Computers, Materials & Continua
DOI: 10.32604/cmc.2023.036317
Article

Tech Science Press

Robust Multi-Watermarking Algorithm for Medical Images Based on GoogLeNet and Henon Map

Wenxing Zhang[1], Jingbing Li[1,2,*], Uzair Aslam Bhatti[1,2], Jing Liu[3], Junhua Zheng[1] and Yen-Wei Chen[4]

[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]Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou, 311100, China
[4]Graduate School of Information Science and Engineering, Ritsumeikan University, Kusatsu, 525-8577, Japan
*Corresponding Author: Jingbing Li. Email: jingbingli2008@hotmail.com
Received: 25 September 2022; Accepted: 19 November 2022

Abstract: The field of medical images has been rapidly evolving since the advent of the digital medical information era. However, medical data is susceptible to leaks and hacks during transmission. This paper proposed a robust multi-watermarking algorithm for medical images based on GoogLeNet transfer learning to protect the privacy of patient data during transmission and storage, as well as to increase the resistance to geometric attacks and the capacity of embedded watermarks of watermarking algorithms. First, a pre-trained GoogLeNet network is used in this paper, based on which the parameters of several previous layers of the network are fixed and the network is fine-tuned for the constructed medical dataset, so that the pre-trained network can further learn the deep convolutional features in the medical dataset, and then the trained network is used to extract the stable feature vectors of medical images. Then, a two-dimensional Henon chaos encryption technique, which is more sensitive to initial values, is used to encrypt multiple different types of watermarked private information. Finally, the feature vector of the image is logically operated with the encrypted multiple watermark information, and the obtained key is stored in a third party, thus achieving zero watermark embedding and blind extraction. The experimental results confirm the robustness of the algorithm from the perspective of multiple types of watermarks, while also demonstrating the successful embedding of multiple watermarks for medical images, and show that the algorithm is more resistant to geometric attacks than some conventional watermarking algorithms.

Keywords: Zero watermarks; GoogLeNet; medical image; Henon map; feature vector

1 Introduction

With the comprehensive improvement of network communication technology and medical intelligence, digital technology has been integrated into the medical system, and more and more clinical

medical images, including computed tomography (CT) images and magnetic resonance imaging (MRI) images, have begun to be stored and shared through the Internet and cloud platforms; at the same time, a large amount of medical information from traditional paper medical records has been replaced by electronic medical records, and electronic medical records (EMR) [1,2] is a digital medical record, which enables a large amount of patient information to be transmitted and stored more easily. It is the arrival of its emerging technology that allows physicians to process pathological information more efficiently and patients to have a better medical experience, largely improving the quality of our entire healthcare system. However, although telemedicine diagnostic platforms provide patients with more real-time and convenient medical services, medical big data information can face malicious attacks such as illegal theft and leakage during the actual network transmission [3–5]. Therefore, how to bring into play the convenience of network transmission and at the same time, effectively enhance the security of medical information systems has become an important issue that needs to be addressed. Digital watermarking of medical images [6] is an effective solution, which ensures the security of its transmission on the Internet by hiding patients' personal information in medical carrier images.

Digital watermarking [7–9] is a popular and very effective information-hiding technology nowadays [10,11], and its essential characteristics are security, robustness, imperceptibility, data capacity, etc. Its main method is to embed secret information in the carrier image to protect the copyright of digital products and prove the real reliability of the products. Therefore, applying digital watermarking technology to the medical system and selecting patient information or diagnostic reports as watermarks for embedding can solve security problems such as illegal tampering, stealing and copying. At present, there are two main categories according to the hiding position of the digital watermark: spatial domain [12] and transform domain [13,14]. The spatial domain is to embed the watermark directly by changing the pixel value of the host image, while the transform domain is to embed the digital watermark into a certain transform domain of the host image by transformation. There are mainly classical algorithms such as LSB (Least Significant Bit) and patchwork in the spatial domain, however, after embedding the watermark information into the spatial domain, although the embedded information is guaranteed to be invisible, the robustness of the algorithm is poor and the watermark information is easily corrupted by geometric attacks because the pixel values on the carrier image are changed. Then, in the transform domain watermarking, it is mainly based on discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT), etc., and the embedded watermark is achieved by modifying the transformed coefficients. Alotaibi et al. [15] proposed a text image watermarking algorithm combining integer wavelet transform (IWT) and discrete cosine transform (DCT). The algorithm first decomposes the text image with IWT to obtain the low-frequency subband LL, then performs the DCT transform on the low-frequency subband, and finally embeds the watermark into the low and medium-frequency DCT coefficients; the experimental results have good imperceptibility and good robustness under conventional attacks, but the poor performance against geometric attacks such as rotation. Cedillo-Hernandez et al. [16] proposed a watermarking algorithm based on the DFT domain. The algorithm first performs the DFT transform on medical images and then embeds the watermark into the IF amplitude of the DFT to achieve the embedding of the watermark, which has better robustness in a few geometric attacks. Assini et al. [17] proposed a watermarking scheme that combines three transforms: DWT, DCT, and singular value decomposition (SVD). In the paper, firstly, the medical carrier image and the watermarked image are separately subjected to the three-level DWT transform, and the obtained high-frequency subbands are separately subjected to the DCT transform, then the coefficients of the DCT transform are subjected to the singular value decomposition using SVD stability, and finally, the singular values of the medical image and the watermark are summed up by the scale factor to achieve

