electronics

MDPI

Article

A Reversible Watermarking System for Medical Color Images: Balancing Capacity, Imperceptibility, and Robustness

Xiaoyi Zhou [1,*,†], Yue Ma [1,†], Qingquan Zhang [1], Mazin Abed Mohammed [2] and Robertas Damaševičius [3,*]

[1] School of Cyberspace Security, Hainan University, Haikou 570228, China; mayuexxaq@126.com (Y.M.); 20182581310162@hainanu.edu.cn (Q.Z.)
[2] Information Systems Department, College of Computer Science and Information Technology, University of Anbar, Ramadi 31001, Iraq; mazinalshujeary@uoanbar.edu.iq
[3] Faculty of Applied Mathematics, Silesian University of Technology, 44-100 Gliwice, Poland
* Correspondence: xy.zhou.xy@gmail.com (X.Z.); robertas.damasevicius@polsl.pl (R.D.)
† These authors contribute equally to this paper and should be considered co-first authors.

Abstract: The authenticity and integrity of medical images in telemedicine has to be protected. Robust reversible watermarking (RRW) algorithms provide copyright protection and the original images can be recovered at the receiver's end. However, the existing algorithms have limitations in their ability to balance the tradeoff among robustness, imperceptibility, and embedded capacity. Some of them are even not completely reversible. Besides, most medical image watermarking algorithms are not designed for color images. To improve their performance in protecting medical color image information, we propose a novel RRW scheme based on the discrete wavelet transform (DWT). First, the DWT provides a robust solution. Second, the modification of the wavelet domain coefficient guarantees the changes of integer values in the spatial domain and ensures the reversibility of the watermarking scheme. Third, the embedding scheme makes full use of the characteristics of the original image and watermarking. This reduces the modification of the original image and ensures better imperceptibility. Lastly, the selection of the Zernike moments order for geometric correction is optimized to predict attack parameters more accurately by using less information. This enhances the robustness of the proposed scheme against geometric attacks such as rotation and scaling. The proposed scheme is robust against common and geometric attacks and has a high embedding capacity without obvious distortion of the image. The paper contributes towards improving the security of medical images in remote healthcare.

Keywords: reversible watermarking; zernike moment; geometric attacks; medical images; telemedicine

check for updates

Citation: Zhou, X.; Ma, Y.; Zhang, Q.; Mohammed, M.A.; Damaševičius, R. A Reversible Watermarking System for Medical Color Images: Balancing Capacity, Imperceptibility, and Robustness. *Electronics* **2021**, *10*, 1024. https://doi.org/10.3390/electronics10091024

Academic Editor: Frederic Ros

Received: 24 March 2021
Accepted: 22 April 2021
Published: 25 April 2021

1. Introduction

The technical revolution associated with the implementation the development of digital technologies in medicine, has led to the emergence and active development of new directions in many areas of medicine. In the last years, medical organizations are actively introducing new communication technologies to optimize the process of diagnostics and receive verified diagnosis such as telemedicine technology [1,2]. The applications of telemedicine include disease management [3], emergency medicine [4], home health care [5], long-term (chronic) care [6], prevention [7], remote medical imaging [8], and many other applications [9]. The use of telemedicine has especially risen since the start of COVID-19 pandemic [10,11].

The use of telemedicine services includes the transmission of private patient's data such as medical examination data and medical images over communication networks. This raises the security and privacy concerns. Poor security measures and error of transmission in telehealth services can have a negative impact on the quality of healthcare [12]. Concerns about the security and privacy of telemedicine systems may negatively affect the trust of patients in telehealth technology and diminish the accessibility and effectiveness of healthcare services in general [13]. The transmission of sensitive patient data such as medical images or medical videos requires the use of cryptographic encryption methods [14,15] and secure transmission protocols [16,17].

Recently, the copyright of medical images has attracted researchers' attention [18,19]. Digital watermarking is one of the prevalent techniques to protect the ownership of images [20–23]. However, the performance of watermarking schemes is constrained by their robustness, imperceptibility, and embedding capacity [24,25]. A medical image watermarking scheme must be distortion-free because any small distortion can lead to misdiagnosis and threaten the patient's life [26,27]. As medical images are highly sensitive to visual quality, most of the copyright protection algorithms use reversible embedding strategies. This approach ensures that after the watermarking is extracted, the medical image can be fully restored [28–31]. For example, Coatrieux et al. [32] combine the reversible watermark scheme with a fragile reversible watermark embedding scheme. They use the histogram shift method for prediction error, which takes advantage of the local characteristics of the image. It improves not only the embedded capacity of the watermark but also the visual quality of the image. They also propose a classification process to select parts of the image that can be embedded in the watermark. However, the above reversible schemes are fragile. Their watermarks are embedded in the space domain and any slight disturbance to the image causes the failure of the watermark extraction process. This limits their application in practice.

Robust watermarking algorithms can better solve the above problems [33]. Therefore, the design of robust and reversible watermarking for images has broad applicability in military, medical and judicial fields that are sensitive. From the perspective of the embedding domain, robust reversible watermarking technology can be divided into spatial and transform watermarking. An et al. [34] proposed an algorithm based on wavelet domain histogram aggregation and translation, and embeds watermarks by selecting thresholds. After the watermark information is embedded, the area of the histogram aggregation changes, according to which the watermark information can be extracted separately. To balance robustness and imperceptibility, the authors quantitatively analyzed the two indicators. According to the human vision system (HVS), the image quality is evaluated by the Just Noticeable Distortion (JND) method, and the strength of a watermark information pair is selected according to the result. As a result, the carrier image can maintain a high level of visual quality after embedding the watermark information. Thabit et al. [35] transformed the original image block with a Slantlet transform matrix and modify the mean value of the sub-band to embed the watermark. A histogram modification process is adopted to avoid overflow and underflow. Compared with its previous scheme, it has improved robustness, imperceptibility, and capacity. It is completely reversible. Choi et al. [36] apply a bit plane manipulation to hide information on bit-planes that are less affected by attacks, and use region filtering to select the block with a lower variance to embed watermarks. This approach improves the algorithm's robustness. To prevent the overflow, one can embed the wrong bit information first, and then use correcting code (ECC) to correct it. Golabi et al. [37] developed non-unit mapped radial moments. Reversible interval phase modulation and diagonal rotation estimation are used to achieve robust geometrically invariant watermarking and reversible data hiding. The algorithm is robust to common attacks and geometric distortions. It also can keep the pixel values of the watermarked image as integers, which provides the possibility of image reversibility. Lei et al. [38] proposed a method based on recursive dither modulation. The watermark is embedded after the host image is transformed by integer wavelet transform and singular value decomposition.

From the above analysis, the current robust watermarking algorithms available in the literature cannot be directly applied to the field of reversible watermarking. The reason is that, after embedding the watermark in the transform domain and then obtaining the watermark image by an inverse transform, the pixel values may not be integers. This causes a certain amount of information loss, and the original image cannot be completely recovered after the watermark is extracted. Therefore, to make the watermark reversible, it is necessary to ensure that the host image changes with integer values in the spatial domain. Giakoumaki et al. [39] discussed the properties of the Haar wavelet transform. The coefficients generated by this transform are binary rational numbers, and their denominator is a power of 2. If the level of the transformation is l, then adding or subtracting 2^l from the coefficients of the l -level transformation can ensure the pixel values are integers after the discrete wavelet inverse transform. This guarantees the reversibility of the watermark. However, the above scheme does not strongly resist geometric attacks. To this end, we combine the invariance of Zernike moments as in [40] for rotation and scaling to solve this problem.

In general, the previous robust reversible watermarking schemes have the following issues:

(1) Some schemes are not completely reversible, especially those based on the transform domain. Because the mapping relationship between the spatial domain and the frequency domain is not considered, the watermarked image pixel values are not integers. This results in the image losing its reversible characteristics, as in [28]. Moreover, when the data set is large, reliability and stability remain problematic, resulting in some carrier images not being fully restored.

(2) Robustness is not strong enough generally. Applying an integer wavelet transform to achieve reversibility while reducing the running time has been reported [23,32]. However, the experimental evaluations revealed the approaches are very sensitive to various attacks [41]. Thus, the watermark cannot be extracted correctly when attacked.

(3) Most algorithms have limitations in balancing the contradiction between watermark embedding capacity and invisibility. For example, in [37] the PSNR is less than 45 dB after embedding 20,000 bits of watermark information. In other algorithms, the embedding capacity is sacrificed to reduce the image distortion [35,36].

(4) At present, most of the reversible medical image watermarking schemes are performed on grayscale images [42,43], and there is little research on color medical images. However, black-and-white medical images can undergo pseudo-color processing for density segmentation technology [44] so that the observer can obtain more information. This presents broad application prospects.

Our scheme improves the reversibility, robustness, imperceptibility, and embedding capacity of the watermark in a more comprehensive way. Firstly, to ensure reversibility, the values change in the spatial domain needs to be integers after modification. This can be achieved if the modification in the frequency domain is 2^l. Secondly, the imperceptibility is improved by combining the characteristics of the host image and the watermark. Thirdly, a hash code of the watermarked image is used to detect whether the image was tampered. Last, the invariance of Zernike moments for rotation, scaling, and translation transformation is applied to improve the order of the selected moment information. The experiments show that the scheme has strong robustness, the original image can be completely recovered under attack, and the embedding capacity reaches a very good level.

The novelty and contributions of this paper are as follows:

- A robust reversible watermarking scheme for medical color images using image block information to represent watermarks is proposed. The watermark embedding flag (WEF) and the embedding status flag (ESF) are set for each block, as well as for representing the watermark. This reduces the modification of the original image as much as possible and improves the imperceptibility.
- The hierarchical embedding strategy is adopted for the different value ranges of the embedding status flag to maximize the imperceptibility.
- The order of the Zernike moment that is stable and suitable for correction is selected through experiments, which improves the accuracy of geometric correction.

The rest of the paper is arranged as follows: Section 2 explains the principle of reversibility using the Haar wavelet transform and discusses the use of some Zernike moment coefficients for image correction. Section 3 elaborates the steps of embedding and extracting in the robust reversible watermarking scheme. Section 4 presents the experimental results of this scheme for watermark reversibility, robustness, imperceptibility, and embedding capacity. Section 5 provides the conclusion.

2. Preliminaries

2.1. Reversibility of the Haar Wavelet Transform (HWT)

The Haar transform is proposed in 1910 by the Hungarian mathematician Alfréd Haar. The Haar wavelet function is shown in Equation (1):

$$\varphi(x) = \phi(2x) - \phi(2x-1) \tag{1}$$

In Equation (1), the Haar scale function $\phi(x)$, which is also known as the parent wavelet, is defined as Equation (2):

$$\phi(x) = \begin{cases} 1,\ 0 \leq x < 1 \\ 0, otherwise \end{cases} \tag{2}$$

The Haar wavelet transform can be decomposed as follows. The original signal is sampled at the discrete point $x = \ldots - \frac{1}{2^i},\ 0,\ \frac{1}{2^i} \ldots$ And thus we obtain Equation (3)

$$a_k = f\left(\frac{k}{2^j}\right) \tag{3}$$

Equation (4) shows that the sampled original signal can be described entirely by the j-scale function

$$f_j(x) = \sum_{k \in Z} a_k^j \phi\left(2^j x - k\right) \tag{4}$$

It can be further decomposed into Equation (5)

$$f_j(x) = \sum_{k \in Z} \frac{a_{2k}^j - a_{2k+1}^j}{2} \varphi\left(2^{j-1}x - k\right) + \frac{a_{2k}^j + a_{2k+1}^j}{2} \phi\left(2^{j-1}x - k\right) \tag{5}$$

As can be seen from the formula, if the change to the coefficient is 2^j, the change in the spatial domain is still an integer, which ensures the reversibility of the watermarking scheme [39].

2.2. Zernike Moments

Zernike moments are continuous orthogonal moments, which are commonly used for image shape representation. The Zernike moment of order n and repetition m of a function $f(x,y)$ inside the unit circle is:

$$Z_{nm} = \frac{n+1}{\pi} \iint_{x^2+y^2<1} f(x,y)\ V_{nm}^*(x,y)\ dxdy \tag{6}$$

where n is a non-negative integer, m is an integer number such that $n - |m|$ is nonnegative and even, and $V_{nm}(x,y)$ is the complex function:

$$V_{nm}(x,y) = V_{nm}(\rho,\theta) = R_{nm}(\rho)e^{jm\theta} \tag{7}$$

where $R_{nm}(\rho)$ are the Zernike polynomials over the unit circle with ρ and θ as the polar coordinates as defined by Equation (8):

$$R_{nm}(\rho) = \sum_{s=0}^{\frac{n-|m|}{2}} \frac{(-1)^n[(n-s)!]\rho^{n-2s}}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!}\rho^{n-2s} \tag{8}$$

The Zernike moments of a discrete image $f(x,y)$ are calculated as follows:

$$Z_{nm} = \frac{n+1}{\pi}\sum_x\sum_y f(x,y)V^*_{nm}(x,y) \tag{9}$$

and $x^2+y^2 \leq 1$.

