

Article

Robust Zero-Watermarking Algorithm for Medical Images Using Double-Tree Complex Wavelet Transform and Hessenberg Decomposition

Tongyuan Huang ^{1,*}, Jia Xu ¹, Yuling Yang ¹ and Baoru Han ^{2,*}¹ School of Artificial Intelligence, Chongqing University of Technology, Chongqing 401135, China; jiaxu@2020.cqut.edu.cn (J.X.); chrisyang@2019.cqut.edu.cn (Y.Y.)² College of Medical Informatics, Chongqing Medical University, Chongqing 400016, China

* Correspondence: tyroneh@cqut.edu.cn (T.H.); baoruhan@cqmu.edu.cn (B.H.); Tel.: +86-139-8395-5665 (T.H.); +86-177-8307-9648 (B.H.)

Abstract: With the rapid development of smart medical care, copyright security for medical images is becoming increasingly important. To improve medical images storage and transmission safety, this paper proposes a robust zero-watermarking algorithm for medical images by fusing Dual-Tree Complex Wavelet Transform (DTCWT), Hessenberg decomposition, and Multi-level Discrete Cosine Transform (MDCT). First, the low-frequency sub-band of the medical image is obtained through the DTCWT and MDCT. Then Hessenberg decomposition is used to construct the visual feature vector. Meanwhile, the encryption of the watermarking image by combining cryptographic algorithms, third-party concepts, and chaotic sequences enhances the algorithm's security. In the proposed algorithm, zero-watermarking technology is utilized to assure the medical images' completeness. Compared with the existing algorithms, the proposed algorithm has good robustness and invisibility and can efficiently extract the watermarking image and resist different attacks.

Keywords: DTCWT; MDCT; Hessenberg decomposition; zero-watermarking; medical image

Citation: Huang, T.; Xu, J.; Yang, Y.; Han, B. Robust Zero-Watermarking Algorithm for Medical Images Using Double-Tree Complex Wavelet Transform and Hessenberg Decomposition. *Mathematics* **2022**, *10*, 1154. <https://doi.org/10.3390/math10071154>

Academic Editors: Wen-Yu Chung and Sebastian Iwaszenko

Received: 25 February 2022

Accepted: 30 March 2022

Published: 2 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the advancement of Internet technology and the continuous maturity of big data, digital technology is extensively infiltrating the medical field. Every day, numerous medical images are communicated and transmitted via the network, and medical images are vulnerable to illegal tampering, copying and leaking, and other issues during this transmission process [1,2]. Therefore, it has become an urgent problem to protect the privacy of patients and prevent the personal information on patients' medical images from being leaked [3,4]. As an important information security technology, digital watermarking is utilized for the authentication of image integrity and copyright protection. Therefore, medical image-watermarking technology based on digital watermarking can solve the above problems effectively [5,6].

Medical image-watermarking technology hides patients' personal information in the corresponding medical image, thereby protecting patients' privacy and ensuring the safe transmission of this information [7]. However, medical images have their unique characteristics. Most medical images are single-channel, grayscale images. The slight change in highly similar background tissues may represent a certain disease. Any subtle change may cause distorted medical images and affect doctor's diagnosis [8,9]. Therefore, the particularity of medical images makes it difficult for traditional medical image digital watermarking algorithms to solve these problems. To diminish watermarking's impact on the original medical images, it is essential to design a lossless watermarking algorithm [10,11].

The zero-watermarking technology uses important features of the image to construct the feature vector. Zero-watermarking, without altering the original medical image, can well overcome the issue of the invisibility and robustness of the watermarking restricting each other [12]. Hence, zero-watermarking is very appropriate for medical images' copyright protection. As an effective method of medical images protection, zero-watermarking has become a popular research topic in the medical field. Xiao et al. proposed a novel algorithm based on enhanced singular value decomposition and cellular neural networks. They combined a neural network with homogenized singular values to solve the problem of diagonal distortion [13]. Wu et al. introduced a robust watermarking algorithm for medical images. They used Contourlet transform to obtain multi-scale image features and then Discrete Cosine Transform (DCT) to generate feature vectors of low-frequency sub-bands. This algorithm has shown excellent utility in medical fields [14]. Qin et al. combined Curvelet-DCT with RSA pseudo-random sequence and used the Curvelet-DCT to construct feature vectors by extracting the medical image with the most concentrated energy. They encrypted the watermarking with the RSA algorithm, which strengthened the protection of patient privacy [15]. Wu et al. utilized Curvelet transform, Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) to present a method for medical images, which integrated Curvelet transform and DWT to obtain image characteristics and used the benefits of subdivision block to further enhance the stability of the algorithm [16]. Xue et al. used Nonsubsampled Shearlet Transform (NSST) and Hessenberg decomposition to propose a zero-watermarking algorithm, which constructed a feature matrix by performing operations, such as NSST transformation and block Hessenberg decomposition, on the image combined with QR codes to form a zero-watermarking, which effectively improved the robustness against rotation and cropping attacks [17]. Liu et al. utilized Dual-Tree Complex Wavelet Transform (DTCWT) and DCT transformation to introduce a scheme for medical images. This algorithm used DTCWT-DCT transformation to construct feature sequences. Furthermore, logistic chaos encryption technology was utilized to enhance the algorithm's security [18]. Xia et al. used FoRHfMs to design a zero-watermarking algorithm. They extended IoRHfMs to FoRHfMs and effectively improved numerical stability and enhanced the algorithm's robustness [19]. Vaidya et al. used hybrid transform to present a watermarking scheme. This algorithm combined the outstanding features of Lifting Wavelet Transform (LWT), DWT, and Local Binary Pattern (LBP) in the hybrid domain and has better robustness and imperceptibility to image attacks [20]. Fang et al. introduced a watermarking algorithm. They added the Scale Invariant Feature Transform (SIFT) for data preprocessing and used an optimized Bandelet and DCT (Bandelet-DCT) to extract visual features. The algorithm is robust under different attacks [21].

In the currently proposed methods for zero-watermarking, robustness is the focus of research. Most algorithms are less robust to geometric attacks. This is because geometric attacks changed the position of the attacked medical image in relation to the original medical image, making the zero-watermarking information seriously out of sync with medical images and resulting in an extremely difficult extraction of zero-watermarking. Therefore, how to extract feature vectors that can resist geometric attacks and make the algorithm well robust without altering the original image is an important issue to be solved urgently [22].

To address the above problems, this paper proposes a new method of zero-watermarking based on the combination of DTCWT and Hessenberg decomposition. This method uses DTCWT and Multi-level Discrete Cosine Transform (MDCT) to obtain the low-frequency sub-band of the medical image and constructs the feature vector through Hessenberg decomposition. The proposed algorithm utilizes chaos technology and the nature of hash function to encrypt the watermarking image and enhance the security of the watermarking. Experimental results show that effective resistance to various attacks is achieved by the proposed algorithm, with better robustness compared to other watermarking algorithms.

Overall, the main contributions of this paper can be summarized as:

- (1) We proposed a novel zero-watermarking algorithm for medical images using DTCWT, MDCT, and Hessenberg decomposition.
- (2) The paper used DTCWT extract multi-directional and multi-scale features to better describe the feature information of medical images. In addition, when medical images are attacked, the proposed algorithm can show better orientation optionality and translation invariance and effectively improve the robustness against translation attacks.
- (3) The authors utilized the MDCT to take full advantage of the energy concentration characteristics of DCT, giving the algorithm fastness and accurate feature extraction capabilities.
- (4) The proposed algorithm used Hessenberg decomposition to effectively improve the execution efficiency and has good rotational invariance, which exhibits strong robustness against geometric attacks.

2. Basic Theory

2.1. DTCWT

Due to the unique physical structure of real DWT, DWT has multi-resolution properties, but it still suffers from disadvantages, such as insufficient translation sensitivity and direction selectivity. To solve these disadvantages of the DWT, Kingsbury et al. [23,24] proposed DTCWT. DTCWT uses a two-way DWT structure of a binary tree, where one tree corresponds to the real part of the DWT, and the other tree corresponds to the imaginary part of the DWT. DTCWT uses a low-pass filter and a high-pass filter bank, the real part and the imaginary part are respectively subjected to multi-scale sub-band decomposition at the same time, and then, multi-scale and multi-directional sub-band coefficients are obtained.

Figure 1 shows the realization structure of the DTCWT. Among them, $l(n)$ and $h(n)$ are the low-pass and high-pass filters, respectively. In the transformation process, one part uses filters $\{l_1(n), l_2(n)\}$ for row transformation and then uses filters $\{h_1(n), h_2(n)\}$ for column transformation. The other part uses filters $\{h_1(n), h_2(n)\}$ for row transformation and then uses filters $\{l_1(n), l_2(n)\}$ as columns transformation. Through the DTCWT, transform obtained one low-frequency sub-band and three high-frequency sub-bands, respectively. The sum or difference of each pair of sub-bands can constitute two low-frequency sub-bands and six high-frequency sub-bands, of which six high-frequency complex sub-bands, respectively, describe the detailed information of the directions $\pm 15^\circ, \pm 45^\circ, \pm 75^\circ$, respectively. Sub-bands can reflect the changes in the image in different directions at different scales to better describe the specific features of the image [25].

The DTCWT has remarkable multi-resolution properties and also has translation invariance and efficient calculation efficiency, thereby improving the watermarking's robustness against geometric attacks.

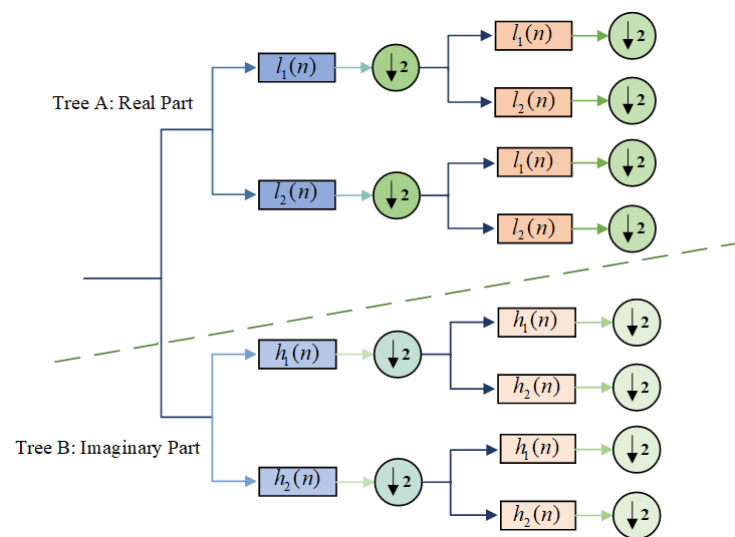


Figure 1. Decomposition structure of DTCWT.

