electronics

MDPI

Article

Robust Zero Watermarking Algorithm for Medical Images Based on Improved NasNet-Mobile and DCT

Fangchun Dong [1], Jingbing Li [1,*], Uzair Aslam Bhatti [1], Jing Liu [2], Yen-Wei Chen [3] and Dekai Li [1]

[1] School of Information and Communication Engineering, Hainan University, Haikou 570228, China; 21220854000140@hainanu.edu.cn (F.D.); uzairaslambhatti@hotmail.com (U.A.B.); 21220854000150@hainanu.edu.cn (D.L.)
[2] Research Center for Healthcare Data Science, Zhejiang Laboratory, Hangzhou 311121, China; liujinglj@zhejianglab.com
[3] Graduate School of Information Science and Engineering, Ritsumeikan University, Kusatsu 525-8577, Japan; chen@is.ritsumei.ac.jp
* Correspondence: jingbingli2008@hotmail.com; Tel.: +86-136-3765-8206

Abstract: In the continuous progress of mobile internet technology, medical image processing technology is also always being upgraded and improved. In this field, digital watermarking technology is significant and provides a strong guarantee for medical image information security. This paper offers a robustness zero watermarking strategy for medical pictures based on an Improved NasNet-Mobile convolutional neural network and the discrete cosine transform (DCT) to address the lack of robustness of existing medical image watermarking algorithms. First, the structure of the pre-training network NasNet-Mobile is adjusted by using a fully connected layer with 128 output and a regression layer instead of the original Softmax layer and classification layer, thus generating a regression network with 128 output, whereby the 128 features are extracted from the medical images using the NasNet-Mobile network with migration learning. Migration learning is then performed on the modified NasNet-Mobile network to obtain the trained network, which is then used to extract medical image features, and finally the extracted image features are subjected to DCT transform to extract low frequency data, and the perceptual hashing algorithm processes the extracted data to obtain a 32-bit binary feature vector. Before performing the watermark embedding, the watermark data is encrypted using the chaos mapping algorithm to increase data security. Next, the zero watermarking technique is used to allow the algorithm to embed and extract the watermark without changing the information contained in the medical image. The experimental findings demonstrate the algorithm's strong resistance to both conventional and geometric assaults. The algorithm offers some practical application value in the realm of medicine when compared to other approaches.

Keywords: NasNet-Mobile network; DCT; chaotic encryption; zero watermarking; migration learning

Citation: Dong, F.; Li, J.; Bhatti, U.A.; Liu, J.; Chen, Y.-W.; Li, D. Robust Zero Watermarking Algorithm for Medical Images Based on Improved NasNet-Mobile and DCT. *Electronics* **2023**, *12*, 3444. https://doi.org/10.3390/electronics12163444

Academic Editors: Yue Wu, Kai Qin, Qiguang Miao and Maoguo Gong

Received: 17 July 2023
Revised: 7 August 2023
Accepted: 13 August 2023
Published: 15 August 2023

1. Introduction

The network is disseminating more data as communication technology advances, whereby digital watermarking technology is being updated and iterated regularly to stop the leaking of user information, and it is gradually becoming a trend to protect the privacy of user information with the help of digital watermarking technology to provide security for personal information [1]. Medical images in medical diagnoses play a crucial role in medical diagnosis, treatment, and scientific research, providing a wealth of clinical data that helps doctors make more accurate diagnoses and more effective treatment plans [2]. The development of technology has promoted the integration of modern information technology with medical care, and more and more physicians and patients are using telemedicine to diagnose [3]. However, with the widespread dissemination of medical image information on the internet, the security and integrity of patient information faces serious challenges [4]. In this context, medical image watermarking technology has emerged to provide technical

support for protecting the privacy of patient information. By embedding invisible or imperceptible watermark data in medical images, medical image watermarking technology achieves copyright protection, integrity verification, and content authentication of medical images [5]. This technique requires embedding watermarks without affecting image quality and diagnostic accuracy and good robustness and invisibility to resist common image attack processing [6].

Spatial domain watermarking technique and frequency domain watermarking technique are two common traditional watermarking techniques [7]. Spatial domain watermarking uses techniques like least significant bit (LSB) replacement and pixel value mapping to insert watermarking information directly in the original data [8]. Such methods are relatively simple, but vulnerable to image attacks. Wang, Huanying et al. proposed a color image watermarking method to obtain the elements of OR decomposition in the spatial domain and perform watermark embedding and extraction in the spatial domain [9]. Basha, Shaik Hedayath et al. used ESP algorithm to compute Euclidean spatial points for watermark embedding process and used Diffie-Hellman key exchange protocol to recover the watermark, wherein the algorithm has some resistance to JPEG compression, cropping, rotation, and other attacks [10]. Cao, H. et al. used quantization technique for watermark embedding extraction by studying the relationship between the DFT DC component and the domain pixel values [11]. The frequency domain watermarking technique converts the original data to the frequency domain and then embeds the watermark information in the converted data [12]. The frequency domain watermarking approach is considerably more secure and attack-resistant than the spatial domain watermarking method [13]. Tang, Ming et al. proposed a robust watermarking algorithm based on DWT and SVD by first applying FRFT transform to the original image and the watermarked image to obtain the magnitude of the image, next applying DWT transform to it, and finally applying SVD to the low frequency sub-band of the second level DWT of the original image and the magnitude of the watermarked image to construct a new matrix to embed the watermark using singular values, and using FRFT transform for watermark encryption to improve the algorithm security, which has good robustness in attacks such as rotation, clipping, Gaussian filtering, and median filtering [14]. Jing, Liu. et al. combine the use of DTCWT-DCT transform and perceptual hashing technique to achieve watermark embedding and extraction using zero watermarking technique. The suggested method performs well against geometric and conventional assaults, and particularly good at resisting geometric attacks [15].

With the development of image local feature extraction algorithms, more and more researchers are applying feature extraction algorithms in the field of watermarking technology [16]. The traditional local feature extraction algorithms mainly include SIFT, SURF, KAZE, etc. [17–19]. They have excellent rotation invariance and scale invariance in image feature extraction and matching. Binary feature extraction algorithms have faster run speeds, and the mainstream ones include BRIEF, ORB, BRISK, etc. [20–22]. Watermarking researchers often combine feature extraction algorithms with frequency domain watermarking techniques. Hamidi, Mohamed. et al. exploit SIFT's geometric invariance to improve watermarking's robustness against geometric attacks and the proposed algorithm combining DWT-DCT and SIFT has good robustness [23]. Soualmi et al. proposed an imperceptible watermarking method for medical image tampering detection by combining SURF descriptors with Weber descriptors (WD) and Arnold algorithm, applying SURF technique to the region of interest (ROI) of medical images and then selecting the region around the SURF points to insert the watermark, thus embedding and extracting the watermark using Weber descriptors [24]. Cheng, Zeng et al. used the KAZE feature extraction algorithm to extract original image features. The extracted features were then DCT transformed to obtain the feature sequence of medical images using perceptual hashing, while embedding and extracting watermarks using the zero-watermarking technique. The proposed KAZE-DCT algorithm has better resistance to geometric attacks, but less resistant to conventional attacks [25].

In recent years, deep learning-based watermarking algorithms have gradually become popular among watermarking technology researchers [26]. Deep learning models for image processing are used in image watermarking systems [27]. Compared with traditional watermarking methods, deep learning-based algorithms can better adapt to different image contents and provide higher robustness and security [28]. Yu, Fan et al. used Inception V3 convolutional neural network to extract image features and then encrypted the embedded watermark using the chaotic mapping system. The algorithm is resistant to a wide range of geometric attacks but is less resistant to conventional attacks [29]. Wenxing, Zhang et al. proposed a method to train the GoogLeNet network using migration learning, and the trained network is used to extract the image features and encrypts the watermark using two-dimensional Henon chaos cryptography, and the proposed GoogLeNet-DCT algorithm has strong resistance to geometric attacks [30].

Based on the studies above, at the current stage, most medical image algorithms still do not fully mitigate the problem of ownership protection, and most of these algorithms can only defend against a small number of attacks. Therefore, watermarking researchers should investigate new robust watermarking algorithms that can cope with more types of attacks. The algorithm proposed in this paper is highly resistant to many conventional and geometric attacks.

The main contributions of this study are as follows:

(1) Proposed a zero-watermarking algorithm for medical images based on improved NasNet-Mobile and DCT.
(2) Double encryption of the watermark using Chen chaos mapping and Arnold transform dislocation.
(3) Changing the NasNet-Mobile network structure to train the medical image dataset and extract robust features.
(4) The proposed algorithm can withstand most of the conventional and geometric attacks and the algorithm is robust.