To restore the image back from its Zernike moments, Equation (10) is used:

$$f'(x,y) = \sum_n\sum_m Z_{nm}V_{nm}(x,y) \tag{10}$$

2.2.1. Rotation Detection

The relationship between the original color image and the image rotated by θ is defined by Equation (11)

$$Z'^{R}_{nm} = Z^{R}_{nm}e^{-\mu m\theta} \tag{11}$$

where $Z\prime^{R}_{nm}$ and Z^{R}_{nm} are the Zernike moments of the original and rotated image. The angle of rotation θ can be calculated using Equation (12)

$$\theta = -\frac{argarg\left(Z'^{R}_{nm}\right) - argarg\left(Z^{R}_{nm}\right)}{m}\ (m \neq 0) \tag{12}$$

where $arg()$ denotes the phase, extraction operator.

2.2.2. Scaling Detection

Let $f\prime$ denote a scaled version of the original color image f, and the scale factor is λ.

$$\text{Let } \kappa_f = \left(\left|Z^{R}_{nm}\right|\right)^{\frac{1}{2}} \tag{13}$$

Considering the definition of k_f, we can define the following relationship:

$$\kappa_{f'} = \lambda\kappa_f \tag{14}$$

Then the scaling factor can be calculated by using Equation (15)

$$\lambda = \frac{\kappa_{f'}}{\kappa_f} = \sqrt{\frac{Z'^{R}_{nm}}{Z^{R}_{nm}}} \tag{15}$$

By using two detection methods above, the geometric distortion parameters of the image under the rotation and scale attacks can be calculated. However, how to choose the moment's order n and m of the correction information is also important. The current algorithm uses either the zero-order or all of the low-order information for correction. However, some of the low-order values have larger errors so it is not suitable for correction. Also, transmitting these values requires further processing, such as encryption, which increases time complexity. Therefore, the selection of orders directly affects the results. We selected a small number of order values, which were more stable for geometric correction and achieved higher correction accuracy.

Other orthogonal moments can be used to achieve the correction of image size and rotation angle, such as quaternion Legendre-Fourier moments [45] and Quaternion Radial Substituted Chebychev Moments [46]. We will continue to explore more precise methods using these moments.

3. Proposed Watermarking Scheme

The host image is split into non-overlapping blocks and decomposed by the Haar wavelet transform. The WEF and ESF values are calculated for each block, and the relationship between the sub-band coefficients is considered. The watermark is embedded by changing the relationship between coefficients. By considering the characteristics of the original image and watermark, this scheme provides good imperceptibility. We use the invariance of the Zernike moment to protect against a geometric attack and select a specific order to record the frequency domain information of the image. When extracting the watermark, the scheme checks for geometric attacks and corrects the host image. This enhances robustness of the watermark.

The proposed scheme has four steps: (1) watermark detection, for making full use of the features of the watermark, (2) watermark embedding, (3) image geometric feature extraction to protect against a geometric attack, (4) watermark extraction.

The notations used in this paper are shown in Table 1.

Table 1. Notations used in the paper.

Notation	Description	Notation	Description
S	Watermark sequence	$LL3^r_{i,j}$	The values of the red channel after three-level DWT of $H_{i,j}$.
A	The number of 1 in the watermark sequence	$LL2^r_{i,j}$ (k_1,k_2)	The values at the coordinates (k_1,k_2) of the red channel after two-level DWT of $H_{i,j}$.
B	The number of 0 in the watermark sequence	T	The threshold used to classify ESF
H	Host image	q	Classifying intensity
(i,j)	The coordinates of each block	w_k	The k-th watermark bit to be embedded
N	The size of the host image	s	Embedded intensity
$I_{i,j}$	Watermark embedding flag (WEF)	$\chi\prime_w$	ESF when the watermark is embedded
χ	Embedding status flag (ESF)	w_{ex_k}	k-th extracted watermark bit

3.1. Watermark Detection

The watermark detection is composed of two steps.

Step 1: Detect the number of 0s and 1s in the binary watermark by using Equation (16)

$$A = num_1(S),\ B = num_0(S) \tag{16}$$

where S represents the watermark sequence to be embedded, A is the number of 1s in the watermark sequence, and B is the number of 0s.

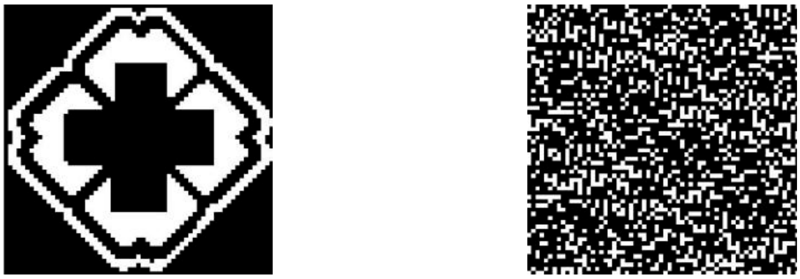
Step 2: Watermark Permutation.

To eliminate the correlation between watermark sequences and to protect patient's privacy, the watermark needs to be scrambled. The chaos model-logistic mapping is defined as Equation (17):

$$X_{n+1} = \mu X_n(1 - X_n),\ 0 < X_n < 1,\ n = 0,1,2\ldots \tag{17}$$

The value $3.5699 < \mu < 4$ is chosen to generate the random key matrix. The initial values of X_0 and μ are regarded as keys. The decryption can't be completed if either of the parameters is missing or incorrect.

The example of original image (logo of the hospital) and the scrambled watermark images are shown in Figure 1. Note that when embedding a watermark, it needs to be read as a sequence.



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

Figure 1. Watermark images. (**a**) Original watermark image, (**b**) Scrambled watermark image.

3.2. Watermark Embedding

The complete process for embedding and extraction is shown in Figure 2.

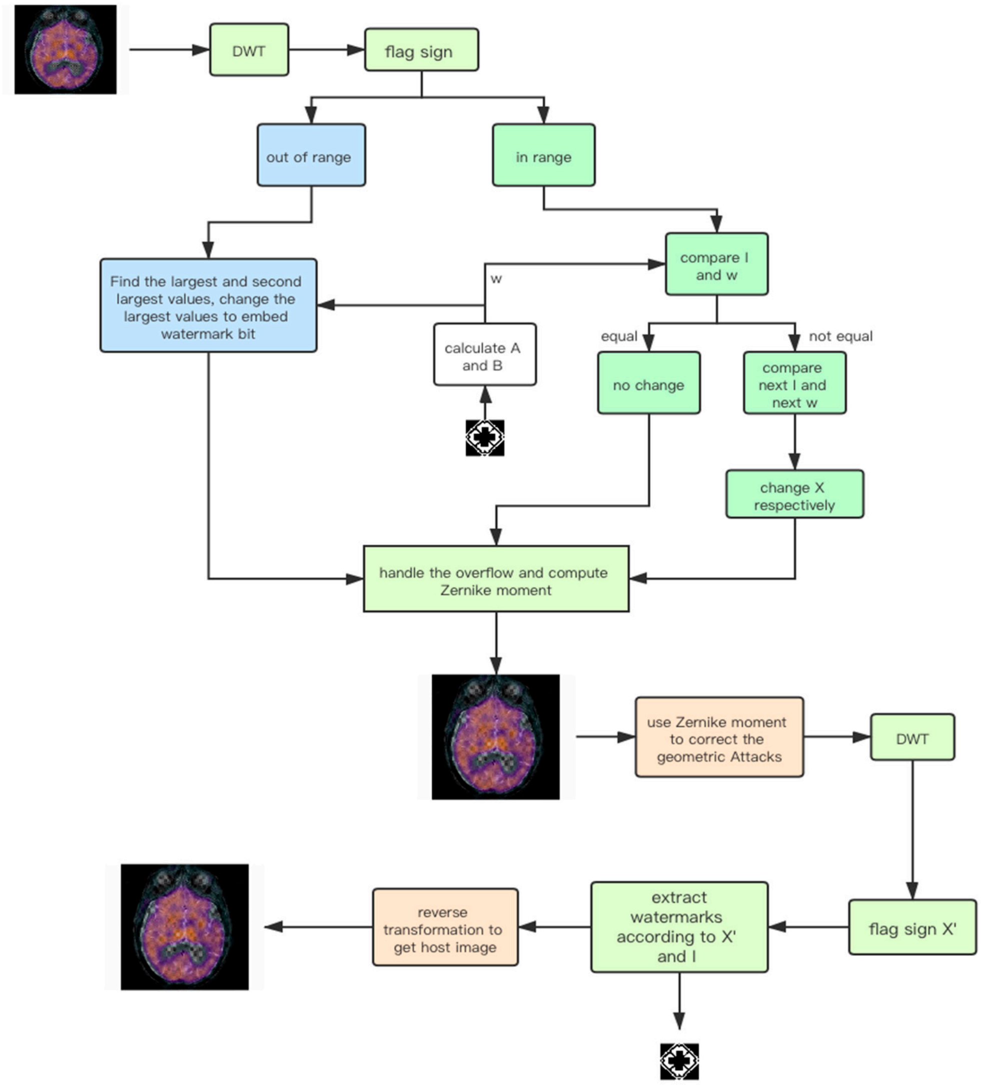

DWT
flag sign
out of range
in range
Find the largest and second largest values, change the largest values to embed watermark bit
w
compare I and w
calculate A and B
equal
not equal
no change
compare next I and next w
change X respectively
handle the overflow and compute Zernike moment
use Zernike moment to correct the geometric Attacks
DWT
flag sign X'
extract watermarks according to X' and I
reverse transformation to get host image

Figure 2. Framework of proposed robust reversible watermarking scheme.

Step 1: The host image is divided into 8 × 8 blocks. Each block is transformed by three-level DWT and embedded with one bit of information. The bit information $I_{i,j}$ is computed to represent each block.

$$\begin{cases} I_{i,j} = \begin{cases} 0 & if(LL3^r_{i,j} > LL3^g_{i,j} \; and \; LL3^r_{i,j} > LL3^b_{i,j}) \\ 1 & else \end{cases} & (A \geq B) \\ I_{i,j} = \begin{cases} 1 & if(LL3^r_{i,j} > LL3^g_{i,j} \; and \; LL3^r_{i,j} > LL3^b_{i,j}) \\ 1 & else \end{cases} & (A < B) \end{cases}, \tag{18}$$

where (i,j) represents the coordinates of each block in the host image. Taking the host image of size $N \times N$, the range of i,j is $[1, \frac{N}{8}]$. $I_{i,j}$ is also called watermark embedding flag (WEF); The watermark is embedded according to it. $LL3^r_{i,j}$, $LL3^g_{i,j}$, $LL3^b_{i,j}$ respectively represent the coefficient values of the red, green, and blue channels after the three-level decomposition of the DWT of $H_{i,j}$.

Step 2: Compute the ESF χ to mark the embedded status of each block. To ensure that the modification of χ does not affect the WEF, it is calculated by

$$\chi = LH2^b_{i,j}(k_1, k_2) - LH2^r_{i,j}(k_1, k_2) \tag{19}$$

where $LH2^b_{i,j}(k_1, k_2)$ and $LH2^r_{i,j}(k_1, k_2)$ refer to the coefficients at the coordinates (k_1, k_2) in the LH sub-band of channel B and R respectively, after the block with coordinates (i,j) are transformed into a two-level DWT. The modification of χ is the modification of $LH2^b_{i,j}(k_1, k_2)$. According to the characteristics of the image, most of the values of χ are 0.

Step 3: Classify and change the watermark status flag $\chi\prime$ as shown in Equation (20).

$$\chi' = \begin{cases} \chi, & abs(\chi) \leq T \\ \chi + q \cdot 2^l, & \chi > T \\ \chi - q \cdot 2^l, & \chi < -T \end{cases} \tag{20}$$

where T is the threshold, which is larger than 0, and q is the classifying intensity. The image distortion becomes more obvious with the increase of q. l is the order of the wavelet transform, and it is equal to 2 in this paper.

