Computers, Materials & Continua
DOI: 10.32604/cmc.2023.036438
Article

Tech Science Press

Zero Watermarking Algorithm for Medical Image Based on Resnet50-DCT

Mingshuai Sheng[1], Jingbing Li[1,2,*], Uzair Aslam Bhatti[1,2,3], Jing Liu[4], Mengxing Huang[1,5] and Yen-Wei Chen[6]

[1]School of Information and Communication Engineering, Hainan University, Haikou, 570228, China
[2]State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, 570228, China
[3]School of Computer Science and Technology, Hainan University, Haikou, 570228, China
[4]Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou, 311121, China
[5]State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, 570228, China
[6]Graduate School of Information Science and Engineering, Ritsumeikan University, Kyoto, 5258577, Japan
*Corresponding Author: Jingbing Li. Email: jingbingli2008@hotmail.com
Received: 30 September 2022; Accepted: 15 November 2022

Abstract: Medical images are used as a diagnostic tool, so protecting their confidentiality has long been a topic of study. From this, we propose a Resnet50-DCT-based zero watermarking algorithm for use with medical images. To begin, we use Resnet50, a pre-training network, to draw out the deep features of medical images. Then the deep features are transformed by DCT transform and the perceptual hash function is used to generate the feature vector. The original watermark is chaotic scrambled to get the encrypted watermark, and the watermark information is embedded into the original medical image by XOR operation, and the logical key vector is obtained and saved at the same time. Similarly, the same feature extraction method is used to extract the deep features of the medical image to be tested and generate the feature vector. Later, the XOR operation is carried out between the feature vector and the logical key vector, and the encrypted watermark is extracted and decrypted to get the restored watermark; the normalized correlation coefficient (NC) of the original watermark and the restored watermark is calculated to determine the ownership and watermark information of the medical image to be tested. After calculation, most of the NC values are greater than 0.50. The experimental results demonstrate the algorithm's robustness, invisibility, and security, as well as its ability to accurately extract watermark information. The algorithm also shows good resistance to conventional attacks and geometric attacks.

Keywords: Medical images; deep residual network; resnet50-DCT; privacy protection; robustness; security

1 Introduction

In digital age, intelligent medicine and telemedicine diagnosis also have a better development. To realize the convenience and speed of medical diagnosis, a large number of medical images have to

be transmitted through the Internet [1], which involves the leakage of medical image information. Whether it is remote diagnosis or data sharing, the protection of patient privacy information is an important concern. Therefore, the protection of medical images are very important. Digital watermarking is an effective means of information protection, which can be used to protect medical images [2,3].

When protecting the medical images, we can't destroy the original medical image, because once the images are destroyed, it will affect the doctor's diagnosis. Therefore, the digital zero watermarking algorithms appear in the research idea of the researchers [4]. Many researchers in the field of image processing use hybrid transformation to solve the problem of leakage in medical image transmission [5–8]. Traditional digital watermarking schemes embed an invisible and detectable watermark in the host image to protect the image. These methods are feasible, but embedding a watermark directly into the image will lead to image distortion, which will affect the doctor's diagnosis. The zero watermarking scheme does not embed any information in the original image, but associates the internal information of watermark with the feature vector of the original image through a logical relationship to form a key [9], and will not modify the original image. Compared with the classical watermarking algorithm, zero watermarking has relatively perfect invisibility and is very suitable for the protection of medical images.

In 2003, Wen et al. proposed zero watermarking, which is a new digital watermarking technique that does not modify the original image data. In this paper, high-order cumulants are used to extract the features of the image to construct zero watermarking [10]. Xiong proposed a robust zero-watermarking algorithm in spatial domain in 2018. The algorithm 1) uses chaotic system to map the location of image blocks, which is sensitive to initial values, and uses chaotic encryption and Arnold space scrambling techniques to preprocess the original watermark signal; 2) uses the robust performance of the relationship between the overall mean and block mean values of all selected blocks in the carrier image to construct feature information; 3) uses chaotic encryption and Arnold space scrambling techniques to post-process the generated zero watermark signal [11]. In 2019, Khan et al. proposed a new zero-watermarking scheme. The scheme generates NDD (neighbor distance difference) contour based on image scanning, whose redundant region shows the perceptual unimportant region of the grayscale image, extracts features from the robust region of the image, and uses reversible XOR operation to generate zero-watermark binary key image [12]. In 2020, Wu and others proposed an image zero watermarking technique based on improved singular value and sub-block mapping. Image features are extracted by Arnold scrambling, Curvelet transform, block segmentation and singular value decomposition (SVD) [13]. At the same time, the original copyright image is divided into different sub-blocks and summed, and different characters are used to represent the watermark sub-blocks. Finally, a feature of the image and watermark sub-block is logically operated by bit to generate zero watermarks [14].

Recently, convolution neural network (CNN) and machine learning algorithms have been applied to computer vision, including the application of extracting image features with trained CNN to complete expected tasks. In this paper, a zero-watermarking algorithm for medical images based on Resnet50 depth residual neural network is proposed. The image features are extracted by the trained CNN to obtain the output of the full connection layer (fc_1000). Then the deep features are further transformed by DCT transform and the feature vector is generated by the hash function. In the image verification phase, the watermark information is restored by a series of operations using the same method, and compared with original watermark information to verify the availability of the algorithm [15].

2 Basic Theoretical Knowledge

2.1 Deep Residual Network ResNet50

The Resnet50 network consists of 49 convolution layers and one fully connected layer. Its network structure can be divided into seven parts. The first part does not contain residual blocks and mainly calculates the convolution, regularization, activation function and maximum pool of the input object. The second, third, fourth and fifth parts of the structure all contain residual blocks, which mainly solve the problem of gradient disappearance with the increase of network layers. In the Resnet50 network structure, the residual block has three convolution layers, so the network has a total of 49 convolution layers. Finally, add a full connection layer, a total of 50 layers, this is the origin of the name Resnet50. The input size of the network is $224 \times 224 \times 3$. After the convolution calculation of the first five parts, the output size is $7 \times 7 \times 2048$. In the pooling layer, it is pooled to reduce the amount of computation and enhance the invariance of image features, and then outputs a feature matrix with a size of 1×1000 after full connection layer processing. The feature of 1×1000 is the [16–18] required by the algorithm, that is, it is used as the image feature vector. The network parameters for ResNet50 are shown in Table 1. The network structure diagram of ResNet50 is shown in Fig. 1.

