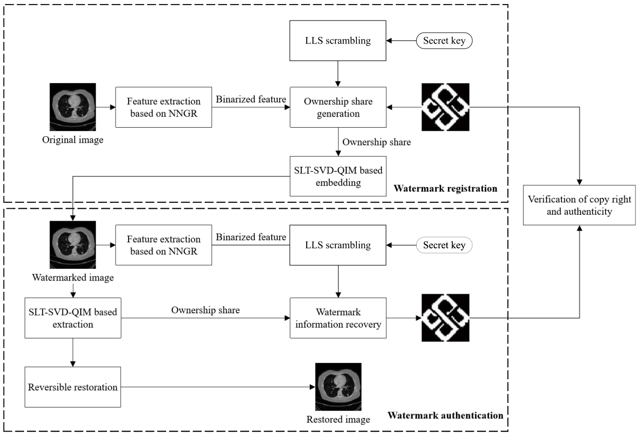

FIGURE 1. Process of reversible-zero hybrid watermark.

In this stage, a chaotic sequence $H = \{h_{i+t}, 1 \leq i \leq 4 \times (N-1) \times L\}$ generated by logistic-logistic system (LLS) and scrambled on the binarized feature to ensure watermarking

Algorithm 1 Feature Extraction Algorithm Based on the NNGR

```
Input: Target image
Output: Image feature $BIF$
1: The target image is converted to its gray-scale form and then normalized to $512 \times 512$ pixels.
2: The geometric center of the grayscale image is deployed as the center point, and the circular regions of image within the radius R are selected as the target region for feature extraction. In our study, $R$ is set to 220.
3: The target region is segmented into $N$ rings with the equal radius. And each ring is then segmented into $M$ fan rings with the equal width to obtain the sub-region set $G = \left\{g_{i,j} \mid | 1 \leq i \leq N, 1 \leq j \leq M\right\}$which contains $M \times N$ sub-regions $g_{i,j}$. In our study, N is set to 44 and M is set to 16.
4: The sum of pixels of each sub-region $g_{i,j}$ is calculated, namely as $Sum(i,j)$.
5: The residual value $R_r(i,j)$ is calculated between the sum value $Sum(i,j)$ of each sub-region $G(i,j)$ and the sum value $Sum(i+1,j)$ of its adjacent sub-region $G(i+1,j)$. In this manner, $(N-1) \times M$ radial nearest neighbor residual values $Rr$ is obtained, according to the order of traversing the tangential direction firstly and traversing the radial direction secondly.
   $$R_r(i,j) = Sum(i,j) - Sum(i+1,j), \quad \text{where} \;\; 1 \leq i \leq N-1 \;\; \text{and} \;\; 1 \leq j \leq M \tag{1}$$
6: Similarly, the residual value $R_r(i,j)$ is also calculated between the sum value $Sum(i,j)$ and the sum value $Sum(i,j+1)$ of its adjacent fan-ring in the tangential direction. $N \times M$ tangential nearest neighbor residual values $R_t$ is obtained.
   $$R_t(i,j) = \begin{cases} Sum(i,j) - Sum(i,1), & \text{where} \;\; 1 \leq i \leq N \;\; \text{and} \;\; j = M \\ Sum(i,j) - Sum(i,j+1), & \text{where} \;\; 1 \leq i \leq N \;\; \text{and} \;\; 1 \leq j \leq M-1 \end{cases} \tag{2}$$
7: The $R_r$ and $R_t$ are binarized to obtain $B_r$ and $B_t$ based on their own median values $T_r$ and $T_t$ as shown in equation3.
   $$\begin{aligned} B_r((i-1) \times N + j) &= \begin{cases} 1, & \text{if } R_r(i,j) > T_r \\ 0, & \text{otherwise,} \end{cases} \quad \text{where} \;\; 1 \leq i \leq N-1 \;\; \text{and} \;\; 1 \leq j \leq M \\ B_t((i-1) \times N + j) &= \begin{cases} 1, & \text{if } R_t(i) > T_t \\ 0, & \text{otherwise,} \end{cases} \quad \text{where} \;\; 1 \leq i \leq N \;\; \text{and} \;\; 1 \leq j \leq M \end{aligned} \tag{3}$$
8: The $B_r$ and $B_t$ are combined to obtain binary feature $BIF$ with dimension $(N-1) \times M + N \times M$.
```

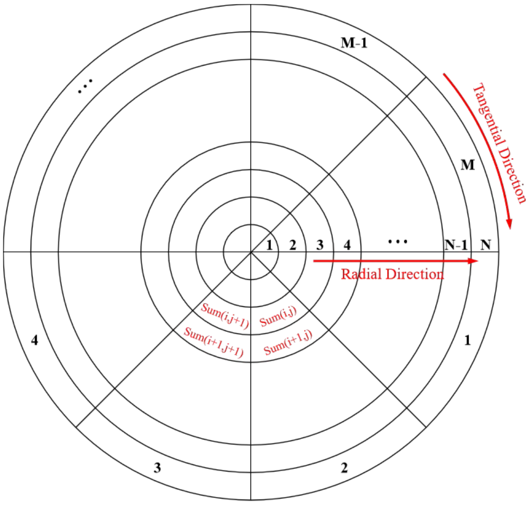

FIGURE 2. An example of image partitions.

security, thus avoiding the false positive issue of the SVD-based watermark [33].