Step 4: Choose a different embedding strategy according to the different range of values of $\chi\prime$.

If $abs(\chi') \leq T$

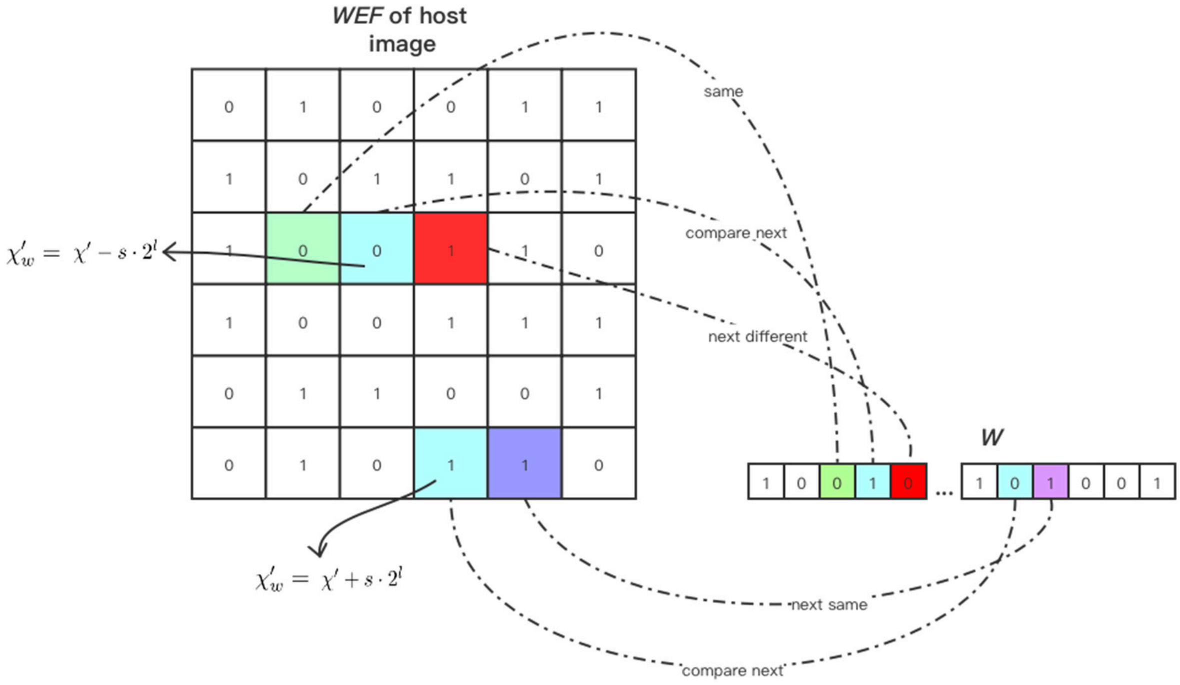
Compare whether the WEF is same to the watermark bit to be embedded. If it is, then the ESF does not need to be modified. Otherwise, the next WEF and the watermark bit are used to do the comparison. Equation (21) presents the three embedding strategies according to the comparison results of $I_{i,j}$ and w_k.

$$\chi'_w = \begin{cases} \chi' & (w_k = I_{i,j}) \\ \chi' + s \cdot 2^l & (w_k \neq I_{i,j}, w_{k+1} \neq I_{i,j+1}) \\ \chi' - s \cdot 2^l & (w_k \neq I_{i,j}, w_{k+1} \neq I_{i,j+1}) \end{cases} \tag{21}$$

Here w_k represents the k-th watermark bit to be embedded in this block and $I_{i,j}$ is the same as in Equation (18). s is the embedding intensity and it meets the conditions of Equation (22).

$$2 \cdot T < s \cdot 2^l < q \cdot 2^l \mathrm{a} = 1, \tag{22}$$

Figure 3 presents an example of various situations in the embedding process. The advantage of this method is that if the WEF value of a block is different from w_k, only the ESF of this block is changed. This means that two bits of watermark information are embedded at a time. When the embedding process completes, the value of the embedding status flag is $\chi\prime_w$.



0	1	0	0	1	1
1	0	1	1	0	1
1	0	0	1	1	0
1	0	0	1	1	1
0	1	1	0	0	1
0	1	0	1	1	0

Figure 3. An example of different embedding strategies in various situation.

If $abs(\chi') > T + q{\cdot}2^l$

The largest and second-largest coefficients of the wavelet transform in the LH_1 subband are selected according to Equation (23):

$$\begin{cases} a_1 = max(LH1) \\ a_2 = secmax(LH1) \end{cases} \tag{23}$$

where $max(\cdot)$ and $secmax(\cdot)$ are denoted as the maximum and second largest value, respectively. The watermark is embedded according to Equation (24):

$$\begin{cases} \lambda_1 = floor(a_1) - floor(a_2) \\ \lambda_2 = 2{\cdot}\lambda_1 + mod(\lambda_1, 4) + 4{\cdot}w_k \\ \max(LH1) = a_1 + \lambda_2 - \lambda_1 \end{cases} \tag{24}$$

The watermarked image is obtained by the inverse DWT.

Step 5: Modify the underflow pixel values

First, the number of underflow pixel values is counted. Then, the hash value of the whole image is computed. The length of the hash code must be the same as the number of underflow pixel values. The underflow pixels are modified and the modification information is recorded. A hash code is added to underflow pixel values by Equation (25)

$$\begin{cases} \nu' = hash(i), \ \ if(\nu < 0) \\ \nu' = 255, \ \ if(\nu > 255) \end{cases} \tag{25}$$

where ν is the pixel value embedded in the watermark while $\nu\prime$ is the pixel value after the overflow processing. $hash(i)$ is the i-th value of the hash code sequence.

3.3. Calculating Zernike Moments

Select the value of the specific coefficient of the Zernike moments and send it as the key, which is used to correct the geometric attack. The detailed information is presented in Section 4.2.

3.4. Watermark Extraction

The detailed steps of the watermark extraction process are as follows:

Step 1: Extract the hash values, and restore the original watermarked image according to the side information of the overflow processing. The hash values are used to detect whether the image is modified.

Step 2: If the image is modified, the values of the Zernike moments are used to detect rotation and scaling parameters and then correct it.

Step 3: Extract the watermark. Divide the watermarked image into 8×8 blocks, and each block is transformed by a three-level DWT. Calculate the WEF as narrated in Section 3.2.

Step 4: Compute the value of the embedding status flag $\chi\prime_{ex}$ as shown in Equation (26).

$$\chi'_{ex} = LH2_{ex^{b}_{i,j}}(k_1,k_2) - LH2_{ex^{r}_{i,j}}(k_1,k_2) \tag{26}$$

The sub-block in the position of (i,j) is transformed by a two-level DWT, and the values at the coordinates of (k_1,k_2) in channel B are taken as the value of $LH2_{ex^{b}_{i,j}}(k_1,k_2)$.

Step 5: The strategies for extracting the watermark and restoring the original image are determined by $\chi\prime_{ex}$.

If $abs(\chi'_{ex}) \le T$, the watermark embedding flag is the same as the watermark bit. Compute the watermark sign as in Equation (27). The image block does not need to be modified.

$$w_{ex_k} = I_{ex_{i,j}} \tag{27}$$

Here, w_{ex_k} and $I_{ex_{i,j}}$ are the k-th extracted watermark bit and the (i,j) bit information of the WEF, respectively. $I_{ex_{i,j}}$ is computed using Equation (18).

If χ'_{ex} of one block is in the range of $\left(T, T+s\cdot 2^{l}\right)$, then the WEF of this block is different from the current watermark bit, but the next WEF and the next watermark bit are the same. The watermarks w_{ex_k} and $w_{ex_{k+1}}$ corresponding to the current and the next blocks are extracted by Equation (28).

$$\begin{cases} w_{ex_k} = abs\left(I_{ex_{i,j}} - 1\right) \\ w_{ex_{k+1}} = I_{ex_{i,j+1}} \end{cases} \tag{28}$$

The embedding status flag is restored by Equation (29):

$$\chi_{ex} = \chi'_{ex} - s\cdot 2^{l} \tag{29}$$

If $-T - s\cdot 2^{l} < \chi\prime_{ex} < -T$, the current and the next watermark embedding flag are different from the corresponding watermark bit. In this case, extract the flags for the current and the next blocks in addition to correcting the flag of the current ESF by using Equations (30) and (31).

$$\begin{cases} w_{ex_k} = abs\left(I_{ex_{i,j}} - 1\right) \\ w_{ex_{k+1}} = abs\left(I_{ex_{i,j+1}} - 1\right) \end{cases} \tag{30}$$

$$\chi_{ex} = \chi'_{ex} + s\cdot 2^{l} \tag{31}$$

If $abs(\chi\prime_{ex}) > T + q\cdot 2^{l}$, find the maximum and the second largest values in the LH sub-band after the one-level wavelet transform using Equation (32).

$$\begin{cases} a1_{ex} = (LH1_{ex}) \\ a2_{ex} = (LH1_{ex}) \end{cases} \tag{32}$$

Then, extract the watermark according to Equations (33)–(36):

$$\lambda'_{2} = floor(a1_{ex}) - floor(a2_{ex}) \tag{33}$$

$$w_{ex_k} = mod\left(floor\left(\frac{\lambda'_2}{4}\right), 2\right) \tag{34}$$

$$\lambda'_1 = floor\left(\frac{\lambda'_2}{4} - w_{ex_k}\right) \cdot 2 + mod(\lambda'_2.4) \tag{35}$$

$$(LH1_{ex}) = a1_{ex} - \lambda_2 + \lambda_1 \tag{36}$$

where w_{ex_k} is the watermark extracted from the k-th block, while $(LH1_{ex})$ is the maximum value of the $LH1$ sub-band after correction.

Step 6: Restore χ_{ex} by using Equation (34)

$$\chi_{ex} = \begin{cases} \chi_{ex} - q \cdot 2^l & \chi_{ex} > T + q \cdot 2^l \\ \chi_{ex} + q \cdot 2^l & \chi_{ex} < -T - q \cdot 2^l \end{cases} \tag{37}$$

Step 7: The original host image is obtained by the inverse DWT.

4. Experiment Results

First, we explain the criteria for measuring the imperceptibility and robustness of the watermark and images used in the experiment (we use images from The Whole Brain Atlas [47]). Then, we analyze the selection of Zernike's moment order and its performance of geometric correction. After that, the performance of the proposed method is tested and compared with the existing methods (Golabi et al. [37], Tian et al. [48], Priyanka and Maheshkar [49], and Thabit and Khoo [50]) in the following. Lastly, the time complexity of the proposed scheme is analyzed.

4.1. Criteria and Database

In the experiment, the original color 512 × 512 MRI brain image is from The Whole Brain Atlas [47], which is a publicly available medical images database provided by Harvard Medical School. The other MRI images are from the Internet. In a robust test, the watermark image is a two-value image and the size is 64×64. Here, we select the hospital logo image as the watermark. The original medical host image and the watermark are shown in Figure 4.

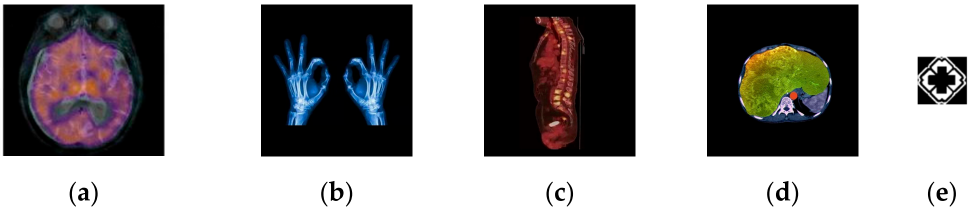


Figure 4. Original medical host image and watermark. (**a**) Brain, (**b**) Hands, (**c**) Spine, (**d**) Brain, (**e**) Watermark image.

We use the Peak Signal to Noise Ratio (PSNR) as the evaluation criterion for image quality, which is calculated by Equations (35) and (36):

$$MSE = \frac{1}{E \times F} \sum_{i=0}^{E-1} \sum_{j=0}^{F-1} \left(I_{new}(i,j) - I_{org}(i,j)\right)^2 \tag{38}$$

$$PSNR = 10 \cdot log\left(\frac{255^2}{MSE}\right) \tag{39}$$

where I_{new} is the watermarked, and I_{org} is the original image, respectively. $E \times F$ is the size of the image. Fundamentally, the higher the PSNR value is, the greater imperceptibility of the watermark in the host image.

