applied sciences

MDPI

Article

A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map

Jing Liu [1,2], Jingbing Li [1,2,*], Jixin Ma [3], Naveed Sadiq [4], Uzair Aslam Bhatti [1,2] and Yang Ai [5]

1 College of Information Science and Technology, Hainan University, Haikou 570228, China; jingliuhnu2016@hotmail.com (J.L.); uzairaslambhatti@hotmail.com (U.A.B.)
2 State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou 570228, China
3 School of Computing and Mathematical Sciences, Faculty of Liberal Arts and Sciences, University of Greenwich, Greenwich, London SE10 9LS, UK; J.Ma@greenwich.ac.uk
4 Ocean College, Zhejiang University, Hangzhou 310058, China; naveedbuttar@hotmail.com
5 Faculty of Network Science, Haikou University of Economics, Haikou 571127, China; yangaihku2010@hotmail.com
* Correspondence: jingbingli2008@hotmail.com; Tel.: +86-136-3765-8206

Received: 21 January 2019; Accepted: 15 February 2019; Published: 18 February 2019

Featured Application: This algorithm combines DTCWT-DCT, Henon map, perceptual hashing and the third-party concepts for medical images with special requirements on images. It uses zero-watermark technology to complete the embedding and extraction of watermarks to effectively protect the safety of medical images and patients' privacy information. With a large payload capacity and a high level of robustness against common attacks and geometric attacks, it can be used for medical security, cloud storage and cloud transmission, security authentication, etc.

Abstract: To resolve the contradiction between existing watermarking methods—which are not compatible with the watermark's ability to resist geometric attacks—and robustness, a robust multi-watermarking algorithm suitable for medical images is proposed. First, the visual feature vector of the medical image was obtained by dual-tree complex wavelet transform and discrete cosine transform (DTCWT-DCT) to perform multi-watermark embedding and extraction. Then, the multi-watermark was preprocessed using the henon map chaotic encryption technology to strengthen the security of watermark information, and combined with the concept of zero watermark to make the watermark able to resist both conventional and geometric attacks. Experimental results show that the proposed algorithm can effectively extract watermark information; it implements zero watermarking and blind extraction. Compared with existing watermark technology, it has good performance in terms of its robustness and resistance to geometric attacks and conventional attacks, especially in geometric attacks.

Keywords: henon map; multi -watermarking; DTCWT-DCT; robustness

1. Introduction

Since the birth of medical imaging technology, medical images that, in the auxiliary diagnosis of the industry, play an increasingly important role in making accurate diagnoses for doctors, include computed tomography (CT) images, X-ray images, ultrasound images, magnetic resonance imaging (MRI) images, electrocardiograms, electroencephalograms, angiography images, radionuclide images etc. generated by medical imaging systems [1]. Especially in recent years, due to the rapid development of life sciences, materials science, robotics engineering and information science, doctors can use imaging

systems that already have microscopic resolution to directly generate medical images, and can even operate nanorobots deep inside patients' bodies to perform molecular-level real-time diagnoses and cancer targeted therapy, according to the micro-camera on the robot and the images returned by various sensors. At present, many hospitals have developed their own smart medical platforms [1,2]. These platforms facilitate patients' access to electronic medical records and medical images. Some rare and precious medical images stored on such systems also provide valuable technical exchanges and case sharing between doctors and peers. For the convenience of diagnoses, doctors usually embed the personal information of the patient directly in the medical images, which brings many safety hazards for the storage and transmission of medical images. Patients' private information may be leaked or subject to malicious attacks. The use of medical image watermarking (MIW) technology can effectively solve this problem [3,4].

Digital watermarking was first proposed to protect the copyright of digital multimedia on the Internet. Now we can hide the personal information of patients in the corresponding medical images according to their characteristics so as to protect the privacy of patients, avoid tampering with patients' data, and make sure that such material is transmitted safely on the Internet. But for medical images, unique characteristics must also be taken into account. Such images are an important means for doctors to obtain pathology information about patients. In the medical field, the quality requirements for patients' pathology medical data are extremely strict, and no changes are allowed [5]. Anything that may affect medical pathology data is not advisable. Hence, study of medical image digital watermarking is particularly important [6].

Kutter et al. proposed the second-generation watermark algorithm in 1999, which applied image features to watermark embedding and extraction, and gave rise to zero-watermark technology. In recent years, numerous medical watermarking algorithms have been developed. Scholars and experts in various countries have done lots of research on the digital watermarking of medical images. These research algorithms are divided into three categories, each of which will now be summarized. (1) Those based on Region of Non-Interest (RONI); Rahman et al. [7] designed a hybrid watermark using bose, ray, hocquenghem (BCH) coding, chaos theory and RRNS in spatial domain, and the RONI was used to embed watermark information; Abokhdair et al. [8] first divided the host medical image, then hid the patient data and the hash values in a Region of Interest (ROI), hid the tamper recovery data and the hash values of tamper detection in RONI. Each embeddable ROI pixel can hide one or two bits to reduce ROI distortion; Parah et al. [9] proposed two different algorithms. By modifying the threshold value, the transform domain coefficient of 8x8 is compared with the size of watermark and Electronic Patients Record (EPR). One algorithm embeds both watermark and EPR into ROI and RONI, and the other keeps the ROI unchanged and hides the watermark and EPR in RONI; Thanki et al. [10], using a human visual system (HVS) model to identify the RONI of the cover medical image, explicitly inserted the watermark into the RONI of the cover medical image to obtain a watermarked medical image; Zhang et al. [11], using Laplacian and a horizontal set segmented the medical images into ROI and RONI, whereby the watermark information was embedded into a RONI based on Contourlet transformation and singular value decomposition (SVD); Taher et al. [12] proposed a blind hybrid watermark algorithm for MRI images, which used a histogram to divide the image into ROI and RONI, and embedded the watermark into the RONI's spatial and wavelet domains; Maedeh Jamali et al. [13] looked for RONI using saliency to find the smallest overlap with the ROI. When embedding, discrete wavelet transform and discrete cosine transformation (DWT-DCT) is used with redundant watermarks. When extracting, a vote is used. (2) The second category is based on reversible watermarking. Arsalan et al. [14] proposed a new technique named 'IRW-Med', using the concept of a compression function to reduce the embedding distortion, and the integer wavelet transform (IWT) as an embedded domain to realize the reversibility of the watermark; Kelkar et al. [15] introduced two innovative reversible algorithms, which were both based on a histogram shift to improve the hidden capacity, and to divide the image into non-overlapping blocks to embed the watermark; Turuk et al. [16] proposed a reversible watermarking scheme using quantization

functions embedded in multiple watermarks and a novel tracking key to restore original medical images; Lei et al. [17] inserted data and signature information into the original medical image via a recursive modulation algorithm after wavelet transform and singular value decomposition. In this method, the watermark strength is controlled by differential evolution. (3) The final category is based on classical conventional digital watermarking. In the literature [18–22], an algorithm of multiple watermarks for medical images is implemented. As Aditi Zear et al. [18] used SVD, DCT, DWT respectively for different type of watermarks, and back propagation neural networks (BPNN) to eliminate the impact of noise when extracting watermarks; they also enhanced its security by using Arnold transform; Rohit Thanki et al. [19] used fast discrete curvelet transform (FDCuT) for medical images to obtain the different frequency coefficients of the curve decomposition, and adopted DCT for high frequency coefficients. Then, the watermark is modified according to the medium frequency coefficient of a white gaussian noise (WGN) sequence image. During extraction, the same sequence of correlation is used to achieve blind recovery; Jinwei Wang et al. [20] proposed a new kind of multi-watermark which is controlled by secret key. The proposed hybrid decoder is optimal and locally optimal. It follows multiple multiplication rules and is based on the minimum risk of bayes. Their DWT coefficients are modeled as generalized gaussian distributions; Xiaochen Yuan et al. [21] proposed a local multi-watermark algorithm, which used the the robust and adaptive feature detector based on daisy descriptor (RAF3D) design adaptive detector to embed multiple watermarks into the orthogonal space of a feature extraction region at the same time. When extracting, the image can be extracted independently; Amit Kumar Singh et al. [22] proposed a spread spectrum watermarking algorithm, which used a haar wavelet to perform the binary sub-band decomposition, and then embedded different forms of watermark information in the intermediate frequency and second order selected frequency bands of the first order DWT respectively, according to the different contexts in which it was used. The three categories are shown in Figure 1.

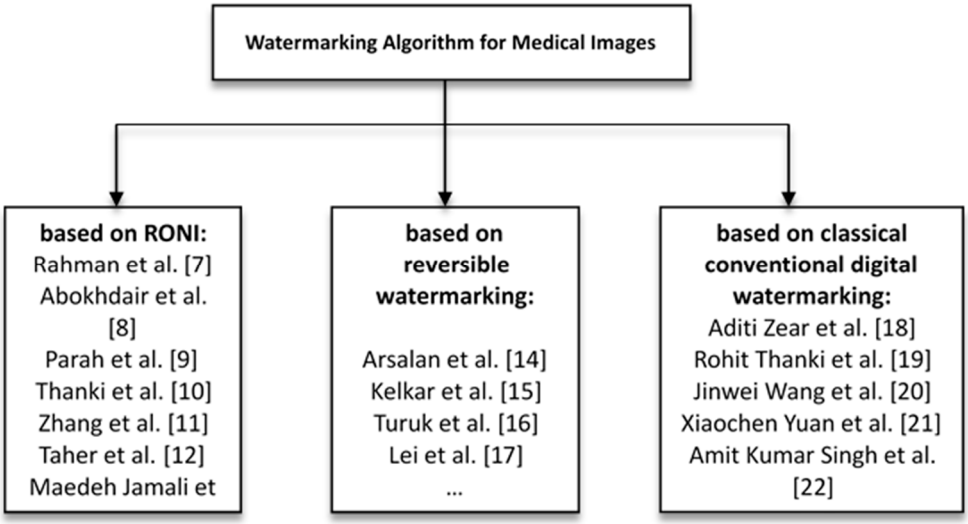


Figure 1. Category of watermarking algorithms for medical images.