This system is one of the hybrid systems defined in [34] by combining two chaotic maps as shown in 4. In our study, we combine two logistic maps defined in 5 and strictly follow the parameter setting in [34] to ensure the effectiveness of chaotic system. According to [34], the hybrid system has better chaotic performance, and thus achieves better security than using single chaotic map.

$$h_{n+1}=E_{chaos}(u, h_n)\times T(v)-floor(E_{chaos}(u, h_n)\times T(v)) \quad (4)$$

with $T(v) = 2^v$, and $E_{chaos}(u, h_n)$ is the logistic map:

$$E_{chaos}(u, h_n) = u \times h_n \times (1 - h_n) \quad (5)$$

where u, v are two control parameters, $0 \leq u \leq 10$, $8 \leq v \leq 20$, h_0 is the initial value of chaotic map, n is the iteration number and h_n is the output chaotic sequence. H is a subsequence of length $4 \times (N - 1) \times L$ in h_n, u, v, h_0 and t are used together as the secret key. Here, t is set to 500 because the chaotic sequences generated after multiple iterations have better chaotic performance.

Then, binarize the chaotic sequence H to obtain a binary chaotic sequence $BH = bh_i, 1 \leq i \leq 4 \times (N - 1) \times L$ as follows.

$$bh_i = \begin{cases} 1 & \text{if } h_{i=t} > T; \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

where T is the average value of H.

Finally, generate a scrambled binary feature F by applying an XOR operation ($\oplus$) between the binary chaotic sequence BH and binary feature BIF.

$$F = BIF \oplus BH \quad (7)$$

3) GENERATION OF OWNERSHIP SHARE

In this stage, the scrambled binary feature and watermark information is used to generate the ownership share. The detailed generation of ownership share is shown below.

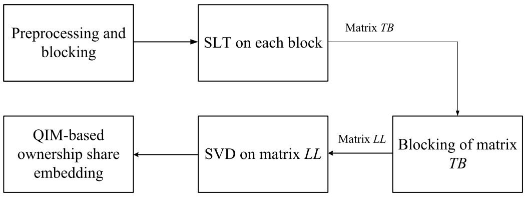

FIGURE 3. Embedding of ownership share.

Step 1: The length of the watermark information is calculated and recorded as L. In our study, L is set at 32×32.

Step 2: The first L bits of the scrambled binary feature F is selected as the master share. The XOR operation is deployed to generate the shared information O using the master share F and the watermark information W.

$$O(i) = F(i) \oplus W(i) \quad (8)$$

where $1 \leq i \leq L$, $\oplus$ is the XOR operator.

4) EMBEDDING OF OWNERSHIP SHARE

In the process of ownership share embedding, the watermarked image will be restored to the original image after extracting the ownership share. As shown in Figure 3, our proposed robust reversible watermarking scheme mainly consists of Singular Value Decomposition (SVD), Slantlet Transform (SLT) and Quantization Index Modulation (QIM). SLT is an equivalent representation of DWT, which ensures both the characteristics of time-localization and smoothness, and thus provides a better trade-off between imperceptibility and robustness for watermark applications. In addition, Moreover, the largest significant value of the singular value matrix S after SVD is further used to enhance the watermarking robustness. QIM is used to embed watermark bits and ensure the reversibility of medical images. In this stage, we embed the ownership shares generated in section 3.1.2 into the medical images, which are described in detail below.

Step 1: The entire medical image is split into 8×8 blocks without overlapping.

Step 2: The divided blocks are scrambly ordered for ownership share embedding according to a scrambled mapping C generated based on a key k. In this manner, the security of embedding ownership share is ensured.

$$C_i = [(k \times Z_i) \bmod N] + 1 \quad (9)$$

where $1 \leq i \leq N$, and N is the number of the blocks. Z is the zigzag ordered mapping, and C is the scrambled mapping. The key k is a random number, and N should not be divisible by k.

Step 3: SLT is applied on the scrambled blocks as shown in equation 10.

$$TB = ABA^T \quad (10)$$

where TB is the SLT coefficient matrix and A is the Slantlet matrix. TB, B and A have the same size which is 8×8.

Step 4: TB is further divided into four sub-bands: LL, HL, LH and HH, and the LL sub-band is selected for ownership share embedding to ensure the watermark robustness.

Step 5: SVD is then performed to the LL sub-band referring to equation 11.

$$LL = USV^T \tag{11}$$

where U and V are orthogonal matrices, S is a singular value matrix. A bit of ownership share is embedded into the largest singular value $S(1, 1)$ in matrix S of each block.

Step 6: The QIM-based reversible method is designed to embed ownership share, as shown in Algorithm 2.

Algorithm 2 QIM-Based Reversible Embedding Method

```
Input: S matrix and quantization step Δ
Output: Watermarked singular values matrix S'
$b = floor(S(1,1)/\Delta)$
if w = 1 then
    $a = b + 1 - \mathrm{mod}(b, 2)$
else
    $a = b + 1 - \mathrm{mod}(b + 1, 2)$
end if
$P = a \times \Delta + \Delta/2$
$D = P - S(1,1)$
$H = D/\Delta$
$S'(1,1) = P + H$
```

On the one hand, to make sure the accurate extraction of the ownership share, $S'(1, 1)$ and P in Algorithm 2 have to be located at the same jitter interval as shown in equation 12, leading that the value of H is supposed to be lower than $\Delta/2$. On the other hand, the embedding-caused distortion D will not be greater than Δ and H will not be greater than 1. Therefore, the ownership share can be extracted correctly when Δ is greater than 2. In our study, Δ is set to 24.

$$floor(P/\Delta) = floor(S'(1, 1)/\Delta) \tag{12}$$

where $floor(\cdot)$ rounds towards negative infinity.

Step 7: LL' is obtained by applying the inverse SVD on U, V and S' referring to equation 13.

$$LL' = US'V^T \tag{13}$$

where S' is the watermarked singular value matrix, and LL' is the watermarked LL sub-band.

Step 8: The inverse SLT is performed on sub-bands LL, HL, LH and LL' referring to equation14.

$$B' = A^T \begin{bmatrix} LL' & HL \\ LH & HH \end{bmatrix} A \tag{14}$$

where B' is a block of the watermarked medical image.

Steps 3-8 are repeated to embed the ownership share and obtain the watermarked medical image.