Distortions with a high sensitivity of human visual system (HVS) caused in low frequency range, some researchers have developed metrics known as PSNR-HVS and HVS with masking (PSNR-HVSm) [51,52] that correlate well with human perceptions. We have incorporated HVS and HVSm into our comparative studies for image quality assessment as follows:

$$PSNR - HVS = 10\left(\frac{255^2}{MSE_H}\right) \tag{40}$$

$$MSE_H = K\sum_{i=1}^{E-7}\sum_{j=1}^{F-7}\sum_{m=1}^{8}\sum_{n=1}^{8}\left((X[m,n]_{ij} - X[m,n]_{ij}^{e})T_c[m,n]\right)^2 \tag{41}$$

where E, F denote image size, $K = \frac{1}{[(E-7)(F-7)64]}$, X_{ij} are Discrete Cosine Transform (DCT) coefficients of the corresponding block in the original image, and T_c is the matrix of correcting factors.

The structural similarity index (SSIM) is defined as follows:

$$SSIM(x,y) = \frac{(2\mu_x\mu_x + C_1)(2\sigma_{xy} + C_2)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{42}$$

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

The reconstruction performance is evaluated by Bit Error Rate (BER) and Normalized Cross-Correlation coefficient (NC) as follows:

$$BER = \frac{B}{p' \times q'} \times 100 \tag{43}$$

$$NC = \frac{\sum_{i=1}^{p'}\sum_{j=1}^{q'}(w(i,j) - \mu_w)(w'(i,j) - \mu_{w'})}{p' \times q'} \tag{44}$$

where $p\prime$ and $q\prime$ are the height and width of the original w and extracted $w\prime$ watermarks; μ and σ are the mean and standard deviation of pixel values. B is the number of bits detected erroneously.

4.2. Geometric Correction of Zernike Moments

4.2.1. Rotating Attack

The phase values of the zero-order moment are often used in the literature to correct rotated images. Although it is possible to detect the rotation parameters, there is still approximately a one-degree error, and the correction accuracy is directly affected. Therefore, one of our contributions is to select two stable order values. The experiment results show not only the accuracy of the correction is improved, but also the amount of information that needs to be transmitted is reduced.

The two-phase values are recorded at (1, −1), (2, −2). Figure 5 compares of the image before and after correction at different rotation angles.

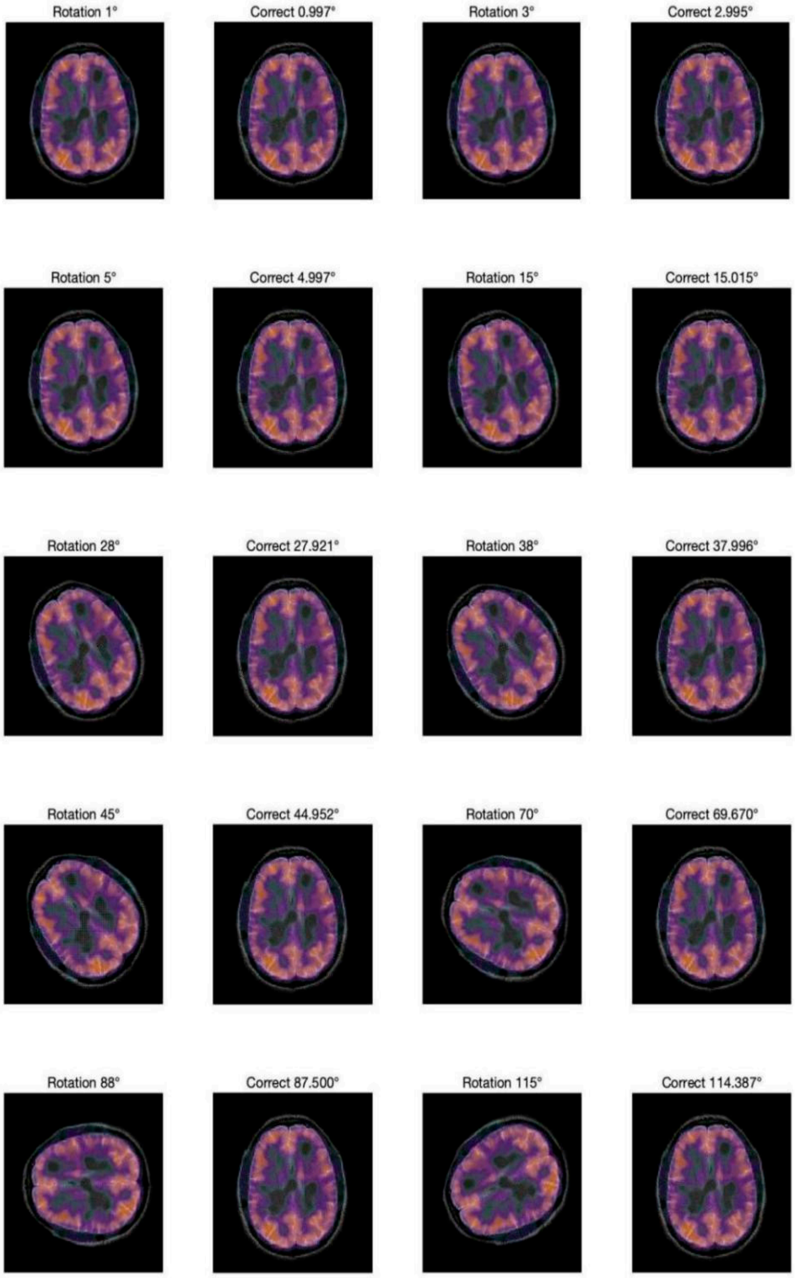


Figure 5. Comparison of the image before and after correction.

To compare the results with those reported in [37], the same rotation angle is used. The results of the experiment show that the Zernike moments have a strong detection ability for a rotation attack, especially for small-angle rotations: the error can be less than 0.005 degrees.

To explore the correction ability of this scheme for small angle rotation, a more detailed experiment is performed on rotation at small angles, which are less than 3 degrees. The results are shown in Figure 6. Note that this scheme has good correction ability for small angle rotation.

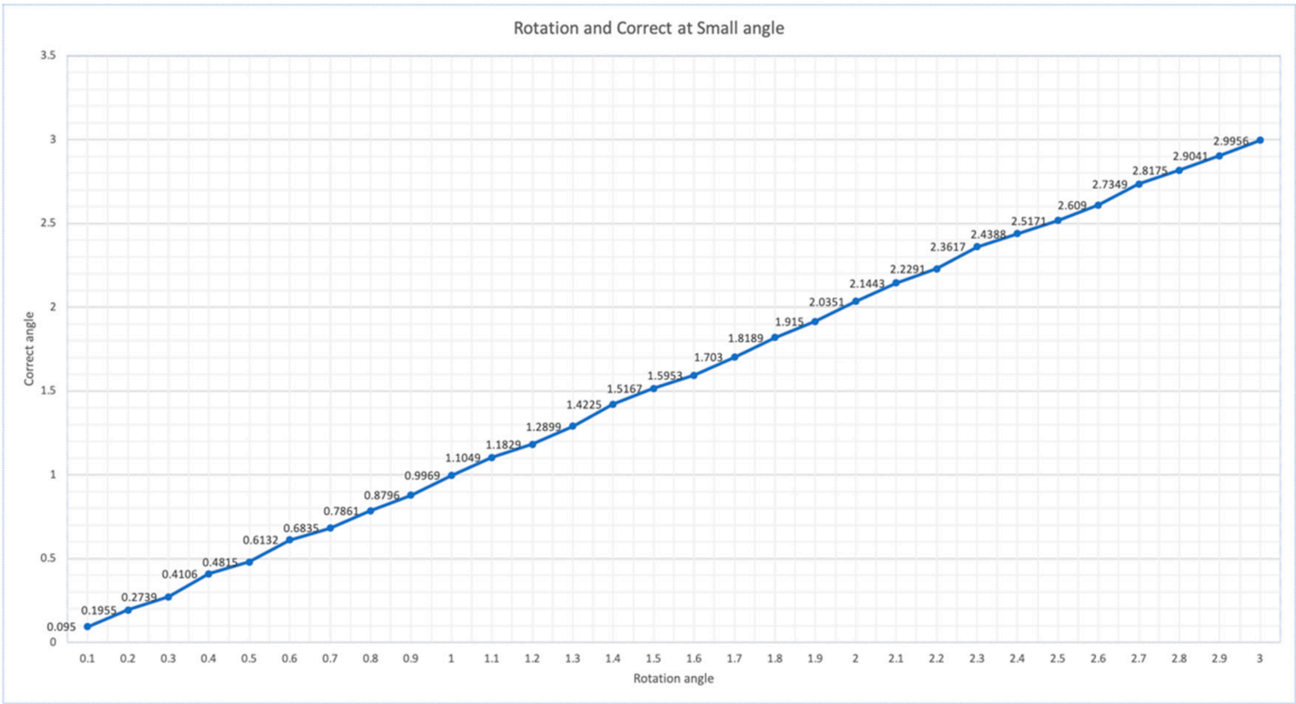


Figure 6. Rotation and correction at small angle.

4.2.2. Scale Attack

The two amplitude information at (0, 0), (3, −1) is recorded. The results are presented in Table 2. As it can be seen, the Zernike moments also have good correction ability for scaling attacks, and most of the errors are within the range of 0.005. Therefore, the Zernike moments can detect the parameters of geometric attack well.

Table 2. Scale parameter detection.

Scale Parameter	Scale 0.6	Scale 0.8	Scale 1.1	Scale 1.3	Scale 1.6
Correct scale parameter	0.60000	0.80338	1.10233	1.30853	1.60320

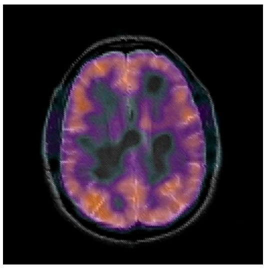
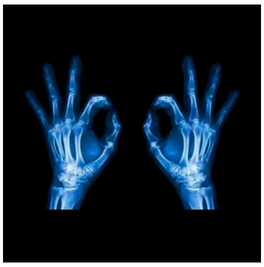
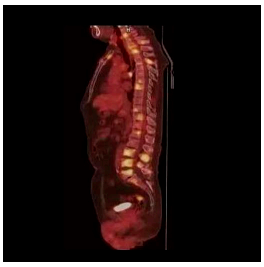
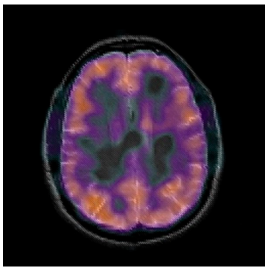
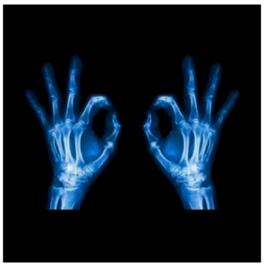
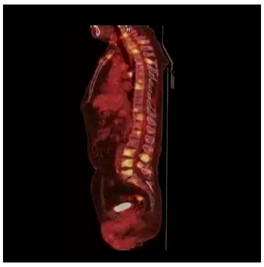
4.3. Imperceptibility and Capacity Results

The imperceptibility of images is an important evaluation criterion. A good watermarking scheme requires that the distortion of an image be as little as possible. In the proposed scheme, three-color medical images are tested, and the LH and HL sub-bands are selected to embedding the watermark. When embedding capacity is 4096 bit, the B channel is selected for embedding because the human eye is more insensitive to channel B [53]. When increasing embedding capacity, other color channels are selected, while using the same embedding method. The following experiments calculate the PSNR of the image at different embedded intensities. The parameters are set as follows: $T = 1.98, l = 2,\ q = 2,\ s = 1$. Table 3 is the Bit per Pixel (BPP) under different embedding capacities. Table 4 shows a comparison of images before and after embedding watermark. Figures 7 and 8 are the PSNR and SSIM of three images, respectively. Then we used PSNR-HVSm and PSNR-HVS to evaluate the proposed scheme. For better visual effect, we increase the embedding strength slightly, by setting $T = 1.98,\ l = 2,\ q = 8,\ s = 4$. The results are shown in Figure 9. Therefore, this scheme can embed more bits while ensuring good visual quality of the host image.

Table 3. Bits per pixel (BPP) under different embedding capacity.

Capacity (Bits)	4096	8192	12,288	16,384	20,480	24,576
BPP	0.005208	0.010417	0.015625	0.020833	0.026042	0.03125

Table 4. Comparison of original and watermarked images.