2. Fundamental Principles

2.1. NasNet-Mobile Convolutional Neural Network

NasNet-Mobile is a lightweight neural network architecture [31] to achieve high-performance, low-latency image recognition tasks. Developed by the Google Brain team and based on Neural Architecture Search (NAS) technology, NasNet-Mobile's network architecture aims to maintain accuracy while significantly reducing computational resource requirements and power consumption. Compared with the original version of NasNet, NasNet-Mobile is optimized in terms of network hierarchy and parameters to provide better performance while reducing computational complexity. The NasNet-Mobile network structure consists of basic modules (Cells), NASNet search space, reinforcement learning, and transfer (Skip) connections. In this paper, the NasNet-Mobile network is applied to digital watermarking.

In NasNet-Mobile, the basic components are Cell structures, and there exist two types of Cell structures called Normal Cells and Reduction Cells, which are a sub-network of multiple convolutional layers with reusable and combinable characteristics. NasNet-Mobile forms the entire network by stacking these basic modules (Normal Cells and Reduction Cells) together. This modular design allows NasNet-Mobile to be highly flexible and can be adapted to different task requirements and resource constraints. The network model architecture is depicted in Figure 1 and the best-performing Normal Cell and Reduction Cell structures are depicted in Figure 2.

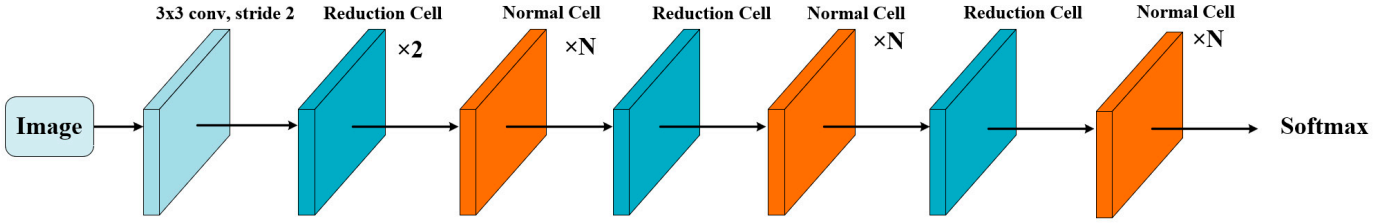

Figure 1. Network model architecture.

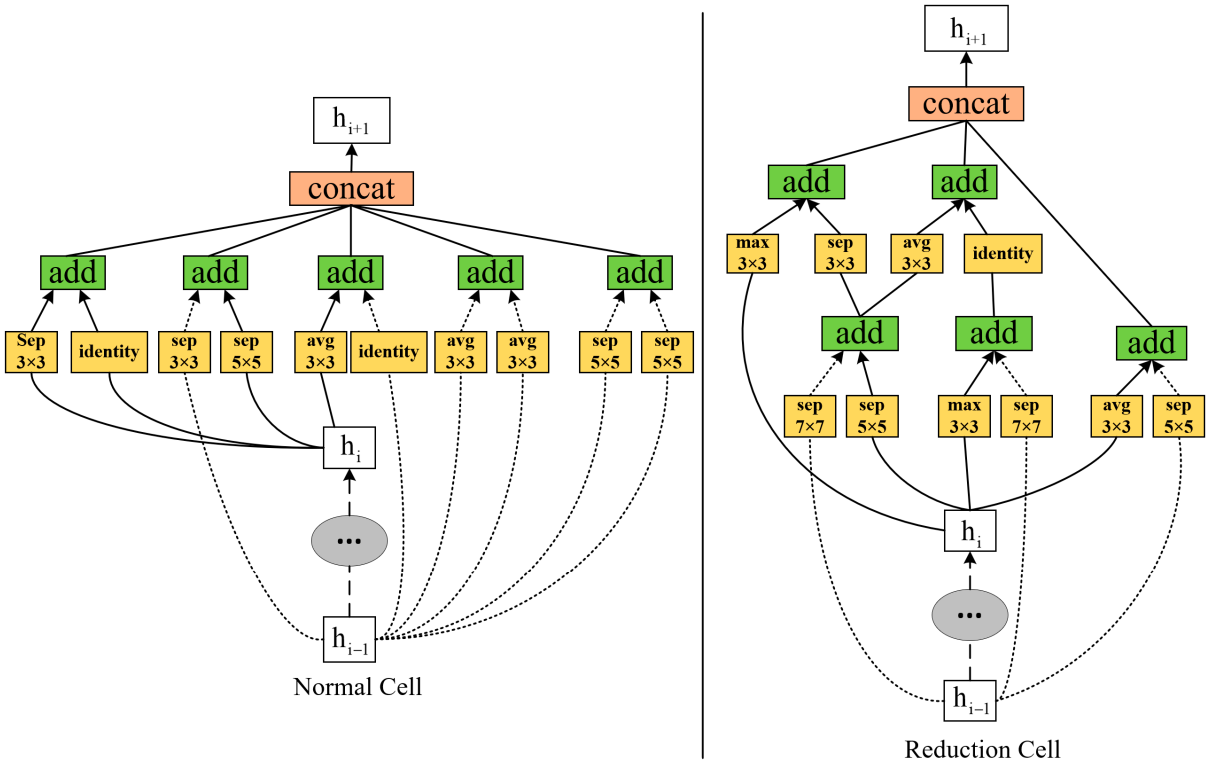

Figure 2. The architecture of the best convolutional cells.

2.2. Discrete Cosine Transform (DCT)

The DCT transform is commonly used for lossy data compression of images with separability and energy concentration. The principle of 1D-DCT is shown in Equation (1). In this case, 2D-DCT applies the one-dimensional discrete cosine transform to two-dimensional data, dividing the two-dimensional image into several small blocks, and then applying the discrete cosine transform to each block to convert the high-frequency signals in the small blocks into low-frequency signals. The 2D-DCT is shown in Equation (3):

$$F(u) = C(u) \sum_{i=0}^{N-1} f(i) \cos\left[\frac{(i+0.5)u\pi}{N}\right] \tag{1}$$

$$C(u) = \begin{cases} \sqrt{\frac{1}{N}}, & u = 0 \\ \sqrt{\frac{2}{N}}, & u = 1, 2, \ldots, M-1 \end{cases} \tag{2}$$

$$F(u,v) = C(u)C(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{(x+0.5)u\pi}{M}\right] \cos\left[\frac{(y+0.5)v\pi}{N}\right] \tag{3}$$
$$u = 0, 1, \ldots, M-1; v = 0, 1, \ldots, N-1$$

$$C(u) = \begin{cases} \sqrt{\frac{1}{M}}, & u = 0 \\ \sqrt{\frac{2}{M}}, & u = 1, 2, \ldots, M-1 \end{cases} \tag{4}$$

$$C(v) = \begin{cases} \sqrt{\frac{1}{N}}, & v = 0 \\ \sqrt{\frac{2}{N}}, & v = 1, 2, \ldots, N-1 \end{cases} \tag{5}$$

2.3. Chen Chaotic System

The Chen chaotic system is a particular type of three-dimensional nonlinear dynamical system. Equation (6) is used to define the Chen chaotic system. Encrypting images with the Chen chaotic system is common, mainly by generating a sequence of random numbers to obfuscate and permute the image pixels for data protection.

$$\begin{array}{c} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x - xz + cy \\ \frac{dz}{dt} = xy - bz \end{array} \tag{6}$$

where a, b, and c are the parameters of the Chen chaotic system, and x, y, and z denote the three state variables of the system, respectively.

2.4. Arnold Mapping

Arnold mapping is a discrete-time mapping widely used in studying dynamical systems and chaos theory. Arnold mapping is a linear mapping defined in a two-dimensional toroidal space as shown in Equation (7). Arnold mapping mainly achieves the encryption of the original image by dislocating the pixels of the image and using a key to control the number of iterations, thus making the original image unrecognizable.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & b \\ a & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \mathrm{mod} N \tag{7}$$

where (x_n, y_n) is the coordinate of the original point, (x_{n+1}, y_{n+1}) is the coordinate of the mapped point, a, b, N should be positive integers, and N is the image pixel size.

3. Zero Watermark Algorithm

This paper proposes a robust zero watermarking algorithm for medical images based on an improved NasNet-Mobile convolutional neural network and discrete cosine transform (DCT), combining NasNet-Mobile network, DCT transform, and perceptual hash function, watermarked image encryption using Chen chaotic system and Arnold transform dislocation dual encryption algorithm, using zero watermarking technique to embed and extract watermark, which has good effect in geometric attacks and some conventional attacks, and can blindly extract watermark.