the embedding of the watermark, and the algorithm has good robustness against conventional attacks. Compared with the spatial domain, the transform domain-based watermarking scheme will have better robustness, but the embedding and extracting watermark information operation of such algorithms above is complicated, and the embedding capacity of the watermark is also low, which still needs to be improved in geometric attacks.

Considering the special nature of medical images, medical images such as CT and MRI, which we study, play an important role in acquiring pathological information and diagnosing conditions, as an important carrier of medical information storage. Therefore, the visual quality requirements for medical images are very strict and often no alterations are allowed. Meanwhile, in practical applications, it is found that the watermark embedding capacity of medical images is contradictory to the imperceptibility of the watermark. Then, based on the general transform domain watermarking algorithm, the proposed and applied zero watermarking technology [18,19] effectively solves this problem, and the medical zero watermarking technology can embed the watermark information without changing the visual effect of the original medical image. The main principle is to combine the feature vector of medical carrier image with the watermark information to obtain the logical key, and extract and restore the watermark by the retained key, thus ensuring the visual quality of the medical image, and there is no limitation of embedding capacity, which has high research value. Sinha et al. [20] used the zero watermarking technique to authenticate medical images, obtained the low-frequency subbands of medical images by wavelet decomposition, then extracted the feature values of the low-frequency subbands using SVD. Finally, the watermark and the feature values were logically operated to achieve watermark embedding. This method can be used in the field of telemedicine to effectively protect images from illegal use, but its research lacks the detection of attack experiments. Liu et al. [21] proposed a zero-watermarking algorithm based on dual-tree complex wavelet transform (DTCWT) and DCT. Firstly, DTCWT-DCT combined transformation is performed on the medical carrier image, and the low-frequency coefficient matrix is extracted. Then, the feature vector is obtained by quantization and coding. Finally, the feature vector of the image and the watermark information are used for XOR operation to embed the watermark. This algorithm has strong robustness to conventional attacks, but weak robustness to geometric attacks such as panning. The comparison of the above existing algorithms is shown in Table 1.

Table 1: Comparison of some existing algorithms

Types	Algorithms	Advantages	Disadvantages
Spatial domain	LSB, Patchwork	Convenient and fast	Weak robustness
Transform domain	IWT-DCT [15] DFT [16] DWT-DCT-SVD [17]	Good robustness under conventional attacks	Complex scheme operation Limited capacity Weak robustness against geometric attacks
	DWT-SVD [20] DTCWT-DCT [21]	Zero watermark No capacity limitation Good robustness under conventional attacks	Weak robustness against geometric attacks

With the development of deep learning, it has become a research hotspot for scholars in computer vision, natural language processing, speech recognition, and other fields, especially Convolutional Neural Networks (CNN) is currently very widely used, and more stable feature information can be extracted by convolutional neural networks [22,23]. Therefore, in response to the weakness of traditional algorithms in resisting geometric attacks, some research scholars have combined deep learning techniques with watermarking technology in recent years to improve the robustness of watermarking algorithms, which has essential research significance for medical privacy protection. Fierro-Radilla et al. [24] used a convolutional neural network to generate stable features of images and combined the feature information with watermark by XOR operation, to realize zero watermark embedding. The results are robust to some geometric attacks, but the types of geometric test attacks are less. Han et al. [25] proposed a zero watermarking scheme for medical images based on the convolutional neural network VGG19, which extracts the depth feature map of medical images by a pre-trained VGG19 network and performs DFT transform on the feature map; then selects the low-frequency coefficients of Fourier transform, converts the low-frequency coefficients into a binary hash sequence, and finally correlate the watermark information with the hash sequence to achieve watermark embedding. In terms of resistance to geometric attacks, the algorithm has improved its robustness compared to conventional algorithms. However, there are few research solutions combining neural networks with zero watermarking techniques, while most of the existing watermarking algorithms show less than optimal robustness in the face of major geometric attacks such as rotation, translation, scaling and shearing.