	Brain	**Hands**	**Spine**
Original Image			
Watermarked Image			

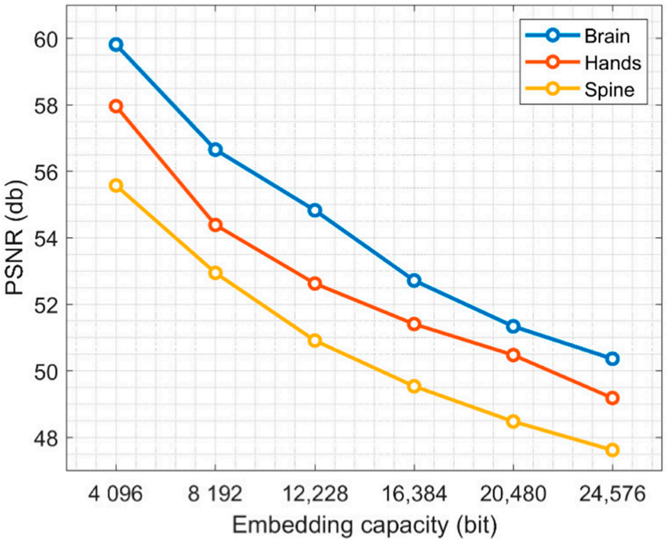


Figure 7. PSNR of three images under different embedding capacity.

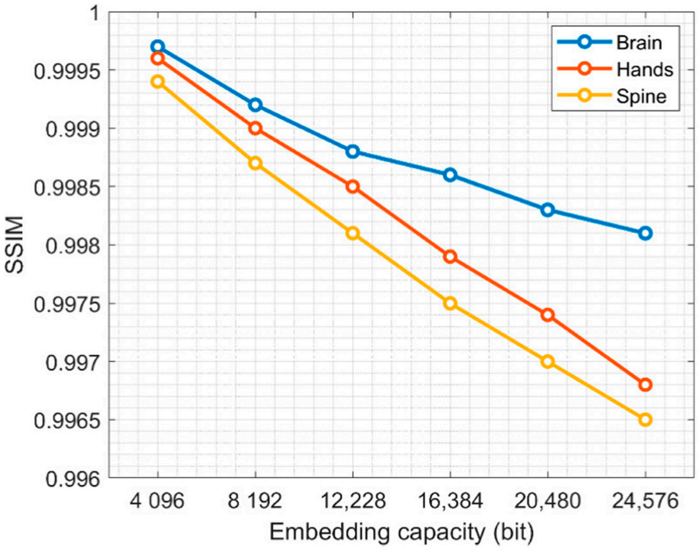


Figure 8. SSIM of three images under different embedding capacity.

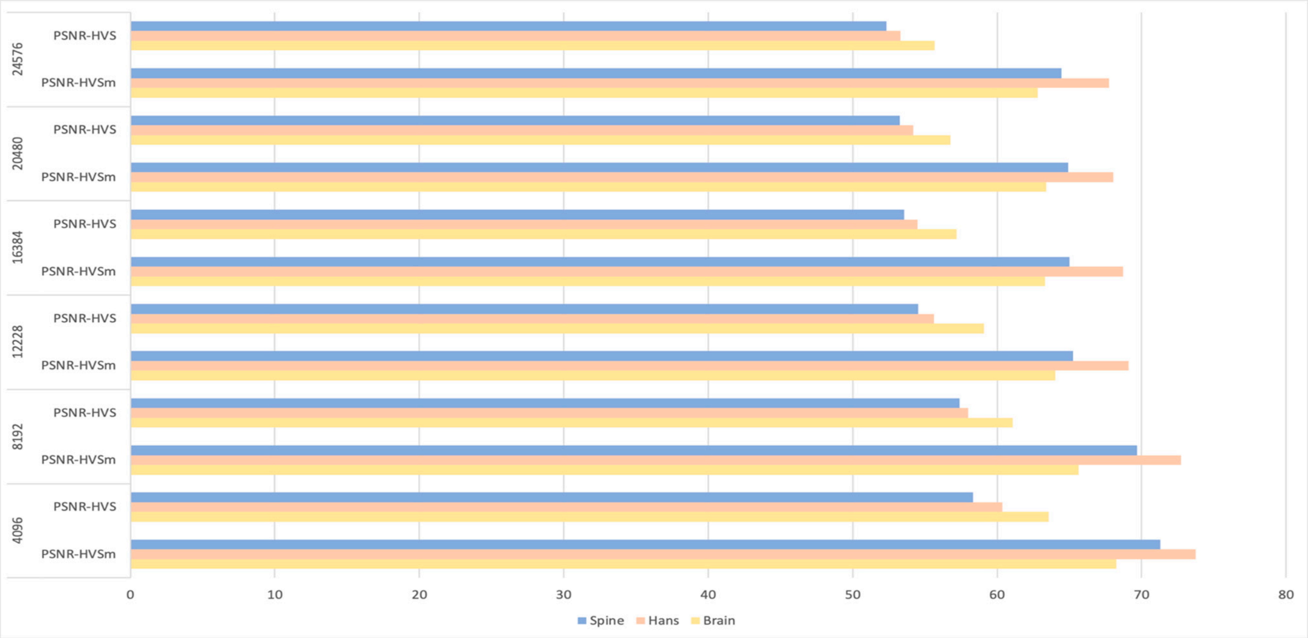


Figure 9. PSNR-HVSm and PSNR-HVS of three images under different embedding capacity.

In Figure 10, we compare the embedding capacity and the PSNR of the proposed scheme with other methods. The proposed embedding scheme has better imperceptibility.

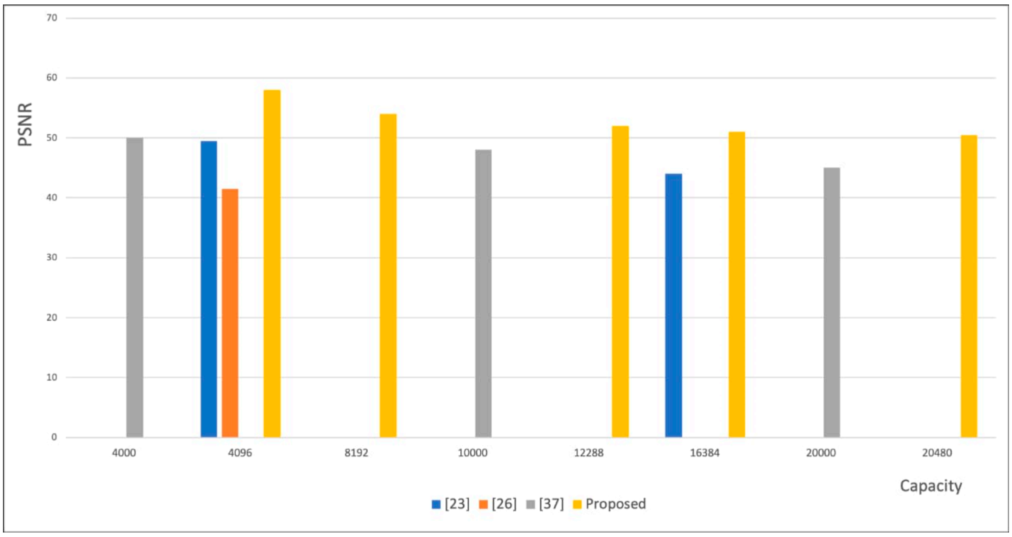


Figure 10. Comparison of the proposed scheme with the schemes of Thabit and Khoo [23], Liu et al. [26] and Golabi et al. [37] based on the PSNR values.

4.4. Robust Scheme

In this section, the watermarked images are under various attacks to evaluate the robustness. In particular, the embedded capacity of 4096 bits is tested and the embedding operation of each block is recorded. The embedding parameters are set as follows: $T = 1.98, l = 2, q = 11, s = 7$.

Figure 11 is a comparison of the BER with the Golabi et al. scheme [37] when the watermark was extracted at various rotational angles. The scheme presented in [37] has poor stability, and when the rotation angle is less than 38° and greater than 45°, the error tends to increase gradually; while the proposed scheme has better stability for rotation attack, and the overall error rate is lower than the one presented in [37].

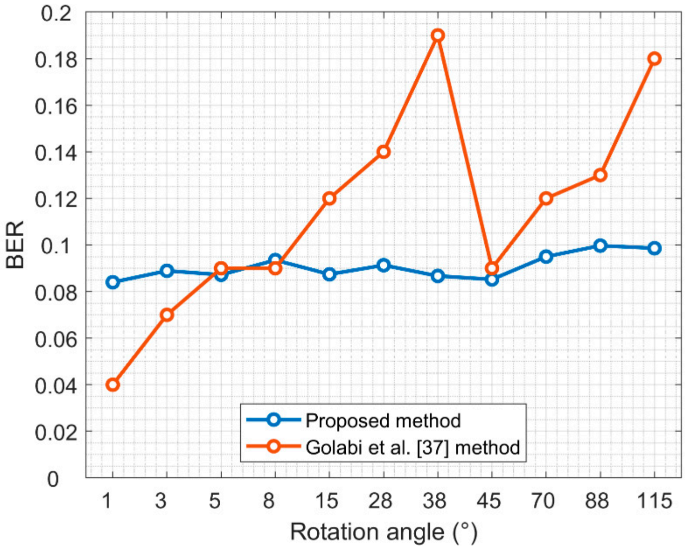


Figure 11. Comparison of BER values with the results of Golabi et al. [37] under various rotation angles.

Figure 12 shows a comparison of BER under different scale parameters. It is important to note that Matlab uses the interpolate method for scaling the image, which can lead to the loss of image information, so we do the scaling experiment in PhotoShop. By analyzing the experimental results, we find that the error of extracting watermark comes from the image distortion caused by saving the picture. After the scaling attack is corrected, the error caused by itself is very small, so BER in this paper keeps a relatively stable value. The work [37] performs scaling in MATLAB. If the scale factor is more than 1, the quality loss of the image is very small, so the BER will be much less when the scaling factor is more than 1.

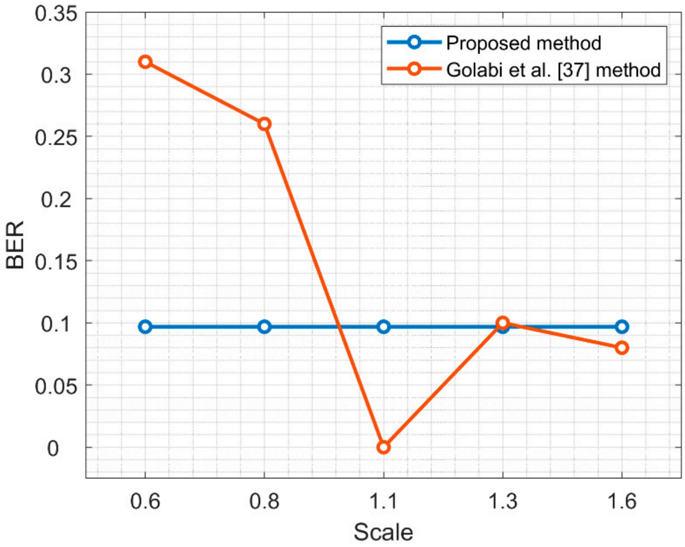


Figure 12. Comparison of BER values with the results of Golabi et al. [37] under different scale parameters.

Figure 13 shows the NC value of the compressed image, the recovered image, the extracted watermark image, and its bit error rate under different JPEG compression factors. Note that the scheme is robust to JPEG compression. It is surprising to see that the worst quality JPEG at 20% yielded the smallest BER. In fact, it is not that 20% compression yields better results, but that they all keep in the same level at about 0.08–0.09. The BER of JPEG at 20% is 0.793 in our experiment, which is closely related to the images we use. Whether their BER can be kept at the same level is related to the embedding scheme. In our research, the embedded watermark is represented by the coefficient relationship between each band after DWT transformation and the relationship between one block and the next. After JEPG compression, the image quality is declined. Take the NC value for example, NC is smaller after compression, but there is not much loss of the relationship between block and sub-band, so the watermark can still be extracted precisely. However, for attacks that destroy the relationship between block and sub-band, such as Gaussian noise, the BER is relatively high, which is about 0.3.

Figure 14 shows BER of the watermark and NC value of the restored host image under different JPEG2000 compression quality factors. With the increase of the quality factor, the NC value increases, and BER decreases. However, BER is less than 0.1, which shows that the scheme is robust to JPEG2000.