For algorithms based on the first and third categories, the embedding of watermarks affects the images themselves, and these watermarking algorithms have poor anti-geometric attack capabilities; they cannot even resist the tiny geometric transformations [9,10,22–24]. For medical images, the particularity is that the embedded watermark cannot affect the diagnosis of doctors, and cannot obviously change the main content of medical images, especially for the region of interest of the image. The second category uses reversible digital watermarks. Although the watermark image can be restored to the original image without loss, the watermark is not robust. Therefore, finding a feature vector that can resist geometric attacks in medical images so that the algorithm can show good robustness without changing the original image is a problem that has long puzzled researchers [7,8,12,13,20,21].

Consequently, this paper proposes a multi-watermark robust algorithm based on a dual-tree complex wavelet transform and discrete cosine transform (DTCWT-DCT) using perceptual hash and henon mapping. By selecting the low frequency coefficients of the medical images in the DTCWT-DCT transform domain and performing symbol transformation, the features of the medical image may be extracted. Then, using henon chaos and hash function properties, different initial values of the chaotic sequences and XOR operation are given to encrypt each watermark. Finally, based on common watermark technology, a set of secret keys are generated by combining the concepts of the "third party", chaotic encryption and cryptography technology to complete the embedding and extraction of the multi-watermark.

The main contribution of the present research is:

(1) A new method is proposed to extract stable features of medical images according to human vision, which does not require any changes to the original images, and is highly resistant to geometric attacks.

(2) The encryption of watermarks uses a chaotic system and hash function properties, which are extremely sensitive to the initial value, to enhance the security of watermarks.

(3) The embedding of watermarks generates a set of secret keys that can be stored by a third party. The region of interest need not be selected, which can effectively protect the privacy of patients.

(4) The extraction of watermarks does not require the original image, i.e., zero watermark and blind extraction.

(5) It solves the problem that existing algorithms cannot simultaneously offer protection against geometric attacks and robustness. The proposed algorithm has good robustness and invisibility.

2. The Fundamental Theory

The fundamental theory involved in the algorithm is dual tree complex wavelet transform and henon mapping.

2.1. Dual-Tree Complex Wavelet Transform (DTCWT)

The dual complex wavelet transform (DTCWT) is a new transform method for improving the sensitivity of wavelet transform to translation operation and the inflexibility of direction selection [23]. It has two trees: one stores the real numbers, and the other stores the imaginary numbers [24]. When transforming, the two trees are played simultaneously. It can be selected in six directions and is stable for translation. The equation for the 2D DTCWT is as follows:

$$\psi_g(x)\psi_h(y) + \psi_h(x)\psi_g(y) \tag{1}$$

where, ψ_h and ψ_g are orthogonal or biorthogonal real wavelets, respectively.

The 2D discrete wavelet is shown in Figure 2a. The first two wavelets represent the vertical and horizontal two main directions, respectively; the third wavelet is the mixed diagonal direction with no main direction and serious chessboard artifacts.

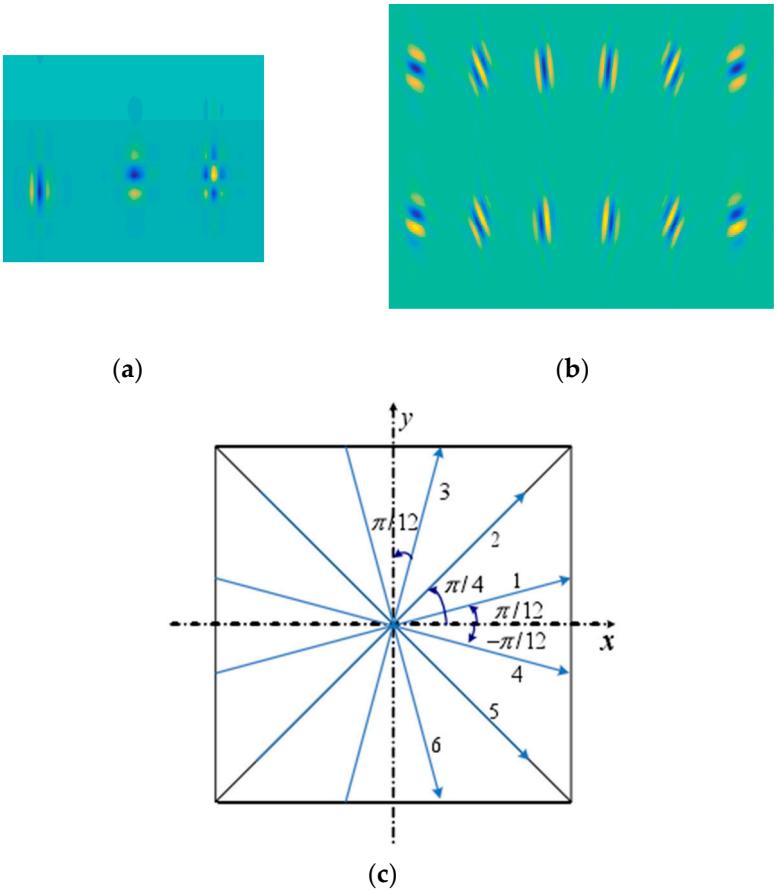
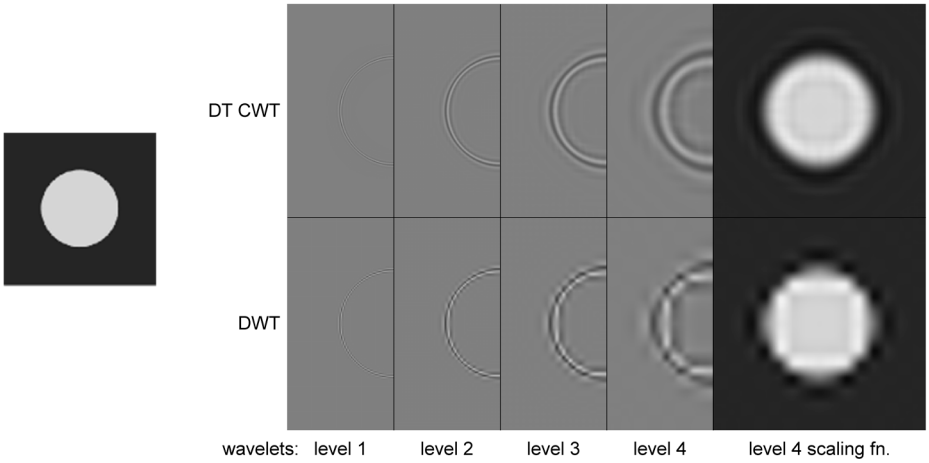


Figure 2. 2D discrete wavelet and 2D DT complex wavelet: (**a**) Two-dimensional discrete wavelet; (**b**) Two dimensional DT complex wavelet; (**c**) The ideal directional distribution of a two-dimensional complex wavelet.

The 2D DTCWT is enforced by using four 2D DWTs which are synchronous for the image, whereby its row and column use different filter banks. The sum and difference of its sub-band diagrams yield 12 wavelets, as shown in Figure 2b. The first line is used as the real part (imaginary part) of the 6 complex-valued wavelets, the second line is the imaginary part (real part), and the third line represents the amplitude of the complex-valued wavelet. Figure 2c shows the ideal directional distribution of a two-dimensional complex wavelet. As shown in Figure 2, 2D DTCWT has 6 main directions and has better directional selectivity compared with 2D DWT. Meanwhile, 2D DWT checkerboard artifacts are eliminated.

In addition, 2D DTCWT can maintain good directional analysis capabilities while having translation invariance, as shown in Figure 3. Figure 3a is an input image. Figure 3b from left to right are the first to the fourth layer of the dual-tree complex wavelet coefficient reconstruction image and the fourth layer scale function coefficient map (to save space, the reconstructed image is only half displayed). The 2D DWT does not have translation invariance; therefore, it will produce many irregular edges and striped derivatives. While the 2D DTCWT performs the same processing on all directions of the input image, the processed image is smooth and continuous.



(**a**) (**b**)

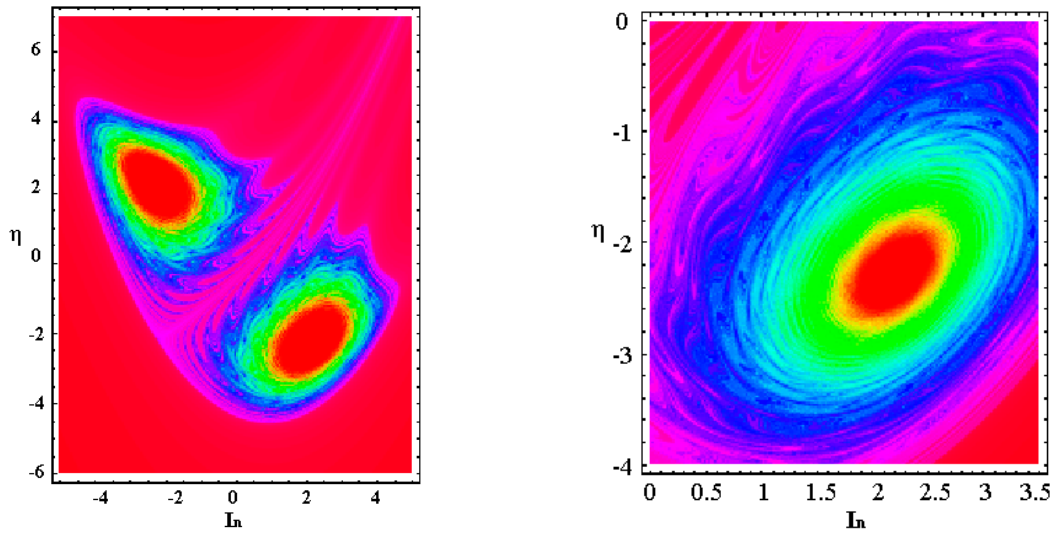
Figure 3. Shift invariance of 2D DTCWT: (**a**) Input image; (**b**) Reconstructed images.