Table 1: The composition parameters of ResNet50 network

Layer name	Conv1	Conv2_x	Conv3_x	Conv4_x	Conv5_x	
Output size	112×112	56×56	28×28	14×14	7×7	1×1
Parameters	7×7, 64, stride 2	3×3 maxpool, stride 2				average pool, 1000-fc, softmax
		$\begin{bmatrix} 1 \times 1, 64 \\ 3 \times 3, 64 \\ 1 \times 1, 256 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 128 \\ 3 \times 3, 128 \\ 1 \times 1, 512 \end{bmatrix} \times 4$	$\begin{bmatrix} 1 \times 1, 256 \\ 3 \times 3, 256 \\ 1 \times 1, 1024 \end{bmatrix} \times 6$	$\begin{bmatrix} 1 \times 1, 512 \\ 3 \times 3, 512 \\ 1 \times 1, 2048 \end{bmatrix} \times 3$	

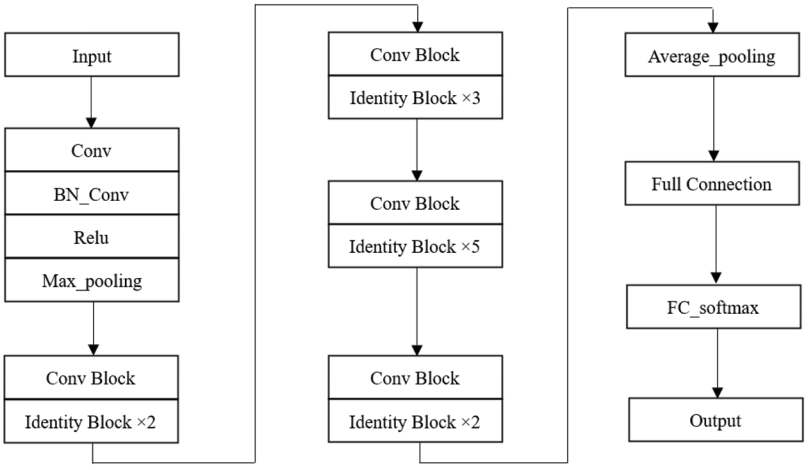


Figure 1: The ResNet50 network structure

The ResNet50 used in this algorithm has two basic blocks, one is Identity Block, the dimensions of input and output are the same, so multiple can be connected in series; the other basic block is Conv Block, the dimensions of input and output are different, so it can't be connected continuously,

its function is to change the dimension of the feature vector. The two residual blocks contained in ResNet50 are shown in Figs. 2a and 2b.

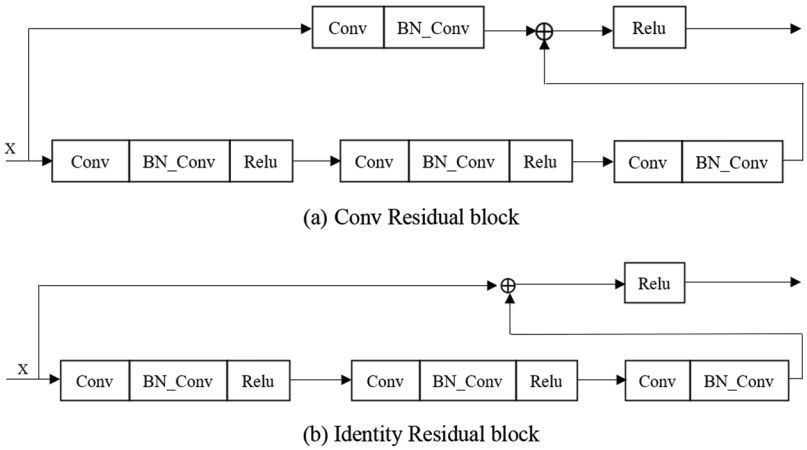


Figure 2: Network structure diagram of the residual blocks

2.2 DCT Transformation

DCT transform, the full name of discrete cosine transform, is mainly used for data or image compression. Because the DCT transform is symmetrical, the DCT inverse transform can be used to recover the original image information after quantization coding. DCT transform has a wide range of applications in the current compression field. It can be used not only in our commonly used JPEG still image coding, but also in MJPEG and MPEG dynamic coding [19,20].

The two-dimensional discrete cosine transform (DCT) is:

$$F(u,v) = c(u)\,c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \quad u = 0,1,2,\ldots,M-1;$$
$$v = 0,1,\ldots,N-1 \tag{1}$$

The inverse two-dimensional discrete cosine transform (IDCT) is:

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u)\,c(v)\,F(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)}{2N} \quad x = 0,1,\ldots,\mathrm{M}-1;$$
$$y = 0,1,\ldots,\mathrm{N}-1 \tag{2}$$

In the formula, x, y is the sampling value of the image in the spatial domain. u, v is sampling value of the image in the frequency domain.

2.3 Logistic Chaotic Map

Logistic map is a very simple chaotic map in mathematical form, which was used to describe the changes in the population as early as the 1950s. This mapping has extremely complex dynamic behavior and is widely used in field of secure communication [21,22]. Its mathematical expression formula is as follows:

$$X_{s+1} = \mu \cdot x_s \cdot (1 - x_s) \cdot x \in [0, 1], \quad \mu \in [0, 4], \tag{3}$$

where μ ∈ [0, 4] is called Logistic parameter. It is shown that when x ∈ [0, 1], the Logistic map works in a chaotic state, that is to say, the sequence generated by the initial condition x the action of the Logistic map is aperiodic and non-convergent. When we use the Logistic chaotic system, we can first let the system iterate a certain number of times, and then use the generated value, which can better cover up the original situation and have better security.

2.4 Algorithm Evaluation Index

2.4.1 Correlation Coefficient

In this paper, normalized correlation degree (NC) is used as one of the indicators to measure the performance of the algorithm, that is, to evaluate the robustness of the algorithm. It is usually required that the value of the correlation coefficient be greater than 0.5 [23]. NC is defined as:

$$NC = \frac{\sum_m \sum_n \left(A_{mn-}\overline{A}\right)\left(B_{mn} - \overline{B}\right)}{\sqrt{\left(\sum_m \sum_n \left(A_{mn} - \overline{A}\right)^2\right)\left(\sum_m \sum_n \left(B_{mn} - \overline{B}\right)^2\right)}} \tag{4}$$

In the formula, m and n are the coordinate points of the image pixels; A and B are the pixel values corresponding to the corresponding coordinate points; $\overline{A}$ and $\overline{B}$ are the average values of A and B, respectively.