There are more recent and powerful compression standards such as X264, X265 and so on [54]. As mentioned in [52], these methods can also be used to compress still images. We will explore this kind of attacks in the future work.

Figure 15 shows a comparison between the proposed scheme and [37] for extracted watermark's BER under JPEG and JPEG2000. When the factor is greater, the BER is smaller. In [37], when the parameter of JPEG compression attack is less than 60, the BER is as high as 0.35, and it drops to about 0.2, when the parameter is greater than 60.

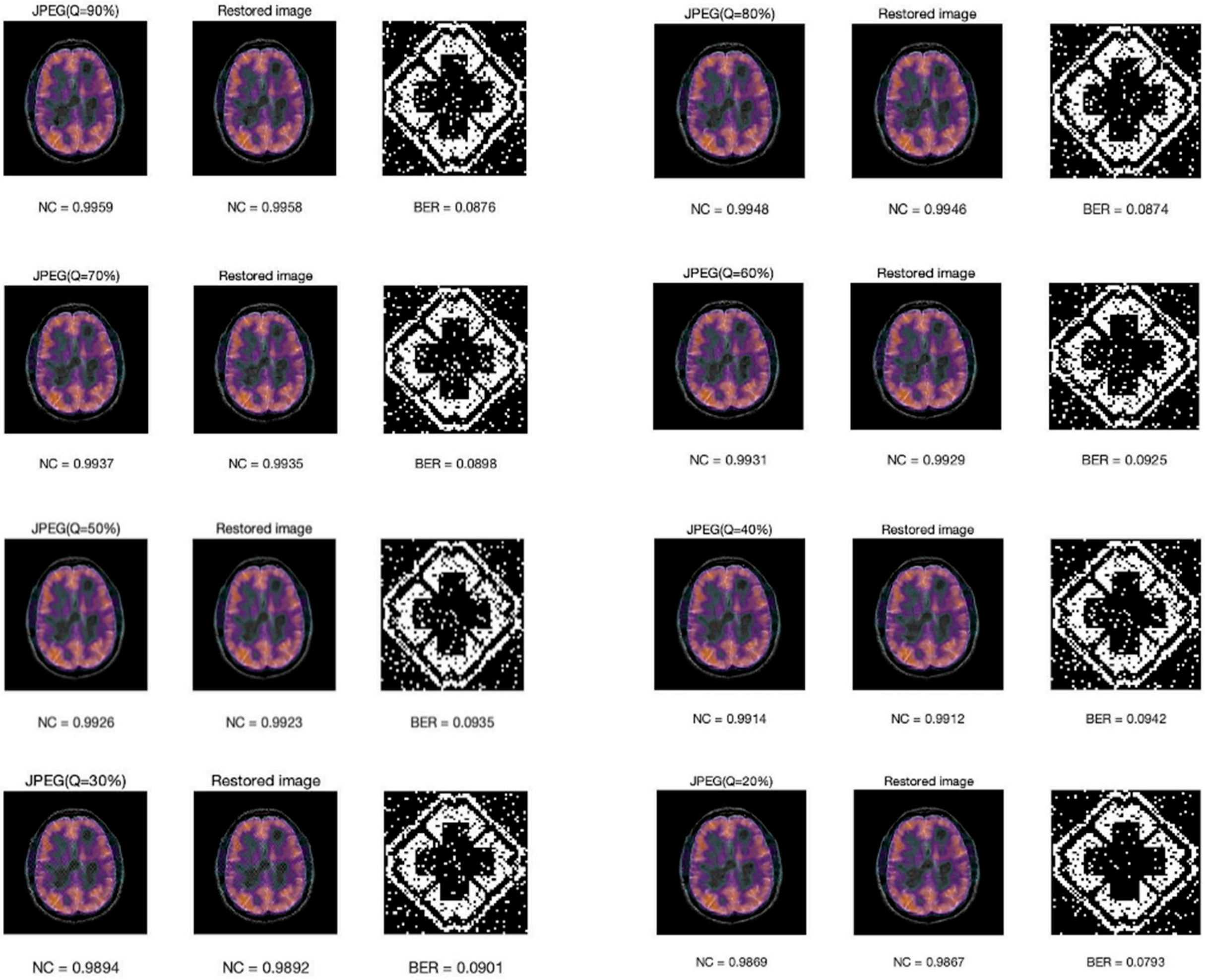


Figure 13. The NC value of the compressed image, the NC value of the recovered image, the extracted watermark image, and its BER under different JPEG compression factors.

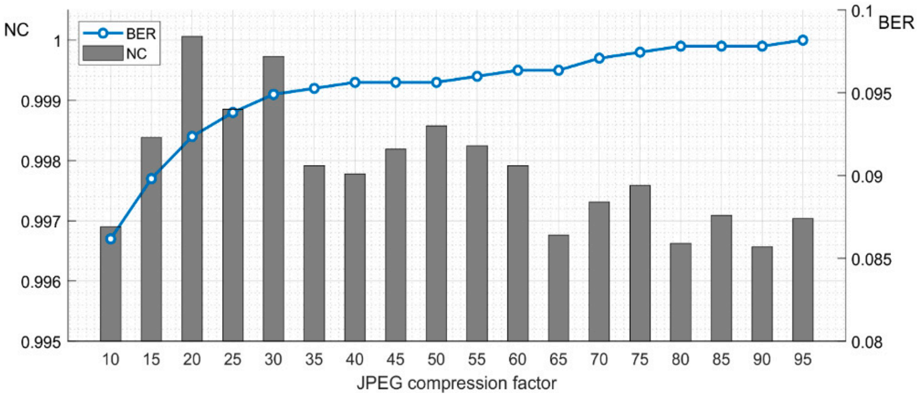


Figure 14. The BER and NC values under different JPEG2000 compression quality factors.

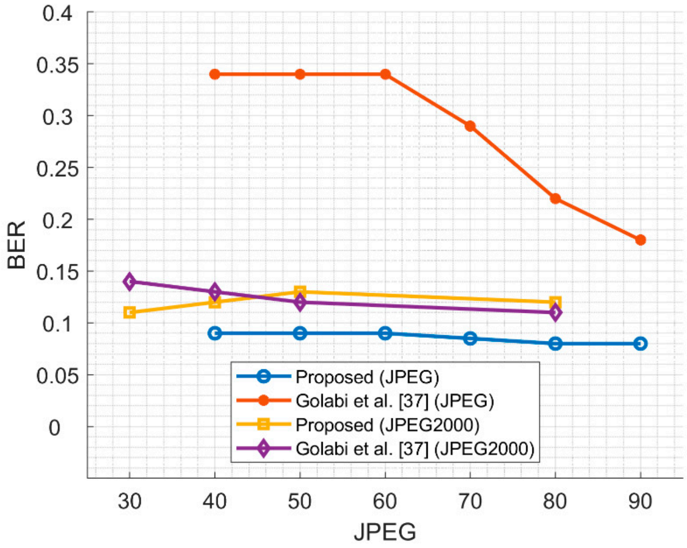


Figure 15. Comparison between the proposed scheme and Golabi et al. [37] scheme based on the BER value of the extracted watermark under JPEG and JPEG2000.

However, the scheme of our research remains below 0.1, which is far robust than [37]. The resistance to JPEG2000 attack is almost equivalent to the scheme proposed in [37].

Table 5 shows the BER of the extracted watermark information under various filtering attacks and the NC value of the original image and recovered image. The proposed scheme has good robustness for all kinds of filter attacks.

Figure 16 is the robustness of various noise attacks. The robustness to Gaussian noise is not robust enough, that is because the noise attack greatly changes the image quality, destroying the relationship between the coefficients, which leads to a larger error in the extracted watermark.

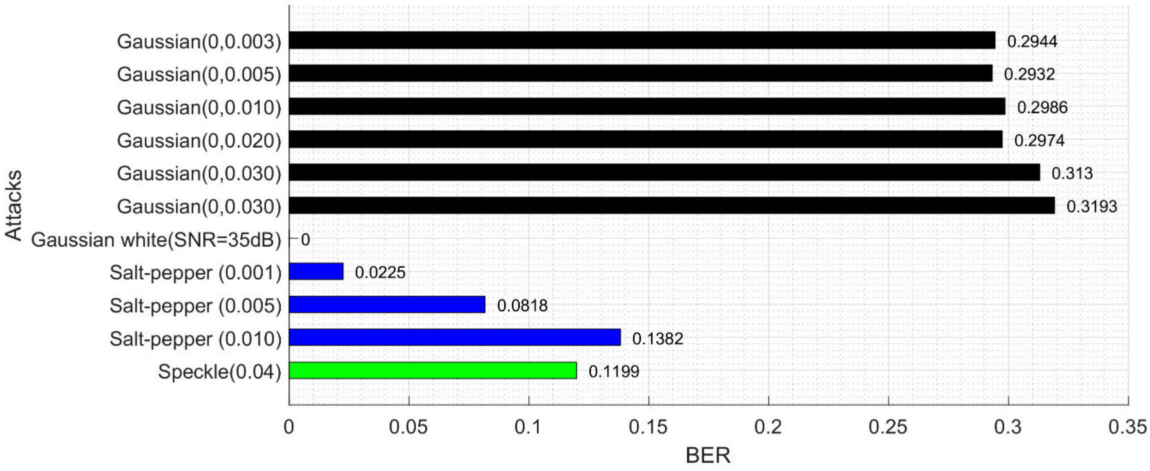
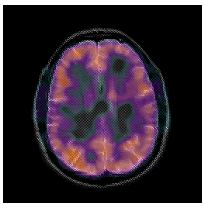
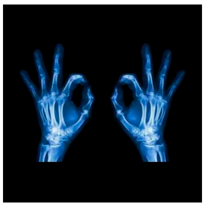
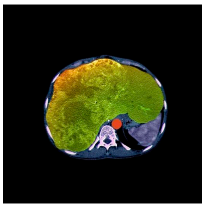
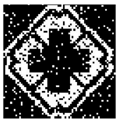
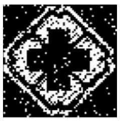
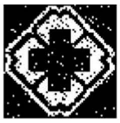
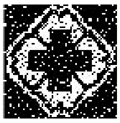


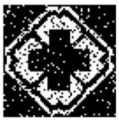
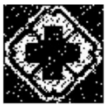
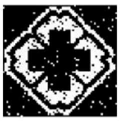
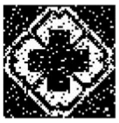
Figure 16. BER under various (Speckle, Salt-pepper, Gaussian white and Gaussian) noise attacks.

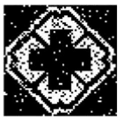
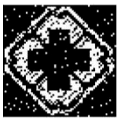
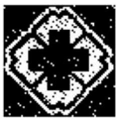
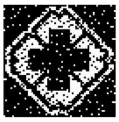
Table 6 shows the images which are attacked, the BER of extracted watermark information and the NC value of the recovered image under various attacks. Note that there is a low BER under various attacks. However, as the scheme does not have tamper detection and recovery capability, the NC value of the recovered image is low.

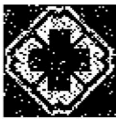
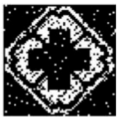
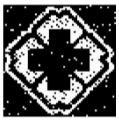
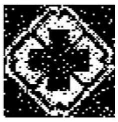
Table 5. The BER of the extracted watermark information under various filtering attacks and the NC value of the original image and recovered image.