Synthesizing the above research progress, the resistance to geometric attacks is still a research difficulty. Therefore, this paper proposes a robust multi-watermarking algorithm for medical images based on the GoogLeNet neural network, which selects a pre-trained GoogLeNet network and trains a medical image feature extraction network using the medical image dataset for transfer learning of the GoogLeNet network. Firstly, the trained network is used to extract the feature vector of the carrier image. Then, several different types of watermark information are chaotically encrypted by Henon mapping. Finally, the zero watermarking technique is used to combine the feature vectors with the encrypted multiple watermark information to generate the key and complete the multiple watermark embedding and blind extraction. The proposed algorithm can effectively resist many different attacks and is especially robust against geometric attacks.

The main contribution of the present research is:

(1) Combining neural networks with zero watermarking techniques to extract more stable image feature vectors, which are more robust than conventional watermarking algorithms in terms of resistance to geometric attacks.
(2) Watermark encryption adopts a two-dimensional chaotic Henon mapping system that is more sensitive to initial values, with higher security performance than one-dimensional chaotic mapping systems such as Logistic mapping, which improves the security of watermark information as well as its concealment.
(3) Combined with zero watermarking technology, it does not change the original characteristics of medical image carriers, which better solves the contradiction between watermark embedding capacity and imperceptibility of medical images.
(4) Selecting several different types of watermark information (symbols, graphics, and text) to verify the algorithm's robustness from multiple perspectives, completing multiple watermark embedding and blind extraction, and improving the embedding capacity of the algorithm.

The organization of this paper consists of five sections: Introduction, The Fundamental Theory, The Proposed Watermarking Algorithm, Experiment and Analysis, and Conclusions. In the remaining part of the organization, the second section focuses on the basic theory of the proposed algorithm, including the GoogLeNet network and Henon Map. The third section presents the detailed process of implementing the algorithm. The fourth section presents the experiments and analysis, mainly to verify the robustness of the algorithm through various attacks and compare it with other algorithms. The fifth section mainly summarizes the ideas and advantages of the algorithm, as well as the future research focus directions.

2 The Fundamental Theory

2.1 GoogLeNet Neural Network Model

With the continuous development of convolutional neural network (CNN) models, general convolutional neural networks will improve their performance by extending the depth and width of the network model; however, more profound or wider networks will face many problems such as too many parameters prone to overfitting, gradient dispersion, and increased computational complexity. Therefore, the proposed GoogLeNet network [26] can effectively improve the problems of traditional networks, which is a convolutional neural network model architecture for multi-scale image information extraction proposed by a team at Google Inc. and won the championship at the ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) in 2014.

The GoogLeNet convolutional neural network has 22 layers of depth, as shown in Fig. 1, and has nine Inception modules at the core of its architecture. Although its network depth reaches 22 layers, its parametric size is much smaller than that of ALexNet and VGG networks, and its performance is much superior. Meanwhile, to avoid the gradient dispersion problem brought about by increasing the network depth, two auxiliary classifiers are added to the GoogLeNet network structure for back-propagating gradients in the training phase, which can effectively avoid the gradient disappearance problem. Then in the testing phase, only the final Softmax3 is used to output the results, and the two auxiliary classifiers will be removed.

Of course, the proposed Inception module structure is an essential innovation in the GoogLeNet network. The main principle of the Inception module is to use multiple different convolutional kernels to extract feature information of different image sizes and fuse this feature information as the output. The Inception module can obtain better image features than a single convolutional kernel size. This structure uses a locally optimal sparse structure instead of the original convolutional neural network's fully connected approach to minimize redundancy and increase the width and depth of the network structure, and the performance is improved. As shown in Fig. 2, it is a net-within-a-network structure, and it can be seen from the structure diagram that 1×1 convolutional layers are added before the 3×3 convolutional layer and the 5×5 convolutional layer, and after the 3×3 maximum pooling layer, respectively, where 1×1 convolution is mainly used for dimensionality reduction, which reduces the number of parameters and thus the complexity of computation. Therefore, when memory or computational resources are limited, GoogLeNet network will play a great advantage.