Step 9: The pixel shifting function is designed to avoid overflow and underflow. Bits "0" and "1" are embedded independently into every block to obtain different watermarked blocks. We calculate the maximum possible distortion of each block by watermark embedding. Then, we adjust the pixels of the watermarked image according to these distortions as below.

$$I_m(i,j) = \begin{cases} I'(i,j) + T & \text{if } I'(i,j) < 0 \\ I'(i,j) & \text{if } 0 \le I'(i,j) \le 255 \\ I'(i,j) - T & \text{if } I'(i,j) > 255 \end{cases} \tag{15}$$

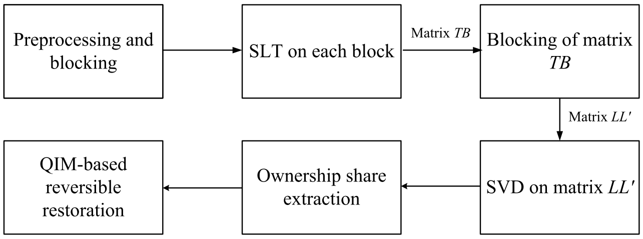
Preprocessing and blocking
SLT on each block
Matrix TB
Blocking of matrix TB
Matrix LL'
SVD on matrix LL'
Ownership share extraction
QIM-based reversible restoration

FIGURE 4. Extraction of ownership share.

B. COPYRIGHT AUTHENTICATION

In this stage, the features of the watermarked image are firstly extracted based on NNGR. Secondly, the ownership share is generated reversibly based on SLT-SVD-QIM and then the image is restored according to the SLT-SVD-QIM restoration process. Finally, the watermark information will be generated by using ownership share and features for medical image verification.

1) FEATURE EXTRACTION

In this section, we use the feature extraction based on NNGR mentioned in section III-A1 to extract the features in the watermarked medical image. Extract the feature R_r and R_t of the watermarked image and perform a binary quantization operation on the feature R_r and Rt to generate BIF. Then, we use the LLS encryption algorithm mentioned in section III-A2 to generate scrambled binary features F for the later calculations in section III-B3. Here, we extract the feature from the watermarked medical image instead of from the recovered medical image for two main reasons. Firstly, if the watermarked medical image is modified by any attacks, the reversible watermarking component cannot restore the original medical image as other reversible watermarking. In this situation, the recovered medical image can even bring additional distortions, which may affect the performance of the feature extraction. Secondly, the imperceptibility of our reversible embedding is remarkable by using the SLT. Therefore, the NNGR based feature is sufficiently robust against the insignificant distortions caused by reversible ownership share embedding. then III-A2

2) EXTRACTION OF OWNERSHIP SHARE

As shown in Figure 4, the ownership share extraction is a reverse process of its embedding function. In addition, medical images are restored losslessly by deploying the QIM function after extracting the ownership share in this stage. The following is the description of the ownership share extraction process:

Step 1: Find the positions of the displaced pixels, and then their corresponding primary pixels can be restored according to the side information, referring to equation 16.

$$I'(i,j) = \begin{cases} I_m(i,j) - T & \text{if } I_m(i,j) < T \\ I_m(i,j) + T & \text{if } I_m(i,j) > 255 - T \end{cases} \tag{16}$$

where $I'(i,j)$ is the pixels of the original watermarked image, $I_m(i,j)$ is the pixels of the modified watermarked, and (i,j) is the coordinate of the pixels. *Step 2:* The entire watermarked image is divided into 8×8 non-overlapping blocks. *Step 3:* Blocks are scrambly ordered using the random embedded sequence C by using equation17 according to the key k.

$$C_i = [(k \times Z_i) \bmod N] + 1 \tag{17}$$

Step 4: The SLT is performed on each block referring to equation 10.

Step 5: The TB' is divided into four sub-bands: LL', HL, LH and HH.

Step 6: The singular value matrix S' is calculated by performing SVD on the sub-band LL' referring to equation 11.

Step 7: The singular value matrix S' is calculated to extract the ownership share bit w using equation 18.

$$w = \mathrm{mod}(floor(S'(1,1)/\Delta), 2) \tag{18}$$

where $floor(\cdot)$ rounds towards negative infinity.

Step 8: The QIM-based reversible method shown in Algorithm 3 is used to recover the original singular values matrix. Obviously, P' and E' should equal to P and E respectively, due to $S'(1,1)$ and P located at the same jitter interval as analyzed in equation 12. Therefore, $S'(1,1)$ can be recovered by using Algorithm 3.

```
Algorithm 3 QIM-Based Reversible Method
Input: $S'$ matrix and quantization step $\Delta$
Output: Restored singular values matrix $S$
$b' = floor(S'(1,1)/\Delta)$
$P' = b' \times \Delta + \Delta/2$
$H' = S'(1,1) - P')$
$P = a \times \Delta + \Delta/2$
$S(1,1) = P' - D'$
```

Step 9: To recover the medical image blocks, inverse SVD and inverse SLT are performed on S'.

Steps 4-9 are repeated to extract ownership share with the recovered medical image.

3) RECOVER COPYRIGHT INFORMATION

In section III-B1, the master share is extracted based on NNGR. In section III-B2, using the SLT-SVD-QIM reversible watermarking algorithm, we generate the ownership share and restore the original image. In section III-B3, the copyright information will be recovered by using master share and ownership share. The specific steps are as follows: Calculate the length of ownership sharing as L, take the first L elements of the binarized feature (master share) as BIF, and generate the copyright information W by XOR operation with the ownership share, as shown in equation 19:

$$W(i) = BIF(i) \oplus O(i) \tag{19}$$

where $1 \leq i \leq L$, $\oplus$ is the XOR operator.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. EXPERIMENTAL SETTING

Several experiments are conducted to evaluate the performance of our proposed scheme. A visual example of embedding and extraction is in section IV-B.The qualitative comparison of ROI lossless watermarking, reversible watermarking and zero-watermarking is evaluated in Section IV-C. The quantitative comparison of reversible watermarking and our proposed scheme is evaluated in Section IV-D. The quantitative comparison of zero-watermarking and our proposed scheme is evaluated in Section IV-E.