2.2. Henon Map

A henon map is a two-dimensional nonlinear discrete chaotic map [25]. It is sensitive to initial values, has unpredictability, and is ergodic, which is very similar to image encryption [26]. Thus, it is often used in the study of image encryption algorithms. It is defined as follows:

$$\begin{cases} x_{n+1} = 1 - ax^2{}_n + y_n \\ y_{n+1} = bx_n \end{cases} \tag{2}$$

where, n represents the number of iterations, x, y represent the iteration values [27]. a, b are two control parameters, $a \in (0, 1.4)$, $0.2 < b \leq 0.314$. Under their control, the henon mapping system can be in a chaotic state, which a = 1.4, b = 0.3. Figures 4 and 5 show images of the non-attractive area and the two attractive domains displayed by the henon map under different parameters. In our proposed algorithm, we take the value of a as 1.399 and the value of b as 0.314.



(**a**) (**b**)

Figure 4. The non-attractive region, color indicates the number of times the iteration has escaped.

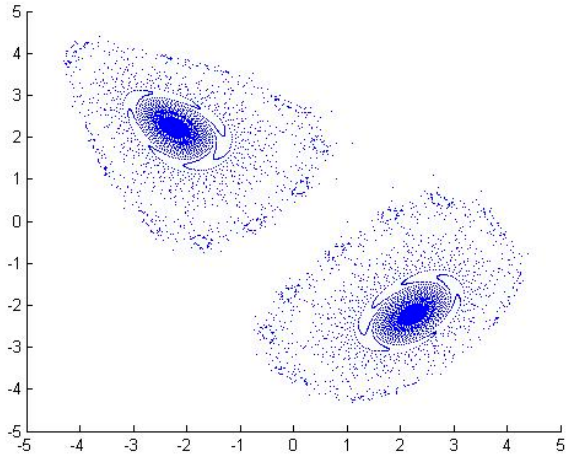


Figure 5. Two domain of attraction.

3. The Proposed Algorithm

The proposed algorithm is based on DTCWT-DCT and a henon map. It is a multi-watermark scheme for medical images, which meets the requirements of zero watermark and blind extraction. It has strong resistance to geometric attacks and displays good robustness. The algorithm consists of five parts: feature extraction of the medical image, preprocessing of multi-watermark, embedding of the multi-watermark, extraction of the multi-watermark and recovery of the multi-watermark. In the feature extraction stage, based on human visual features, a new feature sequence based on perceptual hashing was found in the DTCWT-DCT domain to participate in the watermark operation. In the design of the algorithm, common watermark technology is organically combined with henon chaotic encryption, cryptography and the third-party concept, which not only allows the digital watermark to resist conventional and geometric attacks, but also makes the algorithm strong and robust. Meanwhile, the use of multiple watermarks also enhances the security of medical image transmissions, which can better protect the privacy of patients.

Figure 6 shows the working principle of the proposed algorithm. First, DTCWT-DCT transform was performed on an original medical image for a vector $VF(j)$ conforming to human visual features found in the transformation domain. And binarization was performed on multiple watermarks to obtain multiple corresponding watermarks $W_n(i,j)$. Then, different initial values were taken for henon chaos to generate multiple different chaotic sequences $X_n(j)$. For these chaotic sequences, the symbol operation was applied to obtain the binary encryption matrixes $C_n(i,j)$, and the encrypted watermarks $BW_n(i,j)$ are obtained using $C_n(i,j)$ and $W_n(i,j)$, $W = \{w(i,j)|w(i,j) = 0,1; 1 \leq i \leq M1, 1 \leq j \leq M2\}$. Next, logical operations are performed on $BW_n(i,j)$ and $VF(j)$. According to the encrypted watermarks $BW_n(i,j)$ and the visual feature vector $VF(j)$ of the image, binary logic sequences $Key_n(i,j)$ are generated through the Hash function. These binary logic sequences $Key_n(i,j)$ can be stored in a third-party platform. When testing, the same method was performed to the test medical image to extract the visual feature vector $VF\prime(j)$, and the watermarks $BW_n\prime(i,j)$ contained in the image were extracted by $VF\prime(j)$ and the $Key_n(i,j)$ generated earlier. The chaotic sequences $X_n(j)$ and the encryption matrixes $C_n(i,j)$ were generated using the same henon initial value as the above method. Then, the restored watermarks $W_n\prime(i,j)$ were obtained by hashing $C_n(i,j)$ and $BW_n\prime(i,j)$.

A detailed algorithm description is shown in Figure 6.

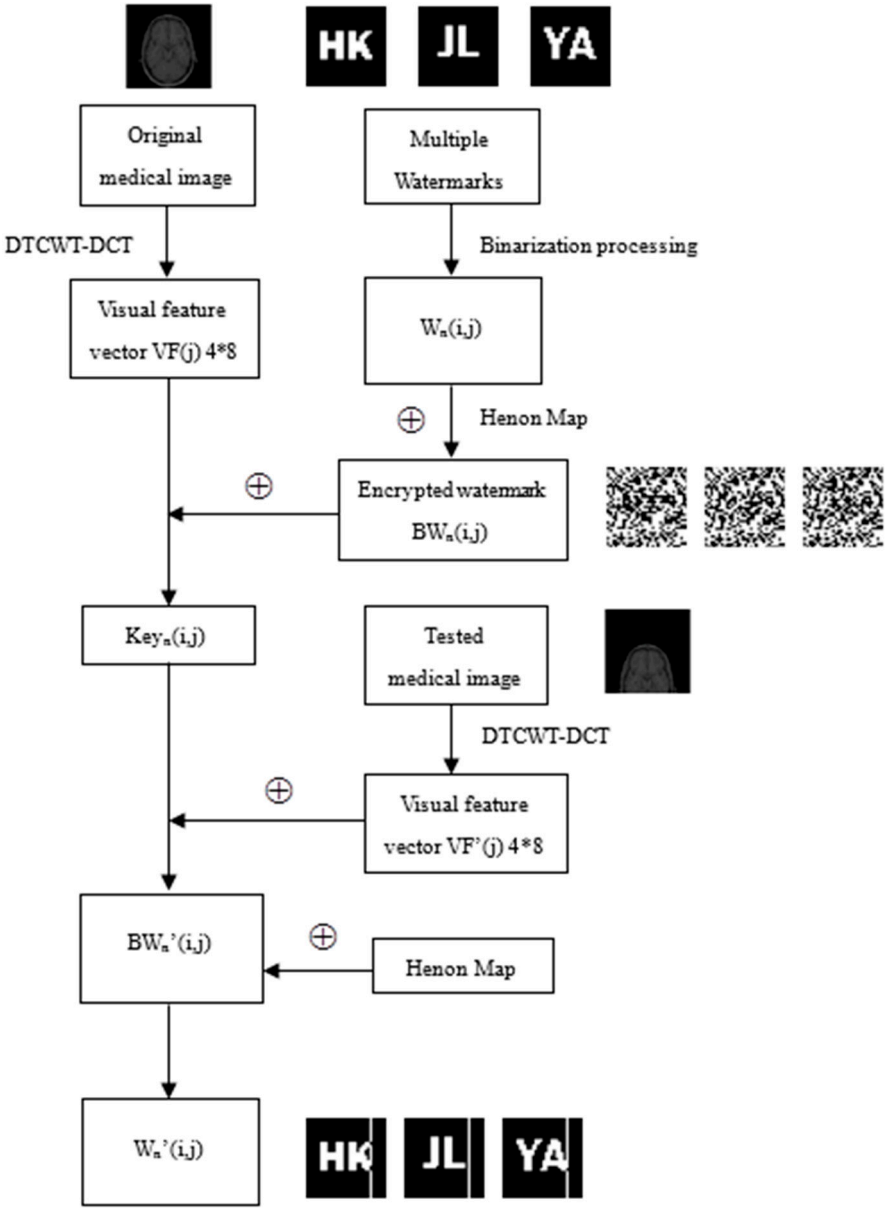


Figure 6. The process of the proposed algorithm.

3.1. Feature extraction

In order to find a visual feature applicable to medical images, a normal human brain image (128 pixels × 128 pixels) was randomly selected to carry out the DTCWT-DCT transformation, and this image was subjected to a variety of different types of attacks, as shown in Figure 7. By observing the coefficient data of the low-frequency part of the image after transformation, we found that although its numerical value changed significantly, its symbol remained basically the same. Table 1 lists the low frequency coefficients of the brain image under different attacks. In this paper, we selected 32 bits of low-frequency data for symbol transformation, and directly replaced data greater than or equal to 0 with 1, and all other data with 0. For the sake of explanation, we only list the first 10 data in the table; all data were in 1.0e+003 units. In this way, we obtained a set of DTCWT-DCT low-frequency coefficient symbol sequences of the original image, i.e., '1100010010'. As seen from Table 1, after transformation, the symbol sequences of all attacked images were consistent with the original image, and the NC values were all equal to 1.00.