2.4.2 Peak Signal-to-Noise Ratio

The second evaluation index in this paper, PSNR, is used to measure image quality. PSNR is required to be greater than or equal to 10 in this article [24]. The following formula is the mathematical expression of the peak signal-to-noise ratio (PSNR):

$$PSNR = 10 \lg \left[\frac{mn \max_{i,j}(I_{(i,j)})^2}{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i,j) - I'(i,j))^2} \right] \tag{5}$$

In the formula, [m, n] refers to the size of the image, and $I(i, j)$ refers to the pixel value at the coordinate point (i, j). If the PSNR value is larger, the smaller the image distortion is.

3 Algorithm Implementation Flow

The algorithm mainly consists of three parts, namely, image feature extraction, zero watermark construction and embedding, and zero watermark extraction. First of all, the image features are extracted by ResNet50 and DCT transform, and the feature vector is generated by perceptual hash. Secondly, the XOR operation between the feature vector generated in the previous step and the encrypted watermark is carried out to get the zero watermark and embed the zero watermark. Finally, the zero-watermark detection algorithm is used to extract the watermark.

3.1 Generation of Image Feature Vector

In this paper, the medical image with the size of 512 × 512 is selected as input image, but the pre-training network ResNet50 requires the image input size to be 224 × 224 × 3 s, so it is necessary

to preprocess the original medical image. We send the preprocessed medical image to the pre-training network ResNet50, and the image is extracted from the deep features through the convolution layer and pooling layer of the network, and then through the full connection layer to get the output-"fc_1000". The DCT transformation of "fc_1000" is performed to obtain a DCT transform coefficient matrix, and then the 64-bit valid coefficients are captured in this matrix and combined with the perceptual hash algorithm to generate the feature vectors of the image [25,26]. The flowchart of the overall implementation is shown in Fig. 3:

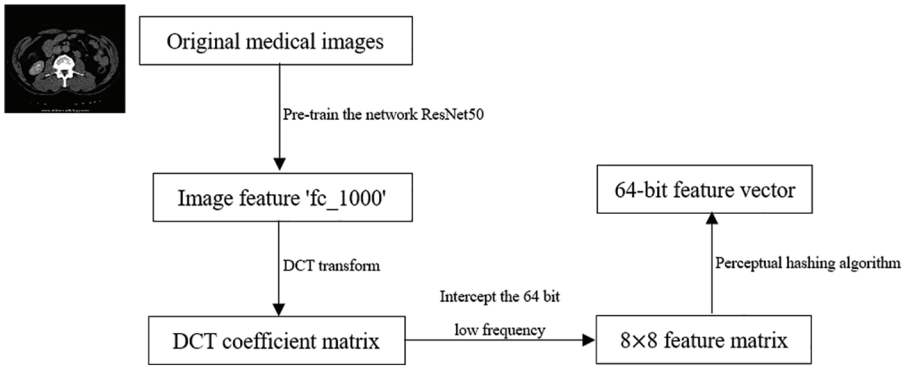


Figure 3: Flowchart of image feature extraction

3.2 Construction and Embedding Process of Zero Watermark

The construction and embedding process of zero watermark is shown in Fig. 4, which is described below. Where i and j refer to the horizontal and vertical coordinate values where a pixel is located.

1. Read the single-channel medical image im(i, j), and convert the image into a three-channel image Im(i, j).
2. Read the original watermark image $b(i,j)$, scramble it using Logistic chaotic map, and obtain the encrypted watermark image $B(i,j)$. The size of the watermark image is set to 64×64.
3. This step is mainly to extract the medical image feature and combine the perceptual hashing algorithm to generate the feature vector $F(i,j)$. The procedure is the same as Section 3.1.
4. The scrambled watermark image performs XOR operation with the medical image feature sequence, that is, the construction and embedding of zero watermark is realized. At the same time, the logical key $Key(i,j)$ is obtained and stored in a third party for subsequent use.

3.3 Extraction Process of Zero Watermark

The extraction process of the zero-watermark image is shown in Fig. 5, which is described as follows. Where i and j refer to the horizontal and vertical coordinate values where a pixel is located.

1. Read the single-channel medical image to be tested $im'(i,j)$, and convert the image into three-channel medical image $\mathrm{Im}'(i,j)$.
2. The main purpose of this step is to extract the feature of the image to be tested and generate the feature vector $F'(i,j)$. The procedure is the same as Section 3.1.
3. The feature vector of the medical image to be tested $F'(i,j)$ and the logical key $Key(i,j)$ obtained from step 4 in Section 3.2 perform XOR operation, and the encrypted watermark $B'(i,j)$ is extracted [27,28].
4. After another XOR operation between the chaotic matrix generated by Logistic chaos and the watermark $B'(i,j)$, the watermark $b'(i,j)$ is obtained.