Our testing database contains 200 medical images, including CT images, Ultrasound images, MRI images, fundus images and X-ray images. The number of each class of test images is equal to 40. In addition, the image with a size of 32×32 is used as watermark information. The attack types and their parameter values are listed in Table 2.

Inspired by [35], we selected three sets of parameters for evaluating watermarking performances as shown in table 3, which are chosen according to the following standards. First, the radius R of the target region was chosen to be 0.43 of the adjusted image width, i.e. $\lfloor 512 \times 0.43 \rfloor = 220$, to discard the region outside the maximum ring and enhance robustness against cropping attacks. Second, the size of the extracted features D should be slightly larger than the size of the watermark L, as shown in equation 20, to ensure an effective mapping between the extracted features and the deployed watermark.

$$D = M \times (\lfloor R/r \rfloor - 1) \times 4 = M \times (N-1) \times 4 \tag{20}$$

First of all, we use inter-BERs to evaluate the distinguishability of our proposed scheme. Inter-BER is defined as the BER between genuine and fake watermarks. For zero-watermarking, the genuine watermark is generated by using the features and the ownership share of the same medical image while the fake watermark is generated using the features and the ownership share of different medical images. For our method, the genuine watermark is generated by using the features and ownership share extracted from a watermarked medical image, while the fake watermark is generated using the features and the ownership share from an unwatermarked medical image. A larger inter-BER value indicates better watermarking distinguishability.

Further, to evaluate the robustness of our proposed scheme, we calculated the intra-BERs of our proposed scheme and other existing zero-watermarking schemes. The intra-BER is calculated as the BER between the original watermarks and the recovered watermarks under various

TABLE 2. Attack types and their parameters.

Types	Parameters
Average filtering (AF)	Window=3x3, 5x5
Median filtering (MF)	Window=3x3, 5x5
Gaussian Blur (GB)	0.5, 1.0
Crop from image edge (CR)	5%, 10%
Gaussian noise (GN)	Variance=0.001, 0.003; Mean=0
Salt and pepper noise (SN)	Noise density=0.001, 0.003
JPEG compression (JC)	Quality factor=70%, 80%
JPEG2000 compression (JPEG2000)	CompressionRatio=4, 8
Resizing (RS)	0.8, 1.2 of original size
Wiener filtering (WF)	Window=3x3, 5x5

TABLE 3. Settings of parameters.

Description	Abbreviation	Set 1	Set 2	Set 3
Radius of target area	R	220	220	220
Width of concentric rings	r	10	20	5
Number of ring partitions	N	22	11	44
Number of downsampled slices	M	8	32	16
Size of extracted features	D	1344	1280	1376

attacks. A smaller intra-BER indicates better watermarking robustness.

Finally, we calculate the false-negative rate P_{fn} with the false positive rate P_{fp} to evaluate the overall performance as the trade-off between distinguishability and robustness. The P_{fp} is defined as the probability of identifying two different medical images as the same medical image. It also indicates the distinguishability of our proposed scheme. The P_{fn} is defined as the probability of identifying the original medical image and its attacked medical image as two different medical images. It also manifests the robustness of our proposed scheme, the smaller the value the better. The P_{fp} and P_{fn} are defined as Equation 21 and Equation 22 respectively.

$$P_{fp} = \frac{N_{fp}}{N_{td}} \tag{21}$$

$$P_{fn} = \frac{N_{fn}}{N_{ts}} \tag{22}$$

Here, N_{fp} is the number of different medical image pairs whose inter-BER is smaller than a predefined threshold T_h, N_{td} is the true number of different medical image pairs, N_{fn} is the number of original medical image pairs and its attacked medical image whose intra-BER is larger than T_h, and N_{ts} represents the true number of attacked medical images.

The results including the average value of inter-BER, mean intra-BER and P_{fp} of 200 test images under 20 attacks by using our proposed scheme of different parameters are given in Table 4.

As can be seen from the last column in table 4, the parameter settings for set 3 achieve a better compromise between watermark distinguishability and robustness compared to set 1 (v.s. robustness) and set 2 (v.s. distinguishability). Therefore, in the later experiments, the parameters of set 3 were set in our proposed scheme.

TABLE 4. Results with different parameters.

Settings	Average value of inter-BER	Average value of mean intra-BER	Average value of $P_{fn}(P_{fp} = 1/19900)$
Set 1	0.4758	0.0690	0.02515
Set 2	0.4556	0.0401	0.00873
Set 3	0.4694	0.0501	0.00121

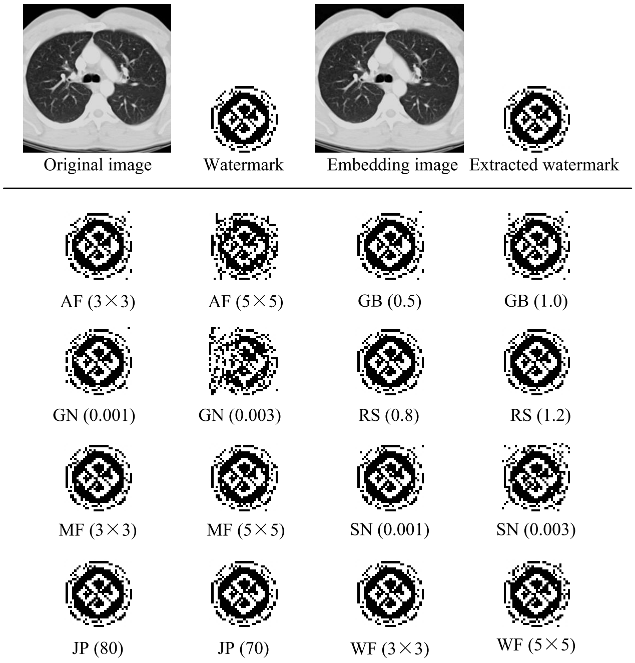

FIGURE 5. Visual examples of the embedding and extraction of our proposed algorithm, including a comparison of the original medical image with the embedded image, a comparison of the original watermarked image with the extracted watermark, and a display of the extracted watermarked image after various attacks.