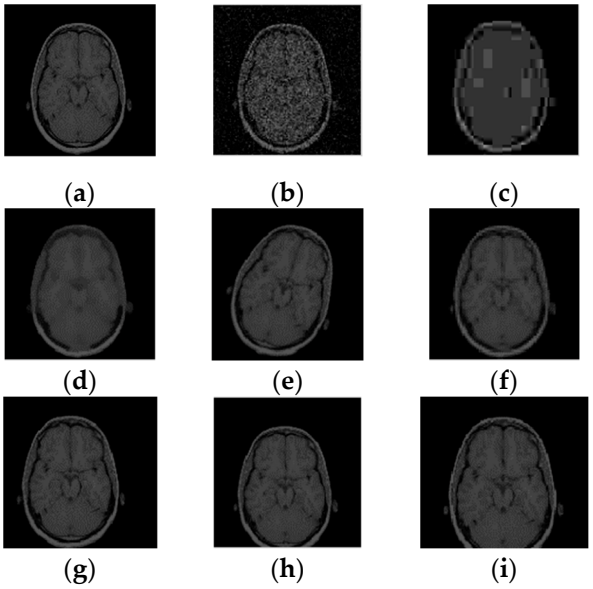


Figure 7. Different attacks on the brain: (**a**) Original image; (**b**) Gaussian noise (1%); (**c**) JPEG compression (4%); (**d**) Median filter [3 × 3] (10 times); (**e**) Rotation (clockwise, 20°); (**f**) Scaling (×0.5); (**g**) Translation (5%, left); (**h**) Translation (7%, down); (**i**) Cropping (10%, Y direction).

Table 1. Changes of DTCWT-DCT coefficients under different attacks for the original image.

Image Processing	PSNR (dB)	O (1,1)	O (1,2)	O (1,3)	O (1,4)	O (1,5)	O (1,6)	O (1,7)	O (1,8)	O (1,9)	O (1,10)	Sequence of Coefficient Signs	NC
Original image	/	3.1649	0.0638	−2.6346	−0.6947	−0.0089	0.4841	−1.3026	−0.0307	0.7381	−0.0505	1100010010	1.00
Gaussian noise (1%)	12.32	3.9336	0.0556	−2.1852	−0.5869	−0.0237	0.4020	−1.0897	−0.0284	0.6235	−0.0657	1100010010	1.00
JPEG compression (4%)	17.61	3.2728	0.0950	−2.3404	−0.5863	−0.0078	0.3856	−1.1486	−0.0304	0.5993	−0.1025	1100010010	1.00
Median filter [3,3] (10 times)	21.85	3.1894	0.0603	−2.6947	−0.7458	−0.0105	0.5370	−1.3083	−0.0270	0.7627	−0.0565	1100010010	1.00
Rotation (clockwise, 20°)	12.38	3.1646	0.3167	−2.4485	−0.6399	−0.4100	0.3595	−1.4398	−0.0410	0.8207	−0.0261	1100010010	1.00
Scaling (×0.5)	/	1.5867	0.0325	−1.3179	−0.3473	−0.0045	0.2412	−0.6513	−0.0157	0.3664	−0.0258	1100010010	1.00
Translation (5%, left)	11.38	3.1649	0.7388	−2.4519	−0.6947	−0.1520	0.4520	−1.3026	−0.2903	0.6846	−0.0505	1100010010	1.00
Translation (7%, down)	12.20	3.0723	0.0611	−2.5176	−1.2228	−0.0188	0.8428	−1.1085	−0.0297	0.7524	−0.0317	1100010010	1.00
Cropping (10%, Y direction)	/	3.1502	0.0660	−2.5637	−1.0598	−0.0196	0.6615	−0.9665	−0.0226	0.6086	−0.1695	1100010010	1.00

Then, taking this conclusion as a reference, we conducted the same test on a large number of randomly selected medical images, and verified the value of the normalized correlation coefficient between the images using their respective 32-bit symbol vectors. Figure 8 and Table 2 show some of the medical images and the NC values between them. From the data, it can be concluded that the NC values of the different images obtained using the feature vector selected with the above method are all less than 0.5, and their own NC values are 1.00. These results are consistent with human visual features. Therefore, we can take the sequence of coefficient symbols in the low-frequency part of the medical image transformed by DTCWT-DCT as its effective visual feature vector, and correlate the watermarks with it to design the multi-watermarking algorithm.

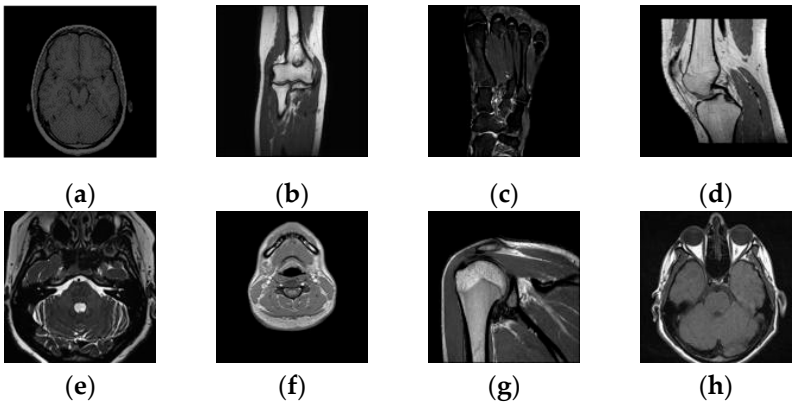


Figure 8. Some tested images: (**a**) Brain; (**b**) Elbow; (**c**) Foot; (**d**) Knee; (**e**) Internal auditory canal; (**f**) Neck; (**g**) Shoulder; (**h**) Orbits.

Table 2. Values of the correlation coefficients between different images (32 bit).

Image	Brain	Elbow	Foot	Knee	Internal Auditory Canal	Neck	Shoulder	Orbits
Brain	1.00	0.13	0.25	−0.07	0.06	−0.04	0.45	0.31
Elbow	0.13	1.00	0.25	−0.19	0.44	0.19	0.06	0.06
Foot	0.25	0.25	1.00	0.19	0.06	0.32	0.19	0.19
Knee	−0.07	−0.19	0.19	1.00	−0.25	0.27	0.25	−0.00
Internal auditory canal	0.06	0.44	0.06	−0.25	1.00	0.27	0.00	−0.25
Neck	−0.04	0.19	0.32	0.27	0.27	1.00	0.37	−0.24
Shoulder	0.45	0.06	0.19	0.25	0.00	0.37	1.00	−0.25
Orbits	0.31	0.06	0.19	−0.00	−0.25	−0.24	−0.25	1.00

3.2. Watermarks Pretreatment

Before embedding the watermark, henon chaos must be applied, and a preprocessing operation is carried out to obtain the watermark of chaotic encryption. Figure 9 shows the steps of watermarks pretreatment.

- Step 1: Choose the initial values x_0, x_1, x_2 to create chaotic sequences $X_n(j)$, and get binary encryption matrixes $C_n(i,j)$ via symbolic operations. Instead the values of $X_n(j)$ with '1' if they are bigger than the average, and instead with '0' if smaller.
- Step 2: Obtain the encrypted watermarks $BW_n(i,j)$ by operating the binary watermarks $W_n(i,j)$ and the binary encryption matrixes $C_n(i,j)$ through the hash function.

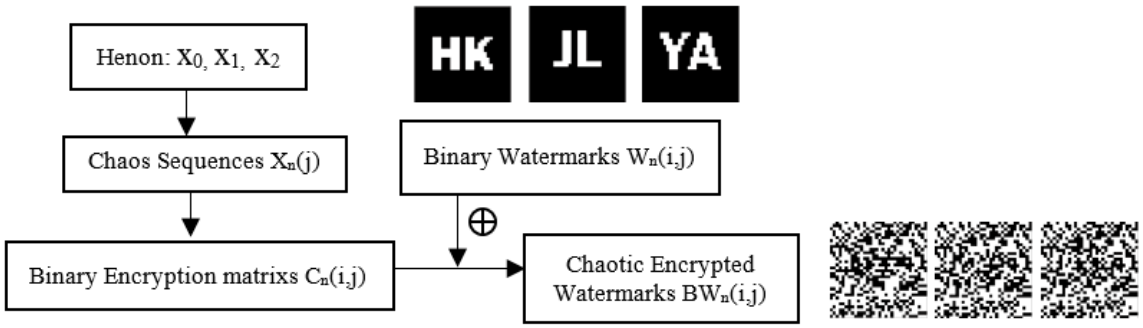


Figure 9. Watermarks pretreatment scheme.

3.3. Watermarks Embedding

- Step 3: Extract the feature vector $VF(j)$ using DTCWT-DCT transform on the original image $Oi(i,j)$, using the feature extraction method above.
- Step 4: Generate binary henon sequences $Key_n(i,j)$ with the following operation:

$$Key_n(i,j) = VF(j) \oplus BW_n(i,j) \tag{3}$$

Figure 10 illustrates this process.

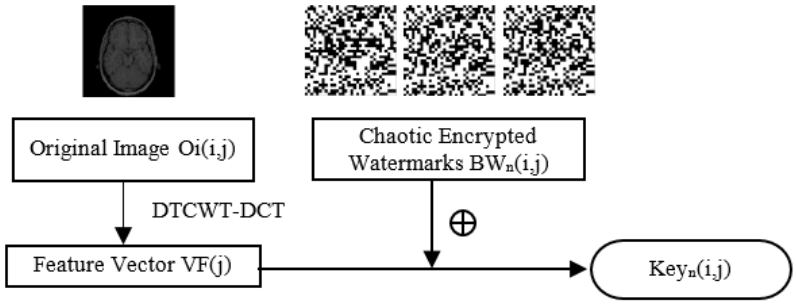


Figure 10. Watermarks embedding algorithm.

3.4. Watermarks Extraction

- Step 5: Apply the same operation as step 3 to the tested image $Oi\prime(i,j)$ to get a feature vector $VF\prime(j)$.
- Step 6: Extract the watermarks $BW_n\prime(i,j)$ via the following operate:

$$BW_n\prime(i,j) = Key_n(i,j) \oplus VF\prime(j) \tag{4}$$

Figure 11 shows the extraction algorithm.