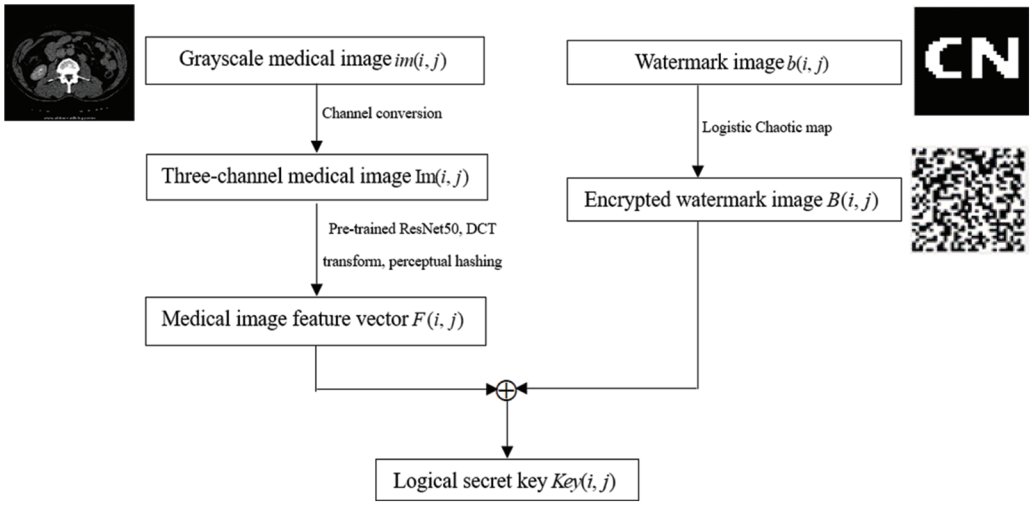


Figure 4: Flowchart of construction and embedding of zero watermark

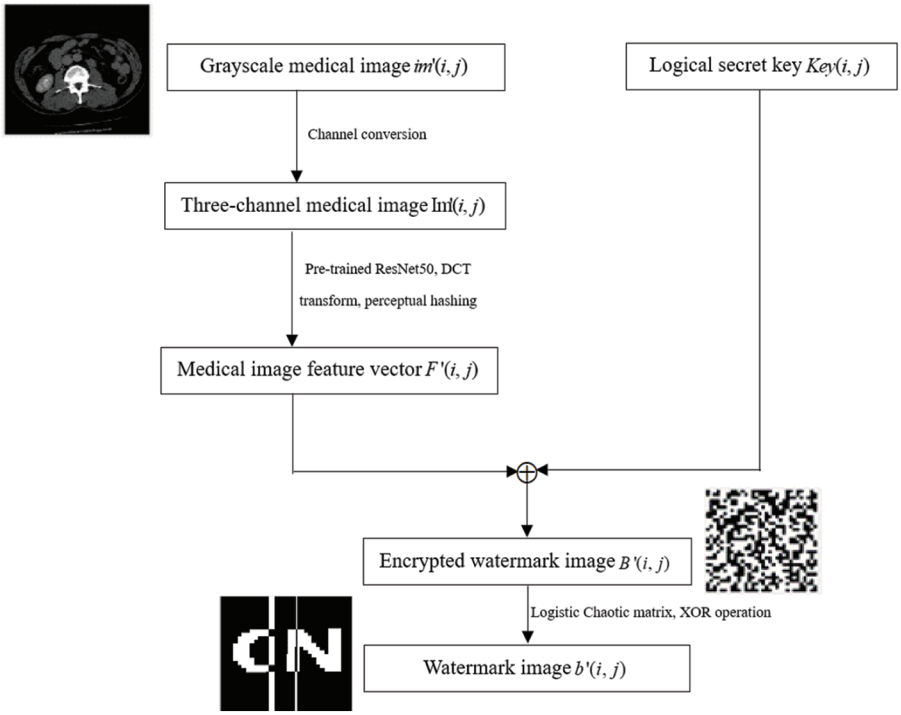


Figure 5: Flowchart of zero-watermark image extraction

4 Analysis of Experiments and Results

The purpose of this experiment is to verify the performance and effectiveness of the algorithm by using conventional attacks (non-geometric attacks) and geometric attacks. Section 4.1.1 lists the experimental results of the algorithm's ability to resist conventional attacks, and Section 4.1.2 lists the experimental results of the algorithm's ability to resist geometric attacks. The medical image used in

the experiment is shown in Fig. 6a, and the watermark image and the scrambled image are shown in Figs. 6b and 6c.

Figure 6: Medical image and watermark image. (a) Original medical image; (b) Original watermark image; (c) Encrypt watermark image

In addition, the NC values between different images are tested, which are all less than 0.5, which can distinguish different images. The experimental figure is shown in Fig. 7 and the results are shown in Table 2. Among them, two values in Table 2 are 0.56, which is greater than the set reference value 0.50 described earlier, which may be because the shapes or types of individual images are somewhat similar.

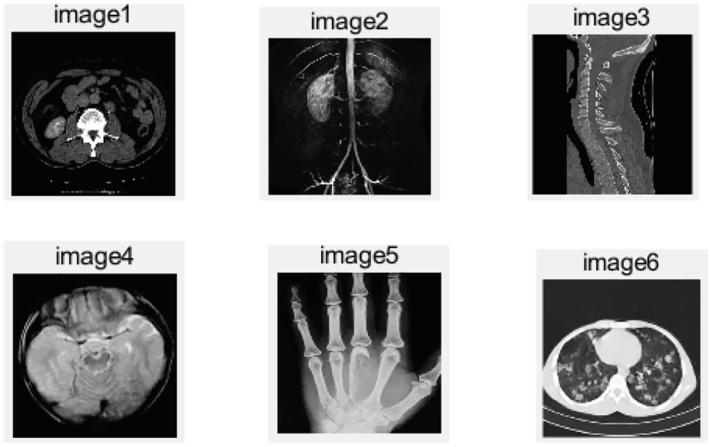


Figure 7: Six different medical images

Table 2: Correlation coefficient between different images

	image1	image2	image3	image4	image5	image6
image1	1.00	0.31	0.37	0.47	0.47	0.56
image2	0.31	1.00	0.31	0.28	0.28	0.06
image3	0.37	0.31	1.00	0.22	0.47	0.31
image4	0.47	0.28	0.22	1.00	0.43	0.22
image5	0.47	0.28	0.47	0.43	1.00	0.34
image6	0.56	0.06	0.31	0.22	0.34	1.00

4.1 Conventional Attacks

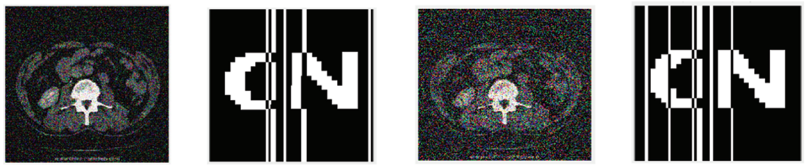
This part shows experimental data when attack intensity increases gradually in the case of a conventional attack. The experimental results show that the algorithm proposed in this paper is robust against non-geometric attacks.

4.1.1 Gaussian Noise Attack

As shown in Table 3 and Fig. 8, We use Gaussian noise with different attack degrees to carry on the experiment. When the interference coefficient of Gaussian noise is 5%, the NC value of the watermark is 0.83. When the set value of the Gaussian interference coefficient is 10%, the NC is 0.68, and the relatively complete watermark information can still be extracted.