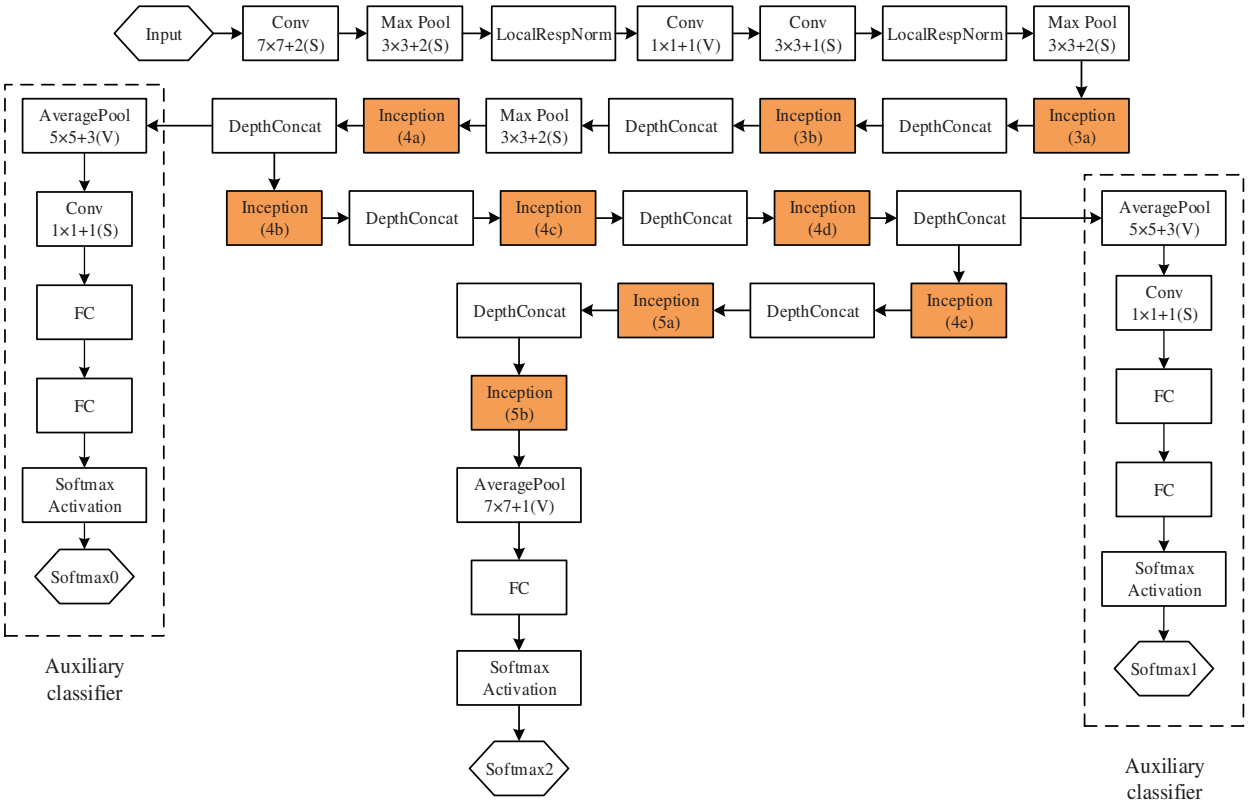


Figure 1: GoogLeNet convolutional neural network structure

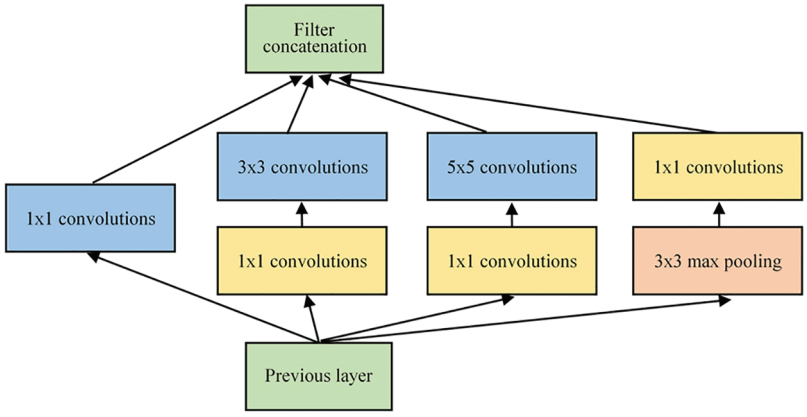


Figure 2: Inception module structure

2.2 Henon Map

Henon map [27] is a two-input two-dimensional nonlinear discrete chaotic mapping system that is very sensitive to chaotic initial values. Since the system is controlled by two variables simultaneously, then its security performance will be better than that of one-dimensional chaotic techniques such as