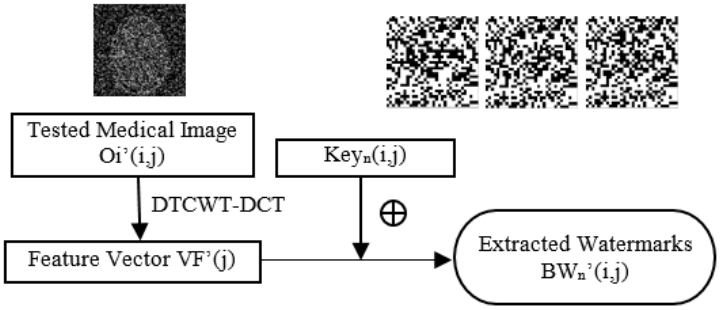


Figure 11. Watermarks extraction algorithm.

3.5. Watermarks Restoration

- Step 7: The chaotic sequences $X_n(j)$ and binary encryption matrixes $C_n(i,j)$ are obtained according to the method of step 1.
- Step 8: Restore the extracted watermarks $W_n\prime(i,j)$ through the following operation (as shown in Figure 12).

$$W_n\prime(i,j) = C_n(i,j) \oplus BW_n\prime(i,j) \tag{5}$$

Then, the ownership of the image to be tested and the patient's personal information were determined according to the correlation degree of $W_n(i,j)$ and $W_n\prime(i,j)$.

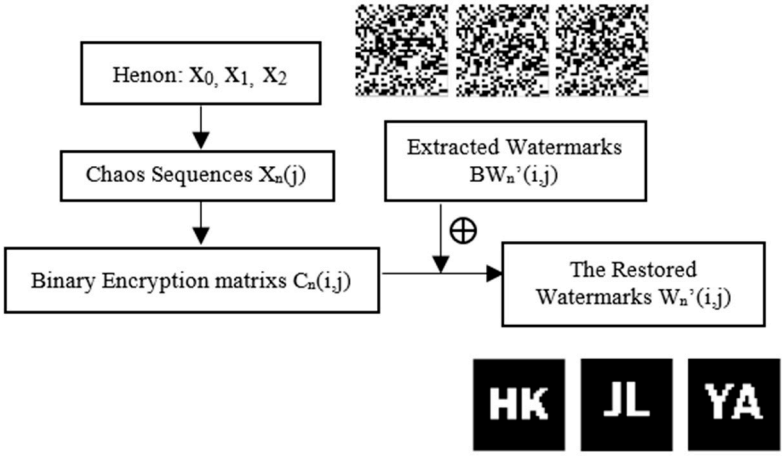


Figure 12. Watermarks restoration algorithm.

4. Experiment and Analysis

In the experiment, we used Matlab 2016a as the test platform, and took the randomly selected medical image 'brain' of Figure 8 as the original image, which is the tenth slice of a medical volume data. We also used three meaningful images as the original watermarks. Three groups of different initial values of henon chaos were selected to verify the robustness of the proposed algorithm and its ability to resist conventional and geometric attacks. Figure 13 shows the encrypted watermarks effect and the watermarked brain image. We observed that the brain image remained the same before and after embedding the watermark. It used the image feature vector associated with the watermarks to conduct the watermark embedding and extraction without any modifications to the original image, which strictly guaranteed the requirement of ROI sensitivity for medical images. However, the encrypted watermarks changed greatly, and could hardly be identified with the naked eye, which improves security. Figure 14 shows the extracted watermarks. They can be extracted precisely without any attacks, and the NC values are all 1.00. The watermarked images under various attacks are discussed in detail below. For the convenience of illustration, although we used all the images in Figure 8 throughout the experiment, we only used the 'brain' image to illustrate the test results of the proposed algorithm.

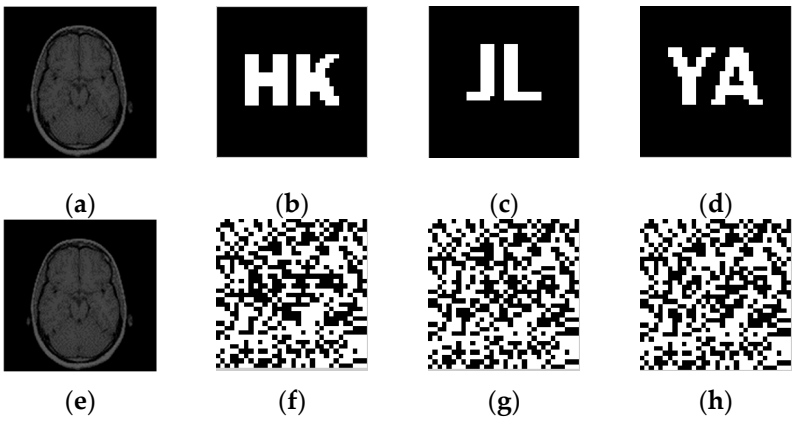


Figure 13. Watermarked medical image and encrypted watermarks: (**a**) Original medical image; (**b**) Original binary watermark 1; (**c**) Original binary watermark 2; (**d**) Original binary watermark 3; (**e**) watermarked medical image; (**f**) encrypted watermark 1; (**g**) encrypted watermark 2; (**h**) encrypted watermark 3.

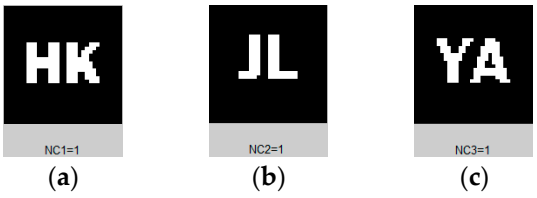


Figure 14. The extracted watermarks without attack: (**a**) extracted watermark 1; (**b**) extracted watermark 2; (**c**) extracted watermark 3.

4.1. Conventional Attacks

4.1.1. Gaussian Noise Attacks

We add different degrees of noise to the watermarked image, as shown in Figure 15 and Table 3. When the intensity is below 15%, the average NC value of the extracted watermarks is 0.92. Even if the noise intensity is as high as 25% and the image is severely distorted, the average NC value of the watermarks extracted can also reach 0.85.

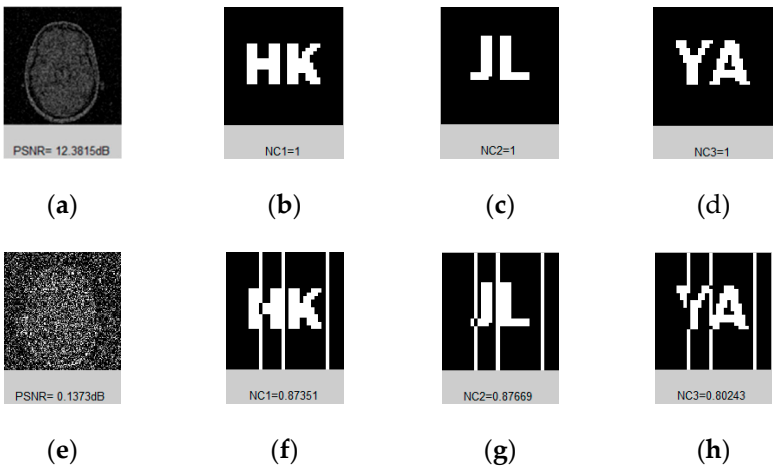


Figure 15. Under Gaussian noise attacks: (**a**) Gaussian noise level of 1%; (**b**) the extracted watermark 1 with a Gaussian noise level of 1%; (**c**) the extracted watermark 2 with a Gaussian noise level of 1%; (**d**) the extracted watermark 3 with a Gaussian noise level of 1%; (**e**) Gaussian noise level of 25%; (**f**) the extracted watermark 1 with a Gaussian noise level of 25%; (**g**) watermark 2 with a Gaussian noise level of 25%; (**h**) watermark 3 with a Gaussian noise level of 25%.

Table 3. Data of Gaussian noise attacks.

Gaussian Noise (%)	1	5	10	15	20	25
PSNR (dB)	12.38	5.93	3.21	1.80	0.75	0.14
NC1	1.00	0.95	0.95	0.93	0.87	0.87
NC2	1.00	0.97	0.97	0.93	0.90	0.88
NC3	1.00	0.96	0.96	0.91	0.87	0.80

4.1.2. JPEG Attacks

For medical images, compression mainly shows three indicators: first, the compression ratio should be large and the compression efficiency should be high; second, the calculation speed should be fast; third, the reliability of medical image must be ensured. As the currently international compression standard, JPEG compression is widely used in watermarking [1,2,7–9]. In the watermarking field, many scholars used JPEG attacks [8–10,13,14,18,19,21,22]. High-intensity JPEG compression may be applied to watermarking images. As shown in Figure 16 and Table 4, the NC value remains at 1.00 when compressed to 40% of the original image. It had a strong patch effect when compressed to 4% of the original image, but the average NC was still as high as 0.78.