Table 3: PSNR and NC value of image after being attacked by noise

Noise attack intensity	1%	3%	5%	8%	10%
PSNR (dB)	21.94	17.43	15.38	12.63	13.48
NC	0.77	0.78	0.83	0.61	0.68



(a) (b) (c) (d)

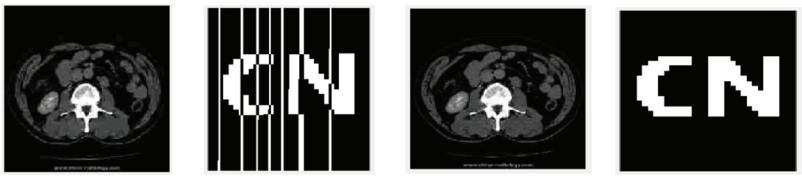
Figure 8: Image under gaussian noise attack. (a) Interference coefficient of 3%; (b) Extracted watermark with Gaussian an interference coefficient of 3%; (c) Interference coefficient of 10%; (d) Extracted watermark with Gaussian interference coefficient of 10%

4.1.2 JPEG Compression Attack

JPEG compression is widely used in image compression processing, and JPEG attacks are also one of the common non-geometric attacks in digital watermarking. As shown in Table 4. When the compression quality reaches 40%, the NC value of the extracted watermark is 0.96. When the compression quality is 30%, the extracted watermark image and the attacked medical image are shown in Fig. 9, and their clarity is very high.

Table 4: PSNR and NC value of image after compression attack

JPEG compress attack strength	5%	10%	15%	20%	30%	40%
PSNR (dB)	25.83	28.92	30.25	30.25	32.69	33.56
NC	0.62	0.74	0.74	0.88	1.00	0.96



(a) (b) (c) (d)

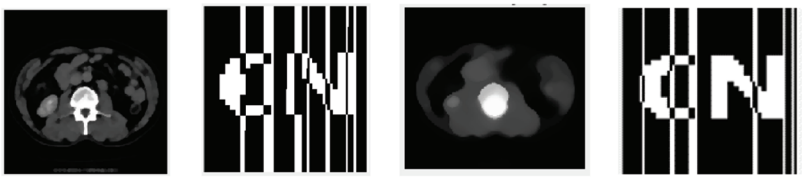
Figure 9: Image under JPEG compression. (a) Compression quality of 30%; (b) Extracted watermark with JPEG quality of 30%; (c) Compression quality of 30%; (d) Extracted watermark with JPEG quality of 30%

4.1.3 Median Filtering Attack

As shown in Table 5, median filter window sizes for testing are 3×3, 5×5 and 7×7. When filtering times is 15 times, NC values of extracted watermarks after the attack are 0.50, 0.72 and 0.62 respectively. When filter window size is 7×7, and the filtering time is 25, the NC value is 0.72. At this time, the valid watermark information can still be extracted, and the extracted watermark image and the attacked medical image are shown in Fig. 10.

Table 5: PSNR and NC value of image after filtering attack

Filter window size	3×3			5×5			7×7		
Filtering times	5	15	25	5	15	25	5	15	25
PSNR (dB)	28.97	27.90	27.64	24.29	22.52	21.98	22.19	20.76	20.35
NC	0.53	0.50	0.50	0.56	0.72	0.66	0.59	0.62	0.72



(a) (b) (c) (d)

Figure 10: Image under median filtering attack. (a) Filter window size of 3×3 and a filtering number of 25 times; (b) Watermark extracted when filter window size is 3×3 and filter times is 25 times; (c) Filter window size of 7×7 and filtering number of 25 times; (d) Watermark extracted when filter window size is 7×7 and filter times is 25 times

4.2 Geometric Attack

The content of this part gives the experimental data of the image under different degrees of geometric attacks. Experimental results show that the proposed algorithm has a good ability to resist geometric attacks, can effectively protect personal privacy information, and has good robustness.

4.2.1 Rotation Attack

Rotate clockwise. After rotating the image by 30°, the NC value of the extracted watermark information is 0.79. When the image is rotated to 80°, the NC is 0.82. After the image is rotated by 80°, the relatively complete watermark information can still be extracted, which shows that the algorithm has good robustness. The experimental results of different degrees of rotation attacks are shown in Table 6, and the extracted images are shown in Figs. 11a and 11b.

Table 6: PSNR and NC value after being attacked by Rotation attack (clockwise)

Rotation attack (clockwise)	5°	15°	30°	40°	60°	80°
PSNR (dB)	19.40	16.38	15.31	15.03	14.26	13.81
NC	0.88	0.81	0.79	0.84	0.80	0.82

(a) (b) (c) (d)

Figure 11: Image under Rotation attack. (a) Rotated 80 °clockwise; (b) Watermark extracted after being rotated 80 °clockwise; (c) Rotated 80 °counterclockwise; (d) Watermark extracted after 80 °counterclockwise rotation

Rotate counterclockwise. After the image is rotated 40°, the NC value of the extracted watermark information is 0.91. When the image is rotated to 80°, the NC value is 0.80. After the image is rotated by 80°, the relatively complete watermark information can still be extracted, which shows that the algorithm has good robustness. The experimental results of different degrees of rotation attacks are shown in Table 7, and the extracted images are shown in Figs. 11c and 11d.

Table 7: PSNR and NC value after being attacked by Rotation attack (counterclockwise)

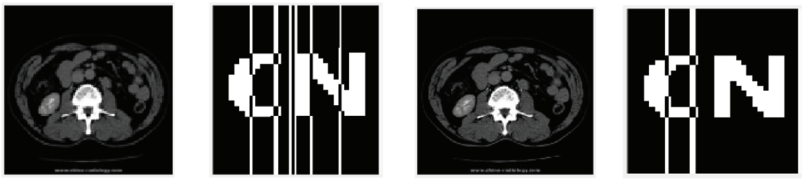
Rotation attack (Counterclockwise)	5°	15°	30°	40°	60°	80°
PSNR (dB)	19.40	16.38	15.31	15.03	14.26	13.81
NC	0.85	0.85	0.88	0.91	0.75	0.80

4.2.2 Zoom Attack

As shown in Table 8, when the magnification is 0.5x, the NC is 0.77. The value is greater than the set standard value of 0.50, that is, a valid value. After the image is scaled 1.6 times, the watermark NC is 0.89. After scaling the image 2 times, the extracted watermark image is clearly visible. The image is shown in Fig. 12.