2.2. DCT

DCT is an orthogonal transformation based on real numbers, which has a higher calculation speed [26]. The formulas for two-dimensional discrete cosine sine transform (2D-DCT) is as follows:

$$F(m, n) = a(m)a(n) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{(2x+1)m\pi}{2N} \cos \frac{(2y+1)n\pi}{2N} \quad (1)$$

$$a(m) = \begin{cases} \sqrt{\frac{1}{N}}, & m = 0 \\ \sqrt{\frac{2}{N}}, & m = 1, 2, \dots, N-1 \end{cases} \quad a(n) = \begin{cases} \sqrt{\frac{1}{N}}, & n = 0 \\ \sqrt{\frac{2}{N}}, & n = 1, 2, \dots, N-1 \end{cases} \quad (2)$$

Among them, $m = 0, 1, \dots, N-1$; $n = 0, 1, \dots, N-1$. $f(x, y)$ represents the image and has dimensions $N \times N$; $F(m, n)$ represents the frequency coefficients.

The frequency coefficient distribution of the image after the DCT is shown in Figure 2. The DCT transforms the image data into the frequency domain, which is divided into direct current coefficient (DC) and alternating current coefficient (AC). The DC coefficient represents the mean value of the brightness of the image. A large part of the image information focuses on the upper left corner. Therefore, DCT has a strong ability to concentrate information, and it can better relieve the correlation between image pixels and concentrate the image energy mainly in the low-frequency coefficients of the DCT spectrum, so it is broadly applied in the image compression field [27,28].

Traditional algorithms are to perform a whole DCT or a block DCT on the original image. Such a transformation cannot take full advantage of low-frequency coefficients and cannot reflect the energy concentration characteristics [29]. Therefore, the proposed algorithm utilizes MDCT. We first performed one-level DCT on the original image, and then, we blocked the low-frequency coefficients and perform two-level DCT on each sub-block matrix. The result of the multi-level DCT is shown in Figure 3.

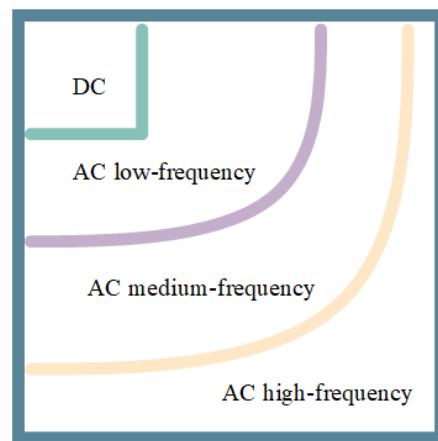


Figure 2. DCT coefficient frequency distribution diagram.



Figure 3. The result of multi-level DCT.

As can be seen from Figure 3, the energy after multi-stage DCT is better concentrated in the upper left corner, which is more conducive to feature extraction. Therefore, a reasonable multi-level DCT can fully utilize the energy concentration property of the DCT, accordingly obtaining more data with larger values, and the MDCT can optimize the algorithm's performance and give the algorithm have the ability to extract features quickly and accurately.

2.3. Hessenberg Decomposition

The Hessenberg decomposition is a specific type of decomposition. The elements below the sub-diagonal of the matrix H after the upper Hessenberg decomposition are all zero [30]. Hessenberg decomposition is to factorize matrix A by orthogonal transformation. The decomposition process can be shown as follows:

$$\begin{aligned} H &= (P_1 P_2 P_3 \cdots P_{n-3} P_{n-2})^T A (P_1 P_2 P_3 \cdots P_{n-3} P_{n-2}) \\ &\Rightarrow H = Q^T A Q \\ &\Rightarrow A = Q H Q^T \end{aligned} \quad (3)$$

where Q is the orthogonal matrix obtained in QR decomposition; H is the upper Hessenberg matrix, as shown in Formula (4), and for any $i > j + 1$, its element $h_{ij} = 0$. P is the Householder matrix, which satisfies Formula (5).

Where u is a non-zero vector in the set R_n , I_n represents the identity matrix of $n \times n$.

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & h_{(n-1)n} \\ 0 & \cdots & h_{n(n-1)} & h_{nn} \end{bmatrix} \quad (4)$$

$$P = \frac{(I_n - 2uu^T)}{u^T u} \quad (5)$$

Hessenberg decomposition is an intermediate step of QR decomposition, and this is because QR decomposition has lower computational complexity than other decomposition ways. Thus, compared with other decomposition methods, the computational complexity of Hessenberg decomposition is relatively low, which effectively improves the execution efficiency of the algorithm [31].

The image is decomposed by Hessenberg, the redundant information will be removed, and a few values can be represented for the entire image. The image after Hessenberg decomposition has better stability; even when the image is geometrically distorted by rotation and cropping, the value will still not be changed dramatically. Hence, Hessenberg decomposition is frequently applied in the watermarking domain.

Hessenberg decomposition enhances the safety and computational efficiency of the watermarking and extracts important features of the image to construct a more robust zero-watermarking.

3. Zero-Watermarking Algorithm

3.1. Watermarking-Generation Algorithm

The key to the watermarking-generation algorithm is extracting image features without altering the original medical image. In this paper, the use of DTCWT can make the generated zero-watermarking contain more directional feature information and has good translation invariance. MDCT is conducive to concentrating the image energy. Hessenberg decomposition extracts essential detail features of the image so that the image has rotation invariance, thus enhancing the algorithm's robustness and computational efficiency.

We assume the original medical image as $I = \{f(i, j) | 1 \leq i \leq M, 1 \leq j \leq M\}$ and the binary watermarking image as $W = \{w(u, v) | 1 \leq u \leq N, 1 \leq v \leq N\}$. The step by step of algorithm is shown below.

(1) Chaotic sequence generation by logistic mapping and logistic chaotic position scrambling was applied to the binary watermarking image to generate a scrambled binary watermarking image BW , and the scrambled key is K_1 .

(2) We performed a two-level DTCWT transform on the original medical image I to obtain the low-frequency sub-band LL_2 .

(3) We computed a DCT on LL_2 to obtain D_1 and then divided D_1 into non-overlapping sub-blocks of size 8×8 and marked sub-block as $S_m, m = 1, 2, \dots, N$.

(4) The DCT was performed on S_m to obtain $DS_m, m = 1, 2, \dots, N$.

(5) We next used Hessenberg decomposition for each sub-block DS_m , extracted the maximum element in the upper Hessenberg matrix of each sub-block, and recorded it as $H_m^{\max}, m = 1, 2, \dots, N$ and then calculated the overall mean value H^{avg} according to Formula (6).

$$H^{avg} = \frac{\sum_{i=1}^r H_r^{\max}}{r} \quad (6)$$

(6) We generated a binary eigenvector L by comparison of the maximum value element $H_r^{\max}$ and the overall mean value H^{avg} . The calculation formula is as follows:

$$L = \begin{cases} 1, & H_r^{\max} > H^{avg} \\ 0, & H_r^{\max} \leq H^{avg} \end{cases} \quad (7)$$

(7) We utilized an XOR operation to generate zero-watermarking from the BW and the feature vector L and saved it on the third-party platform. The formula appears as follows:

$$Key = BW \oplus L \quad (8)$$

Figure 4 displays the watermarking-embedding process.

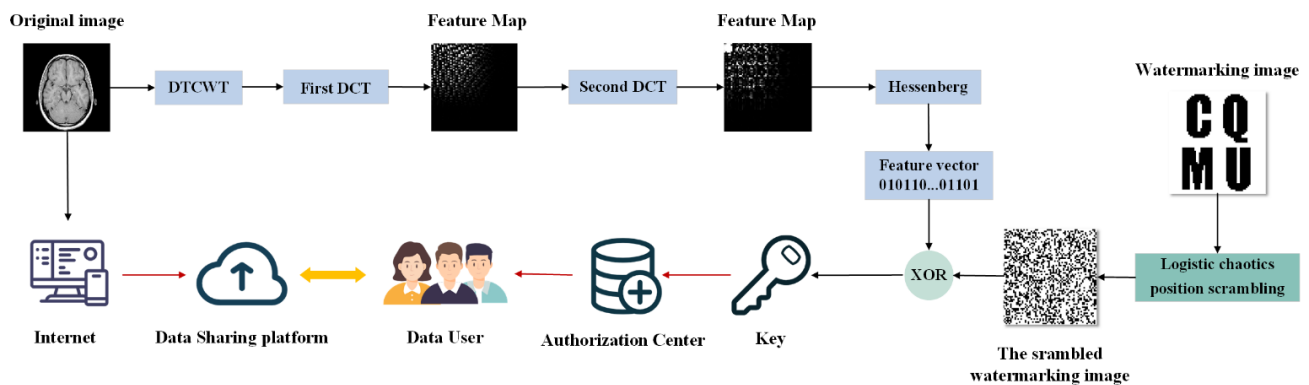


Figure 4. Watermarking-embedding flowchart.

3.2. Watermarking-Extraction Algorithm

During the extraction process, the attacked medical image is represented as $I' = \{f'(i, j) | 1 \leq i \leq M, 1 \leq j \leq M\}$. The step by step of algorithm is shown below.

(1) We performed steps 2 to 6 in Section 3.1 to generate the feature vector L' from the attacked medical image I' .

(2) We next performed the XOR operation between the feature vector L' and the zero-watermarking Key to obtain the watermarking image BW' . The formula appears as follows:

$$BW' = Key \oplus L' \quad (9)$$

(3) We restored the logistic chaotic position restoration of the obtained scrambled watermarking image BW' according to the key K_1 to obtain the decrypted watermarking image W' .

Figure 5 displays the watermarking-extraction process.

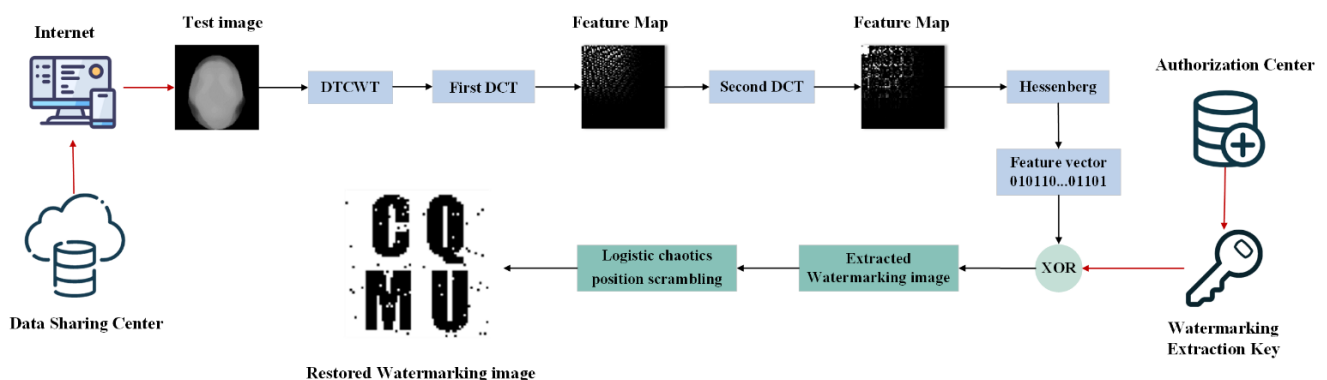


Figure 5. Watermarking-extraction flowchart.