B. VISUALISATION RESULTS

Figure 5 shows the original medical image with the medical image after watermark embedding, the embedded watermark image with the extracted watermark images under the attacks as listed in Table 2.

The extracted watermark images are legible enough for the verification of copyright and authenticity, which also demonstrates that our method is robust against these attacks.

C. QUALITATIVE COMPARISONS WITH OTHER WATERMARKING SCHEMES

Qualitative comparisons are discussed between our proposed scheme and other schemes for medical images in terms of the following seven aspects: 1) distortion of the host images, 2) robustness of the copyright identification, 3) distinguish ability of the copyright identification, 4) durability of the copyright identification, 5) possibility of the verification dispute, 6) accuracy of the ownership share, 7) requirement of third-party storage. The results are listed in Table 5.

TABLE 5. Qualitative comparisons with other schemes.

	Proposed Scheme	ROI lossless watermark scheme [6]–[11]	Reversible watermark scheme [12]–[19]	Zero-watermark scheme [20]–[27]
Distortion of the images	No	**Yes**	No	No
Distinguishability	Sufficient	Sufficient	Sufficient	**Possibly insufficient**
Robustness	Strong	Strong	Strong	Strong
Durability	Durable	Durable	**One-off**	Durable
Verification dispute	No	No	**Exist**	No
Accuracy of the ownership share	Ensured	NA	NA	**Not ensured**
Third-party storage	No	No	No	**Yes**

As shown in Table 5, our proposed scheme outperforms other three watermarking schemes. Compared with the ROI lossless watermarking schemes, our proposed scheme is distortion-free by combining two lossless watermarking technique, which better satisfies the lossless requirements of medical images for accurate diagnosis. Compared with the reversible watermarking schemes, the verification of medical images in our proposed scheme can be executed repeatedly without any dispute by using the associations between the image characteristics and the watermark information. Compared with zero-watermarking schemes, the watermarking distinguish ability and the accuracy of the ownership share for a specific image are ensured and third-party storage is not required by embedding the ownership share into the medical images in our proposed scheme.

D. QUANTITATIVE COMPARISONS WITH REVERSIBLE WATERMARKING SCHEMES

In this phase, we compared our proposed scheme with reversible watermarking schemes. Firstly, mean PSNRs of our proposed scheme and other existing schemes [11], [17]–[19] are compared in Table 6 to evaluate the watermarking imperceptibility. The definition of PSNR is shown below.

$$PSNR = 10\log_{10}\left(\frac{255^2 \times H \times W}{\sum_{i=1}^{H}\sum_{j=1}^{W}(I(i,j) - I'(i,j))^2}\right) \quad (23)$$

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

The mean PSNR of our proposed watermarking scheme is 46.5391. This value is larger than other four benchmark schemes [11], [17]–[19], which are 39.7522, 41.5525, 40.1841 and 45.7832 respectively. The results demonstrate that the imperceptibility of our proposed watermarking scheme ensures remarkable and better imperceptibility comparable with those state-of-art schemes. The reason for this is because our using of SLT, which provides a remarkable trade-off between imperceptibility and robustness for watermark applications.

Then, we calculated the bit error rate (BER) of our scheme and other existing reversible watermarking schemes to evaluate the robustness of our proposed scheme. The definition of BER is shown below.

$$BER = \frac{\sum W(i,j) \oplus W'(i,j)}{m \times m} \quad (24)$$

TABLE 6. The mean Psnrs Of different watermarking schemes.

	Proposed scheme	Maheshkar et al.s [11]	Lei et al. [17]	Thabit et al. [18]	Liu et al. [19]
PSNR	46.5391	39.7522	41.5525	40.1841	45.7832

TABLE 7. Comparisons of mean Bers with reversible watermarking schemes.

Attacks	Proposed scheme	Reversible watermarking			
		Maheshkar et al.s [11]	Lei et al. [17]	Thabit et al. [18]	Liu et al. [19]
AF (3×3)	0.0528	0.1071	0.1485	0.0622	0.0496
AF (5×5)	0.1299	0.2425	0.2659	0.3393	0.1448
MF (3×3)	0.0367	0.0866	0.1039	0.0539	0.0317
MF (5×5)	0.0940	0.2353	0.2170	0.3807	0.1070
GB (0.5)	0.0166	0.0162	0.0217	0.0000	0.0069
GB (1)	0.0704	0.1064	0.1671	0.0491	0.0721
CR (5%)	0.0070	0.0361	0.0526	0.0058	0.0000
CR (10%)	0.0070	0.0793	0.1051	0.0130	0.0000
GN (0.001)	0.0355	0.0722	0.0578	0.0001	0.0082
GN (0.003)	0.0568	0.0730	0.1779	0.0009	0.0291
SN (0.001)	0.0516	0.0565	0.0220	0.0242	0.0340
SN (0.003)	0.1221	0.0691	0.0611	0.0684	0.0929
JC (Q=70)	0.0281	0.1062	0.0155	0.1294	0.0044
JC (Q=80)	0.0224	0.0940	0.0048	0.0470	0.0027
JPEG2000 (4)	0.0163	0.0475	0.0021	0.0012	0.0017
JPEG2000 (8)	0.0259	0.0851	0.0239	0.0227	0.0084
RS (0.8)	0.0145	0.0265	0.0255	0.0035	0.0038
RS (1.2)	0.0113	0.0080	0.0069	0.0001	0.0009
WF (3×3)	0.0244	0.0787	0.1000	0.0539	0.0112
WF (5×5)	0.0820	0.1977	0.2333	0.2347	0.0945
Average	0.0453	0.0912	0.0906	0.0745	0.0352

where $W(i, j)$ and $W'(i, j)$ represent the original and recovered watermarks and m represents the size of the watermark. The smaller BER indicates the stronger watermarking robustness.

