Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.022308

check for updates

ARTICLE

Application of Zero-Watermarking for Medical Image in Intelligent Sensor Network Security

Shixin Tu, Yuanyuan Jia, Jinglong Du* and Baoru Han*

Medical Data Science Academy, College of Medical Informatics, Chongqing Medical University, Chongqing, 400016, China

*Corresponding Authors: Jinglong Du. Email: jldu@cqmu.edu.cn; Baoru Han. Email: baoruhan@cqmu.edu.cn

Received: 03 March 2022 Accepted: 30 August 2022

ABSTRACT

The field of healthcare is considered to be the most promising application of intelligent sensor networks. However, the security and privacy protection of medical images collected by intelligent sensor networks is a hot problem that has attracted more and more attention. Fortunately, digital watermarking provides an effective method to solve this problem. In order to improve the robustness of the medical image watermarking scheme, in this paper, we propose a novel zero-watermarking algorithm with the integer wavelet transform (IWT), Schur decomposition and image block energy. Specifically, we first use IWT to extract low-frequency information and divide them into non-overlapping blocks, then we decompose the sub-blocks by Schur decomposition. After that, the feature matrix is constructed according to the relationship between the image block energy and the whole image energy. At the same time, we encrypt watermarking with the logistic chaotic position scrambling. Finally, the zero-watermarking is obtained by XOR operation with the encrypted watermarking. Three indexes of peak signal-to-noise ratio, normalization coefficient (NC) and the bit error rate (BER) are used to evaluate the robustness of the algorithm. According to the experimental results, most of the NC values are around 0.9 under various attacks, while the BER values are very close to 0. These experimental results show that the proposed algorithm is more robust than the existing zero-watermarking methods, which indicates it is more suitable for medical image privacy and security protection.

KEYWORDS

Intelligent sensor network; medical image; zero-watermarking; integer wavelet transform; schur decomposition

1 Introduction

With the increasing maturity of intelligent sensor network technology and the continuous improvement of hospital information construction, intelligent sensor network technology is more and more widely used in hospital information systems by combining wide area networks (WAN), wireless networks and other network fields [1]. Most of the data collected by the hospital intelligent sensor network terminal itself belongs to sensitive medical information. Once the information is leaked or maliciously modified, it will bring irreparable losses to the hospital. At the same time, medical information will involve patient information in the process of network transmission. If patient information is leaked, it will bring a huge threat to the patient's personal privacy, property security, and information security [2]. Therefore, it is necessary to ensure the security of patient information.

In the current field of healthcare, more and more medical information is collected and transmitted through intelligent sensor networks. Among them, medical images provide a visual way for clinicians to diagnose the condition of patients. An increasing number of medical images are transmitted among different positions through the network. Most of these medical images contain personal privacy details, which may be maliciously intercepted and tampered with by some illegal elements during the transmission. Therefore, the digital watermarking technique has been gradually applied to protect the security of the medical image [3]. It embeds specified information that cannot be visually detected and in the digital carrier without affecting the transmission, which plays a role in copyright protection [4]. The digital watermarking method can be implemented in spatial and transform domains. The spatial domain algorithm is simple and lightweight. In contrast, the transform-based method has better transparency and robustness, so it has become mainstream in the field of digital watermarking.

In the spatial domain, the least significant bit (LSB) is a commonly-used technique [5,6]. For example, Wang et al. proposed a fragile watermarking method based on the LSB, hash functions and chaotic sequences [7]. The commonly-used method in the transform domain is discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT) and so on [8–10]. In addition, many techniques based on the geometric moment of image watermarking are also widely used [11]. A technique of embedding the scrambled binary watermarking into a host color image by adapting the fractional-order multi-channel orthogonal exponent moments (MFrEMs) magnitudes was proposed by Hosny et al. [12]. Besides, some algorithms divide medical images into regions of interest (ROI) and regions of non-interest (RONI) to accurately extract the features matrix [13–15]. However, the division of ROI regions often requires manual evaluation and distinguishing, which limits the application situation of these algorithms. However, most of the above methods construct the watermarking by making some changes to the original image [16].

To solve this problem, Wen et al. proposed a zero-watermarking algorithm to construct the watermarking according to the characteristic information of the image itself, which could solve the contradiction between the perceptibility and robustness of digital watermarking [17]. This type of zero-watermarking algorithm is widely used in the copyright protection of medical images. Aditi et al. designed a multiple watermarking algorithm using DWT, DCT and singular value decomposition (SVD) which used medical block image watermarking, doctor signature and patient diagnosis information as text watermarking [18]. Similarly, Liu et al. [19] proposed a medical image zero-watermarking algorithm based on dual-tree complex wavelet transform and discrete cosine transform. Then, the zero-watermarking was encrypted by a Logistic map. Hu et al. [20] proposed a robust medical image zero-watermarking algorithm combining bi-dimensional empirical mode decomposition (BEMD) with SVD, which could effectively detect image tampering and protect the copyright of medical images. Xia et al. [21] extended the integer-order radial harmonic Fourier moments (IoRHFMs) to fractional-order radial harmonic Fourier moments (FoRHFMs), and then proposed a FoRHFM-based medical image zero-watermarking algorithm, which improved the calculation accuracy of IoRHFMs and effectively alleviated the problem of numerical instability. Dai et al. [22] proposed a hybrid reversible zero-watermarking (HRZW), in which the authors combined the zero-watermarking and reversible watermarking to generate the ownership shares through the characteristics and watermarking information of the nearest neighbor gray residue (NNGR), and then reversibly embed the generated ownership shares based on slantlet transform, singular value decomposition and quantization index modulation (SLT-SVD-QIM). For medical images, a robust zero-watermarking algorithm by fusing Dual-Tree Complex Wavelet Transform (DTCWT), Hessenberg decomposition, and Multi-level Discrete Cosine Transform (MDCT) was proposed by Huang et al. [23].

The current focus of the watermarking algorithm research is on the robustness of this algorithm under various attacks. However, these algorithms are less robust against high-intensity conventional and geometric attacks, especially Gaussian noise, scaling attacks, and cropping attacks. And most algorithms do not test the robustness of multiple attacks.

To address these issues, in this paper, we propose a zero-watermarking algorithm based on IWT, Schur decomposition and image block energy. Specifically, we use IWT to extract low-frequency regions from the original medical image and divide them into non-overlapping blocks, which are subsequently decomposed by the Schur decomposition. Then, we extract the feature matrix by comparing the energy of the image block and the whole image. Finally, we adopt the XOR operation on the encrypted watermarking image and the feature matrix to generate the zero-watermarking. To summarize, we make the following contributions in this work:

(1) We use IWT to avoid the defect of quantization error introduced in the medical image calculation process;
(2) We improve the robustness and stability using the Schur decomposition with vector scale invariance and quantum space invariance;
(3) We utilize the relationship between the block energy of the transform domain and the average energy of medical images to construct the zero-watermarking, which can achieve good robustness against various attacks even with multiple attacks.

2 Theoretical Basis

2.1 Integer Wavelet Transform (IWT)

Sweldens et al. proposed a lifting scheme which accelerates the speed of fast wavelet transform [24]. Afterward, Calderbank et al. proposed IWT on the basis of a lifting scheme [25]. The coefficients of this algorithm are all integers after transformation, so IWT not only retains the characteristics of wavelet transform but also speeds up the operation. The transformation process of the algorithm includes the following three steps: (1) Splitting: splitting the original data set into two disjoint subsets, an even subset and an odd subset. (2) Prediction: on the basis of the original data and based on the relationship between the data, a prediction operator is constructed, and the even subset sequence is used to predict the odd subset sequence. The error between the predicted value and the original odd subset will generate error data. (3) Update: to make the even subset generated in the splitting step always retain some characteristics of the original data set, an update operator is constructed to update the even subset.

The IWT is the same as the traditional wavelet transform. The original image is still decomposed into four sub-bands after a wavelet transform. A schematic diagram of the 2-level IWT decomposition is shown in Fig. 1. It is the low-frequency component LL of the original image in the horizontal and vertical direction; LH is the low frequency in the horizontal direction and the high frequency in the vertical direction; HL is the high frequency in the horizontal direction and the low frequency in the vertical direction; and HH is the high-frequency component in the horizontal and vertical directions. Among them, the LL sub-band is the low-frequency sub-band containing the features of the original image. If the multi-level transformation is to be carried out, only the low-frequency sub-band is further decomposed. Compared with the traditional wavelet transform, the IWT algorithm is faster and simpler, suitable for parallel processing and takes up less memory.

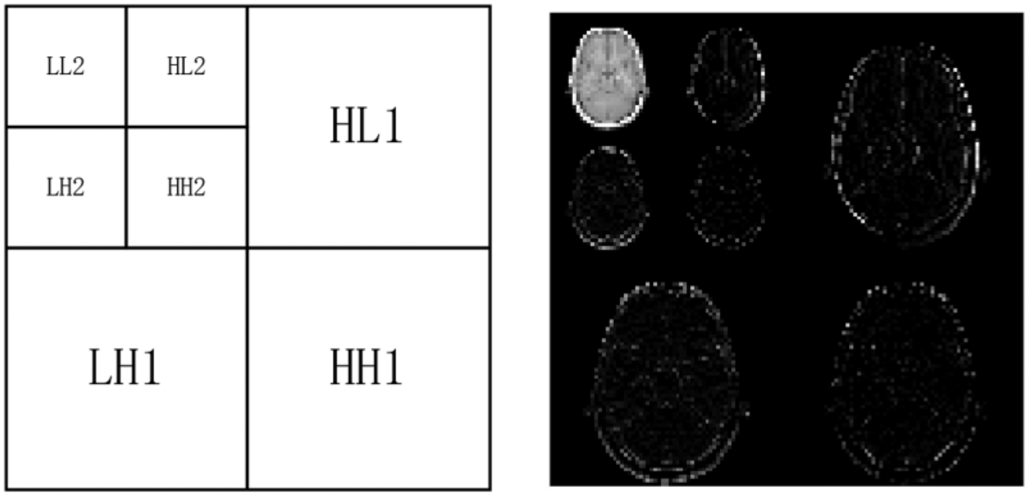

Figure 1: Schematic diagram of the 2-level IWT decomposition

2.2 Schur Decomposition

Schur decomposition is a common matrix decomposition, which is similar to SVD. SVD can be derived from Schur decomposition. Schur decomposition's theorem is as follows:

For any matrix $A \in R^{n\times n}$, then there exists a unitary matrix $U \in R^{n\times n}$ and an upper triangular matrix $T \in R^{n\times n}$ such that $A = UTU^T$, the principal diagonal element of T in the formula is the eigenvalue of A [26], where U^T denotes the conjugate transpose matrix U.

The time complexity of SVD is bigger than the time complexity of Schur decomposition [27]. Thus, it can be seen that Schur decomposition can reduce the computational complexity and save a lot of computing time compared with SVD.

2.3 Image Blocking Energy

Each image has its overall energy, but in the zero-watermarking algorithm, the fact that the original image can effectively resist all kinds of attacks shows that the features constructed by the algorithm are very robust. So, on the basis of the overall image energy, choose to block the image to calculate the energy of the block image. The original image is divided into $x \times y$ sized blocks, and the average energy E of each block is expressed as:

$$E = \sum_{i=1}^{x}\sum_{j=1}^{y} I\left(i,j\right)^2/(x \times y) \tag{1}$$

where $I(i,j)$ is the pixel value of the original medical image and x, y represents the length and width of the original image or chunks, respectively.