Logistic mapping, so it is suitable for generating pseudo-random sequences in image encryption. The iterative equation of its mapping is as in Eq. (1).

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

where x and y are the two variables of the system and n is the number of iterations, the study shows that when the parameters take the values $a = 1.4$ and $b = 0.3$, the system is in a chaotic state, generating both x and y chaotic system variables system, in Fig. 3 is the generated chaotic attractor, this chaotic attractor is two irregular curves. Fig. 4 shows the bifurcation diagram of the x_n component of the Henon system with the variation of the parameter a, where the initial values $x_o = 0$, $y_o = 0$, $b = 0.3$, and $a \in [0, 1.4]$ are taken, and it can be seen that the more the value of a is taken close to 1.4, the higher the complexity of the chaotic system. Therefore, in cryptographic applications, the parameters are usually taken to be $a = 1.4$ and $b = 0.3$.

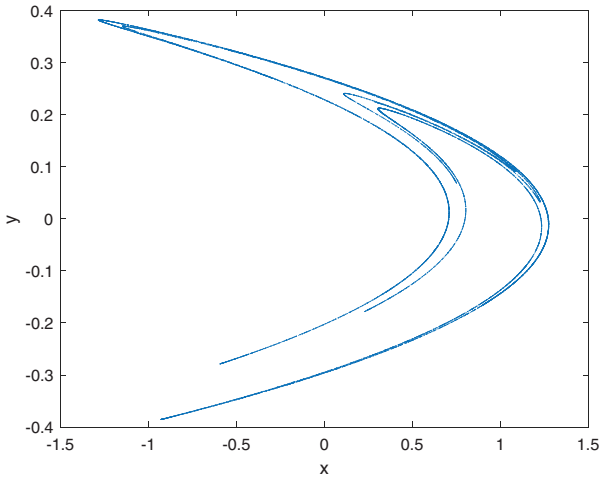


Figure 3: The chaotic attractor of the Henon map

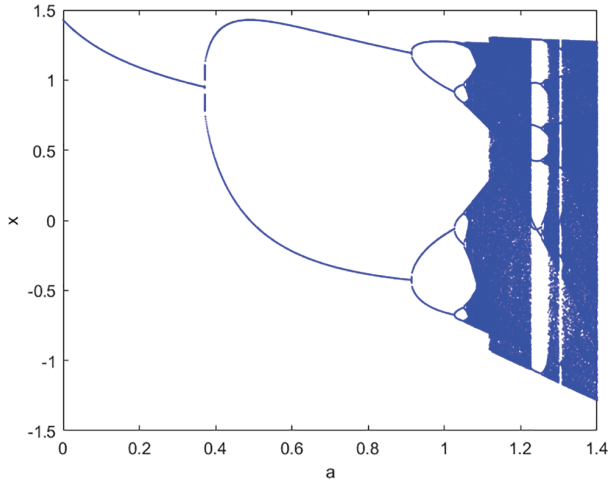


Figure 4: The bifurcation diagram of Henon map

3 The Proposed Watermarking Algorithm

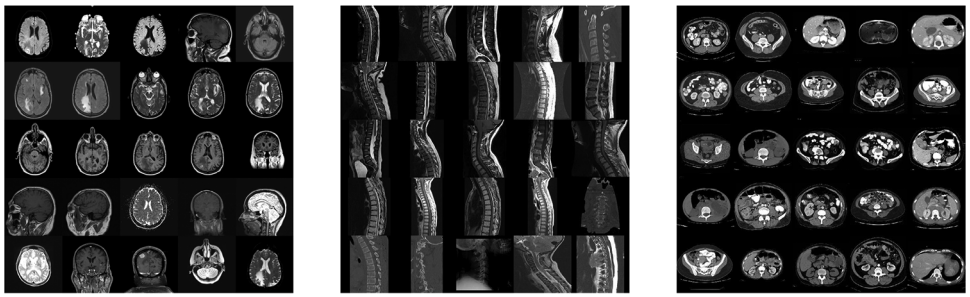
3.1 Transfer Learning for GoogLeNet Neural Network