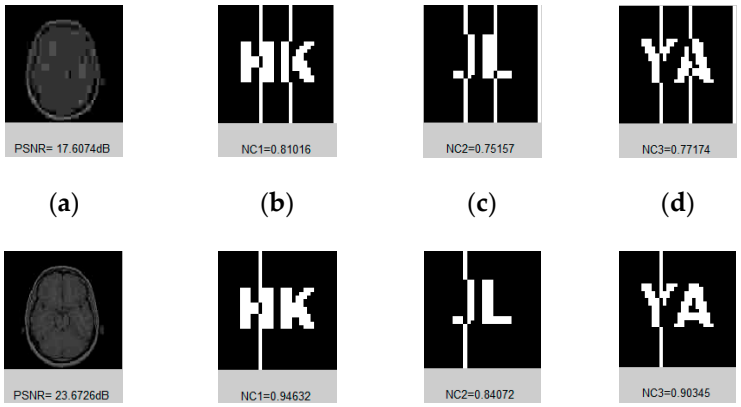


Figure 16. Under JPEG attacks: (**a**) Compression quality set to 4%; (**b**) the extracted watermark 1 with compression quality set to 4%; (**c**) the extracted watermark 2 with compression quality set to 4%; (**d**) the extracted watermark 3 with compression quality set to 4%; (**e**) Compression quality set to 25%; (**f**) the extracted watermark 1 under compression quality set to 25%; (**g**) the extracted watermark 2 under compression quality set to 25%; (**h**) the extracted watermark 3 under compression quality set to 25%.

Table 4. Data of JPEG attacks.

Compression Quality (%)	4	8	15	25	30	40
PSNR (dB)	17.61	19.99	22.01	23.67	24.29	25.06
NC1	0.81	0.95	0.76	0.95	0.90	1.00
NC2	0.75	0.97	0.70	0.84	0.95	1.00
NC3	0.77	0.96	0.66	0.90	0.90	1.00

4.1.3. Median Filter Attacks

We applied median filtering attacks of [3,3], [5,5], [9,9] to our watermarked image 1, 10, and 20 times, as shown in Figure 17 and Table 5. With the increase of the intensity of the attack, the PSNR values gradually decreased, and the image was blurred and became indistinguishable. However, the median filter was 9×9, and after 20 repetitions, and the NC value remained above 0.68.

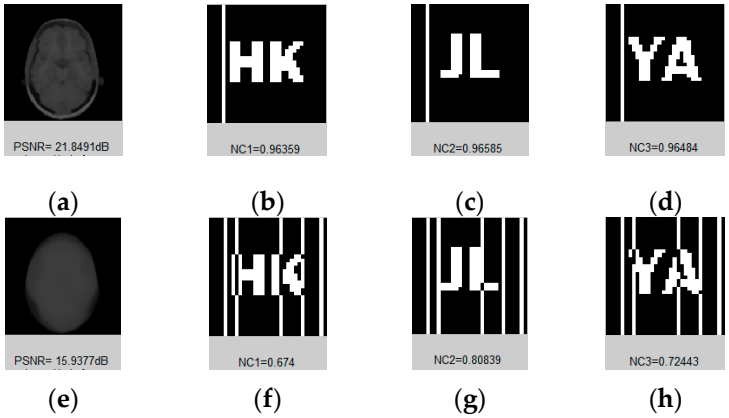


Figure 17. Under Median Filter attacks: (**a**) Median Filter [3 × 3] with 10 repetitions; (**b**) the extracted watermark 1 under median filter [3,3] with 10 repetitions; (**c**) the extracted watermark 2 under median filter[3,3] with 10 repetitions; (**d**) the extracted watermark 3 under median filter [3,3] with 10 repetitions; (**e**) Median Filter [9,9] Repeat times 10; (**f**) the extracted watermark 1 under median filter [9,9] with 10 repetitions; (**g**) the extracted watermark 2 under median filter [9,9] with 10 repetitions; (**h**) the extracted watermark 3 under median filter[9,9] with 10 repetitions.

Table 5. Data of Median Filter attacks.

Median Filter	**[3,3]**			**[5,5]**			**[9,9]**		
Repeat Times	**1**	**10**	**20**	**1**	**10**	**20**	**1**	**10**	**20**
PSNR (dB)	24.52	21.85	21.30	20.44	18.28	17.73	16.90	15.94	15.71
NC1	0.95	0.96	0.93	0.96	0.81	0.71	0.81	0.67	0.60
NC2	0.97	0.97	0.93	0.97	0.88	0.84	0.75	0.81	0.77
NC3	0.96	0.96	0.93	0.96	0.83	0.76	0.77	0.72	0.66

4.2. Geometrical Attacks

4.2.1. Rotation Attacks

The watermarked image is rotated by 5 degrees each time. It can be seen from Figure 18 and Table 6 that the average NC value of extracted watermarks was very high. When rotating 45 degrees, it can still reach 0.64.

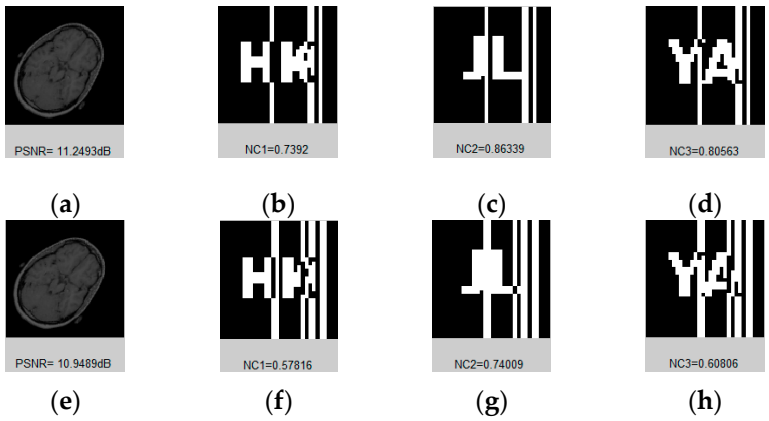


Figure 18. Under rotation attacks: (**a**) Rotation (clockwise) 40°; (**b**) the extracted watermark 1 under rotation (clockwise) 40°; (**c**) the extracted watermark 2 under rotation (clockwise) 40°; (**d**) the extracted watermark 3 under rotation (clockwise) 40°; (**e**) Rotation (clockwise) 45°; (**f**) the extracted watermark 1 under rotation (clockwise) 45°; (**g**) the extracted watermark 2 under rotation (clockwise) 45°; (**h**) the extracted watermark 3 under rotation (clockwise) 45°.

Table 6. Data of rotation attacks.

Rotation (Clockwise)	5°	10°	15°	20°	25°	30°	40°	45°
PSNR (dB)	16.19	13.49	12.70	12.38	12.16	11.90	11.25	10.95
NC1	0.91	0.87	0.87	0.87	0.77	0.70	0.74	0.58
NC2	0.93	0.90	0.90	0.90	0.86	0.83	0.86	0.74
NC3	0.91	0.87	0.87	0.87	0.82	0.76	0.81	0.61

4.2.2. Scaling Attacks

Scale attacks were executed on the watermarked image with different scale factors. When the scaling factor was 0.5 and above 2.0, the NC value of the extracted watermarks were all 1.00. In the remaining cases, the NC values remained at 0.92. Even if the scaling factor was as low as 0.2, average NC values could still reach 0.64. Table 7 and Figure 19 show these data and part of the attack images.

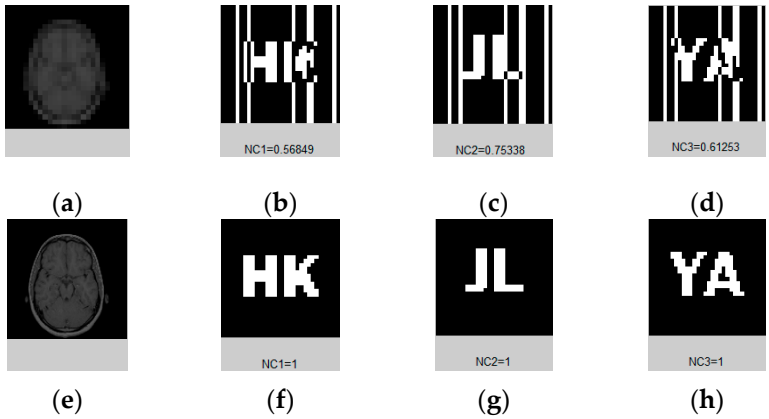


Figure 19. Under scaling attacks: (**a**) Scaling factor 0.2; (**b**) the extracted watermark 1 under scaling factor 0.2; (**c**) the extracted watermark 2 under scaling factor 0.2; (**d**) the extracted watermark 3 under scaling factor 0.2; (**e**) Scaling factor 8.0; (**f**) the extracted watermark 1 under scaling factor 8.0; (**g**) the extracted watermark 2 under scaling factor 8.0; (**h**) the extracted watermark 3 under scaling factor 8.0.

Table 7. Data of scaling attacks.

Scaling Factor	0.2	0.4	0.5	0.8	1.2	2.0	4.0	8.0
NC1	0.57	0.86	1.00	0.86	0.96	1.00	1.00	1.00
NC2	0.75	0.93	1.00	0.93	0.97	1.00	1.00	1.00
NC3	0.61	0.90	1.00	0.90	0.96	1.00	1.00	1.00

4.2.3. Translation Attacks

The watermarked image is moved down and left. When moved down by 22%, where the lower half of the image is lost, the extracted watermarks are still legible, and average NC values are still as high as 0.60. The average left-moving NC was 0.84. When moving left by 11%, the NC value was 0.69. Figure 20, Table 8, Figure 21 and Table 9 respectively show some test images and data moving down and left.