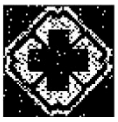
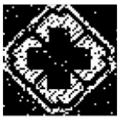
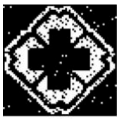
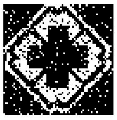
				

Median Filter 2 × 2	
	BER = 0.0857
	NC = 0.9872
		
		BER = 0.0920
		NC = 0.9969
			
			BER = 0.0488
			NC = 0.9957
				
				BER = 0.1025
				NC = 0.9949

Median Filter 3 × 3	
	BER = 0.0798
	NC = 0.9937
		
		BER = 0.0833
		NC = 0.9994
			
			BER = 0.0481
			NC = 0.9984
				
				BER= 0.0938
				NC = 0.9980

Median Filter 5 × 5	
	BER = 0.0725
	NC = 0.9839
		
		BER = 0.0872
		NC = 0.9976
			
			BER = 0.0505
			NC = 0.9944
				
				BER = 0.0896
				NC = 0.9943

Average Filter 3 × 3	
	BER = 0.0779
	NC = 0.9876
		
		BER = 0.0854
		NC = 0.9987
			
			BER = 0.0479
			NC = 0.9977
				
				BER = 0.0874
				NC = 0.9973

Average Filter 5 × 5	
	BER = 0.0713
	NC = 0.9811
		
		BER = 0.0823
		NC = 0.9955
			
			BER = 0.0493
			NC = 0.9925
				
				BER = 0.0808
				NC = 0.9920

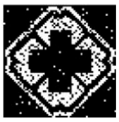
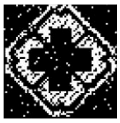
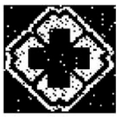
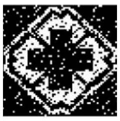
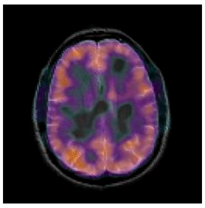
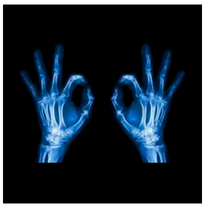
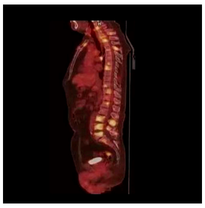
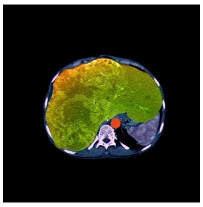
Motion Filter	
	BER = 0.0681
	NC = 0.9819
		
		BER = 0.0884
		NC = 0.9898
			
			BER = 0.0454
			NC = 0.9878
				
				BER = 0.0999
				NC = 0.9889

Table 6. Images under attack with BER value of extracted watermark information, and NC value of the recovered image.

Original images				

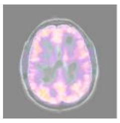
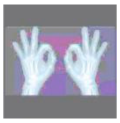
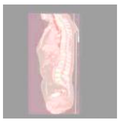
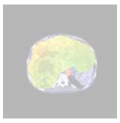
Histogram Equalization	
	BER = 0.0671
	NC = 0.7498
		
		BER = 0.0889
		NC = 0.6014
			
			BER = 0.0476
			NC = 0.5509
				
				BER = 0.0962
				NC = 0.5418

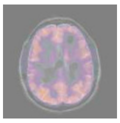
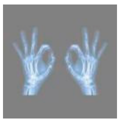
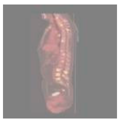
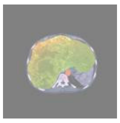
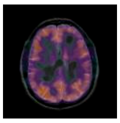
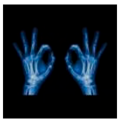
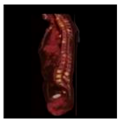
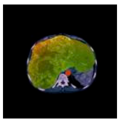
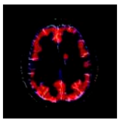
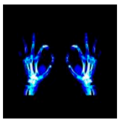
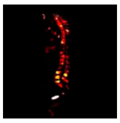
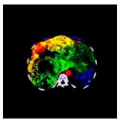
Image Brighten	
	BER = 0.0713
	NC = 0.7091
		
		BER = 0.0920
		NC = 0.5673
			
			BER = 0.0591
			NC = 0.5196
				
				BER = 0.1003
				NC = 0.6017

Image Darken	
	BER = 0.0444
	NC = 1.0000
		
		BER = 0.0461
		NC = 1.0000
			
			BER = 0.0229
			NC = 1.0000
				
				BER = 0.0898
				NC = 1.0000

Contrast Increasing	
	BER = 0.0718
	NC = 0.5417
		
		BER = 0.0920
		NC = 0.8565
			
			BER = 0.3079
			NC = 0.5415
				
				BER = 0.1055
				NC = 0.7564

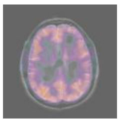
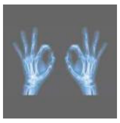
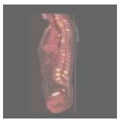
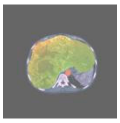
Contrast Decreasing	
	BER = 0.0662
	NC = 0.7549
		
		BER = 0.0801
		NC = 0.6291
			
			BER = 0.0415
			NC = 0.5635
				
				BER = 0.1042
				NC = 0.6610

Figure 17 is a comparison of the BER of our scheme and [37] under the hybrid attacks. Note that the robustness of the rotation attack is greater than the scaling attack, and the performance of our scheme is better than [37] under hybrid attacks.

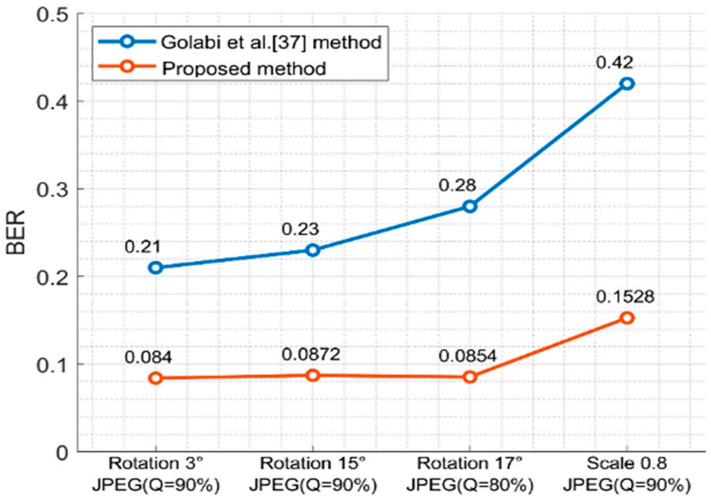


Figure 17. Comparison of BER of our scheme and [37] under hybrid attacks.

Figure 18 is a comparison of BER for extracted watermarks under various attacks of our scheme and the schemes proposed in [37,48–50]. When compared with other schemes, our proposed scheme has better robustness and greater stability.

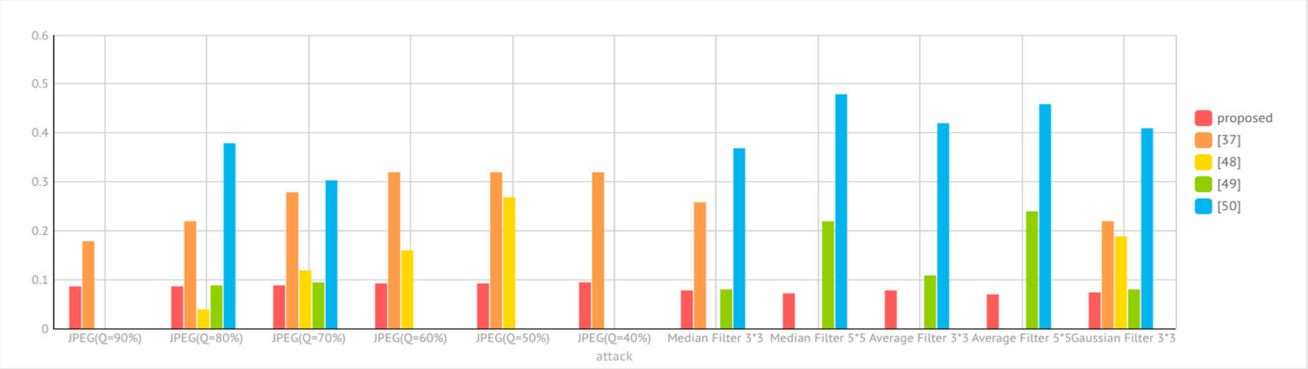


Figure 18. Robustness comparison among our scheme and the schemes of Golabi et al. [37], Tian et al. [48], Priyanka and Maheshkar [49] and Thabit and Khoo [50].

4.5. Complexity Analysis

The complexity is also an issue which needs to be considered for a practical application of a scheme. We analyzed the processing time of each step in the embedding and extraction process. The results show that the 3-level DWT transform of the host image takes up 60% of the time of the entire embedding process while the embedding process takes up 34% of the time, because of the 2-level IDWT is required after the watermark is embedded. Therefore, the processes of DWT and IDWT consume most of the algorithm time. Tables 7 and 8 list the number of DWT and IDWT calls and their time ratio to the whole scheme, respectively. The time complexity of DWT is $O\left(M^2L\right)$ where M represents the size of the image and L represents the length of the filter [55–60]. The extraction process is the same as the embedding process that almost all of the time is spent on DWT and IDWT. The time complexity of the entire algorithm is $O\left(M^2L\right)$ which is not high and can meet the needs of practical application.

Table 7. The number of DWT and IDWT calls and their time ratio in watermark embedding.

Function Name	Calls	% of Time
dwt2	12,288	62.89%
idwt2	6420	33.13%

Table 8. The number of DWT and IDWT calls and their time ratio in watermark extracting.

Function Name	Calls	% of Time
dwt2	12,288	61.11%
idwt2	6420	35.89%

5. Conclusions

In this paper, a robust reversible watermark scheme based on the Haar wavelet transform for watermarking of medical color images is proposed. The watermark embedding flag and the embedding status flag are set according to the characteristics of the host image. The issue that the pixel value of the watermarked image is not an integer is solved by changing the coefficient to the power of 2 in the wavelet domain. The embedding scheme takes the characteristics of the host image into account, which results in better imperceptibility. In this research, the order of the Zernike moment is improved, and more stable Zernike moment information is selected. This approach provides better correction ability for geometric attacks such as rotation and scaling. The experiments show that the scheme balances the relationships among robustness, imperceptibility, and embedded capacity. Medical images have different structures in different fields. The actual medical image is a multislice, which provides us with more embedding space. We consider that by using the proposed method, the expected performance will be as follows: embedding the same amount of bits, the imperceptibility will be better. If we let the image maintain the same level of visual distortion, the embedded capacity can be larger. Besides, the proposed approach is completely reversible. This is of great significance to the copyright protection of color medical images.

In the future, we will consider how to increase the embedded capacity without reducing imperceptibility and use other orthogonal moments with better performance to achieve accurate geometric correction. We will also explore the latest compression algorithms to attack the image to evaluate the robustness of our scheme.

Author Contributions: Conceptualization, X.Z.; Formal analysis, M.A.M. and R.D.; Funding acquisition, Q.Z. and R.D.; Investigation, Y.M. and Q.Z.; Methodology, X.Z.; Project administration, X.Z.; Software, Y.M.; Supervision, X.Z.; Validation, X.Z., Y.M., Q.Z. and M.A.M.; Visualization, Y.M., Q.Z. and R.D.; Writing—original draft, X.Z., Y.M. and Q.Z.; Writing—review & editing, M.A.M. and R.D. The authors have contributed equally to this manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: The research was supported in part by Hainan Provincial High-level Talent Project (Grant No. 2019RC044), and in part by Research project of Education and Teaching Reform of Hainan University (Grant No. hdjy2053).

Data Availability Statement: Data is available from the corresponding author upon reasonable request.