4. Experiments and Results

4.1. The Experimental Description

In the experimental process, we selected different parts and types of medical images for testing. The experimental results show that the proposed watermarking algorithm has good robustness on various medical images. The simulation outcomes are given in this paper using five medical images as examples. The original medical image chooses a gray-scale image of pixels 128×128 in Figure 6. The watermarking image of pixels 64×64 in Figure 7a. The key to chaotic encryption is $x_0 = 0.6, \mu = 4$, and Figure 7b displays the encrypted watermarking image. The watermarking image can be seen to become chaotic, and no valid information can be extracted from it, so it has high concealment, which significantly improves the security of the watermarking. Figure 8 is a watermarked medical image that has not been attacked, showing the obtained watermarking. Observation shows that the medical image has not changed visually before and after the watermarking is embedded. This shows that the embedding of the watermarking does not affect the original medical image, which is in line with the zero-watermarking requirement.

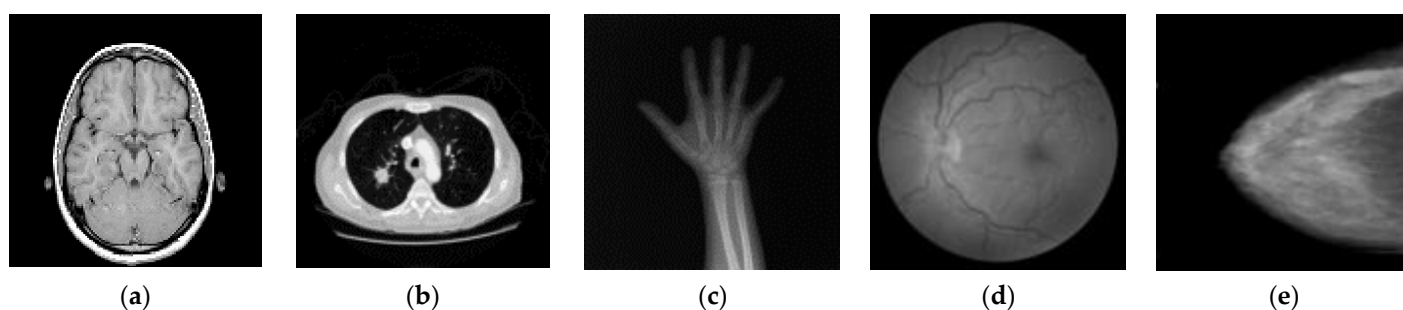


Figure 6. Original medical images: (a) brain; (b) chest; (c) hand; (d) fundus vessels; and (e) breast.

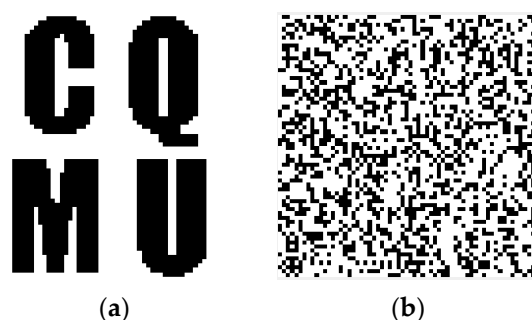


Figure 7. Watermarking image: (a) binary watermarking image; (b) encrypted watermarking image.

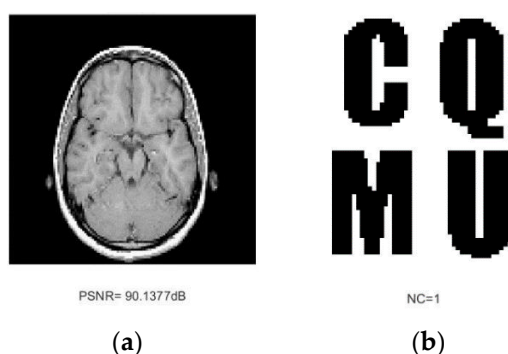


Figure 8. Medical image and extracted watermarking without attack: (a) medical image; (b) extracted watermarking image.

4.2. Robustness Experiment

The proposed algorithm utilizes a zero-watermarking method, so only the robustness of the algorithm needs to be checked. To examine the robustness of the method in this paper, the normalized correlation coefficient (NC) was applied to assess the degree of resemblance of watermarking images, and the peak signal-to-noise ratio (PSNR) was utilized to assess the attack damage to the image [32]. The calculation formulas are described in the following:

$$NC = \frac{\sum_{u=1}^N \sum_{v=1}^N W(u,v) \times W'(u,v)}{\sqrt{\sum_{u=1}^N \sum_{v=1}^N W^2(u,v) \times \sum_{u=1}^N \sum_{v=1}^N W'^2(u,v)}} \quad (10)$$

$$PSNR = 10 \times \log\left(\frac{255^2 \times M \times M}{\sum_{x=1}^M \sum_{y=1}^M (f(x,y) \times f'(x,y))^2}\right) \quad (11)$$

Among them, $W(u,v)$ is the original watermarking image pixel value, $W'(u,v)$ is the extracted watermarking image pixel value, and N is the watermarking image size. $f(x,y)$ and $f'(x,y)$, respectively represent the pixel values at the corresponding coordinates of the original medical image and the tested medical image and the image of size $M \times M$. In the following specific experiments, we conducted common attacks and geometric attacks on different medical images.

4.2.1. Common Attacks

- Gaussian Noise Attacks

We applied various extents of Gaussian noise attacks to different medical images. Figure 9 shows the results under the Gaussian noise attack. It can be seen that the original medical image blends in with the noise when the noise strength is 0.3, but the extracted watermarking image is distinguishable. Table 1 shows that as the noise strength becomes more intense, the quality of the image declines significantly. With noise strengths of 0.5, medical images maintain PSNR values of about 4 dB, and the NC values at this time are still as high as 0.97. Overall, the proposed algorithm has excellent performance.

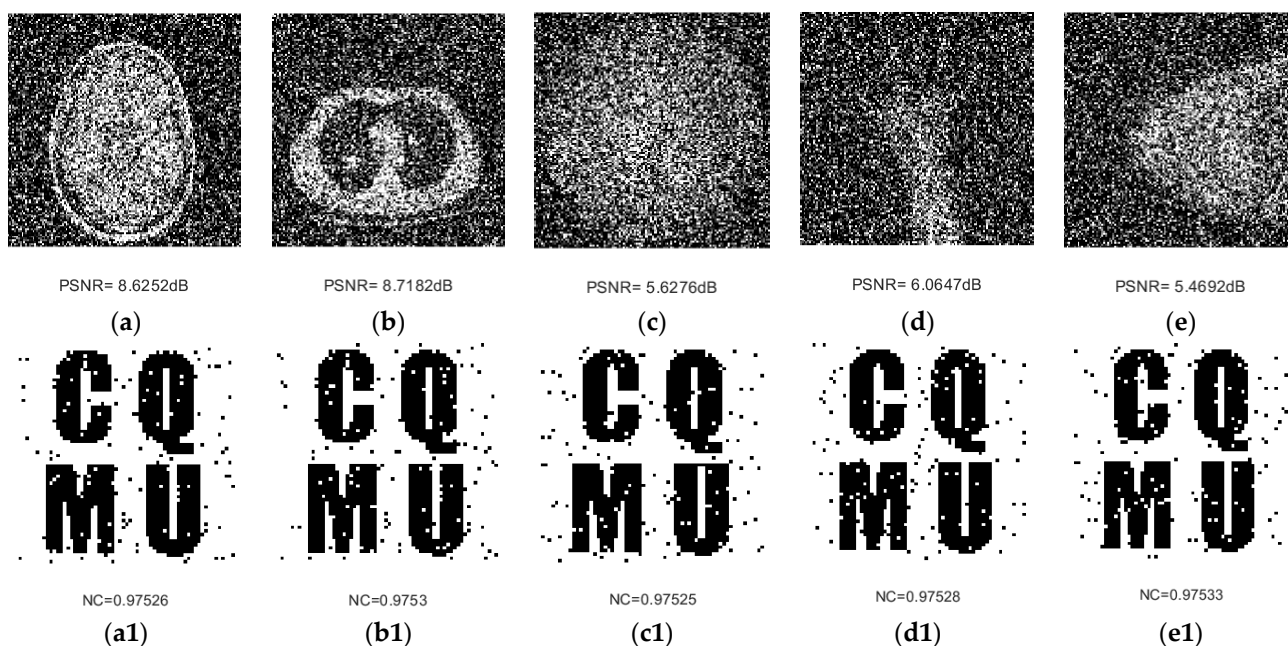


Figure 9. Attacked medical images and restored watermarking images under Gaussian noise 30%: (a,a1) brain and extracted watermarking image; (b,b1) chest and extracted watermarking image; (c,c1) fundus blood vessels and extracted watermarking image; (d,d1) hand and extracted watermarking image; and (e,e1) breast and extracted watermarking image.

Table 1. The result under Gaussian noise attacks.

Name	Noise 1%		Noise 5%		Noise 15%		Noise 30%		Noise 50%	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	21.3809	1.0000	14.6856	1.0000	10.7088	0.9877	8.6252	0.9753	7.9512	0.9754
Medical image B	21.8515	1.0000	15.2301	1.0000	10.9588	0.9753	8.7182	0.9753	7.4081	0.9753
Medical image C	17.7054	1.0000	11.0908	1.0000	7.3532	0.9877	5.6276	0.9753	4.6856	0.9754
Medical image D	19.4994	1.0000	12.8283	1.0000	8.4299	0.9753	6.0647	0.9753	4.7484	0.9754
Medical image E	18.1251	1.0000	11.5601	1.0000	7.4808	0.9877	5.4692	0.9753	4.3108	0.9754

- JPEG Compression Attacks

In order to improve transmission efficiency and reduce the amount of transmitted information, images are generally compressed during transmission. JPEG compression is mainly to remove redundant information from medical images. The result of the compression attack on the medical image is in Figure 10. Even if the image produced obvious blocky effects, the watermarking image could still be extracted correctly. Table 2 shows that the mean NC values are over 0.95 even when the compression quality falls to 2%. In summary, the proposed algorithm has better robustness under compression attacks.