3.1. NasNet-Mobile Pre-Trained Network Migration Learning

3.1.1. NasNet-Mobile Network Restructuring

The NasNet-Mobile network structure uses the idea of repetitive stacking, and the network itself has a strong feature extraction capability. To further improve the accuracy of image feature extraction, we adapt the structure of the pre-trained network NasNet-Mobile by using a fully connected layer with 128 output and a regression layer instead of the original Softmax layer and classification layer, thus generating a regression network with 128 output, and selecting the fully connected layer with output value of 128 for extracting feature values of medical images, as shown in Figure 3. After experiments, the improved network has better feature extraction capability.

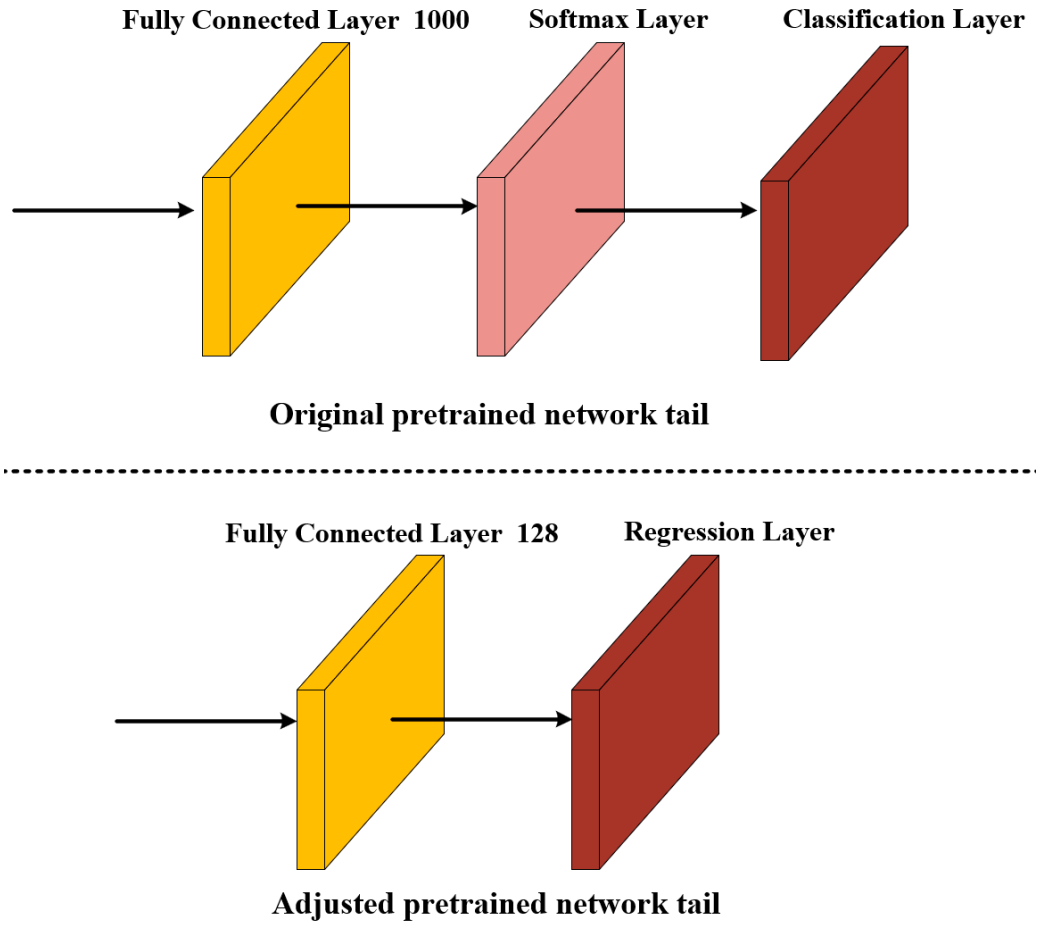

Figure 3. NasNet-Mobile network model adjustment.

3.1.2. Dataset Creation

The datasets in this paper are sourced from Medical Imaging Park and the American Institutes for Research, employing the datasets from the categories of the brain, abdomen, chest, bones, and muscles. We selected 350 original medical images as the training set, 150 original medical images as the validation set, and 100 original medical images as the test set, and some of the medical images are shown in Figure 4. To improve the algorithmis capacity to extract visual features, we perform data enhancement on the selected dataset as shown in Table 1. Because the NasNet-Mobile pre-training network requires the input image pixels to be 224 × 244, the image size needs to be set to 224 × 224, so that we get 37,450 training sets with 224 × 224 pixels and 16,050 validation sets. We perform 2D-DCT transform on the training and test set images and select 128 low-frequency components of 16 × 8 as the data set labels.

3.1.3. Training Network

The programming Matlab 2022b was used for this experiment and the NasNet-Mobile pre-trained network from the Neural Network Toolbox was selected. The computer configuration used for the experiments was a processor (AMD Ryzen7 5800H with Radeon Graphics), a graphics card (NVIDIA GeForce RTX 3060 Laptop GPU 6 G), and memory (Samsung DDR4 3200 MHz 16 G). We trained the NasNet-Mobile pre-trained network. During training, the initial learning rate is set at 0.001. At each iteration, the model will use thirty samples for weight update and is trained for four rounds. At the beginning of each round, the training data will be reordered randomly, and after every 1000 iterations, the model will be evaluated using validation data. After the training, we save the well-trained

grid and use the fully connected layer with an output value of 128 at the tail end of the network as the feature values for image feature extraction.

Figure 4. Some medical images in the dataset.

Table 1. Data Set Enhancement Methods.

Enhanced Type	Intensity	Number of New Images
JPEG compression (%)	5, 10, 15, 20	4
Gaussian noise (%)	2, 4, 6, 8, 10, 12, 14, 16	8
Median filter [3 × 3] (times)	5, 10, 15, 20	4
Median filter [5 × 5] (times)	5, 10, 15, 20	4
Median filter [7 × 7] (times)	5, 10, 15, 20	4
Clockwise rotation (°)	5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	12
Anticlockwise rotation (°)	5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	12
Y-axis shear (%)	5, 10, 15, 20, 25, 30, 35, 40	8
Scaling	0.2, 0.4, 0.6, 0.8, 1.0, 1.2, 1.4, 1.6, 1.8, 2.0	10
Right-shift (%)	5, 10, 15, 20, 25, 30, 35, 40	8
Left-shift (%)	5, 10, 15, 20, 25, 30, 35, 40	8
Down-shift (%)	5, 10, 15, 20, 25, 30, 35, 40	8
X-axis shear (%)	5, 10, 15, 20, 25, 30, 35, 40	8
Up-shift (%)	5, 10, 15, 20, 25, 30, 35, 40	8

3.2. NasNet-Mobile Feature Extraction

In this paper, we use a trained NasNet-Mobile network to extract medical image features and get 128 feature values $N(i,j)$, after DCT transformation of the extracted eigenvalues, 128 DCT transformed feature values $D(i,j)$ are obtained, then select the 32 low frequency coefficients $V(i,j)$ of feature values $D(i,j)$, perform sign transformation on the low frequency coefficients $V(i,j)$, set the elements greater than 0 in the matrix to 1 and the other elements to 0 to get the 32 bit hash value $H(i,j)$, and $H(i,j)$ for the binary feature sequence. The specific steps are shown in Figure 5.