At present, deep learning has been widely used in the field of medical image processing, however, due to the particular characteristics of medical images, it is difficult for us to obtain a large amount of medical image data for training, and the annotation cost is high, and there are few free and publicly available medical datasets. Then it becomes a difficult task to obtain a network model for deep feature extraction by training a large number of medical images. Therefore, combining it with transfer learning can be a good solution to the current problem. Transfer learning [28] is a machine learning method that refers to a pre-trained model being reused in another task, which can effectively circumvent the shortcoming of insufficient training data and improve the performance of neural networks.

Then in the zero watermarking algorithms, extracting stable features of medical images is a very important part. The method in this paper is to select the pre-trained GoogLeNet network on the ImageNet database, which has been trained with more than one million natural images and has a good feature extraction effect; on this basis, the network is fine-tuned for the medical dataset we constructed and transfer learning is performed to train the medical image feature extraction network.

3.1.1 Building the Dataset

Our dataset images were obtained from two open-source medical databases, The National Institutes of Health Clinical Center and The National Library of Medicine present MedPix. In constructing the dataset, we selected three types of medical images from open-source data, brain, spine, and abdomen, as the original sample images, with a total of 390 images, and some of the dataset images are shown in Fig. 5. 80% of these images were used for training, 10% for validation, and 10% for testing. Of course, to increase the diversity of training samples and enhance the robustness of the training model, we utilized data enhancement by performing various attacks on the original training sample images, including Gaussian noise, JPEG compression, median filtering, rotation, panning, cropping, and scaling. After processing, the training samples reached 17160. In addition, since the input size of the GoogLeNet network is $224 \times 224 \times 3$, the sample images of the dataset were all resized to $224 \times 224 \times 3$ pixels.



(a) (b) (c)

Figure 5: Partial images of the dataset. (a) Brain. (b) Spine. (c) Abdomen

In this time, we use a 32-bit image binary feature vector as the label of the dataset, where the 32-bit feature vector just matches the size of the embedded watermark. The steps of feature vector acquisition: (1) DCT is performed on medical images; (2) the values of the 4×8 region in the upper left corner of the DCT coefficient matrix are extracted and combined with the perceptual hash [29], the positive coefficient values or zero are represented by quantization coding with "1" and "0" to represent

the negative coefficient values, generating a 32-bit binary feature vector. Meanwhile, both the original training image and the validation image are subjected to the same steps, and their respective 32-bit feature vectors are used as the labels of the images.

3.1.2 Training the GoogLeNet Network

This experiment utilizes the neural network toolbox of Matlab 2019a with an NVIDIA GeForce GTX 1050Ti hardware graphics card. We also fine-tuned the network by changing the fully connected layer of the GoogLeNet network from the initial 1000 outputs to 32 outputs to match the zero watermarking systems, and by deleting the Softmax and Classification Output layers of the network and adding a Regression Output layer after the fully connected layer, so that the modified network can complete the regression task.

During the training process, we freeze the 1:110 layers of the pre-trained network, so that the parameters of the frozen layers are not updated and only the later layers are trained with the pre-trained parameters to improve the training efficiency and reduce the hardware requirements of the training process. The training process is accelerated by Graphics Processing Units (GPU), and the whole training process takes only about 16 minutes, and the specific hyperparameter settings are shown in Table 2. The final trained network outputs 32 feature values after processing the input image, which can be subsequently matched with the watermarking system.

Table 2: Hyperparameters of the network

Types	Parameters
Optimizer	Stochastic gradient descent with momentum optimizer (SGDM)
Loss function	Mean square error function
Mini-Batch size	32
Learning rate	0.001
Number of epochs	5

3.2 Feature Extraction of Medical Images

Since the algorithm in this paper uses the zero watermarking technique, the main method of this technique is to associate the image features with the watermark. Then extracting a stable image feature vector can guarantee the robustness of the watermarking algorithm. At this time, we utilize the trained GoogLeNet network to extract the feature information, which has the architecture of multi-scale image information extraction and can be well combined with the zero watermarking technique to obtain stable feature vectors. Fig. 6 shows the process of feature extraction with the following steps:

Step 1: Using the original medical image I(i, j) as the input to the trained GoogLeNet network, with the input images all resized to $224 \times 224 \times 3$.