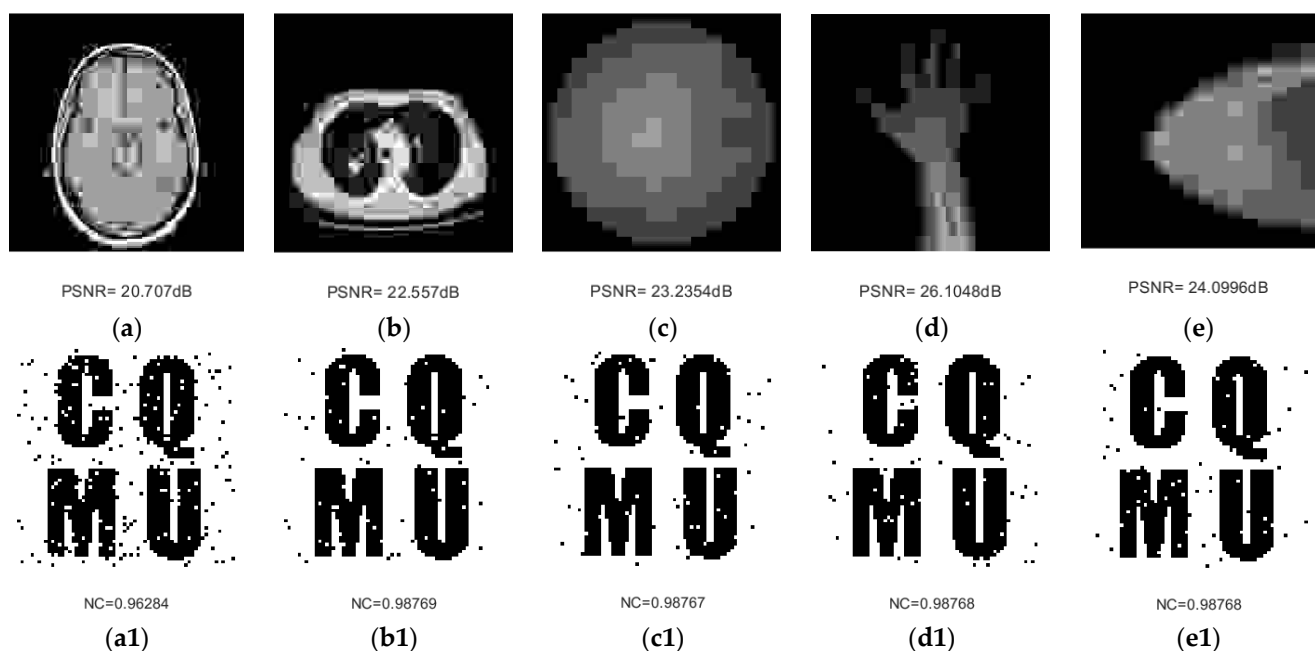


Figure 10. Attacked medical images and restored watermarking images under JPEG compression 2%: (a,a1) brain and extracted watermarking image; (b,b1) chest and extracted watermarking image; (c,c1) fundus blood vessels and extracted watermarking image; (d,d1) hand and extracted watermarking image; and (e,e1) breast and extracted watermarking image.

Table 2. The result under JPEG compression attacks.

Name	Compress 2%		Compress 5%		Compress 9%		Compress 15%		Compress 25%	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	20.707	0.9628	22.0045	0.9877	23.6216	0.9503	24.9075	0.9629	26.7087	0.9628
Medical image B	22.557	0.9877	24.6316	0.9753	26.9914	0.9754	28.9971	0.9628	31.0536	0.9754
Medical image C	23.2354	0.9877	25.2333	0.9877	28.5905	0.9877	30.9748	0.9877	33.1253	0.9753
Medical image D	26.1048	0.9877	26.4586	0.9753	32.8437	1.0000	34.6839	1.0000	35.0334	1.0000
Medical image E	24.0996	0.9877	24.4521	0.9753	29.9548	1.0000	32.1558	0.9877	34.9622	1.0000

- Median Filter Attacks

Figure 11 shows the experimental results under the median filter attack. As can be seen from the figure, when the median filter is (7×7) , and the attack is repeated 20 times, the medical image becomes a white elliptical outline, it has a huge change in shape and detail. However, the extracted watermarking image is still very clear. Table 3 indicates that as the window size and filtering time increase, the NC values show a downward trend, but the NC values can still reach above 0.9. Therefore, the algorithm exhibits strong robustness under median filter attacks.

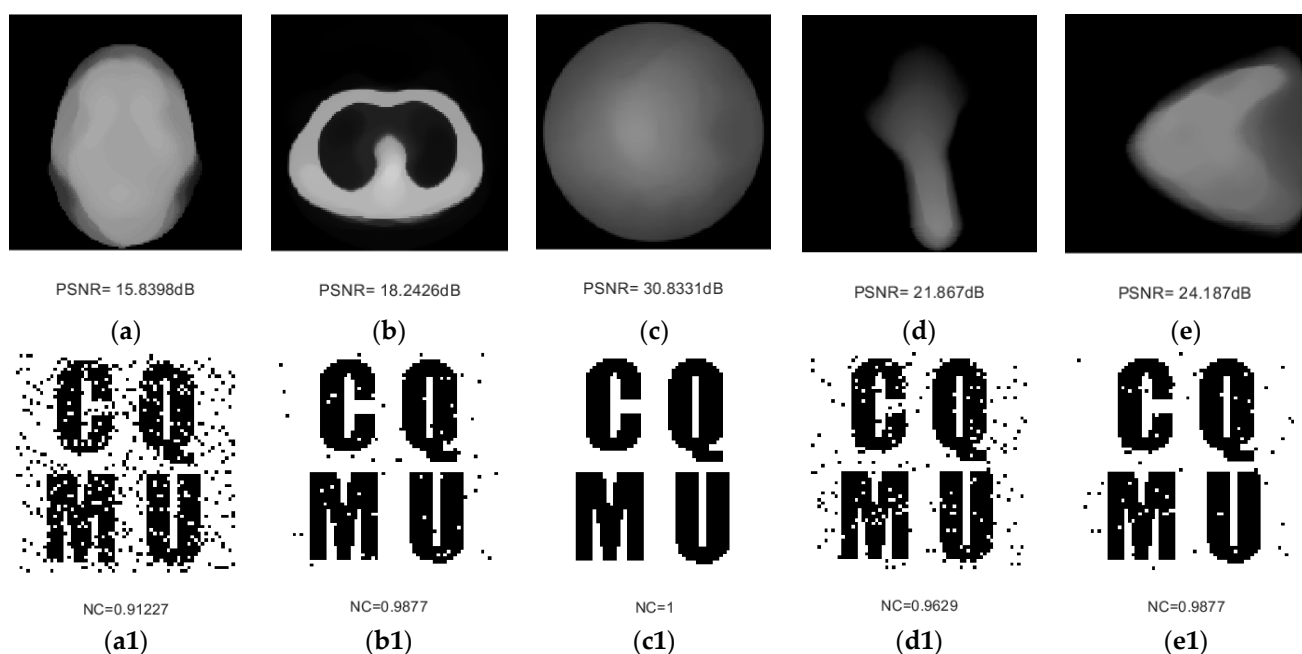


Figure 11. Attacked medical images and restored watermarking images under (7×7) , 20 times median filter attacks: (a,a1) brain and extracted watermarking image; (b,b1) chest and extracted watermarking image; (c,c1) fundus blood vessels and extracted watermarking image; (d,d1) hand and extracted watermarking image; and (e,e1) breast and extracted watermarking image.

Table 3. The result under median filter attacks.

Name	Parameter (3×3)				Parameter (5×5)				Parameter (7×7)	
	10 Times		20 Times		10 Times		20 Times		10 Times	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	20.91	0.9504	20.3341	0.9377	17.2479	0.9126	16.6834	0.9123	15.917	0.9124
Medical image B	26.5736	0.9754	26.02	0.9629	22.609	0.9753	22.1802	0.9754	19.9116	0.9753
Medical image C	35.49	1.0000	35.2661	1.0000	32.6347	0.9877	32.3348	0.9877	31.4819	0.9877
Medical image D	38.0348	1.0000	37.2862	1.0000	28.0059	0.9629	26.3181	0.9753	24.288	0.9629
Medical image E	35.173	1.0000	34.9371	1.0000	29.2758	0.9877	28.4422	0.9877	26.391	0.9877

Experiments demonstrate that the algorithm is consistently more robust under common attacks of various strengths. Because the DTCWT has excellent denoising property and direction selectivity, and the low-frequency sub-bands obtained after MDCT and Hessenberg decomposition have strong stability, the proposed algorithm shows excellent robustness in resistance to common attacks.

4.2.2. Geometric Attacks

• Rotation Attacks

We applied a clockwise rotation attack to the medical image, increasing the rotation angle from 5 to 40. Table 4 presents the results showing that as the strength of the rotation increases, the quality of the image and the NC values drop dramatically. Even when the rotation is 40 degrees, the NC values can still reach 0.9 or more. Figure 12 displays that the position of the medical image after the rotation has changed greatly, but the watermarking image can still be fully presented, which indicates the great robustness of the proposed algorithm to rotational attacks.

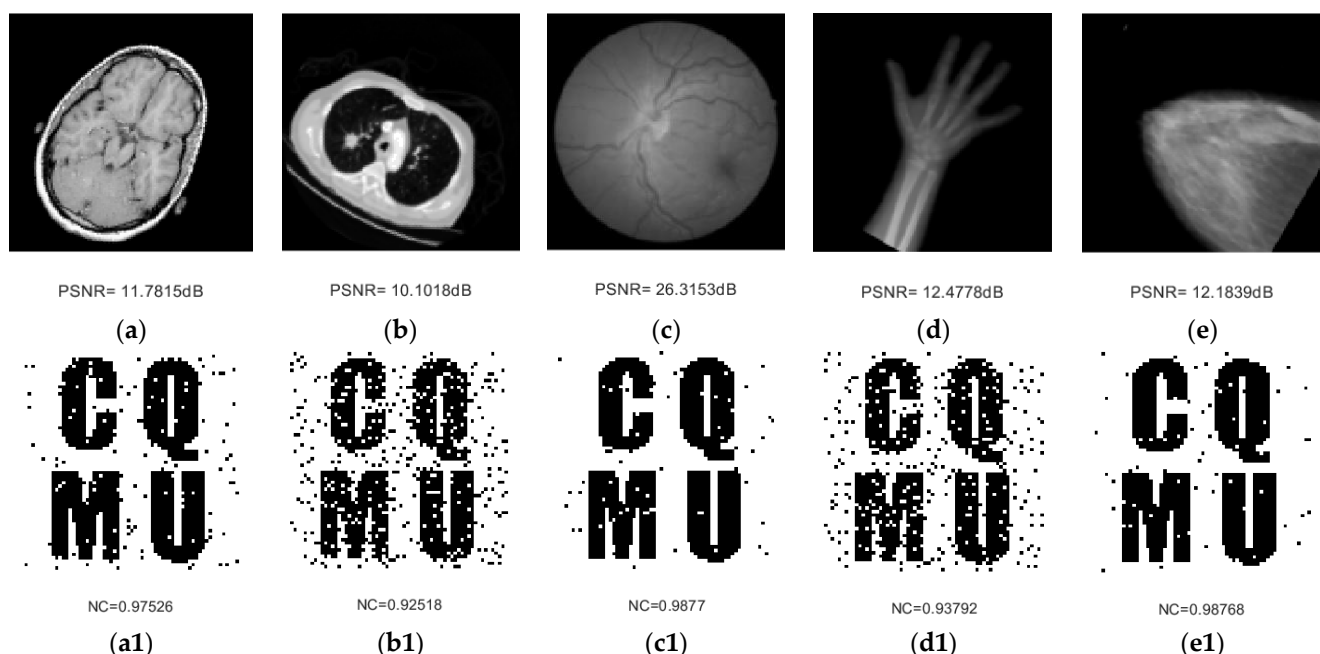


Figure 12. Attacked medical images and restored watermarking images under clockwise rotation 30°: (a,a1) brain and extracted watermarking image; (b,b1) chest and extracted watermarking image; (c,c1) fundus blood vessels and extracted watermarking image; (d,d1) hand and extracted watermarking image; and (e,e1) breast and extracted watermarking image.