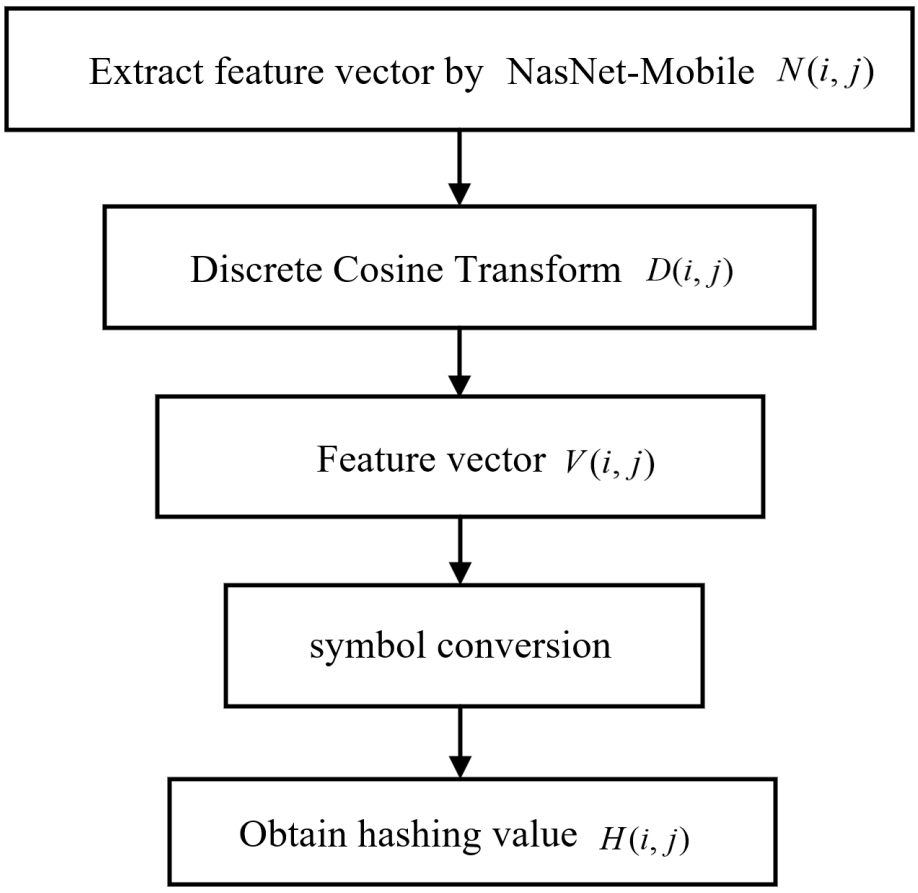

Figure 5. Image feature extraction flow chart.

3.3. Watermark Encryption

Chen chaos system and Arnold chaos mapping are used to encrypt the picture twice in order to improve the anti-interference and security of the embedded watermark. Firstly, the initial values of the Chen chaos system are set as follows: $x = 2$, $y = 1$, $z = 3$, $a = 35$, $b = 3$, $c = 28$. Subsequently, the system enters the chaotic state to obtain the chaotic sequence, and then the chaos matrix is obtained by binarization. XOR operation is performed on the chaotic matrix and the original watermark to obtain the watermark encrypted by the Chen chaos system $C(i,j)$, and finally, the watermark $C(i,j)$ is dislocated by Arnold chaos mapping to obtain the encrypted watermark $L(i,j)$. The parameters of Arnold chaos mapping in this paper are set as $a = 3$, $b = 5$, and the number of iterations is 10. The watermark encryption process is shown in Figure 6.

3.4. Embedding Watermarks

We embed the encrypted watermark into the medical image, whereby first the trained NasNet-Mobile network performs feature extraction on the original image to obtain the hash value $H(i,j)$, and then the binary feature sequence is XOR operation with the en-

crypted watermark to obtain the logical key used to extract the watermark $K(i,j)$. This embedding watermark method uses the zero-watermark embedding technique, which does not alter the original image. The specific embedding watermark steps are shown in Figure 7.

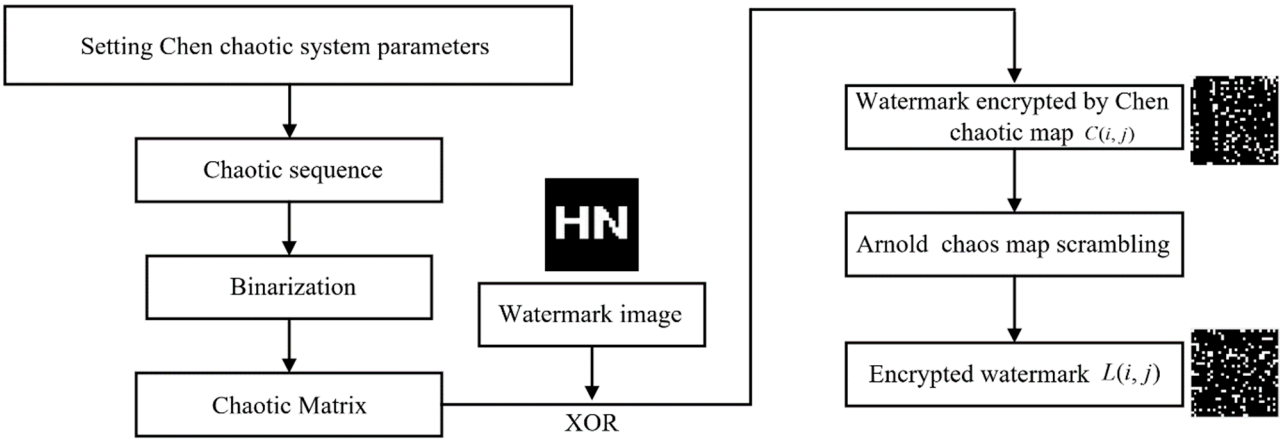

Figure 6. Watermark encryption flow chart.

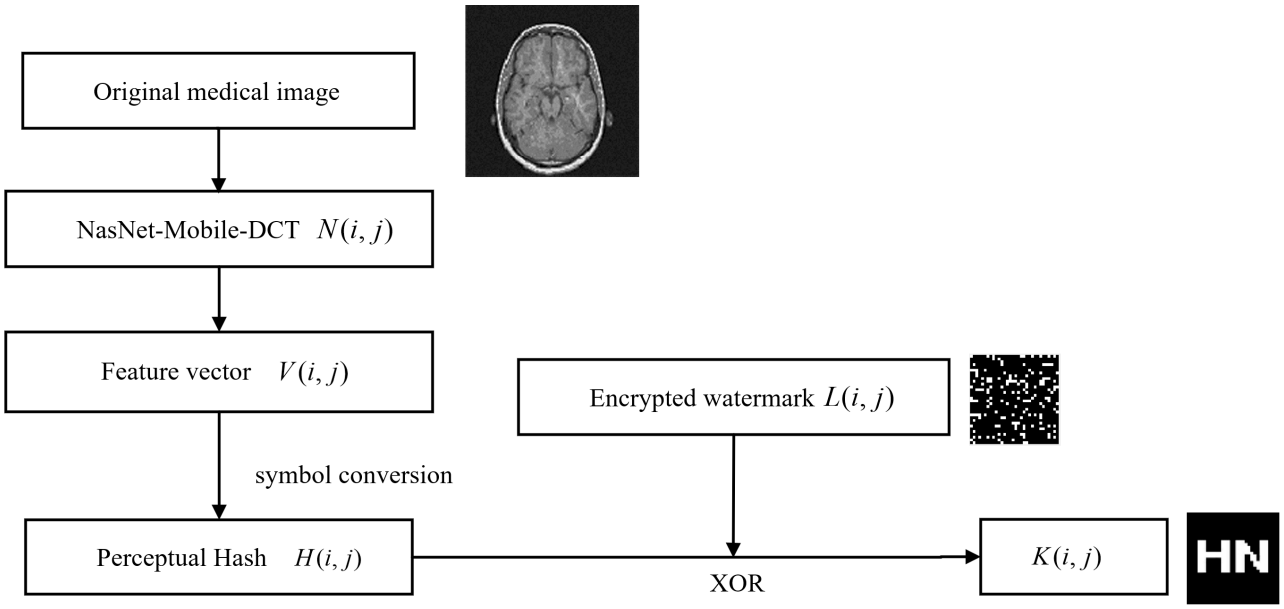

Figure 7. Embed watermark flow chart.

3.5. Watermark Extraction and Decryption

Finally, watermark extraction and decryption are performed. Firstly, the trained NasNet-Mobile network is used to extract features from the image after the attack and obtain the hash value $H'(i,j)$, the extracted encrypted watermark $L'(i,j)$ is obtained by performing the XOR operation between $H'(i,j)$ and the logical key $K(i,j)$, the encrypted watermark $L'(i,j)$ is obtained by the Arnold inverse transformation to the watermark encrypted by Chen chaos system $C'(i,j)$. Finally, the watermark is restored by the initial value of Chen chaos system. The specific watermark extraction step is shown in Figure 8.