In [28], the natural image is used to test the relationship between the overall average energy and the average energy when the original image is attacked by different attacks. While this paper studies the medical image, there are some differences in imaging principles and inherent characteristics between medical images and natural images. Therefore, this paper chooses the MRI image with a size of 128×128 as the original image and divides it into 2×2 blocks for testing. When the original image is attacked by Gaussian noise (10%), JEPG compression (50%), median filtering (3×3), counterclockwise rotation (5°) and scaling (0.25), the relationship between the overall average energy of the medical image and the block average energy is shown in Table 1.

Table 1: Relationship between overall energy and block energy of medical images

Attack type	T_0	T_1	PSNR
None	2543	1553	—
Gaussian noise (10%)	2549	1547	12.1322
JPEG compression (50%)	2545	1551	29.5967
Median filtering (3 × 3)	2520	1576	20.9100
Rotation (5°) (anticlockwise)	2561	1535	15.5834
Scaling (0.25, 4)	2495	1601	17.8888

As shown in Table 1, T_0 represents the number of blocks whose average energy is greater than the overall average energy, while T_1 indicates that the average energy of blocks is less than the number of blocks with overall average energy. And peak signal-to-noise ratio (PSNR) is an objective index to evaluate image quality. After different attacks, except that the value of PSNR fluctuates greatly, but the ratio between T_0 and T_1 is not large, so it has strong robustness. It can be seen that this feature extraction method is also suitable for the construction of zero-watermarking in medical images.

3 Proposed Method

The medical image watermarking algorithm proposed in this paper can be divided into the process of zero-watermarking construction and extraction, as shown in Fig. 2.

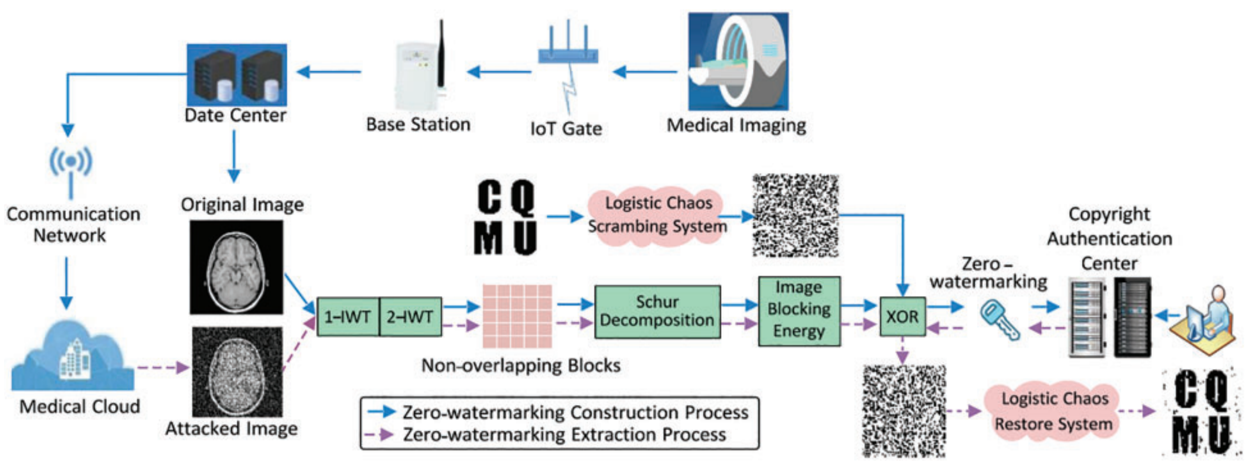

Figure 2: The flow chart of the proposed zero-watermarking construction and extraction process

3.1 Zero-Watermarking Construction

The collected medical images are transmitted to the data center by an intelligent sensor network. Then upload the medical image to the medical cloud platform according to the requirements of medical information management. In order to protect patient information disclosure or authentication, the medical image stored in the data center is used as the original image to construct a zero-watermarking.

We use the logistic chaotic scrambling method to encrypt the binary watermarking image W with size $N \times N$ to generate the scrambled watermarking image W_1. The μ_0 and x_0 are chaotic initial values. It is expressed as:

$$W_1 \leftarrow logistics(W, \mu_0, x_0) \tag{2}$$

where $Logistics(\cdot)$ is the logistic chaotic scrambling function.

To construct the zero-watermarking, we adopt the IWT to extract the feature matrix from the original image features [29]. The IWT not only retains the characteristics of the wavelet transform but also is faster, which meets the requirements of accuracy and accurate decomposition of medical images. Therefore, we utilize the 2-level IWT to extract the low-frequency part of the original medical image I with size $M \times M$, which can be obtained as:

$$I\_LL_2 \leftarrow liftwavedec2(I) \tag{3}$$

where $liftwavedec2(\cdot)$ denotes the two-level IWT function.

Schur decomposition is a commonly-used matrix decomposition method, which is similar to SVD operation [27]. Compared with SVD, it can reduce computational complexity and save a lot of computing time. In addition, Schur decomposition also has vector scaling invariance and quantum space invariance, so it can effectively resist scaling attacks. These important characteristics make the zero-watermarking algorithm faster, more robust and stable. The low-frequency part of the original medical image is divided into non-overlapping blocks. Then decomposes the blocks by the Schur decomposition. The specific realization process can be written as:

$$A_{ij} \leftarrow Block(I\_LL_2, m, m) \tag{4}$$

$$T_{ij} \leftarrow schur(A_{ij}) \tag{5}$$

where $m = \sqrt{N}$, $n = M/4\sqrt{N}$ and $i, j \in (1, 2, 3, \cdots, m)$.

Each image has its overall energy, but in the zero-watermarking algorithm, the fact that the original image can effectively resist all kinds of attacks shows that the features constructed by the algorithm are very robust. Because the relationship between the overall average energy of the medical image and the average energy of each block has strong robustness. The calculation of the overall original medical image I energy is given by:

$$E = \sum_{i=1}^{M} \sum_{j=1}^{M} I(i,j)^2 / (M \times M) \tag{6}$$

On the basis of the overall image energy, we choose to block the image to calculate the energy of the split image. The original image is divided into $n \times n$ sized blocks, and the average energy E_k of each block is expressed as:

$$E_k = \sum_{i=1}^{n} \sum_{j=1}^{n} T(i,j)^2 / (n \times n), k \in \left(1, 2, 3, \cdots, n^2\right) \tag{7}$$

Based on the overall average energy and block average energy of the carrier image calculated in the above steps, the method of constructing the feature matrix can be represented as:

$$T_k = \begin{cases} 1 & E \geq E_k \\ 0 & other \end{cases} \tag{8}$$

Finally, the zero-watermarking Z is generated by the exclusive XOR operation of the feature matrix T and the scrambled watermarking image W_1, therefore we can get:

$$Z = XOR(T, W_1) \tag{9}$$

The final zero-watermarking Z is registered in the copyright authentication center. The construction process is shown in Fig. 2. The specific steps are as Algorithm 1.

3.2 Zero-Watermarking Extraction

The zero-watermarking extraction is similar to the above-described construction process. The difference is that the feature matrix obtained from the attacked medical image is XOR with the zero-watermarking from the copyright authentication center, and then inverse scrambling is carried out to the extraction watermarking image W'. The process of zero-watermarking extraction is shown in Fig. 2. The detailed steps are as Algorithm 2. Here, we use the PSNR, normalization coefficient (NC) and the bit error rate (BER) between the extraction watermarking image W' and the original watermarking image W to measure the robustness of the watermarking algorithm, which can be written as:

$$PSNR = 10 \times \log\left(\frac{(2^n-1)^2}{\left(\sum_{i=1}^{M}\sum_{j=1}^{M}(I'(i,j) - I(i,j))^2\right)/(M \times M)}\right) \tag{10}$$

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j) \times W'(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W^2(i,j) \times \sum_{i=1}^{N}\sum_{j=1}^{N} W'^2(i,j)}} \tag{11}$$

$$BER = \frac{Number\_err}{Number} \times 100\% \tag{12}$$

In formula (10) and formula (11), M is the length and width of the original medical image, N is the length and width of the watermarking image. In formula (12), *Number_err* represents the error bit generated in transmission, *Number* represents the total number of bits transmitted.

Algorithm 1

Input: original image I ($M \times M$), watermarking image W ($N \times N$)
Output: zero-watermarking Z

$W_1 = logistics(W, \mu_0, x_0)$ //generate the scrambled watermarking image
$I\_LL_2 \leftarrow liftwavedec2(I)$
$A_k \leftarrow Block(I\_LL_2, N)$ //$k \in (1, 2, 3, \cdots, N)$
$T_k \leftarrow schur(A_k)$
$E = \sum_{i=1}^{M}\sum_{j=1}^{M} I(i,j)^2/(M \times M)$
$E_k = \sum_{i=1}^{n}\sum_{j=1}^{n} T_k(i,j)^2/(n \times n)$ // $n = M/4\sqrt{N}$

(Continued)

Algorithm 1 (Continued)

for $k = 1, 2, 3, \cdots, N$ **do**
  if $E >= E_k$ **then**
    $B(k) = 0$
  else $B(k) = 1$
  end if
end for
$Z = XOR(B, W_1)$

4 Experiments and Results

4.1 Experimental Setting

In the experiment, we implement the construction and extraction of zero-watermarking using the MATLAB R2018a platform. The original medical images include the brain, lung, chest and hand with the size of 128×128 are used as the original carrier images, as shown in Figs. 3a–3d. The original watermarking images with the size of 64×64 are given in Figs. 3e–3f.