Table 4. The result under clockwise rotation attacks.

Name	Rotation 5%		Rotation 10%		Rotation 20%		Rotation 25%		Rotation 40%	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	15.5831	0.9752	12.9944	0.9377	12.068	0.9378	11.9703	0.9628	11.232	0.9753
Medical image B	18.1468	0.9379	14.5409	0.9629	11.5648	0.9503	10.7143	0.9504	9.448	0.9378
Medical image C	30.0359	0.9877	28.5605	0.9877	27.0817	0.9877	26.5903	0.9877	25.7494	0.9877
Medical image D	20.8156	0.9877	17.0125	0.9877	13.8992	0.9877	13.0057	0.9753	12.16	0.9377
Medical image E	20.5585	0.9877	16.717	0.9754	13.4887	0.9877	12.7267	0.9753	11.4282	0.9877

• Scaling Attacks

From the result in Table 5, for the scaling attack, the NC values obtained under the general scale attack are 1. In the case of high-strength scaling, the NC values remain above

0.87. Figure 13 shows the result of the experiment with a scaling down of 0.125 and then scaling up of 8 times, showing that the image already has a patch effect and has been severely distorted, but the watermarking image can still be extracted accurately. Therefore, the proposed algorithm has good performance under scaling attacks.

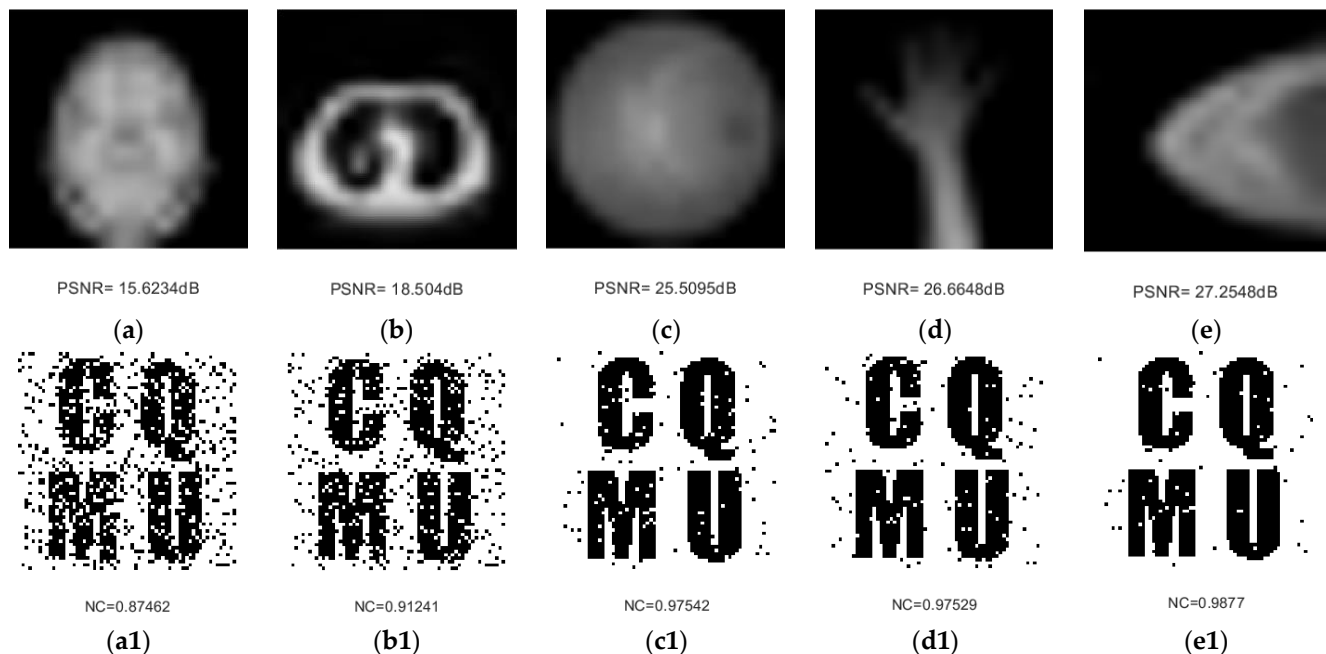


Figure 13. Attacked medical images and restored watermarking images under scaling factors 0.125 then factors 8: (a,a1) brain and extracted watermarking image; (b,b1) chest and extracted watermarking image; (c,c1) fundus blood vessels and extracted watermarking image; (d,d1) hand and extracted watermarking image; and (e,e1) breast and extracted watermarking image.

Table 5. The result under scaling attacks.

Name	Zoom Factor 0.125 then 8		Zoom Factor 0.25 then 4		Zoom Factor 0.5 then 2		Zoom Factor 2 then 0.5		Zoom Factor 4 then 0.25	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	15.6234	0.8746	17.8888	0.9628	21.5809	0.9753	30.2404	1.0000	30.5191	1.0000
Medical image B	18.504	0.9124	21.7819	0.9753	27.4683	1.0000	38.8449	1.0000	39.1239	1.0000
Medical image C	25.5095	0.9754	29.7844	0.9877	35.0533	1.0000	45.9477	1.0000	46.6227	1.0000
Medical image D	26.6648	0.9753	33.0577	0.9877	41.1167	1.0000	52.6998	1.0000	53.3732	1.0000
Medical image E	27.2548	0.9877	31.7092	0.9877	37.6185	1.0000	48.3699	1.0000	49.124	1.0000

- Cropping Attacks

As shown in Table 6 that even when the X-axis is 40%, and the Y-axis is 25%, the NC values remain at about 0.93. Figure 14 shows the experimental results of different medical images with 40% cropping on the X-axis and 30% on the Y-axis. We can see that the attacked images' outer contour changes considerably, and most information is removed, but the extracted watermark is nevertheless distinctly recognizable, and all have NC values above 0.95. Therefore, the algorithm's robust performance under the cropping attack is excellent.

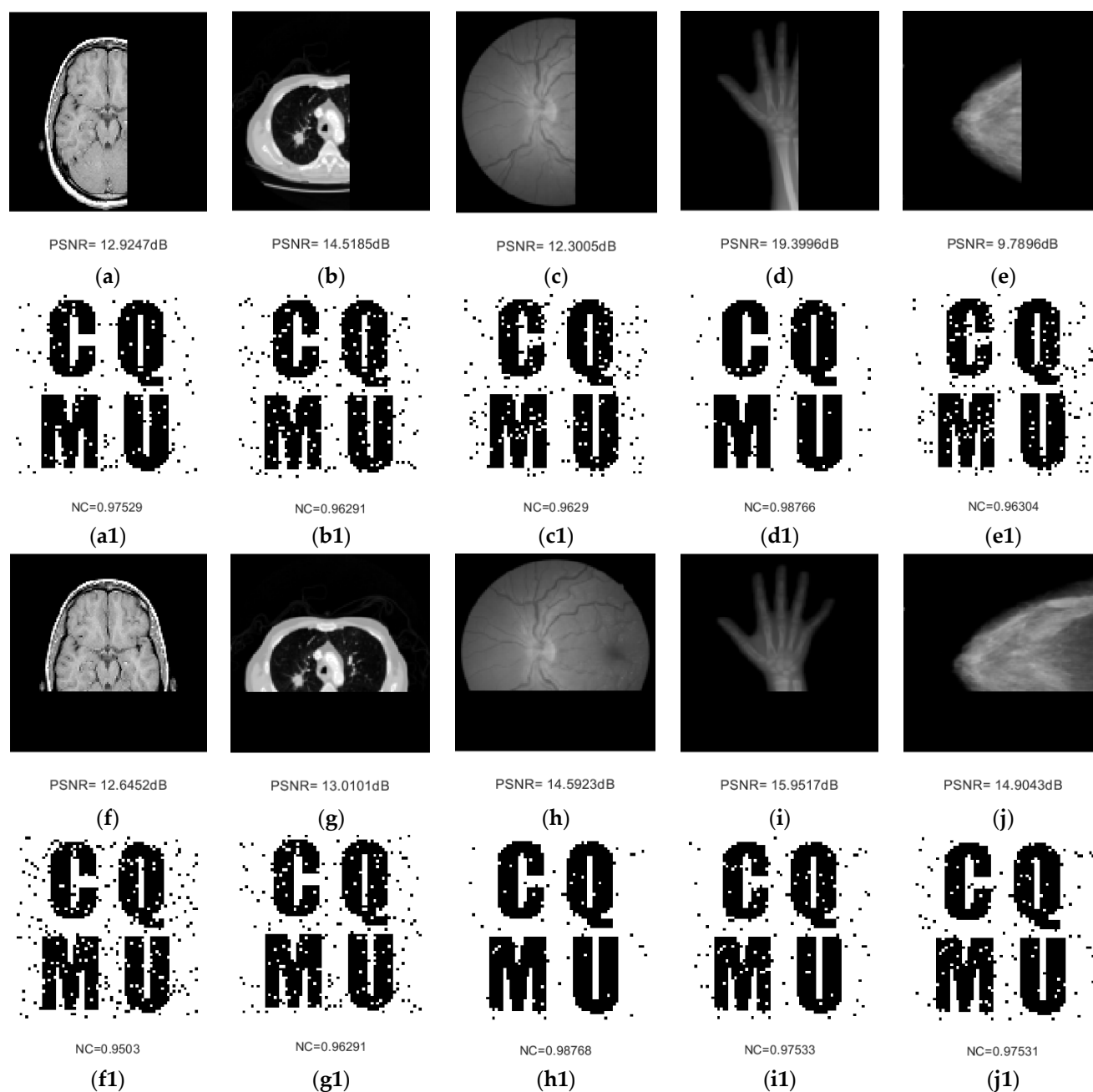


Figure 14. Attacked medical images and restored watermarking images under X-axis cropping 40% and Y-axis cropping 30%: (a,f,a1,f1) brain and extracted watermarking image; (b,g,b1,g1) chest and extracted watermarking image; (c,h,c1,h1) fundus blood vessels and extracted watermarking image; (d,i,d1,i1) hand and extracted watermarking image; and (e,j,e1,j1) breast and extracted watermarking image.