Step 2: Since we previously used the 32-bit image binary feature vector as the label of the dataset, the original 1000 parameter values of the fully connected layer (FC) are adjusted to 32, so the medical image is processed by the trained GoogLeNet network, and the fully connected layer FC outputs 32 feature values D(j).

Step 3: Combined with the perceptual hash, the 32 values D(j) are quantized and encoded, and those greater than or equal to 0.5 are judged as "1" and those less than 0.5 are judged as "0" to generate a binary feature sequence, which is used as the feature vector V(j) of the medical image.

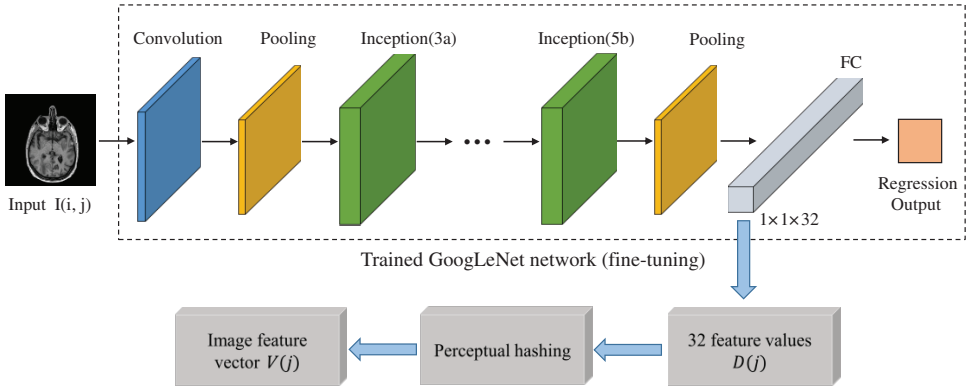


Figure 6: The process of image feature extraction

3.3 Watermark Encryption

This time, Henon mapping is used to perform chaotic encryption of watermark, which is a two-dimensional discrete chaotic system with higher security than one-dimensional chaotic systems such as Logistic mapping. Fig. 7 is the flow chart of the chaotic encryption algorithm with multiple watermarks.

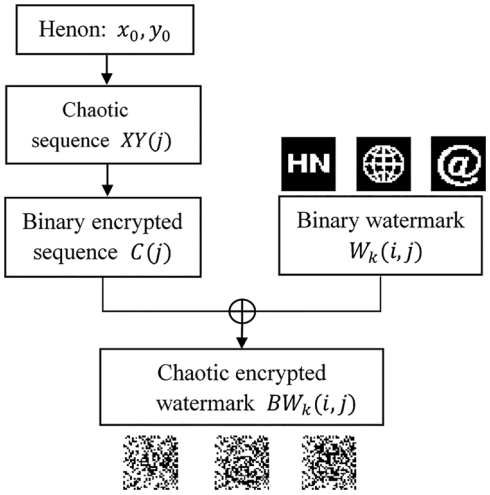


Figure 7: The watermark encryption process

The steps of the watermark encryption principle are:

Step 1: We first generate the chaotic sequence XY(j) given the initial values of the system x_0 and y_0.

Step 2: By quantization coding the chaotic sequence XY(j), the value greater than or equal to 0 is judged as "1" and the opposite is judged as "0", thus converting the chaotic sequence XY(j) into a binary encrypted sequence C(j).

Step 3: Three different types of binary watermark $W_k(i, j)$ were selected, including text, symbols and graphics, with a pixel size of 32 × 32. Finally, XOR operation is performed on each line of the binary watermarking image $W_k(i, j)$ and binary encryption sequence C(j) to obtain chaotic encrypted multi-watermark $BW_k(i, j)$, as shown in Eq. (2), where "⊕" is an XOR operator. The operation rule

is: when the two values are different, the XOR result is 1; conversely, the result is 0.

$$BW_k(i,j) = C(j) \oplus W_k(i,j) \tag{2}$$

3.4 Watermark Embedding

Digital watermarking system mainly has two important processes of watermark embedding and watermark extraction, this section introduces the watermark embedding part, the watermark embedding process is shown in Fig. 8. The specific implementation steps are as follows:

Step 1: The feature vector V(j) of the original medical image I(i, j) is extracted through the trained GoogLeNet network, and the detailed steps of obtaining the feature vector can refer to the chapter: feature extraction of medical images.