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

References

1. Kvedar, J.; Coye, M.J.; Everett, W. Connected health: A review of technologies and strategies to improve patient care with telemedicine and telehealth. *Health Aff.* **2014**, *33*, 194–199. [CrossRef]
2. Vanagas, G.; Engelbrecht, R.; Damaševičius, R.; Suomi, R.; Solanas, A. EHealth solutions for the integrated healthcare. *J. Healthc. Eng.* **2018**, *2018*, 3846892. [CrossRef] [PubMed]

3. Lee, J.Y.; Lee, S.W.H. Telemedicine cost-effectiveness for diabetes management: A systematic review. *Diabetes Technol. Ther.* **2018**, *20*, 492–500. [CrossRef]
4. Prabhakaran, K.; Lombardo, G.; Latifi, R. Telemedicine for trauma and emergency management: An overview. *Curr. Trauma Rep.* **2016**, *2*, 115–123. [CrossRef]
5. Bertoncello, C.; Colucci, M.; Baldovin, T.; Buja, A.; Baldo, V. How does it work? factors involved in telemedicine home-interventions effectiveness: A review of reviews. *PLoS ONE* **2018**, *13*. [CrossRef] [PubMed]
6. Hoffer-Hawlik, M.A.; Moran, A.E.; Burka, D.; Kaur, P.; Cai, J.; Frieden, T.R.; Gupta, R. Leveraging telemedicine for chronic disease management in low- and middle-income countries during covid-19. *Glob. Heart* **2020**, *15*. [CrossRef] [PubMed]
7. Albahri, A.S.; Alwan, J.K.; Taha, Z.K.; Ismail, S.F.; Hamid, R.A.; Zaidan, A.A.; Albahri, O.S.; Zaidan, B.B.; Alamoodi, A.H.; Alsalem, M.A. IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. *J. Netw. Comput. Appl.* **2021**, *173*, 102873. [CrossRef]
8. Chee, R.; Darwish, D.; Fernández-Vega, Á.; Patel, S.N.; Jonas, K.; Ostmo, S.; Chan, R.V.P. Retinal telemedicine. *Curr. Ophthalmol. Rep.* **2018**, *6*, 36–45. [CrossRef] [PubMed]
9. Weinstein, R.S.; Lopez, A.M.; Joseph, B.A.; Erps, K.A.; Holcomb, M.; Barker, G.P.; Krupinski, E.A. Telemedicine, telehealth, and mobile health applications that work: Opportunities and barriers. *Am. J. Med.* **2014**, *127*, 183–187. [CrossRef] [PubMed]
10. Doshi, A.; Platt, Y.; Dressen, J.R.; Mathews, B.K.; Siy, J.C. Keep calm and log on: Telemedicine for COVID-19 pandemic response. *J. Hosp. Med.* **2020**, *15*, 302–304. [CrossRef] [PubMed]
11. Hollander, J.E.; Carr, B.G. Virtually perfect? telemedicine for covid-19. *N. Engl. J. Med.* **2020**, *382*, 1679–1681. [CrossRef] [PubMed]
12. Garg, V.; Brewer, J. Telemedicine security: A systematic review. *J. Diabetes Sci. Technol.* **2011**, *5*, 768–777. [CrossRef] [PubMed]
13. Hall, J.L.; McGraw, D. For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Aff.* **2014**, *33*, 216–221. [CrossRef]
14. Elhoseny, M.; Shankar, K.; Lakshmanaprabu, S.K.; Maseleno, A.; Arunkumar, N. Hybrid optimization with cryptography encryption for medical image security in internet of things. *Neural Comput. Appl.* **2020**, *32*, 10979–10993. [CrossRef]
15. Ramasamy, P.; Ranganathan, V.; Kadry, S.; Damaševičius, R.; Blažauskas, T. An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic-tent map. *Entropy* **2019**, *21*, 656. [CrossRef] [PubMed]
16. Sekar, G.; Valarmathy, S. Embedded crypto compression scheme for secure transmission of biometric data using hot standby router protocol. *J. Comput. Theor. Nanosci.* **2017**, *14*, 5030–5037. [CrossRef]
17. Venčkauskas, A.; Morkevicius, N.; Bagdonas, K.; Damaševičius, R.; Maskeliunas, R. A lightweight protocol for secure video streaming. *Sensors* **2018**, *18*, 1554. [CrossRef] [PubMed]
18. Thanki, R.; Borra, S. Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing. *Multimed. Tools Appl.* **2019**, *78*, 13905–13924. [CrossRef]
19. Xia, Z.; Wang, X.; Li, X.; Wang, C.; Unar, S.; Wang, M.; Zhao, T. Efficient copyright protection for three CT images based on quaternion polar harmonic fourier moments. *Signal Process.* **2019**, *164*, 368–379. [CrossRef]
20. Swaraja, K. Medical image region based watermarking for secured telemedicine. *Multimed. Tools Appl.* **2018**, *77*, 28249–28280. [CrossRef]
21. Huynh-The, T.; Hua, C.-H.; Tu, N.A.; Hur, T.; Bang, J.; Kim, D.; Amin, M.B.; Ho Kang, B.; Seung, H.; Lee, S. Selective bit embedding scheme for robust blind color image watermarking. *Inf. Sci.* **2018**, *426*, 1–18. [CrossRef]
22. Agarwal, N.; Singh, A.K.; Singh, P.K. Survey of robust and imperceptible watermarking. *Multimed. Tools Appl.* **2019**, *78*, 8603–8633. [CrossRef]
23. Thabit, R.; Khoo, B.E. A new robust lossless data hiding scheme and its application to color medical images. *Digit. Signal Process.* **2015**, *38*, 77–94. [CrossRef]
24. Riad, R.; Harba, R.; Douzi, H.; Ros, F.; Elhajji, M. Robust fourier watermarking for ID images on smart card plastic supports. *Adv. Electr. Comput. Eng.* **2016**, *16*, 23–30. [CrossRef]
25. Riad, R.; Ros, F.; Harba, R.; Douzi, H.; Elhajji, M. Enhancement of fourier image watermarking robustness. *Control Eng. Appl. Inform.* **2017**, *19*, 25–33.
26. Liu, X.; Lou, J.; Fang, H.; Chen, Y.; Ouyang, P.; Wang, Y.; Zou, B.; Wang, L. A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images. *IEEE Access* **2019**, *7*, 76580–76598. [CrossRef]
27. Eze, P.; Parampalli, U.; Evans, R.; Liu, D. A new evaluation method for medical image information hiding techniques. In Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Montreal, QC, Canada, 20–24 July 2020; pp. 6119–6122. [CrossRef]
28. Zhang, X.; Wang, S.; Qian, Z.; Feng, G. Reversible fragile watermarking for locating tampered blocks in JPEG images. *Signal Process.* **2010**, *90*, 3026–3036. [CrossRef]
29. Ishtiaq, M.; Ali, W.; Shahzad, W.; Jaffar, M.A.; Nam, Y. Hybrid Predictor Based Four-Phase Adaptive Reversible Watermarking. *IEEE Access* **2018**, *6*, 13213–13230. [CrossRef]
30. Liu, J.; Li, J.; Ma, J.; Sadiq, N.; Bhatti, U.; Ai, Y. A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map. *Appl. Sci.* **2019**, *9*, 700. [CrossRef]
31. Feng, B.; Yu, B.; Bei, Y.; Duan, X. A Reversible Watermark With a New Overflow Solution. *IEEE Access* **2019**, *7*, 28031–28043. [CrossRef]

32. Coatrieux, G.; Pan, W.; Cuppens-Boulahia, N.; Cuppens, F.; Roux, C. Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 111–120. [CrossRef]
33. Deng, X.; Mao, Y.; Hum, J. A Novel Lossless Robust Medical Image Watermarking Algorithm Based on Huffman Coding and K-means Clustering. *Int. J. Digit. Content Technol. Its Appl.* **2012**, *6*, 368–377.
34. An, L.; Gao, X.; Yuan, Y.; Tao, D. Robust lossless data hiding using clustering and statistical quantity histogram. *Neurocomputing* **2012**, *77*, 1–11. [CrossRef]
35. Thabit, R.; Khoo, B.E. Robust reversible watermarking scheme using Slantlet transform matrix. *J. Syst. Softw.* **2014**, *88*, 74–86. [CrossRef]
36. Choi, K.; Pun, C. Difference Expansion Based Robust Reversible Watermarking with Region Filtering. In Proceedings of the 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), Beni Mellal, Morocco, 29 March–1 April 2016; pp. 278–282.
37. Golabi, S.; Helfroush, M.S.; Danyali, H. Non-unit mapped radial moments platform for robust, geometric invariant image watermarking and reversible data hiding. *Inf. Sci.* **2018**, *447*, 104–116. [CrossRef]
38. 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]
39. Giakoumaki, A.; Pavlopoulos, S.; Koutsouris, D. Multiple Image Watermarking Applied to Health Information Management. *IEEE Trans. Inf. Technol. Biomed.* **2006**, *10*, 722–732. [CrossRef] [PubMed]
40. Elshoura, S.M.; Megherbi, D.B. Analysis of noise sensitivity of Tchebichef and Zernike moments with application to image watermarking. *J. Vis. Commun. Image Represent.* **2013**, *24*, 567–578. [CrossRef]
41. Gourrame, K.; Douzi, H.; Harba, R.; Riad, R.; Ros, F.; Amar, M.; Elhajji, M. A zero-bit fourier image watermarking for print-cam process. *Multimed. Tools Appl.* **2019**, *78*, 2621–2638. [CrossRef]
42. Nawaz, S.A.; Li, J.; Bhatti, U.A.; Mehmood, A.; Shoukat, M.U.; Bhatti, M.A. Advance hybrid medical watermarking algorithm using speeded up robust features and discrete cosine transform. *PLoS ONE* **2020**, *15*, 0232902. [CrossRef] [PubMed]
43. Roček, A.; Javorník, M.; Slavíček, K.; Dostál, O. Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging. *J. Digit. Imaging* **2021**, *34*, 204–211. [CrossRef]
44. Wang, Y.; Heidari, M.; Mirniaharikandehei, S.; Gong, J.; Qian, W.; Qiu, Y.; Zheng, B. A hybrid deep learning approach to predict malignancy of breast lesions using mammograms. In Proceedings of the SPIE 10579, Medical Imaging 2018: Imaging Informatics for Healthcare, Research, and Applications, 105790V, Huston, TX, USA, 31 May 2018. [CrossRef]
45. Hosny, K.M.; Darwish, M.M. Robust color image watermarking using invariant quaternion Legendre-Fourier moments. *Multimed. Tools Appl.* **2018**, *77*, 24727–24750. [CrossRef]
46. Hosny, K.M.; Darwish, M.M. Resilient Color Image Watermarking Using Accurate Quaternion Radial Substituted Chebyshev Moments. *ACM Trans. Multimed. Comput. Commun. Appl.* **2019**, *15*, 1–25. [CrossRef]
47. Johnson, K.A.; Becker, J.A. The Whole Brain Atlas. Available online: http://www.med.harvard.edu/AANLIB/home.html (accessed on 23 January 2021).
48. Tian, H.; Zhao, Y.; Ni, R.; Qin, L.; Li, X. LDFT-Based Watermarking Resilient to Local Desynchronization Attacks. *IEEE Trans. Cybern.* **2013**, *43*, 2190–2201. [CrossRef] [PubMed]
49. Priyanka; Maheshkar, S. Region-based hybrid medical image watermarking for secure telemedicine applications. *Multimed. Tools Appl.* **2016**, *76*, 3617–3647. [CrossRef]
50. Thabit, R.; Khoo, B.E. Medical image authentication using SLT and IWT schemes. *Multimed. Tools Appl.* **2015**, *76*, 309–332. [CrossRef]
51. Egiazarian, K.; Astola, J.; Ponomarenko, N.; Lukin, V.; Battisti, F.; Carli, M. New full-reference quality metrics based on HVS. *Proc. Second Int. Workshop Video Process. Qual. Metr.* **2006**, *4*.
52. Kwan, C.; Larkin, J.; Chou, B. Perceptually lossless compression of Mastcam images with Error Recovery. *Signal Process. Sens. Inf. Fusion* **2019**, 1101815. [CrossRef]
53. Cedillo-Hernandez, M.; Cedillo-Hernandez, A.; Garcia-Ugalde, F.; Nakano-Miyatake, M.; Perez-Meana, H. Digital color images ownership authentication via efficient and robust watermarking in a hybrid domain. *Radioengineering* **2017**, 536–551. [CrossRef]
54. Kwan, C. Strange Behaviors and Root Cause in the Compression of Previously Compressed Videos. *Signal Image Process.* **2015**, *1*.
55. Mastoi, Q.; Memon, M.S.; Lakhan, A.; Mohammed, M.A.; Qabulio, M.; Al-Turjman, F.; Abdulkareem, K.M. Machine learning-data mining integrated approach for premature ventricular contraction prediction. *Neural Comput. Applic.* **2021**. [CrossRef]
56. Lakhan, A.; Mastoi, Q.U.A.; Elhoseny, M.; Memon, M.S.; Mohammed, M.A. Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. *Enterp. Inf. Syst.* **2021**. [CrossRef]
57. Leuciuc, F.V.; Craciun, M.D.; Holubiac, I.S.; Mohammed, M.A.; Abdulkareem, K.H.; Pricop, G. Statistical Medical Pattern Recognition for Body Composition Data Using Bioelectrical Impedance Analyzer. *CMC Comput. Mater. Contin.* **2021**, *67*, 2601–2617.
58. Kumar, C.L.; Juliet, A.V.; Ramakrishna, B.; Chakraborty, S.; Mohammed, M.A.; Sunny, K.A. Computational Microfluidic Channel for Separation of Escherichia coli from Blood-Cells. *CMC Comput. Mater. Contin.* **2021**, *67*, 1369–1384.

59. Khalaf, B.A.; Mostafa, S.A.; Mustapha, A.; Mohammed, M.A.; Abduallah, W.M. Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access* **2019**, *7*, 51691–51713. [CrossRef]
60. Mostafa, S.A.; Mustapha, A.; Hazeem, A.A.; Khaleefah, S.H.; Mohammed, M.A. An agent-based inference engine for efficient and reliable automated car failure diagnosis assistance. *IEEE Access* **2018**, *6*, 8322–8331. [CrossRef]