Table 6. The result under cropping attacks.

Name	X-Axis Crop 5%		X-Axis Crop 15%		X-Axis Crop 40%		Y-Axis Crop 10%		Y-Axis Crop 25%	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	90.1377	1.0000	56.9175	1.0000	12.9247	0.9753	18.7664	0.9377	13.59	0.9377
Medical image B	50.2622	1.0000	23.43	0.9630	14.5185	0.9629	28.6074	0.9753	14.3028	0.9754
Medical image C	32.7365	0.9877	20.7318	0.9877	12.3005	0.9629	24.811	0.9877	16.2596	0.9753
Medical image D	87.581	1.0000	87.581	1.0000	19.3996	0.9877	19.4777	0.9629	16.4589	0.9629
Medical image E	20.3824	0.9877	15.3823	0.9754	9.7896	0.9630	32.9291	0.9877	16.7177	0.9877

- Translation Attacks

Figure 15 shows the results of the experiment in which the medical images of different parts are shifted 20% to the left and 30% downwards. The figures show that some information has been missed; however, the restored watermarking image still has a good visible effect. Observing Table 7, we can see that regardless of whether they move largely left or vertically, their NC values perform well. When shifted 41% to the left or 40% downward, the NC means can still reach 0.93. Therefore, under the translation attack, the algorithm shows good robustness.

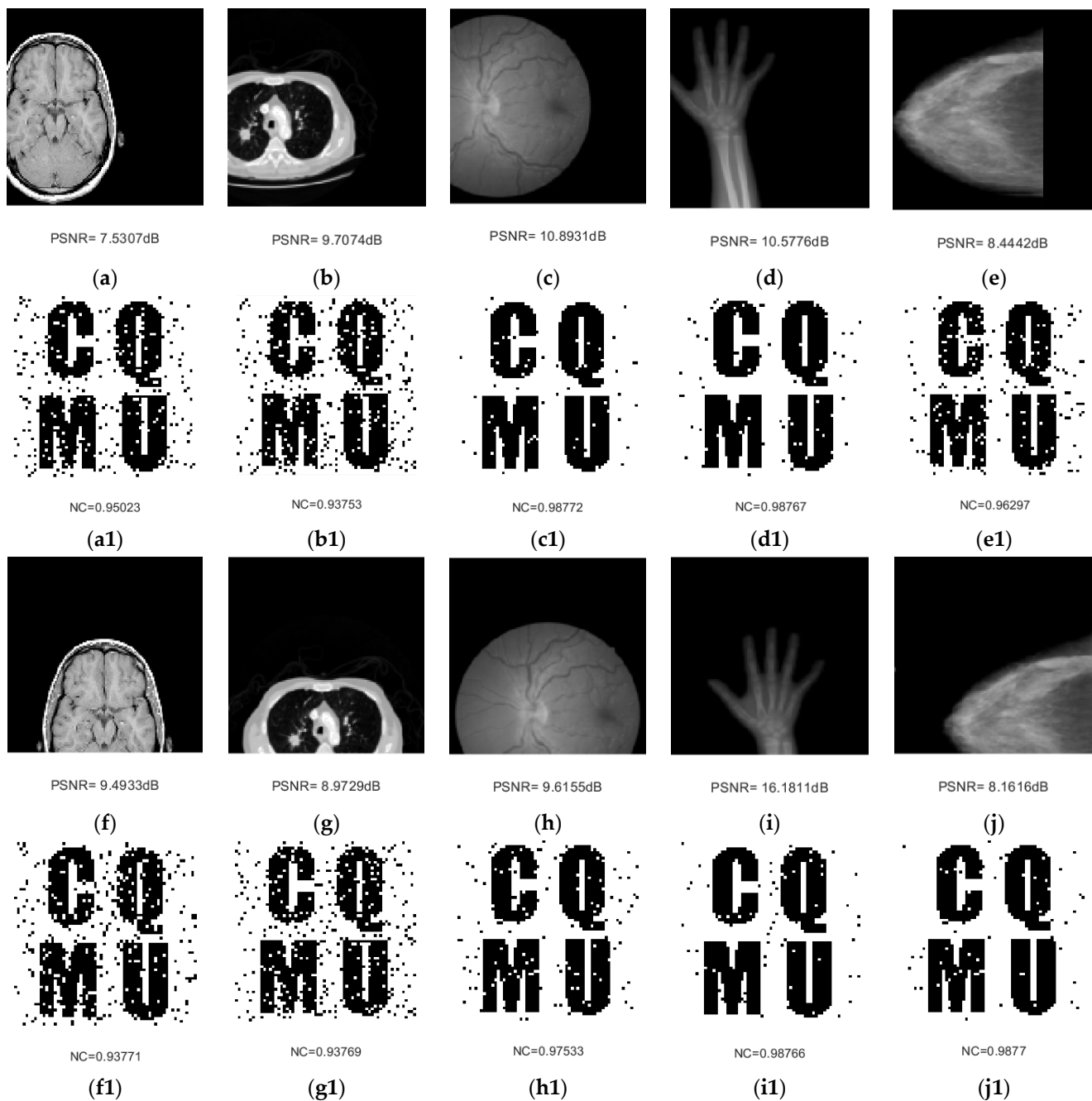


Figure 15. Attacked medical images and restored watermarking images under left translation 20% and down translation 30%: (a,f,a1,f1) brain and extracted watermarking image; (b,g,b1,g1) chest and extracted watermarking image; (c,h,c1,h1) fundus blood vessels and extracted watermarking image; (d,i,d1,i1) hand and extracted watermarking image; and (e,j,e1,j1) breast and extracted watermarking image.

Table 7. The result under translation attacks.

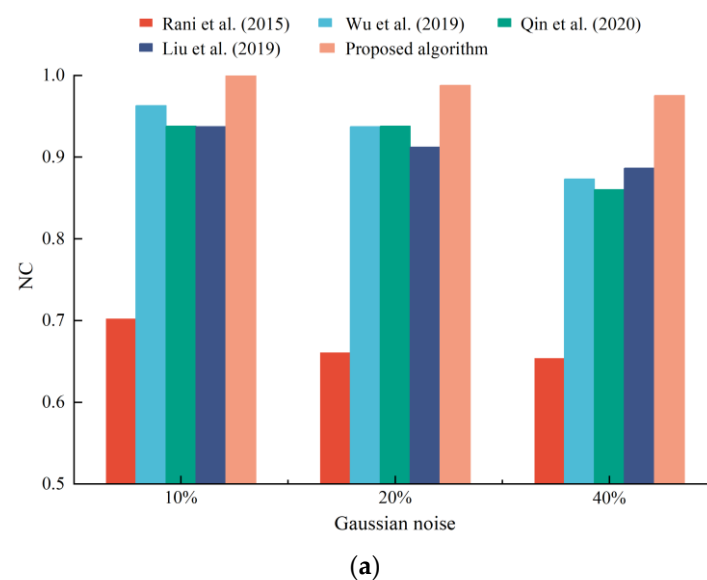
Name	Left 5%		Left 17%		Left 41%		Down 13%		Down 40%	
	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC	PSNR/dB	NC
Medical image A	11.1507	0.9753	8.6638	0.9377	6.6029	0.9503	11.2107	0.9250	8.8705	0.9376
Medical image B	11.8073	0.9752	8.9485	0.9504	8.7963	0.9628	9.1991	0.9628	9.0726	0.9378
Medical image C	17.8609	0.9754	12.6764	0.9877	8.654	0.9877	13.9912	0.9753	8.4723	0.9753
Medical image D	17.481	0.9877	12.2204	0.9877	10.4476	0.9630	19.1956	0.9877	15.9374	0.9753
Medical image E	16.7173	0.9877	10.358	0.9877	6.3622	0.9380	11.2122	0.9877	7.67	0.9877

Experiments show that the algorithm is robust under different intensities of geometric attacks. Because this paper uses DTCWT and Hessenberg decomposition, the constructed feature matrix has translation and rotation invariance. At the same time, the algorithm used by MDCT decreases the contact area with the image and improves the robustness against cropping attacks and translation attacks to some degree. Therefore, the proposed algorithm shows strong robustness in resisting geometric attacks.

4.3. Comparison Experiments

- Robustness comparison

For better verification of the robustness of the proposed algorithm, we selected the MRI brain medical image as the original medical image. Both the proposed algorithm and the comparison algorithm use the watermarking image size 64×64 , but the reference method remains the same as the original. We compared this algorithm with the algorithms of 2. Rani et al. [2], Wu et al. [14], Qin et al. [15], and Liu et al. [18]. The changing trend of the corresponding NC value is illustrated in Figures 16 and 17.



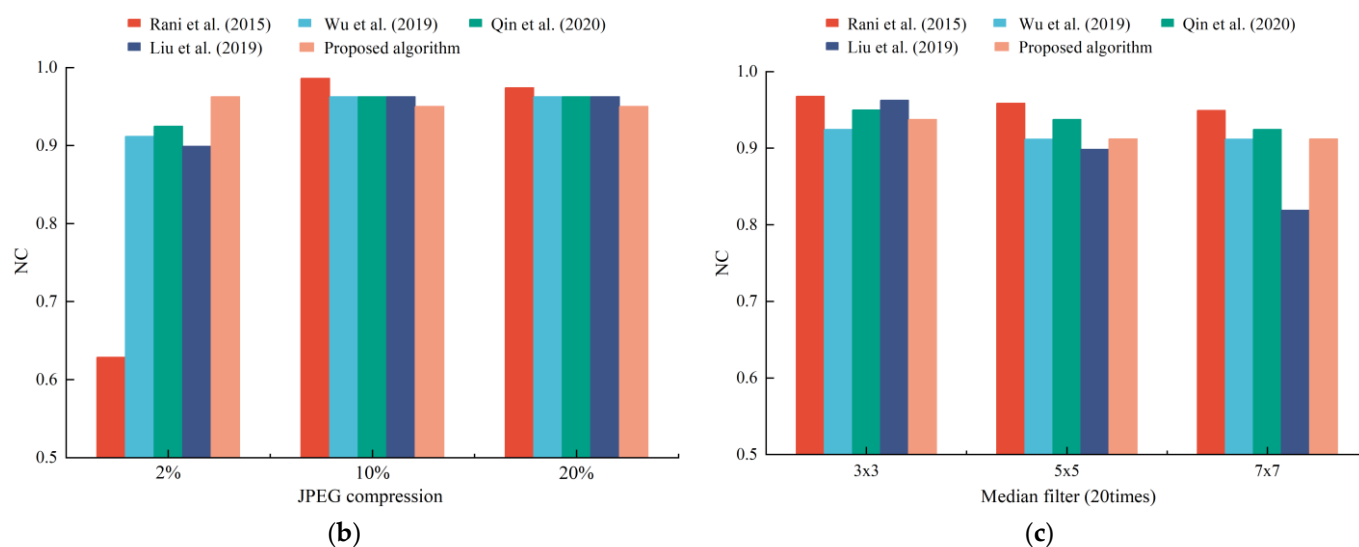
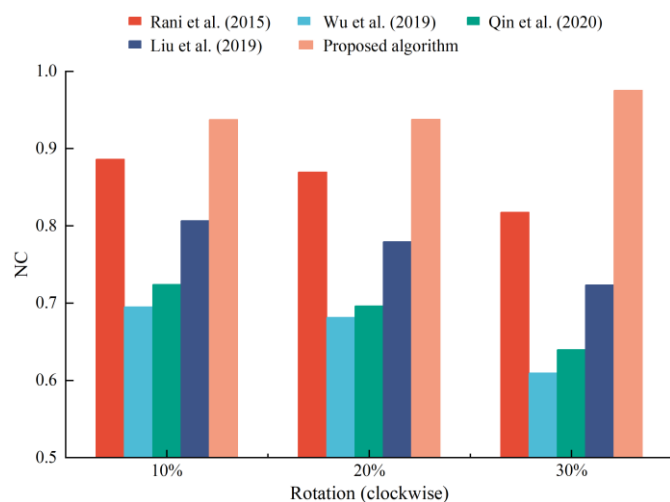