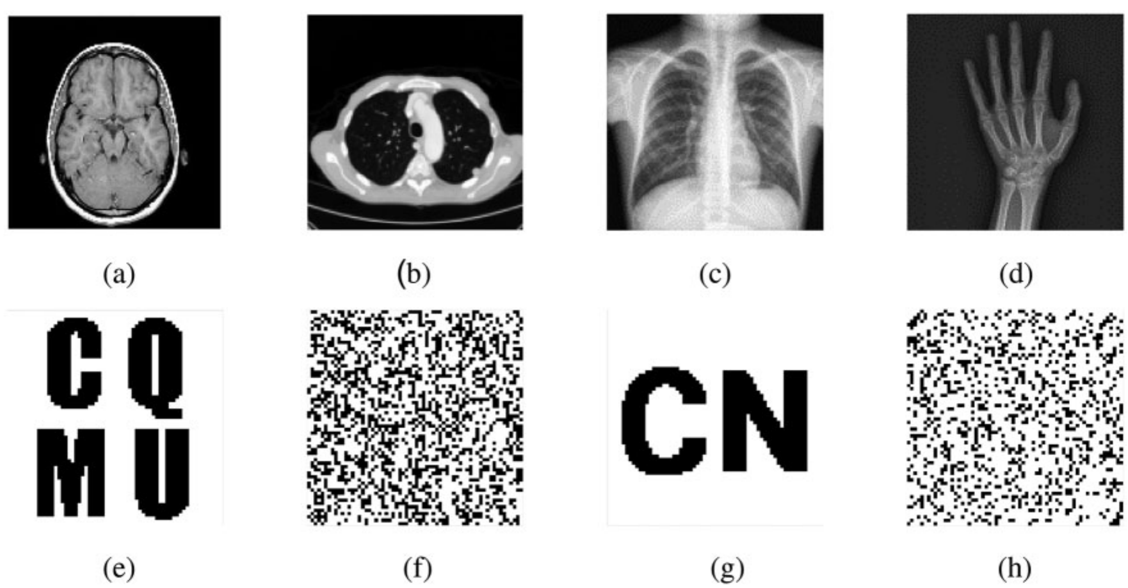

Figure 3: The original carrier medical image and the watermarking image used in the experiment

Algorithm 2

Input: attacked medical image I' $(M \times M)$, zero-watermarking Z $(N \times N)$
Output: the decrypted watermarking W_2

$I'\_LL_2 \leftarrow liftwavedec2(I')$
$A'_k \leftarrow Block(I'\_LL_2, m, m)$ // $k \in (1, 2, 3, \cdots, N)$
$T'_k \leftarrow schur(A'_k)$

(Continued)

Algorithm 2 (Continued)

$E' = \sum_{i=1}^{M}\sum_{j=1}^{M} I'(i,j)^2/(M \times M)$

$E_k' = \sum_{i=1}^{n}\sum_{j=1}^{n} T_k{}'(i,j)^2/(n \times n)$ // $n = M/4\sqrt{N}$

for $k = 1, 2, 3, \cdots, N$ **do**
  if $E' >= E_k'$ **then**
    $B'(k) = 0$
  else $B'(k) = 1$
  end if
end for
$W' = inverse\_logistics(XOR(B', Z), \mu_0, x_0)$

In this paper, we simulate conventional attacks (Gaussian noise, salt & pepper noise, speckle noise, JPEG compression and median filtering, average filtering and Gaussian filtering), geometric attacks (scaling, cropping, rotation, and translation) and combination attacks to evaluate our proposed medical watermarking algorithm. Here, PSNR is used to measure the distortion of the original medical image after being attacked. Besides, we use the NC value given in formula (11) and the BER given in formula (12) to measure the similarity between the extracted watermarking image and the original watermarking image. Due to a large amount of data in the experimental results, only the experimental data of watermarking image Fig. 3e are listed in Tables 2–4.

Table 2: Detection results of medical images after conventional attack

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Gaussian noise	5%	PSNR	14.7642	15.1995	14.0572	12.3400
		NC	1.0000	1.0000	0.9877	0.9627
		BER	0	0	0.0156	0.0469
	10%	PSNR	12.0866	12.5372	11.7086	9.9068
		NC	1.0000	1.0000	0.9502	0.9502
		BER	0	0	0.0625	0.0625
	15%	PSNR	10.7126	10.8986	10.5340	8.7046
		NC	1.0000	0.9877	0.9376	0.9121
		BER	0	0.0156	0.0781	0.1094
	20%	PSNR	9.7727	10.1506	9.6248	7.8319
		NC	0.9877	0.9629	0.8994	0.8993
		BER	0.0156	0.0469	0.1248	0.1248
	25%	PSNR	9.1073	9.3068	9.1064	7.3490
		NC	0.9753	0.9504	0.8865	0.8863
		BER	0.0313	0.0625	0.1406	0.1404

(Continued)

Table 2 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Salt & pepper noise	5%	PSNR	16.7578	17.0762	18.0804	15.8647
		NC	1.0000	1.0000	1.0000	0.9877
		BER	0	0	0	0.0156
	10%	PSNR	13.6868	13.7390	14.5451	13.0412
		NC	1.0000	1.0000	0.9877	0.9753
		BER	0	0	0.0156	0.0313
	15%	PSNR	11.7907	12.0737	12.8125	11.0732
		NC	1.0000	1.0000	0.9753	0.9502
		BER	0	0	0.0313	0.0625
	20%	PSNR	10.7667	10.8368	11.7323	10.1200
		NC	1.0000	0.9629	0.9502	0.9376
		BER	0	0.0469	0.0625	0.0781
	25%	PSNR	9.7068	9.7819	10.6847	8.9041
		NC	0.9877	0.9502	0.9249	0.9122
		BER	0.0156	0.0625	0.0938	0.1091
Speckle noise	5%	PSNR	21.1982	21.4382	17.7929	22.2242
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	10%	PSNR	18.2521	19.0031	15.1206	19.1629
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	15%	PSNR	16.6040	17.4271	13.5238	17.5106
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156
	20%	PSNR	15.5492	16.3898	12.4485	16.2019
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156
	25%	PSNR	14.7916	15.6281	11.5182	15.3433
		NC	1.0000	1.0000	0.9502	0.9877
		BER	0	0	0.0625	0.0156
JPEG compression	5%	PSNR	22.0045	23.9372	26.7095	26.8927
		NC	1.0000	1.0000	0.9753	0.9877
		BER	0	0	0.0315	0.0153
	10%	PSNR	23.8912	26.9916	29.8869	29.6461
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	15%	PSNR	24.9075	28.465	31.7934	31.1542
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156

(Continued)

Table 2 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
	20%	PSNR	25.8223	29.5188	32.9327	32.1163
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156
	25%	PSNR	26.7087	30.3743	33.8355	32.8303
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
Median filtering	3 × 3	PSNR	23.5681	29.2442	37.9383	35.8022
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	5 × 5	PSNR	19.4000	23.9270	32.2365	31.9462
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	7 × 7	PSNR	17.3484	22.2896	28.8159	28.9450
		NC	1.0000	1.0000	0.9753	1.0000
		BER	0	0	0.0313	0
	9 × 9	PSNR	15.8117	21.3870	26.6631	25.8972
		NC	1.0000	1.0000	0.9753	0.9627
		BER	0	0	0.0313	0.0469
	11 × 11	PSNR	14.8774	20.5817	25.1021	23.4141
		NC	1.0000	1.0000	0.9628	0.9627
		BER	0	0	0.0469	0.0469
Average filtering	3 × 3	PSNR	21.3212	26.6291	29.4174	30.8675
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	5 × 5	PSNR	18.4333	22.3107	25.9712	27.4251
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	7 × 7	PSNR	17.0003	20.2281	23.8956	25.2664
		NC	1.0000	1.0000	0.987	0.9877
		BER	0	0	0.0156	0.0156
	9 × 9	PSNR	16.1408	18.8448	22.4341	23.4856
		NC	1.0000	1.0000	0.9877	0.9753
		BER	0	0	0.0156	0.0313
	11 × 11	PSNR	15.6052	17.7630	21.3092	22.0736
		NC	1.0000	0.9879	0.9877	0.9753
		BER	0	0.0154	0.0156	0.0313

(Continued)

Table 2 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Gaussian filtering	3 × 3	PSNR	21.4444	26.7688	29.5766	31.0254
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	5 × 3	PSNR	18.7563	22.7303	26.3948	27.8346
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	7 × 3	PSNR	17.5649	20.9820	24.7006	26.0922
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	9 × 3	PSNR	16.9531	20.0162	23.7148	24.9039
		NC	1.0000	1.0000	0.9877	0.9753
		BER	0	0	0.0156	0.0313
	11 × 3	PSNR	16.6365	19.4445	23.1469	24.1661
		NC	1.0000	1.0000	0.9877	0.9753
		BER	0	0	0.0156	0.0313

Table 3: Detection results of medical images after geometric attack

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Scaling	0.125, 8	PSNR	15.6243	17.6118	24.5495	22.0149
		NC	1.0000	1.0000	0.9877	0.9627
		BER	0	0	0.0157	0.0469
	0.25, 4	PSNR	17.8888	21.8774	29.2038	28.1517
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0157	0
	0.5, 2	PSNR	21.5809	27.0624	35.8517	32.9718
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	2, 0.5	PSNR	30.2404	38.8692	47.1327	43.5692
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	4, 0.25	PSNR	30.5191	39.1329	47.5906	43.8283
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	5%	PSNR	90.1377	22.2412	19.0604	25.2433
		NC	1.0000	1.0000	0.9628	1.0000
		BER	0	0	0.0469	0

(Continued)

Table 3 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Cropping	10%	PSNR	90.1377	18.4078	14.7486	22.0753
		NC	1.0000	0.9752	0.9376	0.98766
		BER	0	0.0313	0.0781	0.0156
	15%	PSNR	56.9175	16.1173	12.4962	20.5341
		NC	1.0000	0.9752	0.8865	0.9877
		BER	0	0.0313	0.1406	0.1563
	20%	PSNR	25.9643	14.8096	11.1329	19.3096
		NC	1.0000	0.9376	0.8603	0.9753
		BER	0	0.0779	0.1719	0.0312
	25%	PSNR	19.9237	13.9273	10.3298	17.7532
		NC	1.0000	0.92476	0.8603	0.9753
		BER	0	0.0935	0.1719	0.0313
Rotation	3°	PSNR	18.2249	19.3431	20.3276	21.9927
		NC	1.0000	1.0000	0.9753	1.0000
		BER	0	0	0.0313	0
	5°	PSNR	15.5834	16.6031	17.3382	18.9684
		NC	1.0000	0.9877	0.9501	0.9627
		BER	0	0.0156	0.0625	0.0469
	10°	PSNR	12.9947	13.2794	13.7619	15.9034
		NC	1.0000	0.9753	0.8994	0.8993
		BER	0	0.0313	0.1248	0.1250
	15°	PSNR	12.2902	11.4540	11.9394	14.9546
		NC	0.9501	0.9252	0.7984	0.8863
		BER	0.0625	0.0938	0.2498	0.1406
	20°	PSNR	12.0683	10.1806	10.8055	14.3554
		NC	0.9376	0.8347	0.7277	0.8465
		BER	0.0781	0.2031	0.3279	0.1873
Translation	1%	PSNR	17.8600	20.2850	25.4793	30.1726
		NC	1.0000	0.9877	0.9877	1.0000
		BER	0	0.0156	0.0156	0
	3%	PSNR	13.2478	14.1042	19.4053	24.0885
		NC	0.9753	0.9877	0.9627	1.0000
		BER	0.0313	0.0156	0.0469	0
	5%	PSNR	11.9854	11.0666	15.9737	20.6979
		NC	0.9503	0.8473	0.9251	1.0000
		BER	0.0625	0.1875	0.0938	0
	7%	PSNR	11.8748	9.8692	14.6068	19.2970
		NC	0.9503	0.7799	0.9125	0.9877
		BER	0.0625	0.2656	0.1094	0.0156

(Continued)

Table 3 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
	9%	PSNR	11.6587	8.8945	13.0342	17.7887
		NC	0.9247	0.7249	0.8732	0.9376
		BER	0.0938	0.3281	0.1563	0.0781