To evaluate the watermarking robustness, attacks with different parameters shown in Table 2, are performed on all the medical images. The mean BERs of 200 medical images under different attacks are compared and the results are listed in Table 7.

As shown in Table 7, all the mean BERs of authenticity data by using our proposed watermarking scheme are close to 0. In addition, the average value of mean BERs of our proposed scheme, which is 0.0453, is smaller than those of the former three benchmark schemes [11], [17]–[19], which are 39.7522, 41.5525, 40.1841 and 45.7832 respectively. In addition, this value is also comparable with that of Liu *et al.*'s scheme [19], which is 0.0352. These results demonstrate that our proposed watermarking scheme outperforms the schemes [11], [17]–[19], and is comparable with Liu *et al.*'s scheme [19] in terms of robustness. The reason for this result is the remarkable invariance of NNGR-based features and SLT-SVD-QIM under different attacks. In addition, as analyzed in Section IV-C, our proposed scheme can provide durable protection without verification dispute, which outperforms all these reversible watermarking schemes.

In summary, our proposed scheme can provide a more effective verification function for medical images than reversible watermarking.

E. QUANTITATIVE COMPARISONS WITH OTHER STATE-OF-ART ZERO-WATERMARKING SCHEMES

In this section, we made the comparison of our proposed watermarking scheme and other existing zero-watermarking schemes, which are Zou *et al.* [25], Seenivasagam *et al.* [22], Du *et al.* [26] and Liu *et al.* [27].

TABLE 8. Comparisons of mean inter-Bers with zero-watermarking schemes.

Distinguishability	Proposed scheme	Zero-watermarking			
		Seenivasagam et al. [22]	Du et al.. [26]	Zou et al. [25]	Liu et al. [27]
max	0.5947	0.7273	0.6280	0.5460	0.3021
min	0.2383	0.0130	0.0782	0.1746	0.0035
mean	0.4885	0.2190	0.4771	0.4037	0.0934

First of all, we use inter-BERs to evaluate the distinguishability of our proposed scheme. The average, maximum and minimum values of inter-BERs by using our proposed scheme and other state-of-art zero-watermarking schemes are shown in Table 8.

As shown in Table 8, we can see that the average and minimum values of inter-BERs by using our proposed scheme are much larger than those of the other zero-watermarking schemes. These results demonstrate that the distinguishability of our proposed scheme is much higher than other zero-watermarking schemes. The reason for this result is two fords. On the one hand, the distinguishability of our used NNGR-based feature is remarkable. On the other hand, the embedding of ownership share into the relative medical image also enhances our distinguishability since the possibility of extracting the accurate ownership share from a similar but unwatermarked image is close to 0.

And we use intra-BERs to evaluate the distinguishability of our proposed scheme. The mean values of intra-BERs under various attacks by using our proposed scheme and other state-of-art zero-watermarking schemes are shown in Table 9.

As shown in Table 9, 20 common attacks with different parameters are applied to test the watermarking robustness. The average value of the mean intra-BER of 200 medical images under all tested attacks by using our proposed scheme is 0.0453, which indicates that our proposed scheme has strong robustness. The reason for this result is also the remarkable invariance of NNGR-based features and SLT-SVD-QIM under different attacks. Although the performance of our proposed scheme is comparable with Seenivasagam *et al.* [22] and slightly worse than Zou *et al.* [25], Du *et al.* [26] and Liu *et al.* [27], which is due to the relatively worse robustness of the reversible watermark component, the distinguishability of our proposed scheme is much better than these zero-watermarking schemes as shown in Table 8. In addition, the overall performance of our proposed scheme is comparable with Zou *et al.* [25] and better than the other three zero-watermarking schemes, which will be analyzed below (in Table 10).

Furthermore, we calculate the false-negative rate P_{fn} with the false positive rate P_{fp} to evaluate the overall performance as the trade-off between distinguishability and robustness. And the results are shown in Table 10.

In our study, the threshold T_h is determined by P_{fp}. The P_{fp} is set to 1/39800 (the smallest P_{fp} except 0 in our experiment) to ensure thigh distinguishability, and P_{fn} is calculated to evaluate the robustness under various attacks. A smaller P_{fn} value indicates better overall performance. The results of P_{fn} calculated by using some state-of-art zero-watermarking schemes and our proposed scheme are given in Table 10.

TABLE 9. Comparisons of mean intra-Bers with zero-watermarking schemes.

Attacks	Proposed scheme	Zero-watermarking			
		Seenivasagam et al. [22]	Du et al.. [26]	Zou et al. [25]	Liu et al. [27]
AF (3x3)	0.0528	0.0406	0.0028	0.0196	0.0392
AF (5x5)	0.1299	0.0476	0.0042	0.0327	0.0575
MF (3x3)	0.0367	0.0199	0.0083	0.0205	0.0325
MF (5x5)	0.0940	0.0288	0.0140	0.0329	0.0524
GB (0.5)	0.0166	0.0242	0.0016	0.0119	0.0116
GB (1)	0.0704	0.0393	0.0031	0.0217	0.0450
CR (5%)	0.0070	0.0585	0.0675	0.0070	0.0040
CR (10%)	0.0070	0.1142	0.1103	0.0070	0.0089
GN (0.001)	0.0355	0.0873	0.0037	0.0274	0.0109
GN (0.003)	0.0568	0.0873	0.0035	0.0281	0.0106
SN (0.001)	0.0516	0.0050	0.0060	0.0185	0.0087
SN (0.003)	0.1221	0.0134	0.0103	0.0343	0.0182
JC (Q=70)	0.0281	0.0878	0.0038	0.0247	0.0082
JC (Q=80)	0.0224	0.0516	0.0027	0.0202	0.0066
JPEG2000 (4)	0.0163	0.0382	0.0021	0.0151	0.0049
JPEG2000 (8)	0.0259	0.0548	0.0032	0.0204	0.0116
RS (0.8)	0.0145	0.0322	0.0015	0.0124	0.0095
RS (1.2)	0.0113	0.0296	0.0012	0.0107	0.0068
WF(3x3)	0.0244	0.0401	0.0016	0.0188	0.0384
WF (5x5)	0.0820	0.0476	0.0028	0.0307	0.0601
Average	0.0453	0.0474	0.0127	0.0207	0.0223