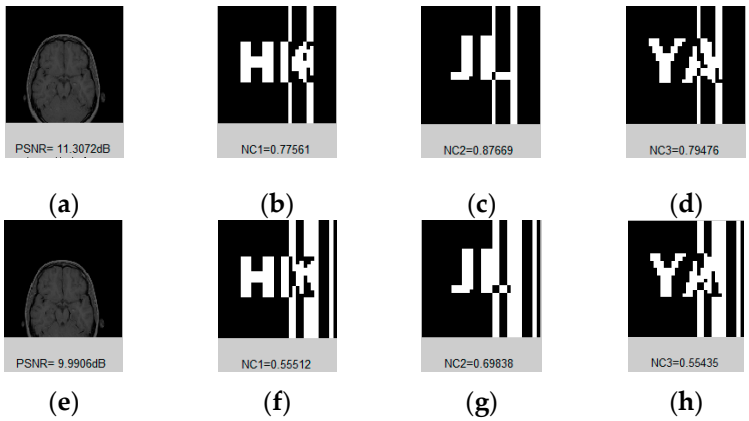


Figure 20. Under down translation attacks: (**a**) Down distance 12%; (**b**) the extracted watermark 1 under down distance 12%; (**c**) the extracted watermark 2 under down distance 12%; (**d**) the extracted watermark 3 under a down distance of 12%; (**e**) Down distance 22%; (**f**) the extracted watermark 1 under a down distance of 22%; (**g**) the extracted watermark 2 under a down distance of 22%; (**h**) the extracted watermark 3 under a down distance of 22%.

Table 8. Data of down translation attacks.

Down Distance (%)	2	4	8	12	13	15	18	22
PSNR1(dB)	15.33	12.59	11.96	11.31	11.20	10.83	10.32	9.99
NC1	1.00	0.85	0.85	0.78	0.74	0.68	0.59	0.56
NC2	1.00	0.91	0.91	0.88	0.84	0.79	0.73	0.70
NC3	1.00	0.86	0.86	0.79	0.76	0.68	0.59	0.55

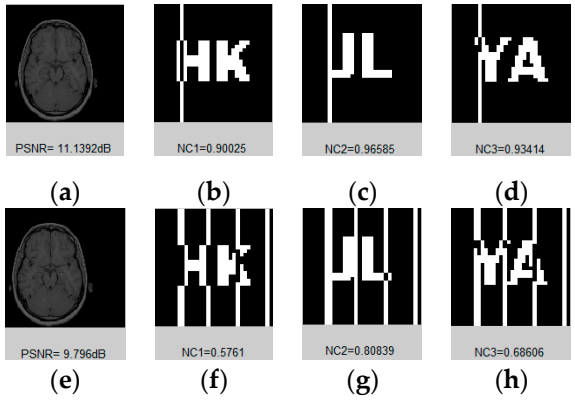


Figure 21. Under left translation attacks: (**a**) Left distance 7%; (**b**) the extracted watermark 1 under left distance 7%; (**c**) the extracted watermark 2 under left distance 7%; (**d**) the extracted watermark 3 under a left distance of 7%; (**e**) Left distance 11%; (**f**) the extracted watermark 1 under a left distance of 11%; (**g**) the extracted watermark 2 under a left distance of 11%; (**h**) the extracted watermark 3 under a left distance of 11%.

Table 9. Data of left translation attacks.

Left Distance (%)	3	5	7	8	9	10	11
PSNR2(dB)	12.28	11.38	11.14	10.80	10.56	10.31	9.80
NC1	0.90	0.90	0.90	0.58	0.58	0.58	0.58
NC2	0.97	0.97	0.97	0.81	0.81	0.81	0.81
NC3	0.93	0.93	0.93	0.69	0.69	0.69	0.69

4.2.4. Cropping Attacks

In order to verify the robustness of the watermarked image to cropping attacks, we designed an operation for y-coordinate extraction, gradually increasing its movement from 2 percent to 37 percent. According to the data in Figure 22 and Table 10, when the image is cropped from 2% to 23%, its NC value is basically 1.00. When the image is cropped by about two-fifths, the average NC value of the extracted watermarks can still reach 0.59. The extracted watermarks can be identified by the naked eye.

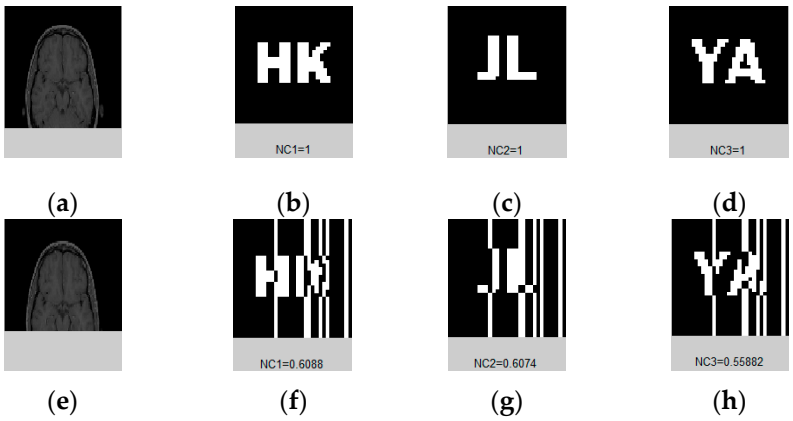


Figure 22. Under cropping attacks: (**a**) Cropping 23%, Y direction; (**b**) the extracted watermark 1 under 23% cropping; (**c**) the extracted watermark 2 under 23% cropping; **(d)** the extracted watermark 3 under 23% cropping; (**e**) Cropping 37%, Y direction; (**f**) the extracted watermark 1 under 37% cropping; (**g**) the extracted watermark 2 under 37% cropping; (**h**) the extracted watermark 3 under 37% cropping.

Table 10. Data of cropping attacks.

Cropping (%) Y Direction	2	8	12	15	23	29	30	37
NC1	1.00	0.90	1.00	1.00	1.00	0.79	0.75	0.61
NC2	1.00	0.94	1.00	1.00	1.00	0.86	0.82	0.61
NC3	1.00	0.90	1.00	1.00	1.00	0.78	0.74	0.56

4.3. Algorithms Comparison

We compared the average NC values of the watermarks using our proposed algorithm under different attacks with Aditi Zear et al. [18], Rohit Thanki et al. [19], Xiaochen Yuan et al. [21] and Amit Kumar Singh et al. [22]. It can be clearly seen from Figure 23 and Table 11 that under conventional attacks, the NC values of the proposed algorithm are significantly higher than the those of the other four algorithms. Figure 24 and Table 12 show the performance of the watermarks under geometric attacks. Observing these data, we can see that with the increase of the attack intensity, the NC values of all of them showed a downward trend. And under cropping attacks, left translation attacks and down translation attacks, our algorithm has obvious advantages over other algorithms in terms of NC values. Figure 24 illustrates that compared with the multi-watermarking scheme based on FDCuT-DCT proposed by Rohit Thanki et al. [19], the proposed algorithm performs slightly worse in rotation (clockwise) attacks. But their NC values are not much different and performance in other geometric attacks was significantly better than the latter. The watermark extraction effect under geometric attacks is generally better than that of Rohit Thanki et al. [19]. When performing scaling attacks, as shown in the radar chart in Figure 24, Amit Kumar Singh et al. [22] proposed the use of a spread spectrum multi-watermark in the wavelet transform domain. The NC values of this algorithm are basically equal to the NC values of our proposed algorithm under scaling attacks; they are only differ by 0.01. However, it is necessary to perform the spread spectrum operation on the wavelet transform, and the embedding of the watermark needs to select different transform layers according to different watermark types. Finally, multi-watermark embedding is achieved by the gain coefficient and the

wavelet decomposition level. Compared with our algorithm, the operation of this algorithm is complex, and it does not perform as well as our algorithm in other geometric attacks.

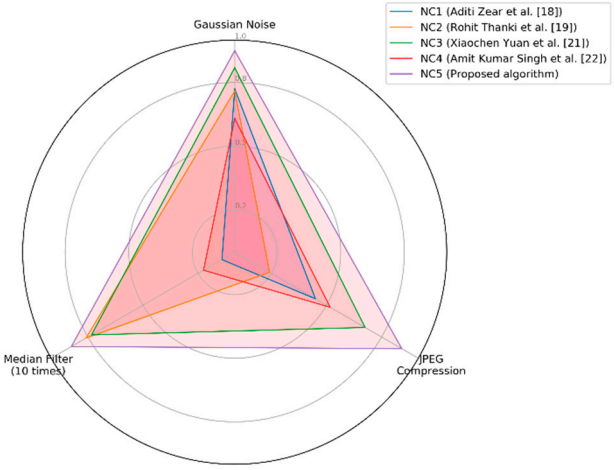


Figure 23. Radar chart of different algorithms under conventional attacks.

Table 11. Comparison values of different algorithms under conventional attacks.

Conventional Attacks	Intensity of Attacks	Aditi Zear et al. [18] NC1	Rohit Thanki et al. [19] NC2	Xiaochen Yuan et al. [21] NC3	Amit Kumar Singh et al. [22] NC4	Proposed Algorithm NC5
Gaussian Noise	1%	0.88	0.86	0.92	0.74	1.00
	10%	0.79	0.78	0.88	0.64	0.97
	25%	0.63	0.65	0.81	0.52	0.88
JPEG Compression	4%	0.11	−0.02	0.51	0.32	0.81
	8%	0.31	0.11	0.77	0.51	0.97
	25%	0.91	0.47	0.85	0.72	0.95
Median Filter (10 times)	[3,3]	0.15	0.91	0.89	0.22	0.97
	[5,5]	0.04	0.80	0.77	0.17	0.88
	[9,9]	0.01	0.72	0.69	0.11	0.81

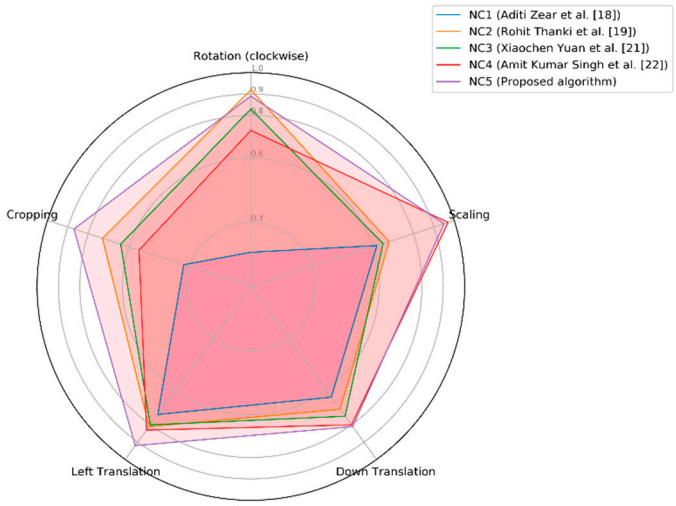


Figure 24. Radar chart of different algorithms under geometric attacks.