Table 4: Detection results of medical images after combination attack

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Gaussian noise and median filtering	5%, 3 × 3	PSNR	19.1489	20.9061	20.7881	18.8019
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	10%, 5 × 5	PSNR	17.5993	20.1135	20.6786	19.1843
		NC	1.0000	1.0000	1.0000	1.0000
		BER	0	0	0	0
	15%, 7 × 7	PSNR	16.3756	19.0191	20.0520	18.9095
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	20%, 9 × 9	PSNR	15.6893	18.1736	18.7612	18.4873
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156
	25%, 11 × 11	PSNR	15.2340	17.1140	17.8346	17.9449
		NC	1.0000	1.0000	0.9753	0.9877
		BER	0	0	0.0313	0.0156
JPEG compression and median filtering	5%, 3 × 3	PSNR	21.1295	24.5684	27.3012	27.5828
		NC	1.0000	1.0000	0.9753	0.9877
		BER	0	0	0.0313	0.0156
	10%, 5 × 5	PSNR	19.2976	24.1588	29.7951	29.1742
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	15%, 7 × 7	PSNR	17.4761	22.3819	28.3498	27.9810
		NC	1.0000	1.0000	0.9753	0.9877
		BER	0	0	0.0313	0.0156
	20%, 9 × 9	PSNR	16.0470	21.4425	26.4696	25.7769
		NC	1.0000	1.0000	0.9753	0.9627
		BER	0	0	0.0313	0.0469
	25%, 11 × 11	PSNR	15.1197	20.6040	25.0580	23.6894

(Continued)

Table 4 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
		NC	1.0000	1.0000	0.9628	0.9627
		BER	0	0	0.0469	0.0469
Cropping and median filtering	5%, 3 × 3	PSNR	23.5681	21.4882	19.0059	24.8774
		NC	1.0000	1.0000	0.9628	1.0000
		BER	0	0	0.0469	0
	10%, 5 × 5	PSNR	19.4000	17.4241	14.6643	21.6490
		NC	1.0000	0.9752	0.9376	0.9877
		BER	0	0.0313	0.0781	0.0156
	15%, 7 × 7	PSNR	17.3443	15.2166	12.3925	19.9473
		NC	1.0000	0.9503	0.8865	0.9752
		BER	0	0.0623	0.1406	0.0313
	20%, 9 × 9	PSNR	15.5347	13.9957	11.0146	18.4451
		NC	1.0000	0.9376	0.8603	0.9753
		BER	0	0.0779	0.1719	0.0313
	25%, 11 × 11	PSNR	14.1811	13.1628	10.1960	16.7092
		NC	1.0000	0.9248	0.8735	0.9877
		BER	0	0.0935	0.1563	0.0156
JPEG compression and scaling	5%, 0.125	PSNR	15.5163	17.4607	24.2929	21.7789
		NC	1.0000	1.0000	0.9753	0.9627
		BER	0	0	0.0313	0.0469
	10%, 0.25	PSNR	17.7903	21.7549	28.5464	27.5526
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	15%, 0.5	PSNR	21.2622	26.3763	32.6142	31.2318
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156
	20%, 2.0	PSNR	25.5233	30.0743	33.4944	32.5491
		NC	1.0000	1.0000	0.9877	0.9877
		BER	0	0	0.0156	0.0156
	25%, 4.0	PSNR	26.2767	30.8143	34.4413	33.3297
		NC	1.0000	1.0000	0.9877	1.0000
		BER	0	0	0.0156	0
	0.125, 5%	PSNR	15.7607	16.4132	18.1330	22.2645
		NC	1.0000	1.0000	0.9628	0.9753
		BER	0	0	0.0469	0.0313
	0.25, 10%	PSNR	18.0261	16.8881	14.7144	23.0562
		NC	1.0000	0.9752	0.9376	0.9877
		BER	0	0.0313	0.0781	0.0156

(Continued)

Table 4 (continued)

Attack type	Attack intensity	Evaluation index	Brain image	Lung image	Chest image	Hand image
Scaling and cropping	0.5, 15%	PSNR	21.7197	15.8221	12.5822	22.2321
		NC	1.0000	0.9629	0.8865	0.9877
		BER	0	0.0466	0.1406	0.0156
	2, 20%	PSNR	24.7837	14.7955	11.2348	21.2317
		NC	1.0000	0.9376	0.8603	0.9753
		BER	0	0.0779	0.1719	0.0313
	4, 25%	PSNR	19.7524	13.9171	10.4319	19.6812
		NC	1.0000	0.9248	0.8603	0.9753
		BER	0	0.0935	0.1719	0.0313
Rotation and scaling	3°, 0.125	PSNR	15.7016	17.0976	21.9632	22.9540
		NC	1.0000	1.0000	0.9753	0.9753
		BER	0	0	0.0313	0.0313
	5°, 0.25	PSNR	16.7363	17.5117	18.5239	21.7308
		NC	1.0000	0.9877	0.9501	0.9627
		BER	0	0.0156	0.0625	0.0469
	10°, 0.5	PSNR	13.8861	13.5584	14.0713	18.0076
		NC	0.9877	0.9753	0.8994	0.8993
		BER	0.0156	0.0313	0.1248	0.1250
	15°, 2.0	PSNR	12.5631	11.4826	12.0792	16.9252
		NC	0.9501	0.9378	0.7954	0.8863
		BER	0.0625	0.0781	0.2498	0.1406
	20°, 4.0	PSNR	12.3288	10.2007	10.9375	16.3234
		NC	0.9376	0.8347	0.7277	0.8465
		BER	0.0781	0.2031	0.3279	0.1873

4.2 Robustness Experiments

4.2.1 Conventional Attacks

The first is to carry out some kinds of noise attacks. In this paper, Gaussian noise, salt & pepper noise and speckle noise with different intensities (5%, 10%, 15%, 20% and 25%) are selected to attack the four original medical images. The NC values of all four medical images under the Gaussian noise attack are above 0.88 with the increasing noise intensity as shown in Table 2. Under salt & pepper noise and speckle noise, the NC values of four medical images are greater than 0.9 under an intensity of 25%. Especially under speckle noise attacks, the NC values are always greater than 0.91. And under all three types of noise attacks, the BER values of the images are less than 0.15. As shown in Figs. 4–6, when all kinds of medical images are attacked by three noises of intensity 15%, the NC values are greater than 0.95 despite the serious distortion of the original images. It indicates that the proposed algorithm is robust to noise attacks.

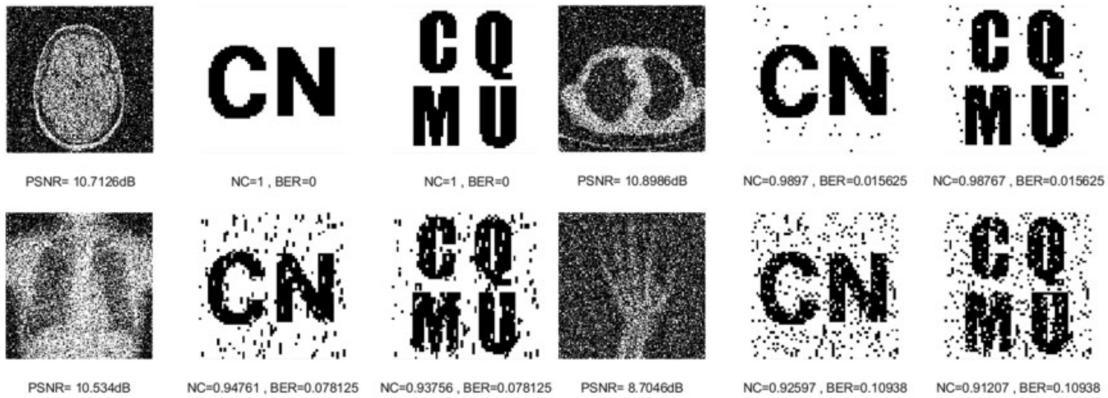

Figure 4: Four medical images and extracted watermarking images with Gaussian noise attack intensity of 15%

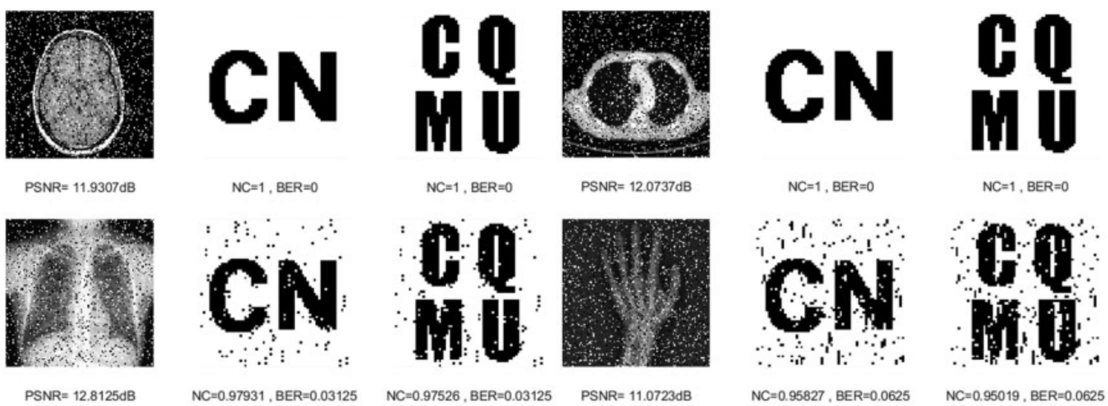

Figure 5: Four medical images and extracted watermarking images with salt & pepper noise attack intensity of 15%

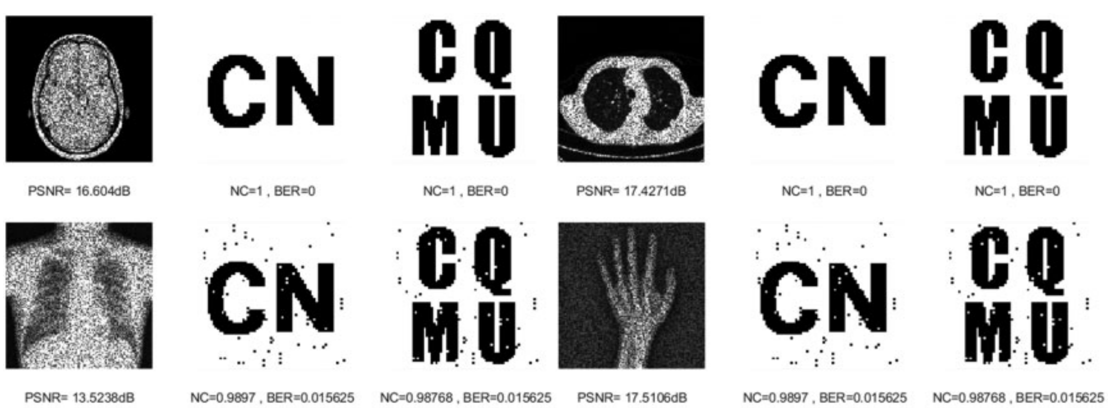

Figure 6: Four medical images and extracted watermarking images with speckle noise attack intensity of 15%

Similarly, the NC values of all four medical images are maintained above 0.97 and their BER values are less than 0.04 through JPEG compression attacks of different intensities. When the strength is 15%, the attack results of the four images are shown in Fig. 7, and we can still see the watermarking pattern clearly through the naked eye. This demonstrates that our algorithm can effectively resist JPEG compression attacks.