TABLE 10. Comparisons of P_{fn} with zero-watermarking schemes when P_{fp} Is 1/39800.

Attacks	Proposed scheme	Zero-watermarking			
		Seenivasagam et al. [22]	Du et al.. [26]	Zou et al. [25]	Liu et al. [27]
AF(3X3)	0.00%	51.02%	0.00%	0.00%	75.00%
AF (5x5)	0.00%	65.31%	0.00%	0.00%	100.00%
MF(3X3)	0.00%	41.50%	0.00%	0.00%	80.00%
MF (5x5)	0.00%	60.54%	0.00%	0.00%	100.00%
GB (0.5)	0.00%	31.97%	0.00%	0.00%	55.00%
GB (1)	0.00%	53.06%	0.00%	0.00%	80.00%
CR (5%)	0.00%	92.52%	36.73%	0.00%	55.00%
CR (10%)	0.00%	95.92%	59.86%	0.00%	85.00%
GN (0.001)	0.00%	55.78%	0.00%	0.00%	80.00%
GN (0.003)	0.00%	55.78%	0.00%	0.00%	65.00%
SN (0.001)	0.00%	6.80%	0.00%	0.00%	70.00%
SN (0.003)	0.00%	24.49%	0.00%	0.00%	75.00%
JC (Q=70)	0.00%	78.91%	0.00%	0.00%	70.00%
JC (Q=80)	0.00%	67.35%	0.00%	0.00%	75.00%
JPEG2000 (4)	0.00%	44.22%	0.00%	0.00%	60.00%
JPEG2000 (8)	0.00%	55.78%	0.00%	0.00%	70.00%
RS (0.8)	0.00%	37.41%	0.00%	0.00%	60.00%
RS (1.2)	0.00%	34.01%	0.00%	0.00%	50.00%
WF(3x3)	0.00%	50.34%	0.00%	0.00%	80.00%
WF (5x5)	0.00%	64.63%	0.00%	0.00%	100.00%
Average	0.00%	53.37%	4.83%	0.00%	74.25%

From Table 10, we can find all P_{fn} of our proposed scheme under different attacks are 0.00%, which are the same with Zou *et al.* [25] and much smaller than those of zero-watermarking schemes Seenivasagam *et al.* [23], Du *et al.* [26] and Liu *et al.* [27]. The results demonstrate that our proposed scheme has a comparable overall performance with Zou *et al.* [25], and yields much better overall performance than Seenivasagam *et al.* [22], Du *et al.* [26] and Liu *et al.* [27]. In addition, as analyzed in Section IV-C, comparing to all these zero-watermarking schemes, third-party storage is not required in our proposed scheme and thus avoids the additional storage security risks. In summary, our proposed scheme is more suitable for protecting medical images compared with zero-watermarking schemes.

V. CONCLUSION

In this paper, a hybrid reversible-zero watermarking scheme is proposed to protect the copyright and authenticity of medical images. The experimental results have demonstrated that our proposed scheme ensures remarkable watermarking robustness, imperceptibility and distinguishability at the same time. Moreover, our proposed scheme has the following merits compared with other existing watermarking schemes for protecting medical images: 1) comparing with ROI lossless watermarking, our scheme is distortion-free which enhance the accuracy of medical diagnosis; 2) comparing with reversible watermarking, our scheme can continuously protect the medical images without any verification dispute; 3) comparing with zero-watermarking, our scheme can ensure the accuracy of ownership share for a specific image and avoid third-party storage, thus confirming more reliable protection for medical images with better security. Our future work includes further improving the robustness of the reversible-zero hybrid watermarking scheme by enhancing the reversible watermarking component, and applying this method for telemedical applications.

REFERENCES

[1] R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. 1st Int. Conf. Image Process.*, vol. 2, 1994, pp. 86–90.

[2] C.-W. Tang and H.-M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 950–959, Apr. 2003.

[3] C. Wang, Y. Zhang, and X. Zhou, "Robust image watermarking algorithm based on ASIFT against geometric attacks," *Appl. Sci.*, vol. 8, no. 3, p. 410, Mar. 2018.

[4] J. Liu, J. Li, J. Ma, N. Sadiq, U. Bhatti, and Y. Ai, "A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon map," *Appl. Sci.*, vol. 9, no. 4, p. 700, Feb. 2019.

[5] Z. Yue, Z. Li, H. Ren, and Y. Yang, "A large capacity histogram-based watermarking algorithm for three consecutive bins," *Appl. Sci.*, vol. 8, no. 12, p. 2617, Dec. 2018.

[6] B. W. T. Agung, Adiwijaya, and F. P. Permana, "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression," in *Proc. IEEE Int. Conf. Commun., Netw. Satell. (ComNetSat)*, Jul. 2012, pp. 167–171.

[7] H.-K. Lee, H.-J. Kim, K.-R. Kwon, and J.-K. Lee, "ROI medical image watermarking using DWT and bit-plane," in *Proc. Asia–Pacific Conf. Commun.*, 2005, pp. 512–515.