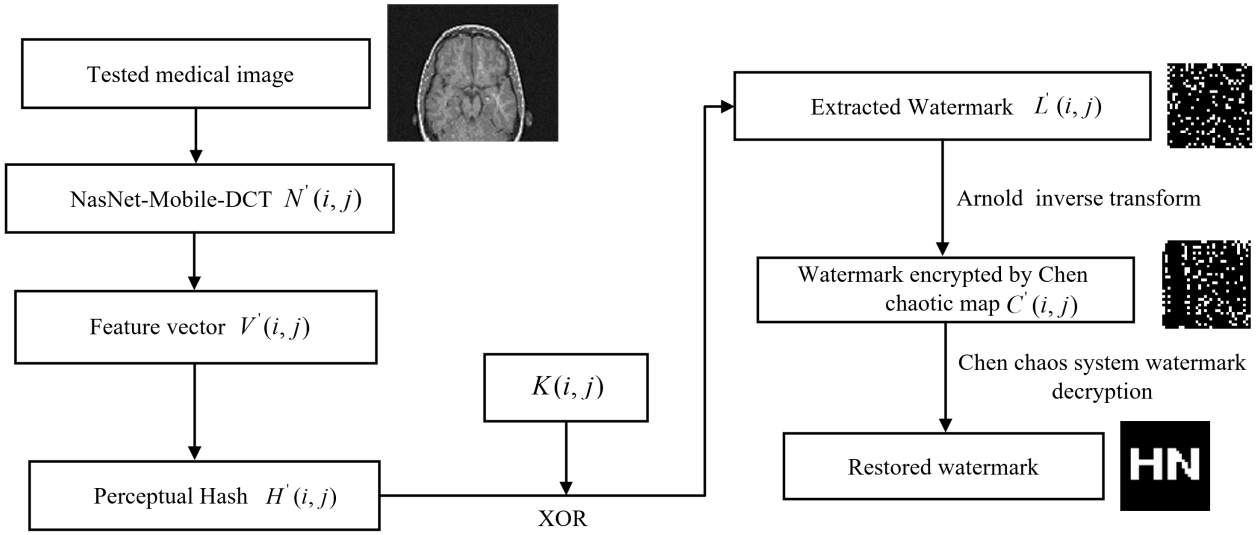

Figure 8. Watermark extraction and decryption flow chart.

4. Experiments and Results

This paper uses MATLAB 2022b software to simulate and experiment on medical images. Since the network input image pixel is 224 × 224, the medical image pixel used for testing is 224 × 224. In this paper, three medical images from the test set are chosen at random for testing, and the watermark image pixel size is chosen as 32 × 32, as seen in Figure 9. The normalized correlation coefficient (NC), as shown in Equation (8), is employed to determine how well the method can withstand assault by comparing how similar the original watermark is to the watermark that was retrieved from the picture after attack. The peak signal-to-noise ratio (PSNR), as shown in Equation (9), is used to represent the quality of the image. In the case of medical images without any attacks, the NC values are all 1.

$$NC = \frac{\sum_i \sum_j W_{(i,j)} W'_{(i,j)}}{\sum_i \sum_j W^2_{(i,j)}} \tag{8}$$

$$PSNR = 10\lg\left[\frac{MN\max_{i,j}(\mathrm{I}(i,j))^2}{\sum_i \sum_j (\mathrm{I}(i,j) - \mathrm{I}'(i,j))^2}\right] \tag{9}$$

Figure 9. Tested images and watermarks. Brain image (**a**), palm image (**b**), abdominal image (**c**), watermark image (**d**).

4.1. Testing Different Images

Before testing the anti-attack performance of medical images, we first need to test ten different medical images with the algorithm, as shown in Figure 10. At the same time, their correlation coefficients are calculated to verify whether the algorithm can distinguish different medical images. The outcomes of the experiment are displayed in Table 2. The outcomes demonstrate that the NasNet-Mobile-DCT algorithm's NC values for different medical pictures are less than 0.5, which proves that the algorithm can distinguish different medical images.

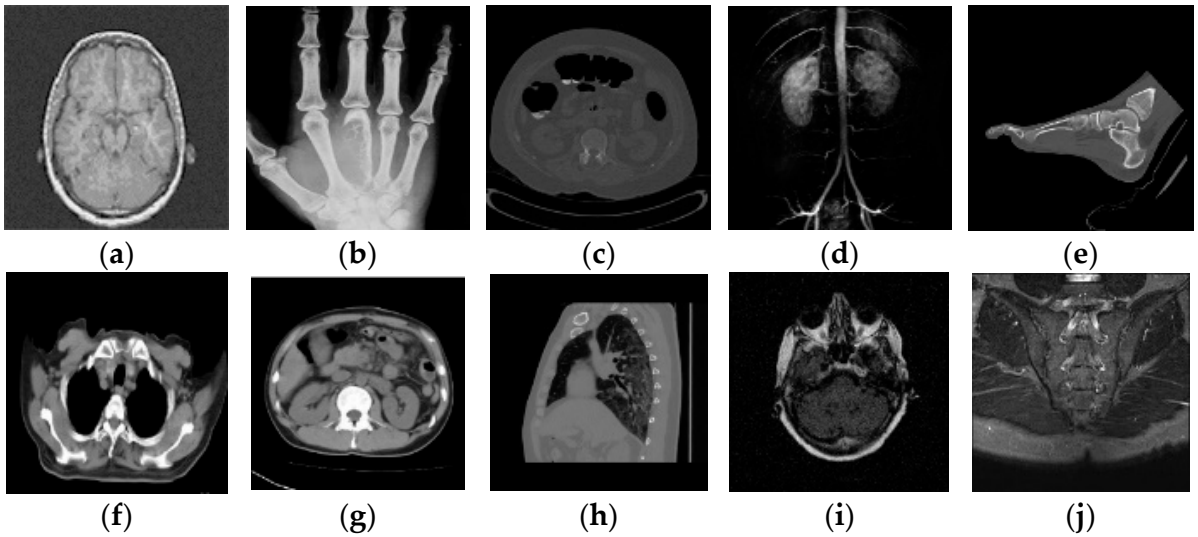

Figure 10. Different medical images within the test (**a**–**j**).

Table 2. Correlation coefficient values between different images (32 bits).

Image	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
(a)	1.00									
(b)	0.14	1.00								
(c)	0.42	0.25	1.00							
(d)	0.39	0.22	0.37	1.00						
(e)	0.18	0.30	0.33	0.34	1.00					
(f)	0.41	0	0.41	0.41	0.27	1.00				
(g)	0.43	0.07	0.05	0.24	0.07	0.10	1.00			
(h)	0.23	0.29	0.27	0.21	0.43	0.38	0.32	1.00		
(i)	0.39	0.03	0.17	0.35	0.06	0.18	0.33	0.39	1.00	
(j)	0.30	0.03	0.14	0.10	0.03	0.23	0.31	0.23	0.32	1.00

4.2. Conventional Attacks

The NasNet-Mobil-DCT algorithm is used to perform different levels of conventional attacks on medical images that already contain encrypted watermarks, and then the watermarks are extracted, and Figure 11 displays the conventionally attacked images along with the extracted watermarks. Then the algorithm's robustness for conventional attacks is observed, and Table 3 displays the trial outcomes. The findings demonstrate that the Gaussian attack strength is 0.02 and 0.04, the NC value is greater than 0.85, even if the Gaussian attack strength is 0.10, the NC value is greater than 0.55, which indicates that the proposed algorithm has certain ability to resist Gaussian attack. The NC value is greater than 0.85 even when the JPEG compression quality is 5%, and when the quality of the JPEG compression is greater than 20%, the NC value is 1, which indicates that the proposed algorithm has good robustness to JPEG compression attack. When the attack strength is 20 times [5 × 5] median filtering, the measured NC values are higher than 0.74, even if the

attack intensity is 10 times [7 × 7] median filter, the NC value is greater than 0.70, and this shows that the algorithm is effectively resistant to median filtering. Experimental results show that the algorithm proposed in this paper has good resistance to conventional attacks.

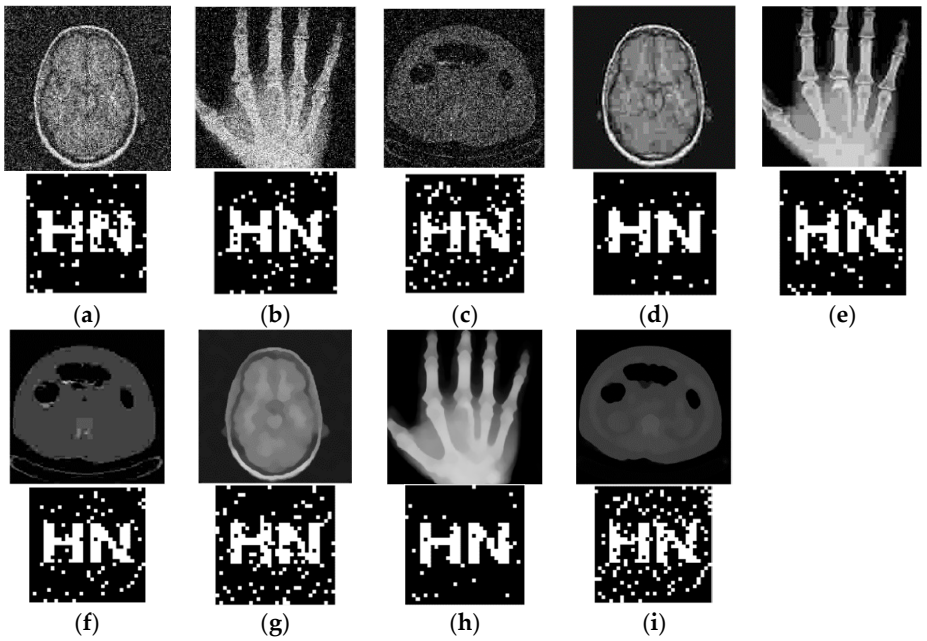

Figure 11. Medical images and watermarks for conventional attacks. (**a**–**c**) denote medical images and extracted watermarks after a Gaussian attack intensity of 0.06; (**d**–**f**) denote medical images and extracted watermarks at a compression quality of 5%; (**g**–**i**) denote medical images and extracted watermarks after 20 Me-dian filtering [5 × 5] attacks.