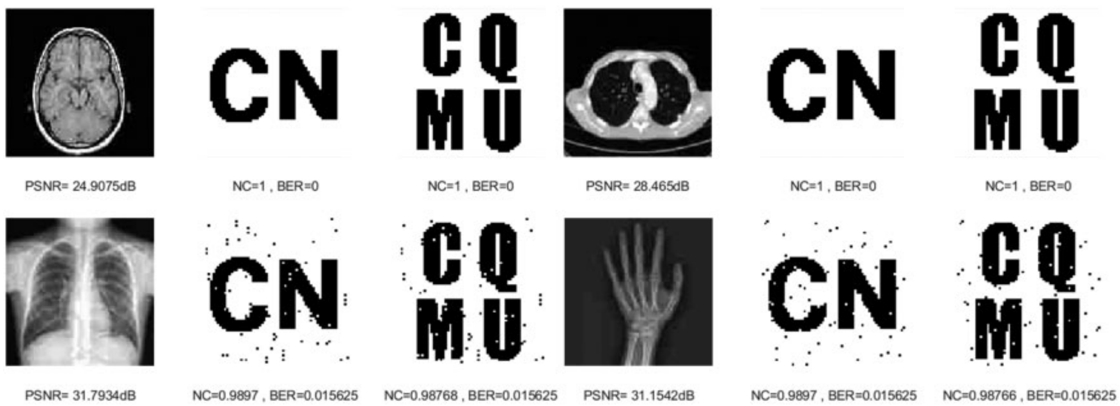

Figure 7: Four medical images and extracted watermarking images with JPEG compression attack intensity of 15%

Three kinds of filtering attacks are also selected in this paper, namely, median filtering, average filtering, and Gaussian filtering. As can be seen from Table 2, as the attack intensity increases, the NC values of the brain image and lung image are almost 1, while the other two images have NC values above 0.96, and the BER values are also very close to 0. As shown in Figs. 8–10, we can see that the median filtering intensity and the mean filtering intensity are 7×7, and the Gaussian filtering intensity is 7×3. The images have been very blurred, but the watermarking image is still relatively complete, even the NC values of brain image and lung image are still equal to 1. The two observations mentioned above verify the good performance against various filtering attacks. Overall, these results shown in Table 2 demonstrated that the proposed algorithm has strong resistance to conventional attacks.

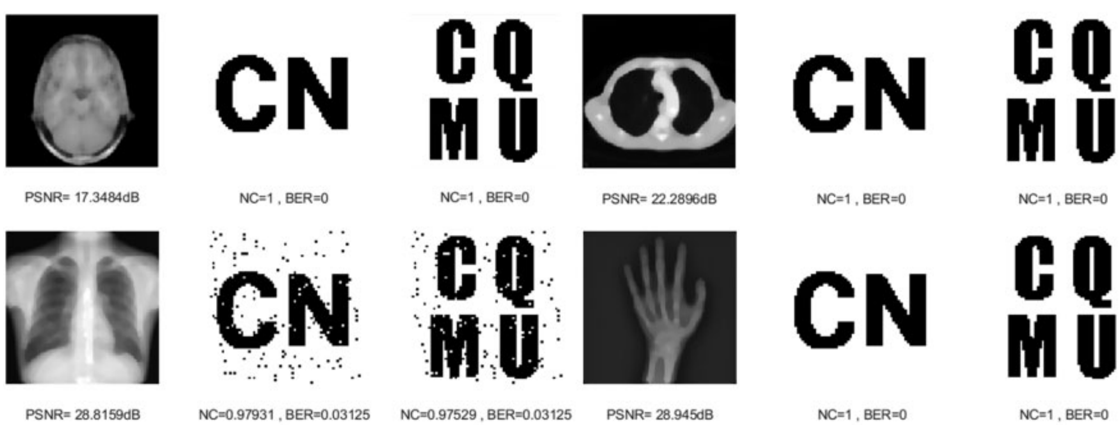

Figure 8: Four medical images and extracted watermarking images with median filtering attack intensity of 7×7

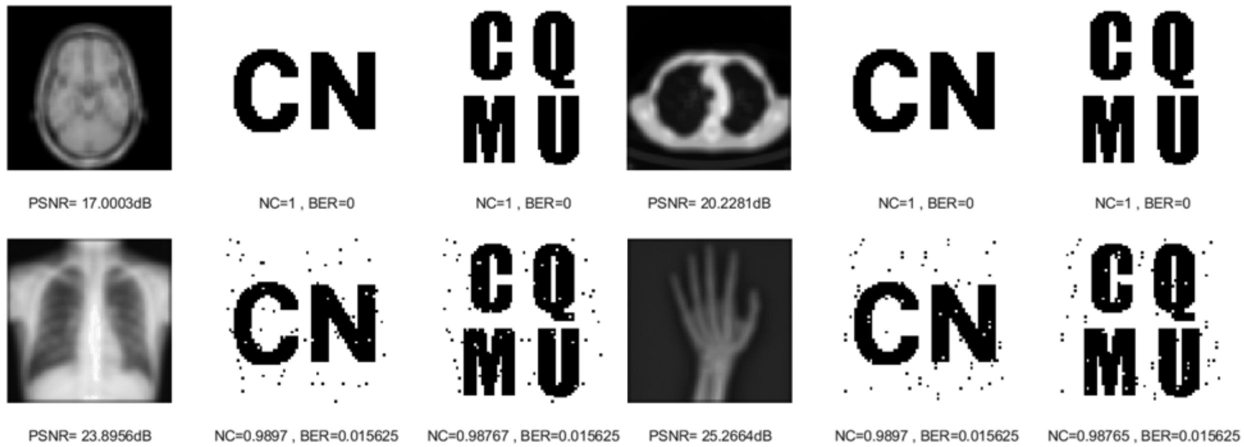

Figure 9: Four medical images and extracted watermarking images with average filtering attack intensity of 7×7

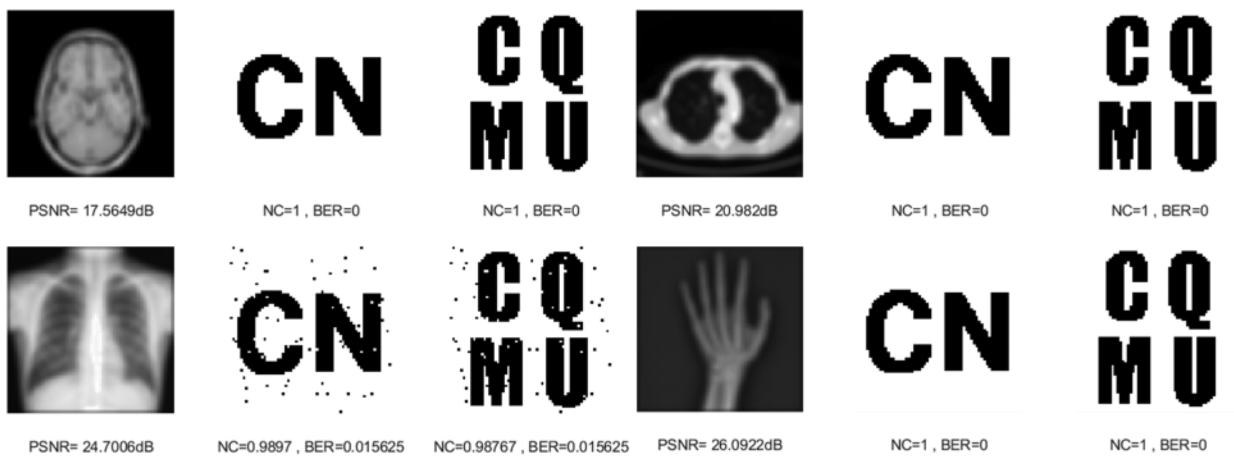

Figure 10: Four medical images and extracted watermarking images with Gaussian filtering attack intensity of 7×3

4.2.2 Geometric Attacks

Table 3 shows the results of our proposed method against geometric attacks. As the scaling attack intensity increases, the NC and PSNR value increases gradually. Besides, no matter what the scaling factor, the NC values of the brain image and lung image are always equal to 1.0 and the BER values are almost always 0. Fig. 11 shows the experimental results when the scaling factors are 0.5 and 2. This shows that the proposed algorithm has strong robustness under scaling attacks.

For medical images such as the chest radiograph, when subjected to a slightly stronger cropping attack, the pixels of the extracted watermarking image are somewhat distorted, but the average value of NC is still higher than 0.86. Fig. 12 shows the experimental results after cropping 15% along the X-axis direction. Their NC values are greater than 0.88. It shows that this proposed algorithm can effectively resist cropping attacks.

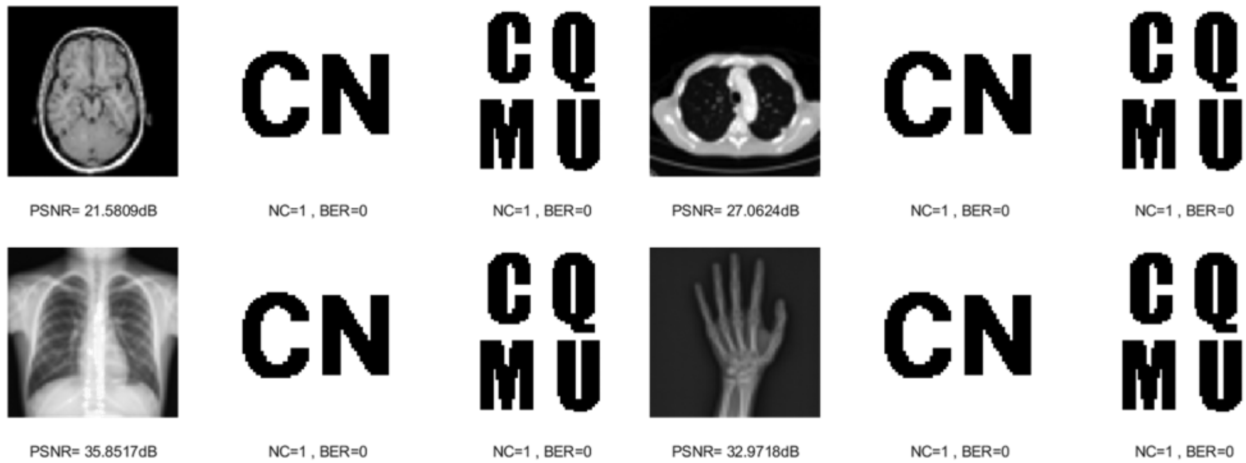

Figure 11: Four medical images and extracted watermarking images with scaling attack intensity of 0.5 and 2

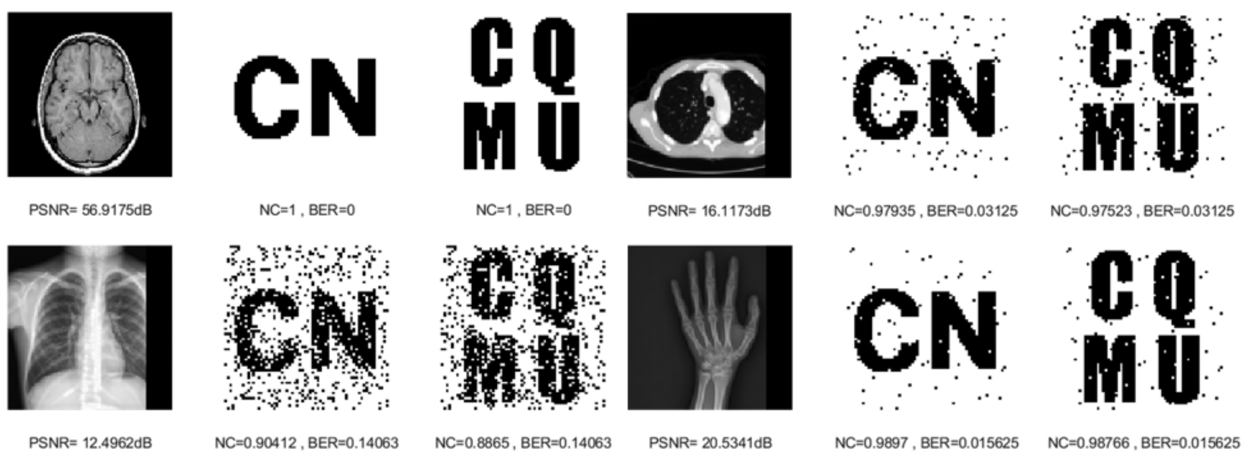

Figure 12: Four medical images and extracted watermarking images with cropping attack intensity of 15%

Image rotation is a common geometric attack that changes the position of image pixels. After rotating 10 degrees counterclockwise, as shown in Fig. 13, the smallest NC value is 0.8993. The rotation attack experimental data in Table 3 further verify that the proposed algorithm has a strong ability to resist counterclockwise rotation attacks.