Table 8: PSNR and NC value of an image after zoom attack

Zoom attack times	0.2	0.5	1.0	1.2	1.6	2.0
PSNR (dB)	–	–	–	–	–	–
NC	0.62	0.77	1.00	0.89	0.89	0.89



(a) (b) (c) (d)

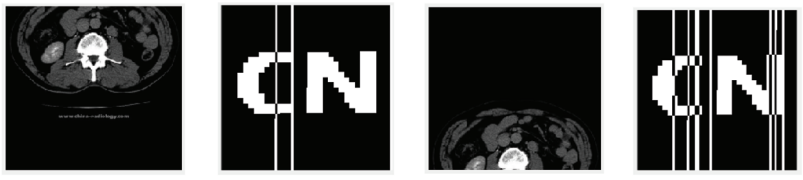
Figure 12: Image under Zoom attack. (a) Scaled 0.5 times; (b) Watermark extracted after scaling 0.5 times; (c) Scaled 2.0 times; (d) Watermark extracted after scaling 2.0 times

4.2.3 Translation Attack

Table 9 shows the experimental data of the image after being attacked. The image is moved up by 10% and the score NC is 0.92. When the image is moved up by 30%, the NC value of the watermark is 0.93, close to 1.00. The medical image after 30% translation is shown in Fig. 13a, and the extracted watermark image is shown in Fig. 13b. As shown in Table 10, move the image down 15%, and the NC value is 0.91. When the image moves down 40%, the NC value of the watermark is 0.75. The medical image after 40% translation is shown in Fig. 13c, and the extracted watermark image is shown in Fig. 13d.

Table 9: PSNR and NC value of image after translation attack (upward)

Translation attack (upward)	5%	10%	15%	20%	30%	40%
PSNR (dB)	15.46	14.05	13.17	12.48	11.59	11.31
NC	0.93	0.92	0.93	0.91	0.93	0.74



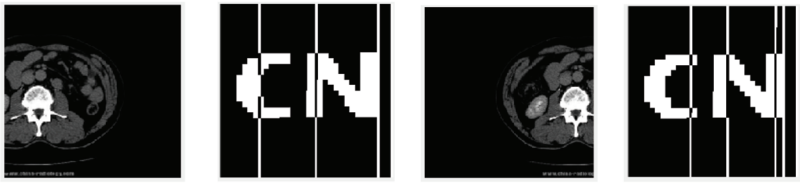
(a) (b) (c) (d)

Figure 13: Image under Translation attack. (a) Translate 30% (up); (b) Watermark extracted after 30% translation upward; (c) Translate 40% (down); (d) Watermark extracted after 40% translation down

Table 10: PSNR and NC value of image after translation attack (downward)

Translation attack (downward)	5%	10%	15%	20%	30%	40%
PSNR (dB)	15.69	14.27	13.29	12.65	11.90	12.26
NC	0.88	0.88	0.91	0.79	0.61	0.75

The proportion of the image translating to the left is 15%. The NC is 0.98, which is very close to 1.00. When the image is translated 40% to the left, NC value is 0.85. The image translating 30% to the left is shown in Fig. 14a, and the extracted watermark image is shown in Fig. 14b. The experimental results here are shown in Table 11. As shown in Table 12, the ratio of translation to the right of the image is 10% and the proportion of pencil NC is 0.93. When the image is translated 40% to the right, the NC value is 0.84. The image translated 40% to the right is shown in Fig. 14c, and the extracted watermark image is shown in Fig. 14d.



(a) (b) (c) (d)

Figure 14: Image under Translation attack. (a) Translate 30% (left); (b) Translate 30% of the extracted watermark image to the left; (c) Translate 40% (right); (d) Translate 40% of the extracted watermark image to the right

Table 11: PSNR and NC value of image after translation attack (left)

Translation attack (left)	5%	10%	15%	20%	30%	40%
PSNR (dB)	15.14	14.17	13.29	12.87	12.43	12.19
NC	0.92	0.87	0.98	0.92	0.88	0.85

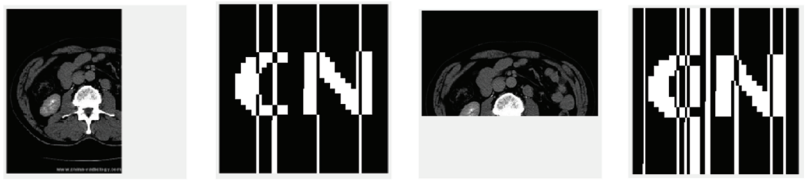
Table 12: PSNR and NC value of image after translation attack (right)

Translation attack (right)	5%	10%	15%	20%	30%	40%
PSNR (dB)	15.29	14.32	13.36	12.98	12.39	12.08
NC	0.97	0.93	0.93	0.90	0.92	0.84

4.2.4 Clipping Attack

The effect of the experiment is shown in Fig. 15. Fig. 15a is the experimental object that has been cut by 30%, and Fig. 15b is the extracted watermark image. As can be seen from Table 13, when the image is cut by 15%, the NC still reaches 0.91. When the cut ratio reaches 40%, the NC is 0.77, which is still greater than 0.50. Fig. 15c is the experimental object that was cut by 40%, and Fig. 15d is the

watermark image extracted at this time. As can be seen from Table 14, the image cut ratio of 15% of the image is still 0.88. When the cut ratio reaches 40%, the NC is 0.65, which is still greater than 0.50.



(a) (b) (c) (d)

Figure 15: Image under Clipping attack. (a) Cut 30%; (b) Watermark extracted after clipping attack 30%; (c) Cut 40%; (d) Watermark extracted after clipping attack (40%)

Table 13: PSNR and NC value of image after clipping attack (X-axis)

Clipping attack (X axis)	5%	15%	20%	30%	40%
PSNR (dB)	–	–	–	–	–
NC	0.94	0.91	0.84	0.81	0.77

Table 14: PSNR and NC value of image after clipping attack (Y axis)

Clipping attack (Y axis)	5%	15%	20%	30%	40%
PSNR (dB)	–	–	–	–	–
NC	0.75	0.88	0.80	0.74	0.65

5 Algorithm Comparison

To further illustrate the anti-geometric attack ability of the algorithm, some experimental data are compared. The comparison results are shown in Table 15. As can be seen from the table, for non-geometric attacks, such as Gaussian noise and JPEG compression (the attack intensity of the two is 5%), the performance of the proposed algorithm is slightly lower than that of the algorithm proposed by others in Table 15 [29–32], but the NC value of the two kinds of attacks is more than 0.5, which shows that the algorithm is robust.