Table 3. Experimental data of watermarking based on conventional attacks.

Conventional Attacks		PSNR (dB)			NC		
	Intensity	Img1	Img2	Img3	Img1	Img2	Img3
Gaussian noise	0.02	17.81	16.76	17.29	1.00	0.93	0.94
	0.04	15.12	14.06	14.55	0.86	0.93	0.89
	0.06	13.65	12.55	13.04	0.85	0.88	0.82
	0.08	12.66	11.42	12.04	0.67	0.87	0.76
JPEG compression	0.10	11.86	10.67	11.21	0.56	0.85	0.63
	25%	33.39	32.03	34.27	1.00	1.00	1.00
	20%	32.51	31.17	33.39	1.00	1.00	1.00
	15%	31.25	30.03	32.37	0.90	0.94	1.00
	10%	29.26	28.39	30.65	0.95	1.00	0.88
Median filtering [5 × 5]	5%	26.46	25.16	27.68	0.95	0.86	0.88
	5 (times)	25.13	27.00	28.35	1.00	0.86	0.83
	10 (times)	24.29	25.99	27.60	0.92	0.92	0.83
	15 (times)	23.86	25.48	27.24	0.89	0.92	0.83
Median filtering [7 × 7]	20 (times)	23.56	25.09	27.07	0.84	0.92	0.75
	5 (times)	22.49	24.75	26.61	1.00	0.86	0.83
	10 (times)	21.77	23.14	25.70	0.72	0.86	0.83

4.3. Geometric Attacks

The NasNet-Mobil-DCT algorithm is robust under conventional attacks and the following tests are performed on geometric attacks. The medical images that already contain the encrypted watermark are subjected to different degrees of rotation attack, scaling attack, translation attack, *X*-axis shearing attack, and *Y*-axis shearing after extracting the

watermark, and Figure 12 displays the extracted watermark and medical images following the geometric attack. Following that, the algorithm's resistance to geometrical assaults is seen, and the experimental findings are displayed in Table 4. The experimental findings demonstrate that the NC values were higher than 0.85 when the images were rotated by 5, 15, and 30 degrees, even after rotating the observed picture by 60 degrees, the NC value remains higher than 0.80, it shows that the algorithm can effectively fend against rotational attacks. When the scaling ratio is equal to 0.3 and 2.0, the NC value exceeds 0.86, and this suggests that the algorithm is rather resistant to scaling attacks. When the measured cryptomedical images were shifted upwards by 5%, the NC values were all greater than 0.92, the NC value exceeds to 0.75 when it is shifted to the up by 35%, the NC value is higher than or equal to 0.75 when the measured encrypted medical image is shifted to the right by 25%, demonstrating the algorithm's strong robustness to translation attacks. When the encrypted medical images are cut by 20% on the *Y*-axis, the NC value is greater than 0.85, even when the encrypted medical image is cropped 40% on the *Y*-axis, the NC value is greater than 0.82, when they are cut by 40% on the *X*-axis, the NC values are greater than 0.80, indicating that the algorithm has strong resistance to shear attacks. In conclusion, the algorithm proposed in this paper performs well against multiple geometric attacks.

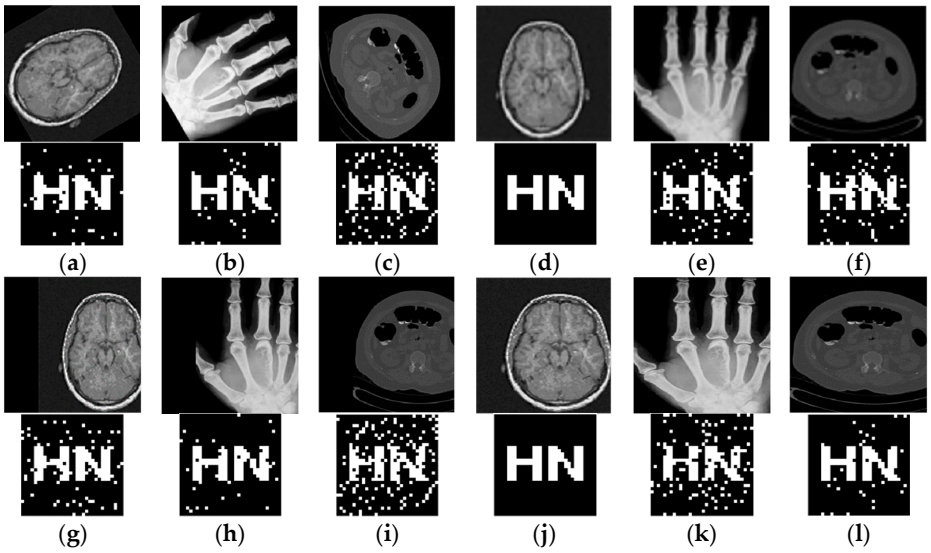

Figure 12. Medical images and watermarks for geometric attacks. (**a**–**c**) represent the medical image and extracted watermark after a 60-degree clockwise rotation attack; (**d**–**f**) represent the medical image and extracted watermark at a scaling of 0.3; (**g**–**i**) represent the medical image and extracted watermark after a 25% right shift; (**j**–**l**) denote the medical image and extracted watermark after a 20% *X*-axis clipping of the medical image and the extracted watermark.

Table 4. Experimental data of watermarking based on geometric attacks.

Geometric Attacks		PSNR (dB)			NC		
	Intensity	Img1	Img2	Img3	Img1	Img2	Img3
Rotation (clockwise)	5°	18.36	14.63	22.50	0.95	0.94	0.94
	15°	15.05	10.06	19.58	0.95	0.87	0.94
	30°	14.56	9.14	18.11	1.00	0.86	1.00
	45°	13.99	8.24	17.72	1.00	0.80	0.93
	60°	13.68	7.44	17.03	0.95	0.94	0.83
Scaling	0.3	20.97	21.32	25.67	1.00	0.88	0.88
	0.6	27.13	27.25	29.70	1.00	1.00	0.94
	1.5	46.44	43.72	45.19	1.00	1.00	0.93
	2.0	46.40	43.61	44.94	1.00	1.00	0.93

Table 4. *Cont.*

Geometric Attacks		PSNR (dB)			NC		
	Intensity	Img1	Img2	Img3	Img1	Img2	Img3
Right translation	5%	14.60	10.37	19.13	1.00	1.00	0.93
	15%	12.98	8.12	16.04	0.95	0.92	0.89
	25%	11.34	6.62	15.25	0.90	0.92	0.75
	40%	10.11	5.75	14.50	0.90	0.80	0.82
Up translation	5%	14.67	13.42	17.99	0.95	0.92	1.00
	15%	13.17	8.81	15.08	1.00	0.92	0.82
	25%	11.97	7.08	14.32	1.00	0.73	0.82
	35%	11.08	6.06	13.34	1.00	0.92	0.76
Y-axis cropping	10%	15.66	15.14	18.75	1.00	0.86	1.00
	20%	15.26	12.27	16.21	1.00	0.86	0.89
	30%	14.95	11.29	15.02	1.00	0.86	0.83
	40%	14.69	10.57	14.48	0.95	0.94	0.83
X-axis cropping	10%	14.70	10.00	19.52	1.00	0.94	1.00
	20%	13.14	8.80	18.07	1.00	0.81	0.94
	30%	12.55	7.48	17.04	1.00	0.75	0.86
	40%	12.14	7.70	16.67	1.00	0.81	0.88

4.4. Algorithm Comparison

To demonstrate the robustness of the NasNet-Mobil-DCT algorithm and use this algorithm to compare with other algorithms, this comparison experiment uses a brain image as the experimental object, as shown in Figure 9a, because this image is often used by a wide range of medical image watermarking researchers in comparative experiments and is representative. The comparison data are shown in Figure 13, in which black represents the DCT algorithm [32], green represents the DWT-DCT algorithm [33], blue represents the SIFT-DCT algorithm [34], purple represents the KAZE-DCT algorithm [25], orange represents the Inception V3-DCT algorithm [34], and red represents the NasNet-Mobil-DCT algorithm proposed in this paper. The NasNet-Mobil-DCT algorithm offers strong resilience to conventional and geometric attacks, as observed from the experimental data.