[8] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: A robust medical image watermarking system for E-healthcare," *Multimed Tools Appl.*, vol. 76, no. 8, pp. 10599–10633, Apr. 2017.

[9] R. L. Priya and V. Sadasivam, "Protection of health imagery by region based lossless reversible watermarking scheme," *Sci. World J.*, vol. 2015, pp. 1–10, Nov. 2015.

[10] A. Al-Haj and A. Amer, "Secured telemedicine using region-based watermarking with tamper localization," *J. Digit. Imag.*, vol. 27, no. 6, pp. 737–750, Dec. 2014.

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

[12] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[13] X. Deng, Y. Mao, and J. Hu, "A novel lossless robust medical image watermarking algorithm based on Huffman coding and K-means clustering," *Int. J. Digit. Content Technol. Appl.*, vol. 6, no. 13, pp. 368–377, Jul. 2012.

[14] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[15] G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 111–120, Jan. 2013.

[16] L. An, X. Gao, X. Li, D. Tao, C. Deng, and J. Li, "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Trans. Image Process.*, vol. 21, no. 8, pp. 3598–3611, Aug. 2012.

[17] B. Lei, E.-L. Tan, S. Chen, D. Ni, T. Wang, and H. Lei, "Reversible watermarking scheme for medical image based on differential evolution," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3178–3188, Jun. 2014.

[18] R. Thabit and 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, Mar. 2015.

[19] X. Liu, J. Lou, H. Fang, Y. Chen, P. Ouyang, Y. Wang, B. Zou, and L. Wang, "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images," *IEEE Access*, vol. 7, pp. 76580–76598, 2019.

[20] B. Han, L. Cai, and W. Li, "Zero-watermarking algorithm for medical volume data based on Legendre chaotic neural network and perceptual hashing," *Int. J. Grid Distrib. Comput.*, vol. 8, no. 1, pp. 201–212, Feb. 2015.

[21] C. Dong, H. Zhang, J. Li, and Y.-W. Chen, "Robust zero-watermarking for medical image based on DCT," in *Proc. 6th Int. Conf. Comput. Sci. Converg. Inf. Technol. (ICCIT)*, 2011, pp. 900–904.

[22] V. Seenivasagam and R. Velumani, "A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud," *Comput. Math. Methods Med.*, vol. 2013, pp. 1–16, Jun. 2013.

[23] S. Vellaisamy and V. Ramesh, "Inversion attack resilient zero-watermarking scheme for medical image authentication," *IET Image Process.*, vol. 8, no. 12, pp. 718–727, 2014.

[24] T.-Y. Fan, H.-C. Chao, and B.-C. Chieu, "Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient," *Signal Process., Image Commun.*, vol. 70, pp. 174–183, Feb. 2019.

[25] B. Zou, J. Du, X. Liu, and Y. Wang, "Distinguishable zero-watermarking scheme with similarity-based retrieval for digital rights management of fundus image," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28685–28708, Nov. 2018.

[26] J. Du, B. Zou, X. Liu, F. Li, and H. Zhao, "A lossless fingerprinting-watermarking hybrid scheme for digital right management of fundus images," *J. Inf. Hiding Multim. Signal Process.*, vol. 8, no. 1, pp. 31–41, 2017.

[27] X. Liu, J. Lou, Y. Wang, J. Du, B. Zou, and Y. Chen, "Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images," *Proc. SPIE*, vol. 10579, Mar. 2018, Art. no. 105791I.

[28] N. Bhoskar, P. Ithape, B. Gavali, and P. Kasture, "A survey on secrete communication through QR code steganography for military application," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 1, pp. 728–731, 2022.

[29] G. Yuan and Q. Hao, "Digital watermarking secure scheme for remote sensing image protection," *China Commun.*, vol. 17, no. 4, pp. 88–98, Apr. 2020.

[30] D. Tong, N. Ren, and C. Zhu, "Secure and robust watermarking algorithm for remote sensing images based on compressive sensing," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 16053–16076, Jun. 2018.

[31] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigm in digital watermarking," *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 2, pp. 1–12, Dec. 2002.

[32] E. Ganic and A. M. Eskicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition," *J. Electron. Imag.*, vol. 14, no. 4, 2005, Art. no. 043004.

[33] G. Kasana and S. S. Kasana, "Reference based semi blind image watermarking scheme in wavelet domain," *Optik*, vol. 142, pp. 191–204, Aug. 2017.

[34] C. Pak and L. L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

[35] X. Liu, Y. Sun, J. Wang, C. Yang, Y. Zhang, L. Wang, Y. Chen, and H. Fang, "A novel zero-watermarking scheme with enhanced distinguishability and robustness for volumetric medical imaging," *Signal Process., Image Commun.*, vol. 92, Mar. 2021, Art. no. 116124.

ZHEN DAI received the M.S. degree in software engineering from Central South University, in 2010. She is currently an Associate Professor at the Hunan Vocational College of Science and Technology. Her research interests include information security, deep learning, and data mining.

CHUNYAN LIAN received the B.S. and M.S. degrees in computer science and technology from Central South University, in 2015 and 2018, respectively. She is currently a Teaching Assistant at the Hunan Vocational College of Science and Technology. Her research interests include information security, deep learning, and computer vision.

ZHUOHAO HE received the B.S. degree in computer science and technology from Central South University, in 2022. His research interests include information security, deep learning, and computer vision.

HUAILONG JIANG received the master's degree in software engineering from Wuhan University, in 2014. He is currently a Lecturer at the Hunan Vocational College of Science and Technology. His research interests include virtual reality, software technology, game development, and deep learning.

YIFAN WANG received the B.S. degree in information management and information system from Beijing Technology and Business University, in 2016, and the M.S. degree in computer science from Central South University, in 2019. He is currently pursuing the Ph.D. degree with Loughborough University. His research interests include information security, deep learning, and computer vision.