For geometric attacks, when the rotation angle reaches 10°, the NC value can reach 0.88 respectively, while the NC value of the algorithm [29,30] is 0.82 and 0.61 respectively. When the rotation angle reaches 20°, the NC values of the algorithm [29,30] are 0.79 and 0.53 respectively. In this paper, it is proposed that the clockwise rotation angle of the algorithm can reach 80°, which is much higher than that of the algorithm [29–32]. For the downward translation attack with 15% attack intensity, the NC values of algorithm [30] and algorithm [32] are 0.61, 0.90 respectively, and the proposed algorithm NC is 0.91. For the left translation attack with 10% attack intensity, the NC value of the algorithm [29] is 0.63, and the proposed algorithm NC is 0.87. For the right translation attack with 5% attack intensity, the NC value of the algorithm [31,32] is 0.90, and the proposed algorithm NC is 0.97. When cutting in Y direction, when the shear ratio is 20%, the NC value of algorithm [29] is 0.64, the NC value of algorithm [31] is 0.79, and the NC of the proposed algorithm is 0.80. at the same time, it

shows that the algorithm has a stronger ability to resist geometric attacks and a better effect than the algorithm [29–32].

To sum up, the proposed algorithm has good robustness and invisibility. The algorithm can effectively prevent information leakage and protect personal privacy information.

Table 15: Comparison of experimental results of different algorithms

Attack type	Attack intensity	Yang et al. [29]	Liu et al. [30]	Zeng et al. [31]	Yi et al. [32]	Proposed algorithm
Gaussian noise	5%	0.92	0.93	0.79	0.90	0.83
JPEG compression	5%	-	-	0.79	0.90	0.62
Rotation(clockwise)	10°	0.82	0.61	-	-	**0.88**
	20°	0.79	0.53	-	-	**0.86**
	80°	-	-	-	-	**0.82**
Translation(down)	15%	-	0.61	-	0.90	**0.91**
Translation(left)	10%	0.63	-	-	-	**0.87**
Translation(right)	5%	-	-	0.90	0.90	**0.97**
Cropping(Y-axis)	20%	0.64	-	0.79	-	**0.80**

6 Conclusion

In recent years, the algorithm for watermarking medical images against geometric attacks has been a hot topic and a challenge in the study of robust watermarking technology. A zero watermarking algorithm based on Resnet50-DCT is designed to withstand geometric attacks in this paper. Resnet50-DCT is used to extract the deep features of medical images, while a two-dimensional discrete cosine transform and a mean-aware hashing algorithm are used to generate the zero watermark. Combining the concepts of Deep Residual Neural Network, Discrete Cosine Transform, and zero watermarking, the algorithm's design process primarily solves the problem of watermarks resisting geometric attacks. Likewise, the scrambling encryption of the watermark image ensures the algorithm's safety. According to the aforementioned experimental findings, the proposed algorithm is efficient and trustworthy, and has some practical value for the protection of medical and patient-specific data.

However, the algorithm needs to be improved. From the experimental data, it is difficult for the algorithm to strike a balance between geometric attacks and non-geometric attacks. Not only will this algorithm encounter this problem, but also the same kind of algorithms proposed by others will encounter this dilemma. Therefore, I have some ideas: as the core tools of the algorithm-ResNet50 and DCT transform, the combination of them or changing the type of transformation will also affect the performance of the algorithm. The function of the core tool is to extract image features, and the future research direction may be to find the optimal feature extraction method to balance the performance of the algorithm under geometric and non-geometric attacks.

Funding Statement: This work was supported in part by the Natural Science Foundation of China under Grants 62063004, the Key Research Project of Hainan Province under Grant ZDYF2021SHFZ093, the Hainan Provincial Natural Science Foundation of China under Grants 2019RC018 and 619QN246, and the postdoctor research from Zhejiang Province under Grant ZJ2021028.

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

References

[1] U. A. Bhatti, M. X. Huang, D. Wu, Y. Zhang, A. Mehmood *et al.*, "Recommendation system using feature extraction and pattern recognition in clinical care systems," *Enterprise Information Systems*, vol. 13, no. 3, pp. 329–351, 2019.

[2] N. Nouioua, A. Seddiki and A. Ghaz, "Blind digital watermarking framework based on DTCWT and NSCT for telemedicine application," *Traitement du Signal*, vol. 37, no. 6, pp. 955–964, 2020.

[3] S. Sharma, U. Chauhan, R. Khanam and K. K. Singh, "Digital watermarking using grasshopper optimization algorithm," *Open Computer Science*, vol. 11, no. 1, pp. 330–336, 2021.

[4] Z. Q. Xia, X. Y. Wang, C. P. Wang, C. X. Wang, B. Ma *et al.,* "A robust zero-watermarking algorithm for lossless copyright protection of medical images," *Applied Intelligence*, vol. 52, no. 1, pp. 1–15, 2021.

[5] A. Zulfiqar, F. Amin and H. Muhammad, "A novel fragile zero-watermarking algorithm for digital medical images," *Electronics*, vol. 11, no. 5, pp. 710, 2022.

[6] S. U. Bazai and J. Jang-Jaccard, "In-memory data anonymization using scalable and high performance RDD design." *Electronics*, vol. 9, no. 10, pp. 1732, 2020.

[7] Q. N. Dai, J. B. Li, U. A. Bhatti, Y. W. Chen and J. Liu, "SWT-DCT-based robust watermarking for medical image," In: Y. W. Chen, A. Zimmermann, R. Howlett and L. Jain (Eds.), *Innovation in Medicine and Healthcare Systems, and Multimedia. Smart Innovation, Systems and Technologies*, vol 145, pp. 93–103, Singapore: Springer, 2019.