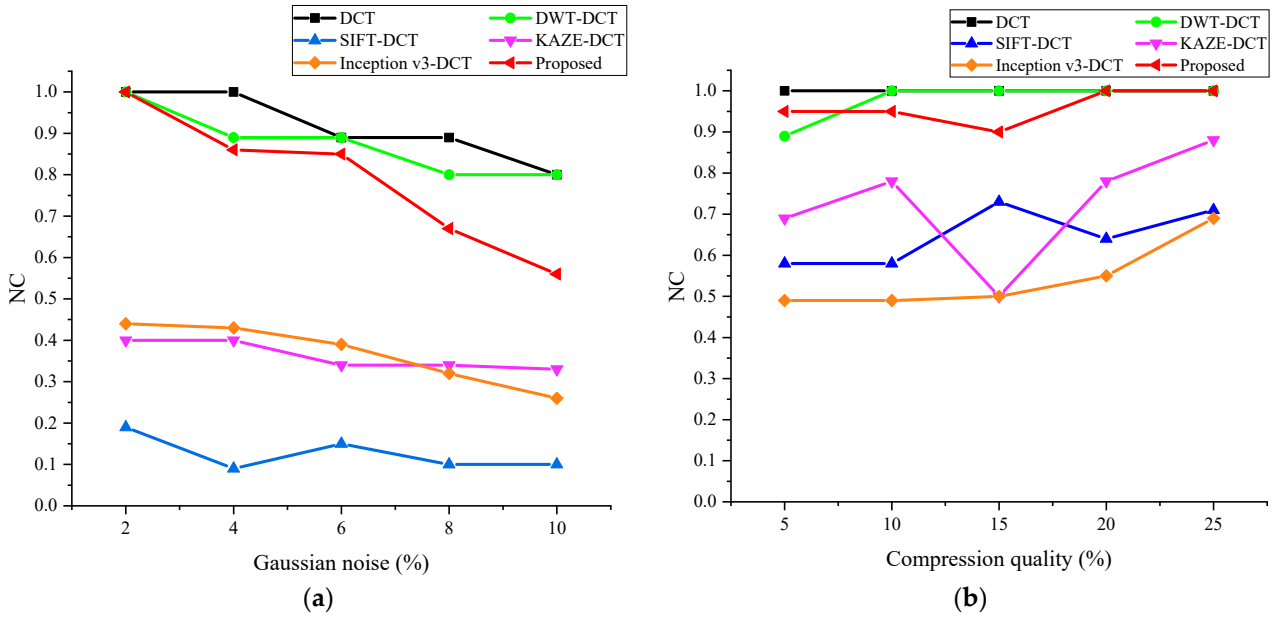

Figure 13. *Cont.*

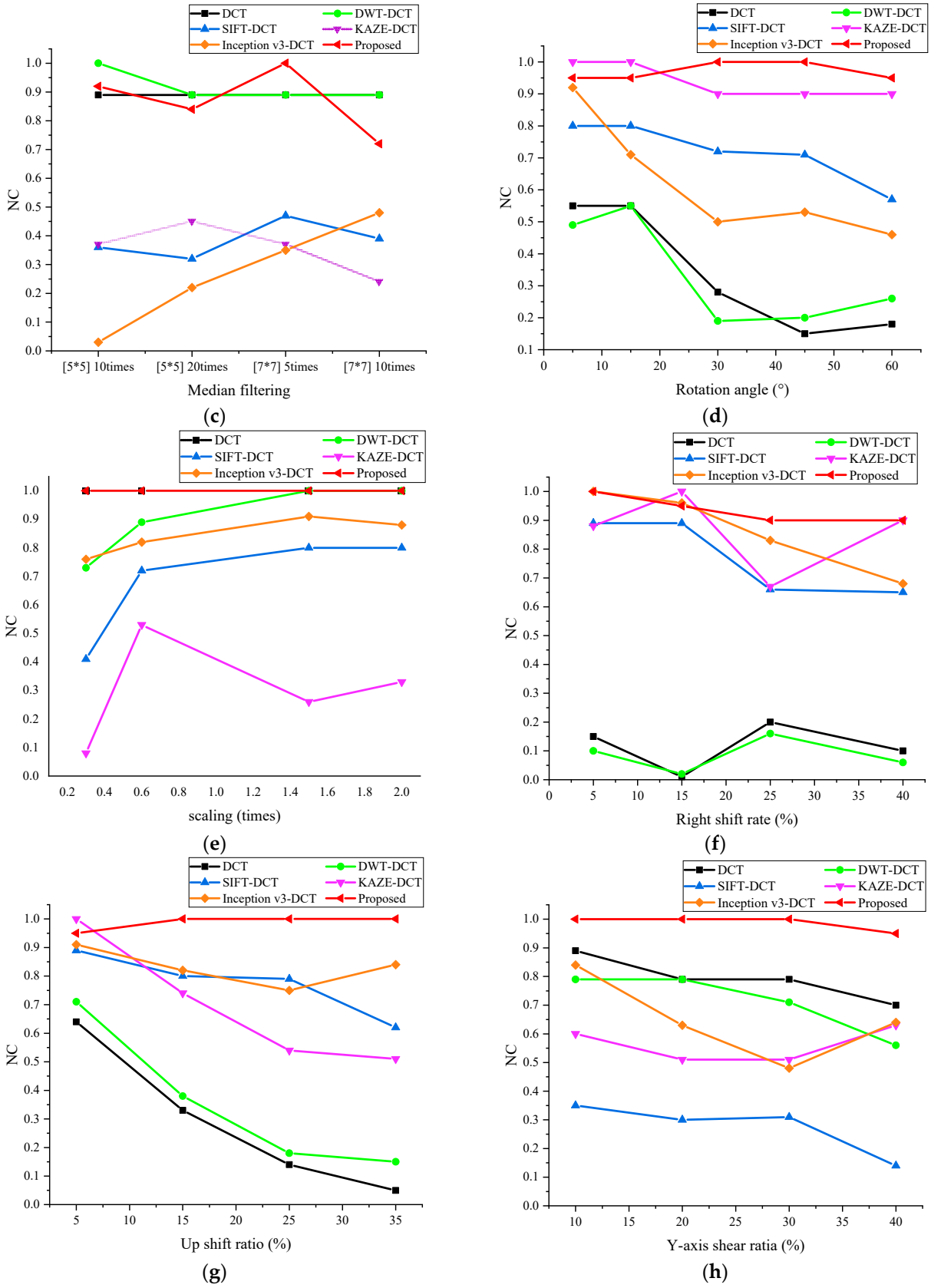

Figure 13. Algorithm comparison results. Comparison of NC values between different algorithms, where (**a**–**h**) indicate the results after Gaussian noise, JPEG compression, median filter, clockwise rotation, scaling, right-shift, up-shift, and *Y*-axis shear attacks, respectively.

5. Conclusions

In this paper, we propose a robust zero watermarking algorithm for medical images based on improved NasNet-Mobile convolutional neural network and discrete cosine transform (DCT), which uses deep learning algorithm, chaotic encryption technique, perceptual hashing algorithm, and zero watermarking technique to provide security for medical image watermarking information. Before watermark embedding, Chen chaotic system and Arnold mapping algorithm are used to double encrypt the watermarked data, which improves the security of the data, and then migration learning is carried out on the improved NasNet-Mobile network to get the trained medical image feature extraction network, and finally, the extracted image features are subjected to DCT transformation to extract the low-frequency data and the extracted data are processed by the perceptual hash algorithm to get the 32-bit binary feature vectors, and finally, the zero-watermarking technology is utilized for encrypting the medical images. The experimental results show that the algorithm proposed in this paper can resist a variety of conventional attacks, and at the same time, it is excellent in resisting geometric attacks such as rotation, translation, scaling, shearing, etc., and shows strong robustness. Therefore, the algorithm can be used for medical images. In the next research, we will improve the algorithm and look for algorithms that can extract image features more effectively to cope with the watermarking techniques' weak resistance against various attacks.