Table 12. Comparison values of different algorithms under geometric attacks.

Geometrical Attacks	Intensity of Attacks	Aditi Zear et al. [18] NC1	Rohit Thanki et al. [19] NC2	Xiaochen Yuan et al. [21] NC3	Amit Kumar Singh et al. [22] NC4	Proposed Algorithm NC5
Rotation (clockwise)	10°	0.21	0.88	0.86	0.85	0.90
	20°	0.17	0.92	0.84	0.81	0.90
	40°	0.10	0.95	0.80	0.53	0.86
Scaling	0.4	0.39	0.52	0.59	0.93	0.93
	0.8	0.54	0.61	0.63	0.99	0.93
	2.0	0.92	0.91	0.74	0.99	1.00
Down Translation	8%	0.73	0.80	0.86	0.90	0.91
	15%	0.66	0.69	0.77	0.79	0.80
	20%	0.54	0.63	0.61	0.71	0.71
Left Translation	3%	0.77	0.88	0.90	0.91	0.97
	5%	0.74	0.84	0.83	0.81	0.97
	8%	0.70	0.72	0.66	0.77	0.81
Cropping	12%	0.76	0.95	0.97	0.88	1.00
	23%	0.21	0.92	0.92	0.64	1.00
	35%	0.03	0.33	0.02	0.14	0.61

Therefore, the algorithm presented in this paper is outstanding in all kinds of attack situations, especially so in solving the problem that existing algorithms cannot balance resistance to geometric attacks and robustness. It has strong resistance to geometric attacks and shows a good level of robustness.

5. Conclusions

This paper proposes a new, robust, multi-watermarking algorithm for medical images based on DTCWT-DCT and a henon Map, which combines encryption technology, transform domains perception of the low frequency coefficient invariance and the zero-watermarking concept. It uses a robust multi-watermark which effectively increases the watermark's capacity to embed medical images, and reduces the complexity of the algorithm. The security of watermarks is enhanced by using henon chaotic encryption. When embedding and extracting watermarks, it is unnecessary to select the region of interest in advance. The experimental data show that the proposed method not only improves the security of the watermark's information, but also has a good level of robustness against both conventional and geometric attacks without affecting the quality of the original medical image. The proposed method can be used for medical security, cloud storage and cloud transmission, security authentication, etc.

Author Contributions: Conceptualization, N.S.; Data curation, J.L. (Jing Liu), U.A.B. and Y.A.; Formal analysis, J.L. (Jing Liu); Funding acquisition, J.L. (Jingbing Li); Investigation, J.M.; Methodology, J.L. (Jing Liu) and J.L. (Jingbing Li); Project administration, N.S.; Software, U.A.B. and Y.A.; Visualization, N.S. and Y.A.; Writing—original draft, J.L. (Jing Liu); Writing—review & editing, J.M.

Funding: This work is supported by the Key Research Project of Hainan Province (ZDYF2018129), the National Natural Science Foundation of China (No. 61762033), the Hainan Provincial Higher Education Research Project (Hnky2019-73) and the Key Research Project of Haikou College of Economics (HJKZ18-01).

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

References

1. Qasim, A.F.; Meziane, F.; Aspin, R. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Comput. Sci.* **2018**, *27*, 45–60. [CrossRef]
2. Zhen, Y.; Li, Z.C.; Ren, H.; Yang, Y.X. A Large Capacity Histogram-Based Watermarking Algorithm for Three Consecutive Bins. *Appl. Sci.* **2018**, *8*, 2617.
3. Sk, A.; Masilamani, V. A novel digital watermarking scheme for data authentication and copyright protection in 5g networks. *Comput. Electr. Eng.* **2018**, *72*, 589–605. [CrossRef]

4. Cox, I.J.; Miller, M.L. The first 50 years of electronic watermarking. *EURASIP J. Adv. Signal Process.* **2002**, *2*, 126–132. [CrossRef]
5. Mousavi, S.M.; Naghsh, A.; Abu-Bakar, S.A.R. Watermarking techniques used in medical images: A survey. *J. Digit. Imaging* **2014**, *27*, 714–729. [CrossRef] [PubMed]
6. Nyeem, H.; Boles, W.; Boyd, C. A review of medical image watermarking requirements for teleradiology. *J. Digit. Imaging* **2013**, *26*, 326–343. [CrossRef]
7. Atta-ur-Rahman; Mahmud, M.; Sultan, K.; Aldhafferi, N.; Alqahtani, A.; Musleh, D. Medical Image Watermarking for Fragility and Robustness: A chaos, error correcting codes and redundant residue number system based approach. *J. Med. Imaging Health Inform.* **2018**, *8*, 1192–1200.
8. Abokhdair, N.O.; Abd Manaf, A.; Alfagi, A.; Ab Sultan, M.; Mousavi, S.M.; Abd Manaf, Z.; Mohamad, F.S. Patient data hiding and integrity control using prediction-based watermarking for brain MRI and CT scan images. *J. Med. Imaging Health Inform.* **2018**, *8*, 691–702. [CrossRef]
9. Parah, S.A.; Sheikh, J.A.; Ahad, F.; Loan, N.A.; Bhat, G.M. Information hiding in medical images: A robust medical image watermarking system for e-healthcare. *Multimed. Tools Appl.* **2017**, *76*, 10599–10633. [CrossRef]
10. Thanki, R.; Borra, S.; Dwivedi, V.; Borisagar, K. A roni based visible watermarking approach for medical image authentication. *J. Med. Syst.* **2017**, *41*, 143. [CrossRef]
11. Zhang, Z.; Wu, L.; Li, H.; Lai, H.; Zheng, C. Dual watermarking algorithm for medical image. *J. Med. Imaging Health Inform.* **2017**, *7*, 607–622. [CrossRef]
12. Taher, F.; Kunhu, A.; Alahmad, H. A new hybrid watermarking algorithm for MRI medical images using DWT and hash functions. In Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Orlando, FL, USA, 16–20 August 2016; pp. 1212–1215.
13. Jamali, M.; Samavi, S.; Karimi, N.; Soroushmehr, S.M.; Ward, K.; Najarian, K. Robust watermarking in non-ROI of medical images based on DCT-DWT. In Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Orlando, FL, USA, 16–20 August 2016.
14. Arsalan, M.; Qureshi, A.; Khan, A.U.; Rajarajan, M. Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Appl. Soft Comput.* **2017**, *51*, 168–179. [CrossRef]
15. Vishakha, K.; Kushal, T.; Hitesh, N. Novel variants of a histogram shift-based reversible watermarking technique for medical images to improve hiding capacity. *J. Healthc. Eng.* **2017**, *6*. [CrossRef]
16. Turuk, M.P.; Dhande, A.P. A novel reversible multiple medical image watermarking for health information system. *J. Med. Syst.* **2016**, *40*, 269–279. [CrossRef] [PubMed]
17. Lei, B.; Tan, E.L.; Chen, S.; Ni, D.; Wang, T.; Lei, H. Reversible watermarking scheme for medical image based on differential evolution. *Expert Syst. Appl.* **2014**, *41*, 3178–3188. [CrossRef]
18. Zear, A.; Singh, A.K.; Kumar, P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed. Tools Appl.* **2018**, *77*, 4863–4882. [CrossRef]
19. Thanki, R.; Borra, S.; Dwivedi, V.; Borisagar, K. An efficient medical image watermarking scheme based on FDCuT-DCT. *Eng. Sci. Technol.* **2017**, *20*, 1366–1379. [CrossRef]
20. Wang, J.W.; Lian, S.G.; Shi, Y.Q. Hybrid multiplicative multi-watermarking in DWT domain. *Multidimens. Syst. Signal Process.* **2017**, *28*, 617–636. [CrossRef]
21. Yuan, X.C.; Li, M. Local multi-watermarking method based on robust and adaptive feature extraction. *Signal Process.* **2018**, *149*, 103–117. [CrossRef]
22. Singh, A.K.; Kumar, B.; Dave, M.; Mohan, A. multiple watermarking on medical images using selective discrete wavelet transform coefficients. *J. Med. Imaging Health Inform.* **2015**, *5*, 607–614. [CrossRef]
23. Yang, P.; Yang, G. Statistical model and local binary pattern based texture feature extraction in dual-tree complex wavelet transform domain. *Multidimens. Syst. Signal Process.* **2018**, *29*, 851–865. [CrossRef]
24. Jung, C.; Yang, Q.; Sun, T.; Fu, Q.; Song, H. Low light image enhancement with dual-tree complex wavelet transform. *J. Vis. Commun. Image Represent.* **2017**, *42*, 28–36. [CrossRef]
25. Sheela, S.J.; Suresh, K.V.; Tandur, D. Image encryption based on modified Henon map using hybrid chaotic shift transform. *Multimed. Tools Appl.* **2018**, *77*, 25223–25251. [CrossRef]

26. Roy, A.; Misra, A.P. Audio signal encryption using chaotic Henon map and lifting wavelet transforms. *Eur. Phys. J. Plus* **2017**, *132*, 524–624. [CrossRef]
27. Yan, T.; Liu, F.X.; Chen, B. New Particle Swarm Optimisation Algorithm with Henon Chaotic Map Structure. *Chin. J. Electron.* **2017**, *26*, 747–753. [CrossRef]