In the process of downward translation, the PSNR obtained from the original medical image decreases gradually, but the NC values are high enough and the BER values are also close to 0. In Fig. 14, when the translation attack intensity is 5%, their NC values are much greater than 0.84. Therefore, for geometric attacks (scaling, cropping, rotation and translation downward), this proposed algorithm also shows attractive robustness.

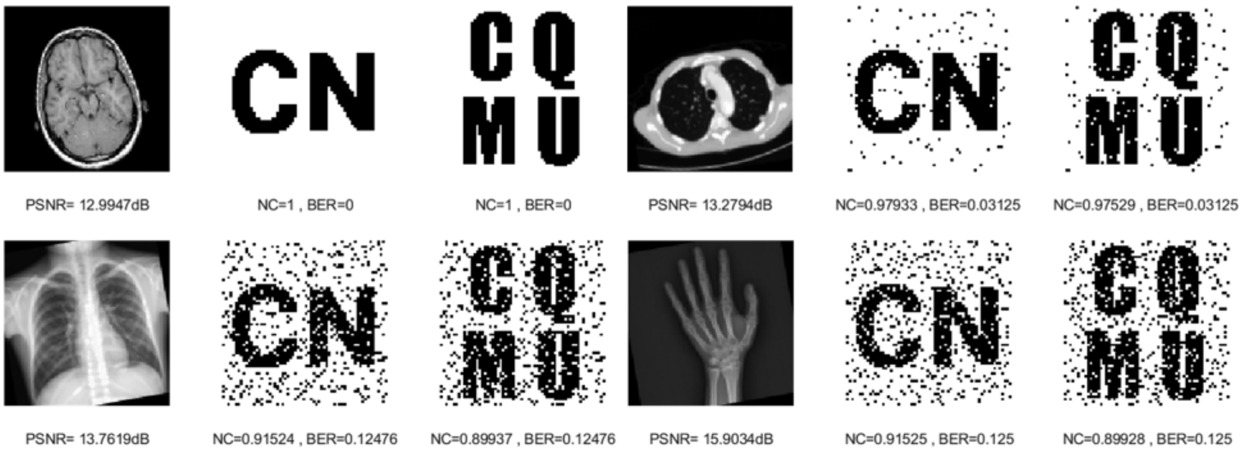

Figure 13: Four medical images and extracted watermarking images with rotation attack intensity of 10°

Figure 14: Four medical images and extracted watermarking images with translation attack intensity of 5%

4.2.3 Combination Attacks

Six combined attacks are selected in this paper. The first is the combination of two conventional attacks. The first kind is the Gaussian noise attack on the medical image and then the median filtering attack, and the second is the JPEG compression attack on the medical image and then the median filtering attack. As can be seen in Table 4, under both attacks, despite the gradually decreasing PSNR values of the four medical images, their NC values are consistently greater than 0.96. From Figs. 15 and 16, the NC values of the brain image and lung image are maintained at 1 under both attacks. In addition, the overall BER values are below 0.05 for both attacks.

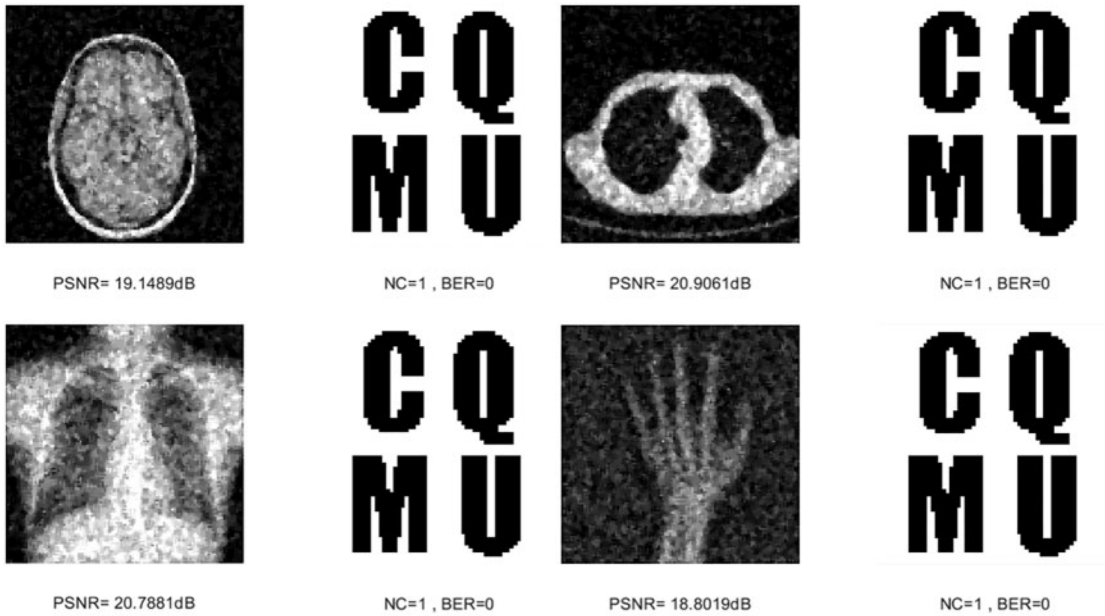

Figure 15: Four medical images and extracted watermarking images with Gaussian noise attack intensity of 5% and median filtering attack intensity of 3×3

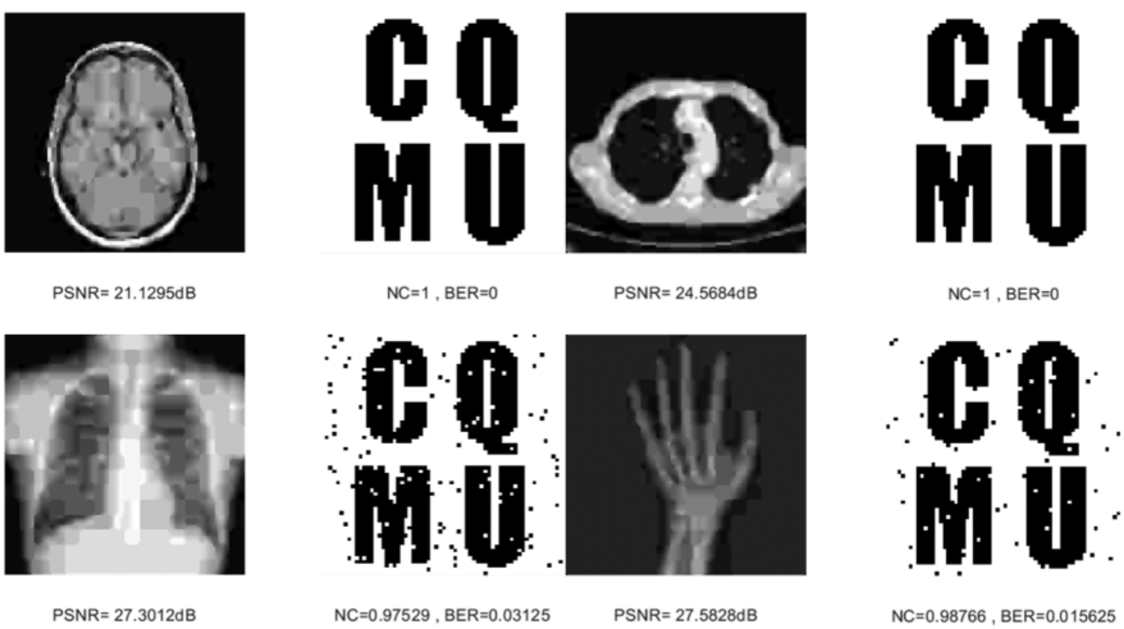

Figure 16: Four medical images and extracted watermarking images with JPEG compression attack intensity of 5% and median filtering attack intensity of 3×3

The second major category is the combination of conventional attacks and geometric attacks. The first one cuts the image along the X-axis and then performs the median filtering attack. Compared with the four images, the NC values of the chest image are slightly lower but still above 0.85, and the

NC values of the other three images remain above 0.9. The second attack is the JPEG compression attack on the image and then the scaling attack. In Figs. 17 and 18, when the medical images become very blurred and distorted, the NC values of the four images are greater than 0.96, and the BER values are also close to 0.

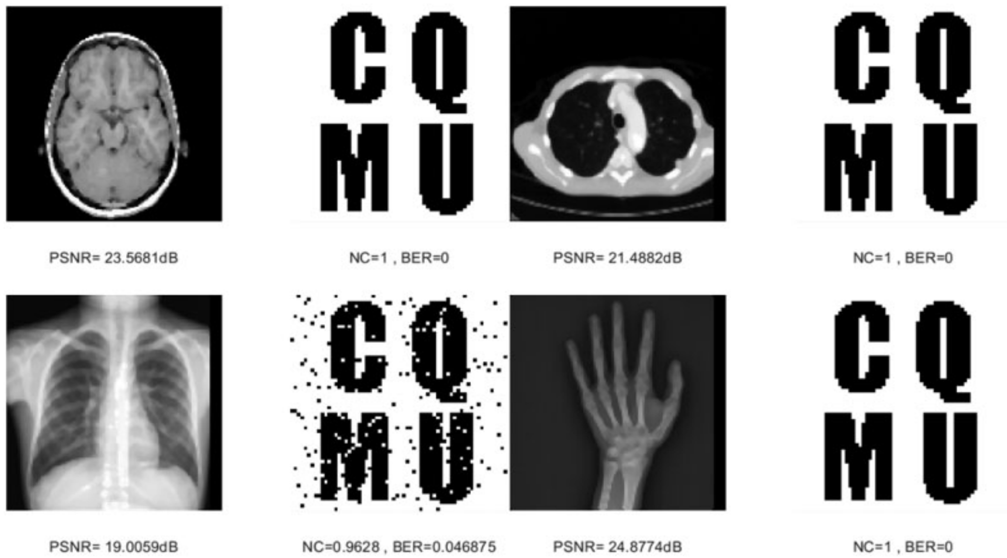

Figure 17: Four medical images and extracted watermarking images with cropping attack intensity of 5% and median filtering attack intensity of 3×3