Author Contributions: Formal analysis, validation, data curation, and writing—original draft preparation, F.D.; funding acquisition, J.L. (Jingbing Li); supervision, J.L. (Jing Liu); software, Y.-W.C.; investigation, D.L. Data curation, Supervision, Resources, Writing—original draft, U.A.B. All authors have read and agreed to the published version of the manuscript.

Funding: 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 post doctor research from Zhejiang Province under Grant ZJ2021028.

Data Availability Statement: Data is contained within this article.

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

References

1. Evsutin, O.; Melman, A.; Meshcheryakov, R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions. *IEEE Access* **2020**, *8*, 166589–166611. [CrossRef]
2. Tian, Y.; Fu, S. A Descriptive Framework for the Field of Deep Learning Applications in Medical Images. *Knowl.-Based Syst.* **2020**, *210*, 106445. [CrossRef]
3. Amine, K.; Fares, K.; Redouane, K.M.; Salah, E. Medical Image Watermarking for Telemedicine Application Security. *J. Circuits Syst. Comput.* **2022**, *31*, 2250097. [CrossRef]
4. Venkateswarlu, I.B. Fast Medical Image Security Using Color Channel Encryption. *Braz. Arch. Biol. Technol.* **2020**, *63*, e20180473. [CrossRef]
5. Thabit, R. Review of Medical Image Authentication Techniques and Their Recent Trends. *Multimed. Tools Appl.* **2021**, *80*, 13439–13473. [CrossRef]
6. Raj, N.R.N.; Shreelekshmi, R. A Survey on Fragile Watermarking Based Image Authentication Schemes. *Multimed. Tools Appl.* **2021**, *80*, 19307–19333. [CrossRef]
7. Verma, V.S.; Jha, R.K. An Overview of Robust Digital Image Watermarking. *IETE Tech. Rev. (Inst. Electron. Telecommun. Eng. India)* **2015**, *32*, 479–496. [CrossRef]
8. Kumar, S.; Singh, B.K. Entropy Based Spatial Domain Image Watermarking and Its Performance Analysis. *Multimed. Tools Appl.* **2021**, *80*, 9315–9331. [CrossRef]
9. Wang, H.; Su, Q. A Color Image Watermarking Method Combined QR Decomposition and Spatial Domain. *Multimed. Tools Appl.* **2022**, *81*, 37895–37916. [CrossRef]
10. Basha, S.H.; Jaison, B. A Novel Secured Euclidean Space Points Algorithm for Blind Spatial Image Watermarking. *EURASIP J. Image Video Process.* **2022**, *2022*, 21. [CrossRef]
11. Cao, H.; Hu, F.; Sun, Y.; Chen, S.; Su, Q. Robust and Reversible Color Image Watermarking Based on DFT in the Spatial Domain. *Optik* **2022**, *262*, 169319. [CrossRef]

12. Chopra, A.; Gupta, S.; Dhall, S. Analysis of Frequency Domain Watermarking Techniques in Presence of Geometric and Simple Attacks. *Multimed. Tools Appl.* **2020**, *79*, 501–554. [CrossRef]
13. Tian, C.; Wen, R.-H.; Zou, W.-P.; Gong, L.-H. Robust and Blind Watermarking Algorithm Based on DCT and SVD in the Contourlet Domain. *Multimed. Tools Appl.* **2020**, *79*, 7515–7541. [CrossRef]
14. Tang, M.; Zhou, F. A Robust and Secure Watermarking Algorithm Based on DWT and SVD in the Fractional Order Fourier Transform Domain. *Array* **2022**, *15*, 100230. [CrossRef]
15. Liu, J.; Li, J.; Cheng, J.; Ma, J.; Sadiq, N.; Han, B.; Geng, Q.; Ai, Y. A Novel Robust Watermarking Algorithm for Encrypted Medical Image Based on DTCWT-DCT and Chaotic Map. *Comput. Mater. Contin.* **2019**, *61*, 889–910.
16. Jose, A.; Subramaniam, K. Comparative Analysis of Reversible Data Hiding Schemes. *IET Image Process.* **2020**, *14*, 2064–2073. [CrossRef]
17. Lowe, D.G. Distinctive Image Features from Scale-Invariant Keypoints. *Int. J. Comput. Vis.* **2004**, *60*, 91–110. [CrossRef]
18. Bay, H.; Ess, A.; Tuytelaars, T.; Van Gool, L. Speeded-Up Robust Features (SURF). *Comput. Vis. Image Underst.* **2008**, *110*, 346–359. [CrossRef]
19. Alcantarilla, P.F.; Bartoli, A.; Davison, A.J. KAZE Features. In Proceedings of the Computer Vision—ECCV 2012, Florence, Italy, 7–13 October 2012; Fitzgibbon, A., Lazebnik, S., Perona, P., Sato, Y., Schmid, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 214–227.
20. Sjöstrand, T.; Mrenna, S.; Skands, P. A Brief Introduction to PYTHIA 8.1. *Comput. Phys. Commun.* **2008**, *178*, 852–867. [CrossRef]
21. Rublee, E.; Rabaud, V.; Konolige, K.; Bradski, G. ORB: An Efficient Alternative to SIFT or SURF. In Proceedings of the 2011 International Conference on Computer Vision, Barcelona, Spain, 6–13 November 2011; pp. 2564–2571.
22. Leutenegger, S.; Chli, M.; Siegwart, R.Y. BRISK: Binary Robust Invariant Scalable Keypoints. In Proceedings of the 2011 International Conference on Computer Vision, Barcelona, Spain, 6–13 November 2011; pp. 2548–2555.
23. Hamidi, M.; El Haziti, M.; Cherifi, H.; El Hassouni, M. A Hybrid Robust Image Watermarking Method Based on Dwt-Dct and Sift for Copyright Protection. *J. Imaging* **2021**, *7*, 218. [CrossRef]
24. Soualmi, A.; Alti, A.; Laouamer, L. An Imperceptible Watermarking Scheme for Medical Image Tamper Detection. *Int. J. Inf. Secur. Priv.* **2022**, *16*, 18. [CrossRef]
25. Zeng, C.; Liu, J.; Li, J.; Cheng, J.; Zhou, J.; Nawaz, S.A.; Xiliang, X.; Bhatti, U.A. Multi-Watermarking Algorithm for Medical Image Based on KAZE-DCT. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–9. [CrossRef]
26. Meng, R.; Cui, Q.; Yuan, C. A Survey of Image Information Hiding Algorithms Based on Deep Learning. *CMES Comput. Model. Eng. Sci.* **2018**, *117*, 425–454. [CrossRef]
27. Bao, Z.; Xue, R. Survey on Deep Learning Applications in Digital Image Security. *Opt. Eng.* **2021**, *60*, 120901. [CrossRef]
28. Chacko, A.; Chacko, S. Deep Learning-Based Robust Medical Image Watermarking Exploiting DCT and Harris Hawks Optimization. *Int. J. Intell. Syst.* **2022**, *37*, 4810–4844. [CrossRef]
29. Fan, Y.; Li, J.; Bhatti, U.A.; Shao, C.; Gong, C.; Cheng, J.; Chen, Y. A Multi-Watermarking Algorithm for Medical Images Using Inception V3 and DCT. *Comput. Mater. Contin.* **2023**, *74*, 1279–1302.
30. Zhang, W.; Li, J.; Bhatti, U.A.; Liu, J.; Zheng, J.; Chen, Y.-W. Robust Multi-Watermarking Algorithm for Medical Images Based on GoogLeNet and Henon Map. *Comput. Mater. Contin.* **2023**, *75*, 565–586. [CrossRef]
31. Zoph, B.; Vasudevan, V.; Shlens, J.; Le, Q.V. Learning Transferable Architectures for Scalable Image Recognition. In Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake City, UT, USA, 18–23 June 2018; IEEE: New York, NY, USA, 2018; pp. 8697–8710.
32. Liu, Y.L.; Li, J.B. DCT and Logistic Map Based Multiple Robust Watermarks for Medical Image. *Appl. Res. Comput.* **2013**, *30*, 3430–3433.
33. Liu, Y.; Li, J. The Medical Image Watermarking Algorithm Using DWT-DCT and Logistic. In Proceedings of the 2012 7th International Conference on Computing and Convergence Technology (ICCCT), Seoul, Republic of Korea, 3–5 December 2012; pp. 599–603.
34. Fang, Y.; Liu, J.; Li, J.; Cheng, J.; Hu, J.; Yi, D.; Xiao, X.; Bhatti, U.A. Robust Zero-Watermarking Algorithm for Medical Images Based on SIFT and Bandelet-DCT. *Multimed. Tools Appl.* **2022**, *81*, 16863–16879. [CrossRef]