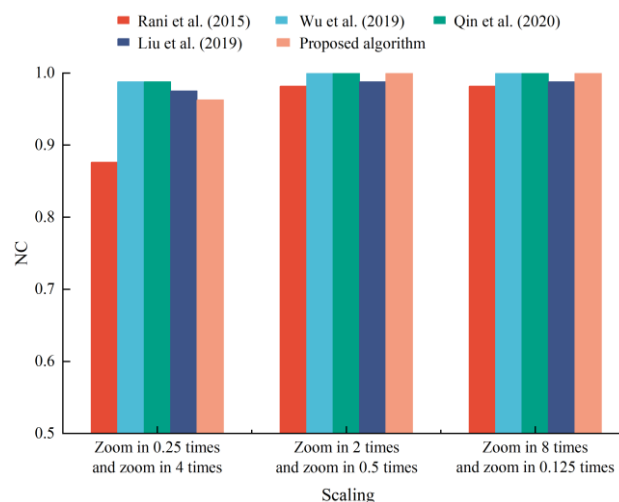
Figure 16. Comparison of the robustness of different algorithms under common attacks: (a) Gaussian noise; (b) JPEG compression; and (c) median filtering.

Figure 16 displays that for Gaussian noise attacks, as the strength of the noise attack gradually became larger, the NC values of the five algorithms all show a downward trend, but the downward trend of the algorithm in this paper is relatively slow, and the noise intensity of 30% the NC value obtained can still reach 0.97. For compression attacks, the five algorithms are not much different in the NC values. Although the NC value is slightly lower than the other four algorithms at a compression strength of 10, when the compression strength is 2, the NC value remains above 0.96.

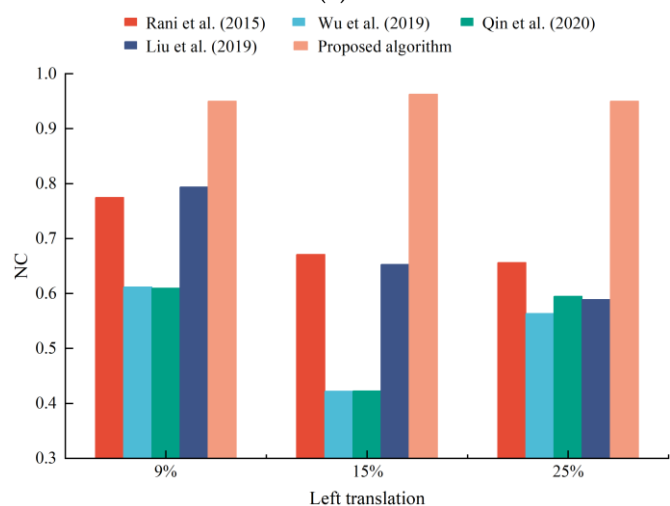
This is because DCT has good robustness against small-range noises and compression attacks, but when the attack intensity increases, the DCT changes quickly, which in turn leads to poor structural feature stability. The algorithm in this paper also uses the upper triangular matrix of Hessenberg decomposition for information integration, which makes the image more robust. In terms of median filtering attacks, the NC values of the algorithm in this paper have no big gap with the literature [2,14,18] and are slightly lower than the literature [15]. This is because the DWT used in the literature [2] has poor direction information, and some contour information of the image would be lost. The Contourlet transform, Curvelet transform, and DTCWT transform used in the literature [14,15,18] have direction selectivity, which improves the image contour information significantly; however, the Curvelet transform in the literature [15] has better performance for the singular characteristics of the image curve and at the same time has better performance in filtering and denoising, so it is more robust in resisting filtering attacks. In summary, the proposed algorithm is more robust under common attacks.



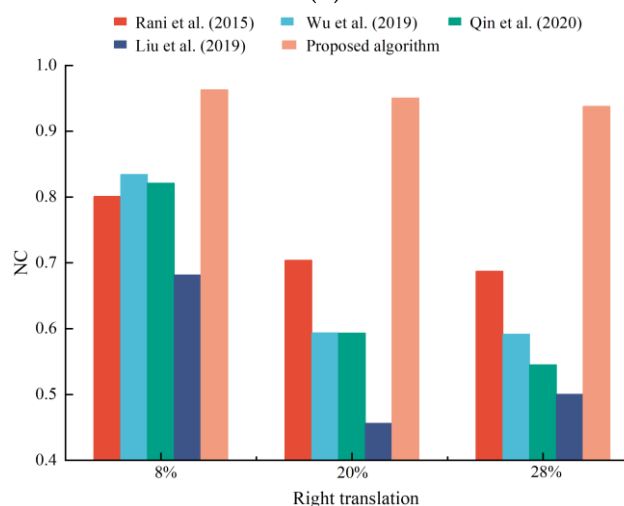
(a)



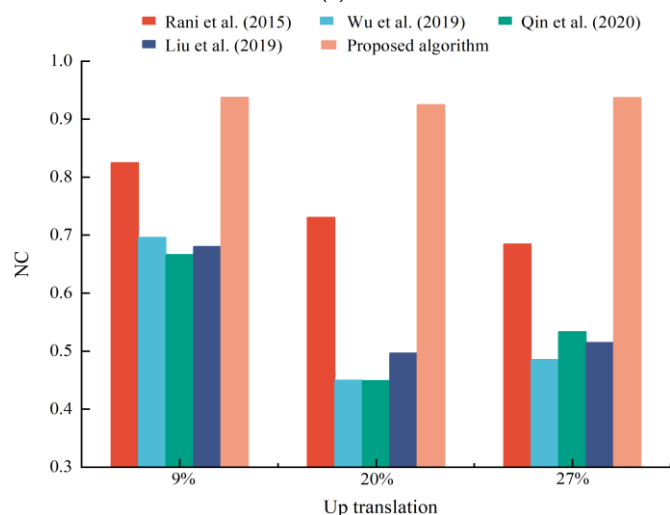
(b)



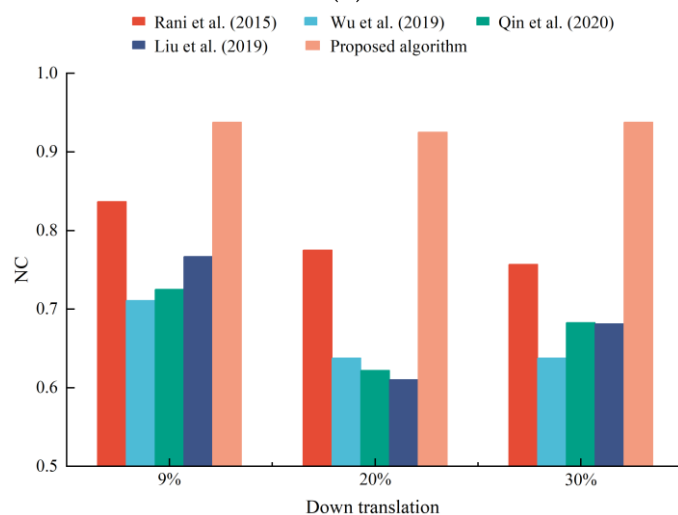
(c)



(d)



(e)



(f)

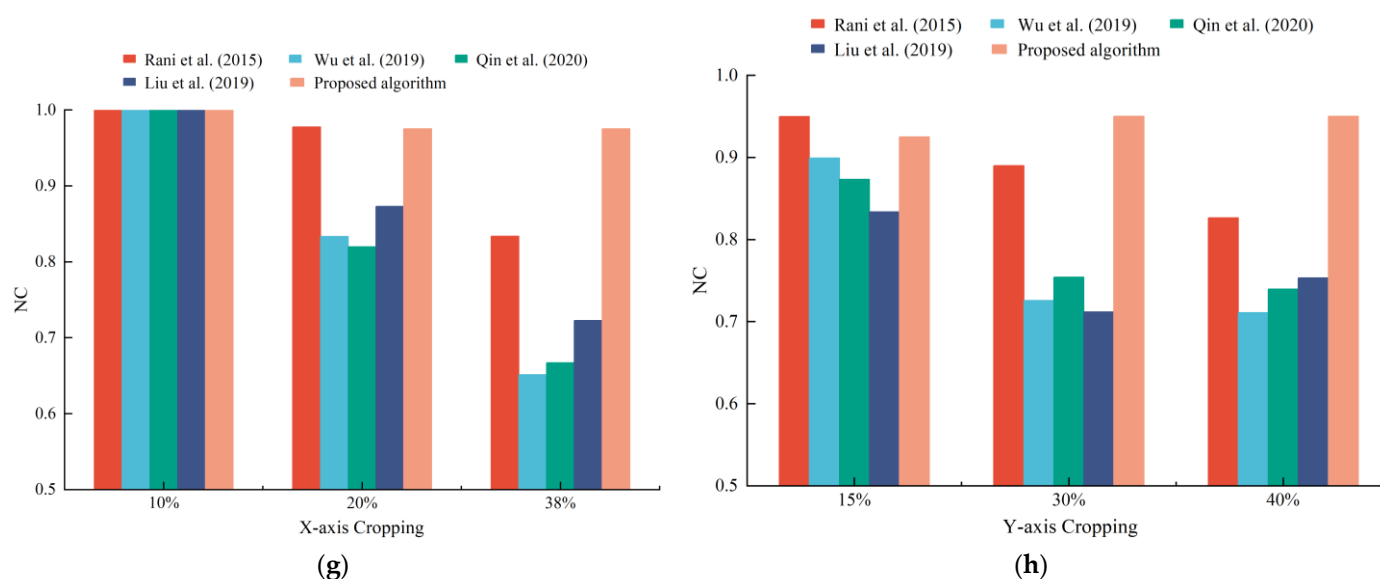


Figure 17. Comparison of the robustness of different algorithms under geometric attacks: (a) rotation; (b) scaling; (c) left translation; (d) right translation; (e) up translation; (f) down translation; (g) X-axis cropping; and (h) Y-axis cropping.