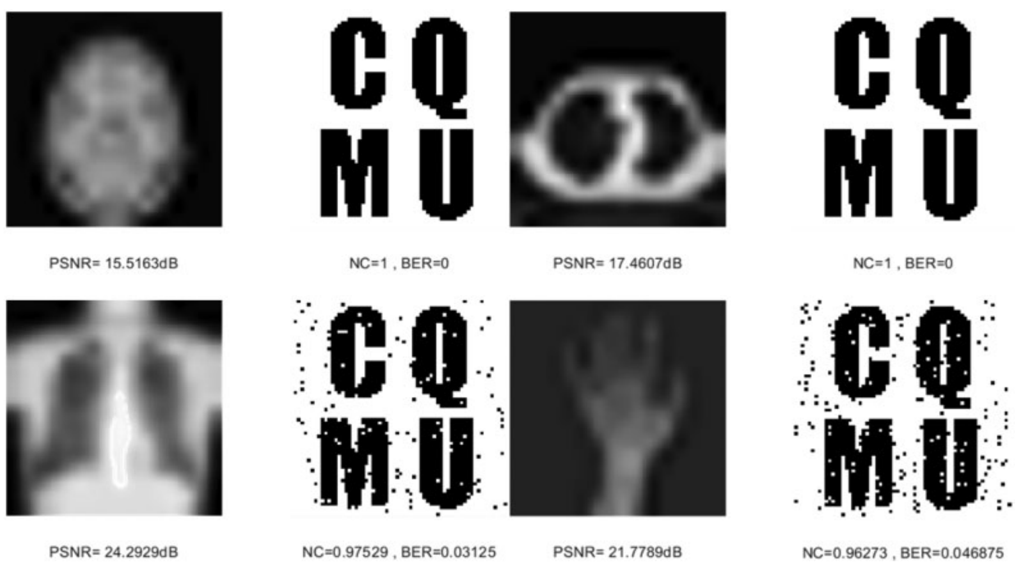

Figure 18: Four medical images and extracted watermarking images with JPEG compression attack intensity of 5% and scaling attack intensity of 0.125

The third category of attacks is two geometric attacks on images, namely, scaling attack combined with cropping attack, and rotation attack combined with scaling attack. From the data in Table 4, only the chest image has the lowest NC value of 0.7277 under both attacks, while the other three images have NC values above 0.83 under both attacks. In Figs. 19 and 20, under both attacks, it is obvious that even if the image distortion is serious, the extracted watermarking image is very clearly visible. From the overall results of these three types of attacks, the proposed algorithm can effectively resist the attacks of different combinations.

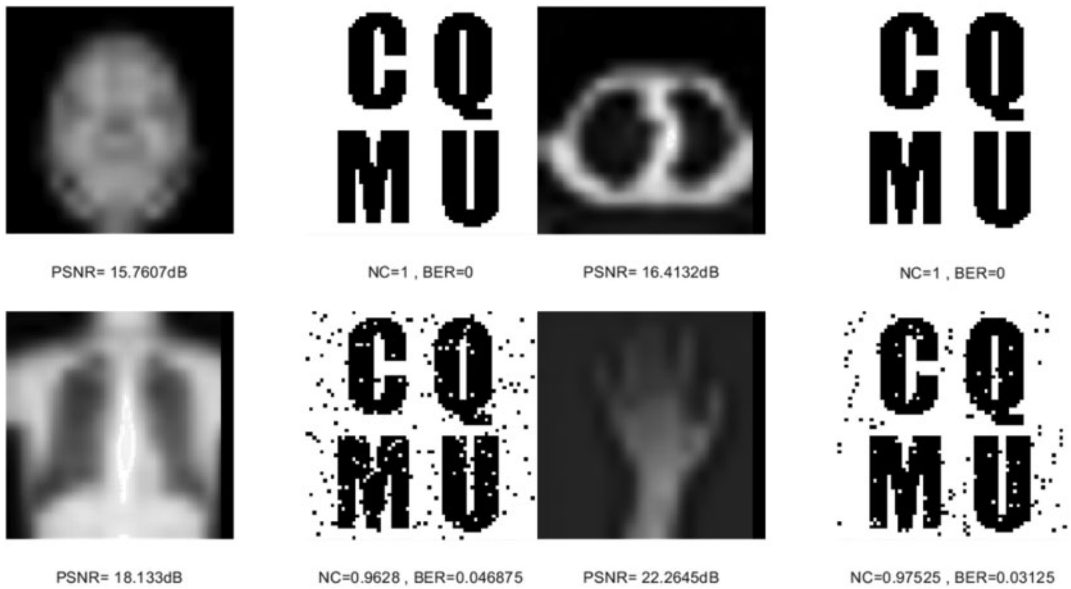

Figure 19: Four medical images and extracted watermarking images with scaling attack intensity of 0.125 and cropping attack intensity of 5%

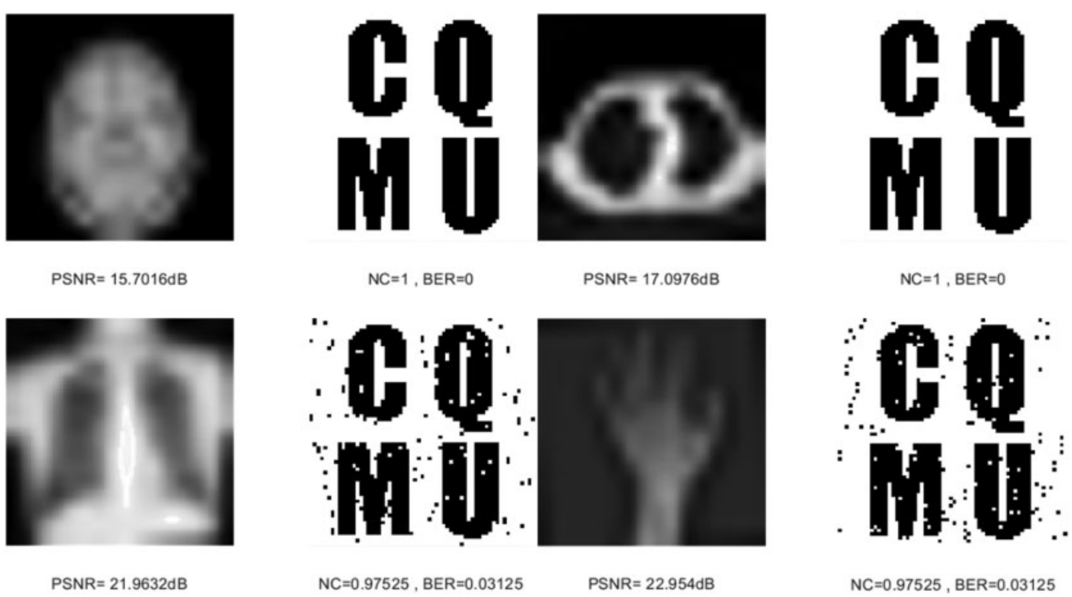

Figure 20: Four medical images and extracted watermarking images with rotation attack intensity of 3° and scaling attack intensity of 0.125

4.3 Comparisons with Other Algorithms

To verify the advantage of our proposed algorithm, we used the same experiment condition to compare it with other representative works [23,28,30,31]. In the contrast experiment, the 128 × 128 brain image shown Fig. 3a is selected as the original medical image, and the watermarking image is shown in Fig. 3e. The specific experimental results are shown in Tables 5–9.

Table 5: NC values of different algorithms under conventional attacks

Attack type	Attack intensity	Proposed algorithm	Algorithm [23]	Algorithm [28]	Algorithm [30]	Algorithm [31]
Gaussian noise	5%	1.0000	0.9375	0.9749	0.6830	0.7366
	10%	1.0000	0.9504	0.9514	0.6667	0.6671
	15%	1.0000	0.9504	0.9199	0.6555	0.6447
JPEG compression	5%	1.0000	0.9877	0.9863	0.5748	0.6738
	10%	1.0000	0.9502	0.9882	0.6518	0.9863
	15%	1.0000	0.9629	0.9935	0.7126	0.8530
Median filtering	3 × 3	1.0000	0.9377	0.9888	0.7088	0.9969
	5 × 5	1.0000	0.9123	0.9713	0.7511	0.9649
	7 × 7	1.0000	0.9123	0.9532	0.7671	0.9579

Table 6: BER values of different algorithms under conventional attacks

Attack type	Attack intensity	Proposed algorithm	Algorithm [23]	Algorithm [28]	Algorithm [30]	Algorithm [31]
Gaussian noise	5%	0	0.0781	0.0332	0.5313	0.3127
	10%	0	0.0625	0.0637	0.5469	0.4143
	15%	0	0.0625	0.1028	0.6250	0.4263
JPEG compression	5%	0	0.0156	0.0173	0.4844	0.3831
	10%	0	0.0625	0.0149	0.4063	0.0173
	15%	0	0.0469	0.0083	0.3438	0.1731
Median filtering	3 × 3	0	0.0781	0.0142	0.3438	0.0039
	5 × 5	0	0.1094	0.0361	0.2966	0.0442
	7 × 7	0	0.1094	0.0586	0.2810	0.0505

Table 7: NC values of different algorithms under geometric attacks

Attack type	Attack intensity	Proposed algorithm	Algorithm [23]	Algorithm [28]	Algorithm [30]	Algorithm [31]
Scaling	0.125, 8	1.0000	0.8746	0.9284	0.6690	0.8037
	0.25, 4	1.0000	0.9628	0.9670	0.6989	0.8763
	0.5, 2	1.0000	0.9753	0.9908	0.7372	0.9579

(Continued)

Table 7 (continued)

Attack type	Attack intensity	Proposed algorithm	Algorithm [23]	Algorithm [28]	Algorithm [30]	Algorithm [31]
Cropping	20%	1.0000	0.9753	0.9969	0.9754	0.9776
	25%	1.0000	0.9377	0.9834	0.9377	0.9316
	30%	1.0000	0.9502	0.9655	0.8998	0.9214
Rotation	5°	1.0000	0.9628	0.9441	0.6649	0.9492
	10°	1.0000	0.9753	0.9089	0.6351	0.8890
	15°	0.9501	0.9502	0.8901	0.6666	0.8619
Translation	5%	0.9503	0.9378	0.8996	0.7532	0.8840
	10%	0.9247	0.9378	0.8819	0.7106	0.8371
	15%	0.9118	0.9753	0.8548	0.6966	0.7920

Table 8: BER values of different algorithms under geometric attacks

Attack type	Attack intensity	Proposed algorithm	Algorithm [23]	Algorithm [28]	Algorithm [30]	Algorithm [31]
Scaling	0.125, 8	0	0.1563	0.0891	0.3906	0.2388
	0.25, 4	0	0.0469	0.0415	0.3591	0.1526
	0.5, 2	0	0.0313	0.0117	0.3125	0.0530
Cropping	20%	0	0.0313	0.0039	0.0313	0.0283
	25%	0	0.0781	0.0210	0.0781	0.0857
	30%	0	0.0625	0.0435	0.1248	0.0984
Rotation	5°	0	0.0469	0.0698	0.3904	0.0637
	10°	0	0.0313	0.1133	0.4216	0.1375
	15°	0.0625	0.0625	0.1355	0.3904	0.1694
Translation	5%	0.0625	0.0781	0.1235	0.2966	0.1431
	10%	0.0938	0.0781	0.1450	0.3435	0.1985
	15%	0.1094	0.0313	0.1768	0.3591	0.2498

Table 9: Comparison of results of running time

	Proposed algorithm	Algorithm [23]	Algorithm [28]	Algorithm [30]	Algorithm [31]
Average times (sec)	0.9406	1.0975	0.9524	0.9540	1.3329

When carrying out conventional attacks, as shown in Tables 5 and 6, in the attack of Gaussian noise, the NC value of both algorithm [30] and algorithm [31] is lower than 0.7. According to the JPEG compression attack, the NC value of algorithm [30] appears below the value of 0.6. Under the median filtering attack, except that the value of algorithm [30] is lower than 0.8, the NC value of the other algorithms is greater than 0.9. Only in the algorithm [23,28] and the proposed algorithm, the NC value is always above 0.9 under different degrees of three attacks, and the NC value of the proposed algorithm is always equal to 1. Moreover, the BER values of the algorithm under different conventional attack intensities are equal to 0, while other algorithms have BER values greater than 0, or even have values greater than 0.5. So far, it can be seen that under conventional attack, the proposed algorithm has stronger stability and robustness than the compared algorithms [23,28,30,31].