[8] P. Aparna and P. V. V. Kishore, "Biometric-based efficient medical image watermarking in E-healthcare application," *IET Image Processing*, vol. 13, no. 3, pp. 421–428, 2019.

[9] M. Cedillo-Hernandez, A. Cedillo-Hernandez, M. Nakano-Miyatake and H. Perez-Meana, "Improving the management of medical imaging by using robust and secure dual watermarking," *Biomedical Signal Processing and Control*, vol. 56, pp. 101695, 2020.

[10] Q. Wen, T. F. Sun and S. X. Wang, "Concept and application of zero-watermark," *Journal of Electronic Science*, vol. 31, no. 2, pp. 214–216, 2003.

[11] X. G. Xiong, "Strong robust zero watermarking scheme in spatial domain," *Journal of Automation*, vol. 44, no. 1, pp. 160–175, 2018.

[12] M. F. Khan, S. M. G. Monir and I. Naseem, "A novel zero-watermarking based scheme for copyright protection of grayscale images," *Mehran University Research Journal of Engineering and Technology*, vol. 38, no. 3, pp. 627–640, 2019.

[13] D. Y. Wu, J. Zhao, G. P. Wang, X. D. Zhang, L. Sheng *et al.,* "An image zero watermarking technique based on improved singular value and subblock mapping," *Journal of Optics*, vol. 40, no. 20, pp. 85–97, 2020.

[14] S. U. Bazai, J. Jang-Jaccard and H. Alavizadeh, "Scalable, high-performance, and generalized subtree data anonymization approach for apache spark," *Electronics*, vol. 10, no. 5, pp. 589, 2021.

[15] A. Fierro-Radilla, M. Nakano-Miyatake, M. Cedillo-Hernandez, L. Cleofas-Sanchez and H. Perez-Meana, "A robust image zero-watermarking using convolutional neural networks," in *2019 7th Int. Workshop on Biometrics and Forensics (IWBF)*, Cancun, Mexico, 2019.

[16] N. Behar and M. Shrivastava, "ResNet50-based effective model for breast cancer classification using histopathology images," *Computer Modeling in Engineering & Sciences*, vol. 130, no. 2, pp. 823–839, 2022.

[17] J. T. Yuan, Y. Y. Fan, X. Y. Lv, C. Chen, D. B. Li *et al.,* "Research on the practical classification and privacy protection of CT images of parotid tumors based on resnet50 model," *Journal of Physics: Conference Series*, vol. 1576, no. 1, pp. 012040, 2020.

[18] B. R. Han, J. L. Du, Y. Y. Jia and H. Z. Zhu, "Zero-watermarking algorithm for medical image based on VGG19 deep convolution neural network," *Journal of Healthcare Engineering*, vol. 2021, pp. 5551520–5551520, 2021.

[19] J. Liu, J. Li, Y. Chen *et al.,* "A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain," *Computers, Materials and Continua*, vol. 61, no. 1, pp. 363–378, 2019.

[20] J. T. Huang, S. S. Shi, Z. Y. He and T. Luo, "A novel zero watermarking based on DT-CWT and quaternion for HDR image," *Electronics*, vol. 10, no. 19, pp. 2385, 2021.

[21] Y. Yang, X. X. Xiao, X. Cai and W. M. Zhang, "A secure and privacy preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images," *IEEE Signal Processing Letters*, vol. 27, pp. 256–260, 2020.
[22] S. Thakur, A. K. Singh, S. P. Ghrera and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimedia Tools and Applications*, vol. 79, pp. 4263–4276, 2020.
[23] B. W. Wang, W. S. Wang and P. Zhao, "A Zero-watermark algorithm for multiple images based on visual cryptography and image fusion," *Journal of Visual Communication and Image Representation*, vol. 87, pp. 103569, 2022.
[24] S. Khafaga Doaa, K. Karim Faten, M. Darwish Mohamed and M. Hosny Khalid, "Robust zero-watermarking of color medical images using multi-channel Gaussian-hermite moments and 1D chebyshev chaotic Map,"*Sensors*, vol. 22, no. 15, pp. 5612, 2022.
[25] C. Gong, J. B. Li, U. A. Bhatti, M. Gong, J. X. Ma *et al.,* "Robust and secure zero-watermarking algorithm for medical images based on harris-SURF-DCT and chaotic map," *Hindawi Limited*, vol. 2021, 2021.
[26] L. Jing, Z. T. Sun, K. X. Chen, X. Wen and X. Y. Cheng, "Remote sensing image zero watermarking algorithm based on DFT," *Journal of Physics: Conference Series*, vol. 1865, no. 4, pp. 042034, 2021.
[27] H. Shi, Y. N. Li, B. Y. Hu, M. H. Chen and Y. G. Ren, "A robust and secure zero-watermarking copyright authentication scheme based on visual cryptography and block G-H feature,"*Multimedia Tools and Applications*, vol. 81, no. 26, pp. 1–33, 2022.
[28] X. C. Wang, M. Z. Wen, X. D. Tan, H. Y. Zhang, J. P. Hu *et al.,* "A novel zero-watermarking algorithm based on robust statistical features for natural images," *The Visual Computer*, vol. 38, pp. 9–10, 2022.
[29] C. S. Yang, J. B. Li, U. A. Bhatti, J. Liu, J. X. Ma *et al.,* "Robust zero watermarking algorithm for medical images based on zernike-DCT," *Security and Communication Networks*, vol. 2021, 2021.
[30] J. Liu, J. B. Li, J. R. Cheng, J. X. Ma, N. Sadiq *et al.,* "A novel robust watermarking algorithm for encrypted medical image based on DTCWT-DCT and chaotic map," *Computers, Materials and Continua*, vol. 61, no. 2, pp. 889–910, 2019.
[31] C. Zeng, J. Liu, J. B. Li, J. R. Chen, J. J. Zhou *et al.,* "Multi-watermarking algorithm for medical image based on KAZE-DCT," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–9, 2022.
[32] D. Yi, J. B. Li, Y. X. Fang, W. F. Cui, X. L. Xiao *et al.,* "A robust zero-watermarking algorithm based on PHTs-DCT for medical images in the encrypted domain," In: Y. W. Chen, S. Tanaka, R. J. Howlett, L. C. Jain (Eds.), *Smart Innovation in Medicine and Healthcare*, vol. 242, pp. 101–113, Singapore: Springer, 2021.