For geometric attacks, compared with the literature [2,14,15,18], the proposed algorithm has a greater degree of enhancement, especially in rotation attacks, translation attacks, and cropping attacks. Figure 17 demonstrates that for rotation attacks at different angles, the proposed algorithm consistently achieves higher NC values than the literature [2,14,15,18]. When rotating 20% clockwise, the algorithm in this paper still maintains the NC value of around 0.95, and the NC values of other documents are lower than 0.9; even the NC values of the literature [14,15] are only about 0.65, which is less robust. For translational attacks, the NC values of other algorithms have a rapid downward trend, while the algorithm in this paper changes slowly, and the minimum NC value is greater than 0.92. For cropping at different positions, for small parts of cropping, the NC values of the five algorithms can be equal, but when the cropping part is larger, the NC value of the algorithm in this paper is improved, compared to the literature [2,14,15,18], around 5%–15%.

Because the literature [2] uses chunk singular values to construct image features, the chunk singular values are more sensitive to pixel position and easier to change. The algorithm in the literature [14,15,18] uses the DCT means for constructing the feature matrix; when rotating and cropping attacks, the image means can be significantly influenced. The DWT transformation, Contourlet transformation, and Curvelet transformation used in the literature [2,14,15] do not have translation invariance and so have poor robustness in geometric attacks. The DTCWT used in this algorithm has direction selectivity and translation invariance, while MDCT and Hessenberg decomposition have energy concentration solidity and rotation invariance. Additionally, the maximum value of each sub-block decomposition is directly used to construct the feature vector of the image, which can directly reflect the changes in the image. Therefore, even if it is geometrically attacked, the changes in the maximum value are relatively small, and it can better resist geometrical attacks.

All in all, compared with the literature [2,14,15,18], the algorithm in this paper has higher stability, especially in the solution of problems that have no resistance to geometric attacks. The proposed algorithm shows great resistance to geometric attacks and excellent robustness.

5. Conclusions

In this paper, we propose a robust, zero-watermarking algorithm based on DTCWT-MDCT-Hessenberg for medical images, which solves the information security problems during the process of medical image storing and transmitting. The algorithm uses the direction selectivity, translation invariance of DTCWT, the stability of energy concentration of DCT, and the rotation invariance of Hessenberg decomposition to solve the problem of poor robustness of traditional zero-watermarking algorithms against geometric attacks. The algorithm does not require watermarking of original medical images. Extraction realizes the requirement of zero-watermarking and ensures the reliability of doctor's diagnosis. Meanwhile, combining cryptographic algorithms and third-party concepts, encryption of the watermarking with a chaotic sequence of initial value sensitivity enhances the algorithm's security. Experimental results demonstrate that the algorithm in this paper has high computational efficiency, exhibits good robustness under common attacks and geometric attacks, and has high practical value in the protection of medical images.

Author Contributions: B.H. and T.H. proposed the research conceptualization and methodology; the software and improvement were performed by J.X.; the validation was performed by J.X.; writing of original draft, preparation, and editing were performed by J.X. and Y.Y.; and the funding acquisition was performed by B.H. and T.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the General Project of Chongqing Natural Science Foundation of China (No. cstc2020jcyj-msxmX042), the Hainan Provincial Natural Science Foundation of China (No. 620MS067), and the National Natural Science Foundation of China (No. 61702063).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: In this research, all datasets are freely available at <https://aistudio.baidu.com/aistudio/projectdetail/462184?qq-pf-to=pcqq.c2c>; <https://www.kaggle.com/> (accessed on 14 February 2022).

Conflicts of Interest: The authors declare no conflict of interest.

References

- Manuel, C.H.; Antonio, C.H.; Garcia-Ugalde, F.J. Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm. *Mathematics* **2021**, *9*, 1795.
- Rani, A.; Bhullar, A.K.; Dangwal, D.; Kumar, S. A Zero-Watermarking Scheme using Discrete Wavelet Transform. *Procedia Comput. Sci.* **2015**, *70*, 603–609.
- Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80.
- Malayil, M.V.; Vedhanayagam, M. A novel image scaling based reversible watermarking scheme for secure medical image transmission. *ISA Trans.* **2021**, *108*, 269–281.
- Li, Y.; Wang, J.W.; Jia, H.Y. A Robust and Reversible Watermarking Algorithm for a Relational Database Based on Continuous Columns in Histogram. *Mathematics* **2020**, *8*, 1994.
- Wang, B.W.; Zhao, P. An Adaptive Image Watermarking Method Combining SVD and Wang-Landau Sampling in DWT Domain. *Mathematics* **2020**, *8*, 691.
- Gangadhar, Y.; Giridhar Akula, V.S.; Reddy, P.C. An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. *Biomed. Signal Process. Control.* **2018**, *43*, 31–40.
- Balasamy, K.; Suganyadevi, S. A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. *Multimed. Tools Appl.* **2020**, *80*, 7167–7186.
- Fares, K.; Amine, K.; Redouane, K.; Salah, E. DCT & DWT based watermarking scheme for medical information security. *Biomed. Signal Process. Control.* **2021**, *66*, 102403.
- Cedillo-Hernandez, M.; Cedillo-Hernandez, A.; Nakano-Miyatake, M.; Perez-Meana, H. Improving the management of medical imaging by using robust and secure dual watermarking. *Biomed. Signal Process. Control.* **2020**, *56*, 101695.
- Kavitha, C.; Sakthivel, S. An effective mechanism for medical images authentication using quick response code. *Clust. Comput.* **2019**, *22*, 4375–4382.
- Wen, Q.; Sun, T.F.; Wang, S.X. Concept and application of zero-watermarking. *Acta Electron. Sin.* **2003**, *31*, 214–216.

13. Xiao, Z.J.; Zhang, H.; Chen, H.; Gao, T. Zero-watermarking based on boost normed singular value decomposition and cellular neural network. *J. Image Graph.* **2017**, *22*, 288–296.
14. Wu, X.Q.; Li, J.B.; Tu, R.; Cheng, J.R.; Bhatti, U.A.; Ma, J.X. Contourlet-DCT based multiple robust watermarkings for medical images. *Multimed. Tools Appl.* **2019**, *78*, 8463–8480.
15. Qin, F.M.; Li, J.B.; Li, H.; Liu, J.; Nawaz, S.A.; Liu, Y.L. A robust zero-watermarking algorithm for medical images using curvelet-dct and RSA pseudo-random sequences. In *The International Conference on Artificial Intelligence and Security*; Springer: Cham, Switzerland, 2020; Volume 12240, pp. 179–190.
16. Wu, D.Y.; Tang, Y.; Zhao, W.; Wan, Y.C.; Qu, C.B. Zero-watermarking algorithm based on Curvelet-DWT-SVD. *J. Yanshan Univ.* **2020**, *44*, 42–52.
17. Xue, H.F.; Chi, W.D.; Liu, X.X. Zero-Watermark Algorithm based on NSST and Hessenberg Decomposition. *Mod. Comput.* **2020**, *10*, 89–93.
18. Liu, J.; Li, J.B.; Zhang, K.; Bhatti, U.A.; Ai, Y. Zero-watermarking algorithm for medical images based on dual-tree complex wavelet transform and discrete cosine transform. *J. Med. Imaging Health Inform.* **2019**, *9*, 188–194.
19. Xia, Z.Q.; Wang, X.Y.; Wang, C.P.; Wang, C.X.; Ma, B.; Li, Q.; Wang, M.X.; Zhao, T.T. A robust zero-watermarking algorithm for lossless copyright protection of medical images. *Appl. Intell.* **2022**, *52*, 607–621.
20. Vaidya, S.P. Fingerprint-based robust medical image watermarking in hybrid transform. *Vis. Comput.* **2022**, *38*, 1–16.
21. Fang, Y.X.; Liu, J.; Li, J.B.; Cheng, J.R.; Hu, J.B.; Yi, D.; Xiao, X.L.; Bhatti, U.A. Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT. *Multimed. Tools Appl.* **2022**, *81*, 1–17.
22. Liu, J.; Ma, J.X.; Li, J.B.; Huang, M.X.; Sadiq, N.; Ai, Y. Robust watermarking algorithm for medical volume data in internet of medical things. *IEEE Access* **2020**, *8*, 93939–93961.
23. Nick, K. Image processing with complex wavelets. *Philos. Trans. Math. Phys. Eng. Sci.* **1999**, *357*, 2527–2542.
24. Nick, K. Complex wavelets for shift invariant analysis and filtering of signals. *Appl. Comput. Harmon. Anal.* **2001**, *10*, 234–253.
25. Nouioua, A.; Seddiki, N.; Ghaz, A. Blind digital watermarking framework based on DTCWT and NSCT for telemedicine application. *Traitement Du Signal* **2020**, *37*, 955–964.
26. Li, Z.Y.; Zhang, H.; Liu, X.L.; Wang, C.P.; Wang, X.Y. Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHFM and DWT-DCT. *Digit. Signal Process.* **2021**, *115*, 103062.
27. Mahbuba, B.; Shorif, U.M. Multiple image watermarking with discrete cosine transform. *J. Comput. Commun.* **2021**, *9*, 88–94.
28. Zhou, K.; Zhang, Y.M.; Li, J.; Zhan, Y.T.; Wan, W.B. Spatial-Perceptual Embedding with Robust Just Noticeable Difference Model for Color Image Watermarking. *Mathematics* **2020**, *8*, 1506.
29. Qu, C.B.; Yan, Y. A robust digital watermarking algorithm based on multiple level DCT and SVD. *Comput. Appl. Softw.* **2012**, *29*, 288–291.
30. Su, Q.T.; Chen, B.J. A novel blind color image watermarking using upper Hessenberg matrix. *AEU—Int. J. Electron. Commun.* **2017**, *78*, 64–71.
31. Cheng, Y.Y. Image watermarking algorithm based on discrete cosine transform and Hessenberg composition. *J. Jinggangshan Univ. Nat. Sci. Ed.* **2019**, *40*, 45–51.
32. Huang, T.Y.; Xu, J.; Yang, Y.L.; Tu, S.X.; Han, B.R. Zero-Watermarking Algorithm for Medical Images Based on Nonsubsampled Contourlet Transform and Double Singular Value Decomposition. In *Proceedings of the 2021 5th Asian Conference on Artificial Intelligence Technology (ACAIT)*, Haikou, China, 29–31 October 2021; pp. 65–76.