As shown on the right in Table 7, when faced with the increased intensity of different geometric attacks, the NC values of the algorithms showed in [23,28,30,31] all decrease, while the proposed algorithm is almost maintained at 1.0 in terms of NC metric. When facing different degrees of translation attacks, the NC values of the algorithms in [28,30,31] are lower than 0.9, and the algorithm in [30] is even lower than 0.8, but the proposed algorithm and the algorithm [23] are still above 0.9. Under the geometric attack, in Table 8, the largest BER value of the proposed algorithm is 0.1094, and the remaining BER values are equal to 0, which are much smaller than the BER values of other algorithms. From these observations, we can obviously see that the proposed algorithm is more robust when it is subjected to geometric attack compared with the other algorithms [23,28,30,31].

To more comprehensively detect the algorithm's performance, under the same experimental environment, the computing time of the proposed algorithm and the literature [23,28,30,31] for comparison, the average time for the 20 runs is displayed in Table 9. Table 9 shows that the computing time of the proposed algorithm to construct zero-watermarking is low relative to the literature [23,28,30,31]. This is because the IWT has high computational efficiency, and the computational complexity of the Schur decomposition is lower than that of the SVD in [30,31], which effectively enhances the algorithm's execution efficiency.

5 Conclusion

Aiming to protect the security of the medical image and not damage original information, we have proposed a new zero-watermarking algorithm in this work. Specifically, we used the IWT to extract low-frequency information from the original medical image, which was then divided into blocks by the Schur decomposition. After that, we constructed the feature matrix according to the relation between image block energy. Meanwhile, we encrypted the watermarking information using logistic position scrambling. Finally, zero-watermarking is generated via the XOR operation between the scrambled watermarking information and the feature matrix. We compared our algorithm with other representative works under a series of conventional attacks and geometric attacks in the experiment. Experimental results show that the proposed algorithm could improve the robustness of the medical image zero-watermarking, especially for the high-intensity of conventional attacks and geometric attacks. This algorithm can efficiently ensure the safety and privacy of patients and the confidentiality and reliability of medical images. However, this algorithm in this paper is aimed at 2D medical images. It has not been applied to 3D medical images, our future work will consider applying the proposed algorithm to the protection of 3D medical images, and we will attempt to design a robust zero-watermarking algorithm that can protect 2D and 3D medical images.

Funding Statement: This work was supported in part by the Hainan Provincial Natural Science Foundation of China (No. 620MS067), the Intelligent Medical Project of Chongqing Medical University (ZHYXQNRC202101), and the Student Scientific Research and Innovation Experiment Project of the Medical Information College of Chongqing Medical University (No. 2020C006).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Xun, Y., Bouguettaya, A., Georgakopoulos, D., Song, A., Willemson, J. (2016). Privacy protection for wireless medical sensor data. *IEEE Transactions on Dependable and Secure Computing, 13(3),* 369–380. DOI 10.1109/TDSC.2015.2406699.
2. Rault, T., Bouabdallah, A., Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks, 67,* 104–122. DOI 10.1016/j.comnet.2014.03.027.
3. Qasim, A. F., Meziane, F., Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review, 27,* 45–60. DOI 10.1016/j.cosrev.2017.11.003.
4. Makbol, N. M., Khoo, B. E., Rassem, T. H. (2015). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing, 10(1),* 34–52. DOI 10.1049/iet-ipr.2014.0965.
5. Hussain, M., Wahab, A. W. A., Idris, B. Y. I., Ho, A. T. S., Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication, 65,* 46–66. DOI 10.1016/j.image.2018.03.012.
6. Xia, Z., Wang, X., Sun, X., Liu, Q., Xiong, N. (2016). Steganalysis of LSB matching using differences between nonadjacent pixels. *Multimedia Tools and Applications, 75(4),* 1947–1962. DOI 10.1007/s11042-014-2381-8.
7. Wang, G., Rao, N. N. (2005). A fragile watermarking scheme for medical image. *IEEE Engineering in Medicine and Biology 27th Annual Conference*, pp. 3406–3409. Shanghai, China.
8. Singh, S. P., Bhatnagar, G. (2018). A new robust watermarking system in integer DCT domain. *Journal of Visual Communication and Image Representation, 53,* 86–101. DOI 10.1016/j.jvcir.2018.03.006.
9. Atawneh, S., Almomani, A., Bazar, H. A., Sumari, P., Gupta, B. (2017). Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimedia Tools and Applications, 76(18),* 18451–18472. DOI 10.1007/s11042-016-3930-0.
10. Hamidi, M., Haziti, M. E., Cherifi, H., Hassouni, M. E. (2018). Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. *Multimedia Tools and Applications, 77(20),* 27181–27214. DOI 10.1007/s11042-018-5913-9.
11. Hosny, K. M., Darwish, M. M., Li, K., Salah, A. (2018). Parallel multi-core CPU and GPU for fast and robust medical image watermarking. *IEEE Access, 6,* 77212–77225. DOI 10.1109/ACCESS.2018.2879919.
12. Hosny, K. M., Darwish, M. M., Fouda, M. M. (2021). Robust color images watermarking using new fractionalorder exponent moments. *IEEE Access, 9,* 47425–47435. DOI 10.1109/ACCESS.2021.3068211.
13. Al-Haj, A., Mohammad, A., Amer, A. (2017). Crypto-watermarking of transmitted medical images. *Journal of Digital Imaging, 30(1),* 26–38. DOI 10.1007/s10278-016-9901-1.
14. Khor, H. L., Liew, S. C., Zain, J. M. (2017). Region of interest-based tamper detection and lossless recovery watermarking scheme (ROI-DR) on ultrasound medical images. *Journal of Digital Imaging, 30(3),* 328–349. DOI 10.1007/s10278-016-9930-9.
15. Gao, G., Wan, X., Yao, S., Cui, Z., Zhou, C. et al. (2017). Reversible data hiding with contrast enhancement and tamper localization for medical images. *Information Sciences, 385,* 250–265. DOI 10.1016/j.ins.2017.01.009.
16. Priyanka, S., Maheshkar, S. (2017). Region-based hybrid medical image watermarking for secure telemedicine applications. *Multimedia Tools and Applications, 76(3),* 3617–3647. DOI 10.1007/s11042-016-3913-1.
17. Wen, Q., Sun, T., Wang, S. (2003). Concept and application of zero-watermark. *ACTA Electonica Sinica, 31(2),* 214–216.
18. Zear, A., Singh, A. K., Kumar, P. (2018). A proposed secure multiple watermarking technique based on dwt, dct and svd for application in medicine. *Multimedia Tools and Applications, 77(4),* 4863–4882. DOI 10.1007/s11042-016-3862-8.

19. Liu, J., Li, J., Ma, J., Sadiq, N., Bhatti, U. A. et al. (2019). A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and henon map. *Applied Sciences, 9(4),* 700. DOI 10.3390/app9040700.
20. Hu, K., Wang, X., Hu, J., Wang, H., Qin, H. (2021). A novel robust zero-watermarking algorithm for medical images. *The Visual Computer, 37(9),* 2841–2853. DOI 10.1007/s00371-021-02168-5.
21. Xia, Z., Wang, X., Wang, C., Wang, C., Ma, B. et al. (2022). A robust zero-watermarking algorithm for lossless copyright protection of medical images. *Applied Intelligence, 52(1),* 607–621. DOI 10.1007/s10489-021-02476-2.
22. Dai, Z., Lian, C., He, Z., Jiang, H., Wang, Y. (2022). A novel hybrid reversible-zero watermarking scheme to protect medical image. *IEEE Access, 10,* 58005–58016. DOI 10.1109/ACCESS.2022.3170030.
23. Huang, T., Xu, J., Yang, Y., Han, B. (2022). Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and Hessenberg decomposition. *Mathematics, 10(7),* 1–19. DOI 10.3390/math10071154.
24. Sweldens, W. (1996). The lifting scheme: A custom-design construction of biorthogonal wavelets. *Applied & Computational Harmonic Analysis, 3(2),* 186–200. DOI 10.1006/acha.1996.0015.
25. Calderbank, A. R., Daubechies, I., Sweldens, W., Yeo, B. L. (1998). Wavelet transforms that map integers to integers. *Applied and Computational Harmonic Analysis, 5(3),* 332–369. DOI 10.1006/acha.1997.0238.
26. Liu, W., Sun, S., Qu, H. (2019). Fast zero-watermarking algorithm based on Schur decomposition. *Journal of Frontiers of Computer Science & Technology, 13(3),* 494–504. DOI 10.3778/j.issn.1673-9418.1712040.
27. Zermi, N., Khaldi, A., Kafi, M. R., Kahlessenane, F., Euschi, S. (2021). A lossless DWT-SVD domain watermarking for medical information security. *Multimedia Tools and Applications, 80(16),* 24823–24841. DOI 10.1007/s11042-021-10712-7.
28. Li, W., Amandeep, K. X., Deepak, D., Sanjeev, K. (2019). Robust zero-watermarking algorithm based on chaotic and block energy relationship. *Microelectronics and Computer, 36(11),* 30–36. DOI 10.19304/j.cnki.issn1000-7180.2019.11.007.
29. Durafe, A., Patidar, V. (2022). Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover. *Journal of King Saud University-Computer and Information Sciences, 34(7),* 4483–4498. DOI 10.1016/j.jksuci.2020.10.008.
30. Rani, A., Bhullar, A. K., Dangwal, D., Kumar, S. (2015). A zero-watermarking scheme using discrete wavelet transform. *Procedia Computer Science, 70,* 603–609. DOI 10.1016/j.procs.2015.10.046.
31. Zeng, F., Zhou, A. (2008). Image zero-watermarking algorithm based on contourlet transform and singular value decomposition. *Journal of Computer Applications, 28(8),* 2033–2035. DOI 10.3724/SP.J.1087.2008.02033.