Step 2: Before watermark embedding, Henon chaos encryption is performed on different types of multi-watermark information to improve information security, and chaos encrypted multi-watermark $BW_k(i, j)$ is obtained.

Step 3 : The feature vector V(j) and the encrypted watermark $BW_k(i, j)$ are performed XOR operation to generate the logical key $Key_k(i, j)$, which is saved in the third party to realize the embedding of multiple watermarks, as shown in Eq. (3).

$$Key_k(i,j) = V(j) \oplus BW_k(i,j) \tag{3}$$

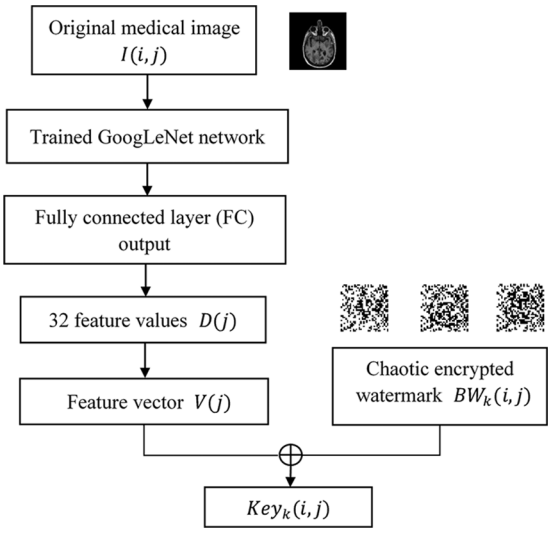


Figure 8: The watermark embedding process

3.5 The Extraction and Decryption of Watermark

This section includes the extraction and decryption of the watermark, the process of which is shown in Fig. 9, with the following implementation steps:

Step 1: Firstly, extract the feature vector V′(j) of the medical image I′(i, j) to be tested using the same method as watermark embedding.

Step 2: The feature vector V′(j) and key $Key_k(i,\ j)$ are XOR operation, and then the encrypted multi-watermark information $BW'_k(i,j)$ is extracted, as shown in Eq. (4).

$$BW'_k(i,j) = Key_k(i,j) \oplus V'(i) \tag{4}$$

Step 3: Watermark decryption process: the extracted encrypted watermark $BW'_k(i,j)$ and the binary encryption sequence C(j) are performed XOR operation to restore the watermark information $W'_k(i,j)$, as shown in Eq. (5).

$$W'_k(i,j) = BW'_k(i,j) \oplus C(j) \tag{5}$$

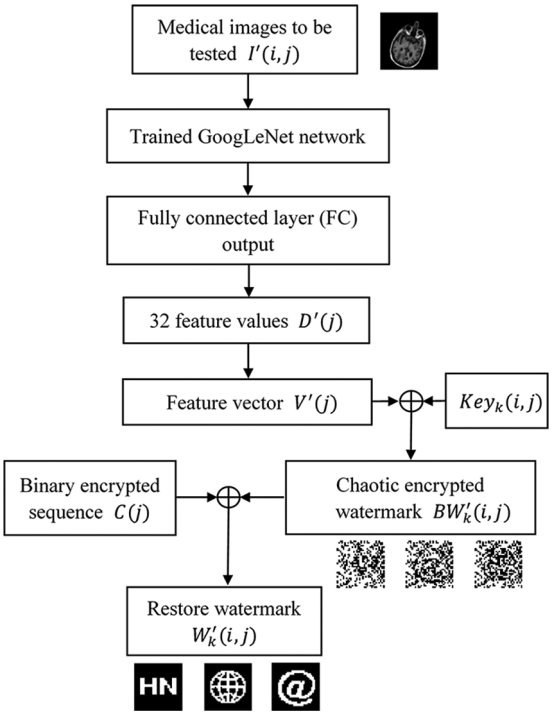


Figure 9: The process of watermark extraction and decryption

4 Experiment and Analysis

This experimental system uses MATLAB 2019a as a platform, and the main research process is to test the watermarking algorithm by conventional and geometric attacks. In the experiments, we randomly selected a brain slice image from the test set as the original medical image for testing, and also selected three 32 × 32 pixel binary watermarked maps including text, graphics and symbols, which can verify the robustness of the algorithm from several aspects. In addition, to further improve the security, we use the Henon chaos encryption technique to encrypt the original watermark information, as shown in Fig. 10.

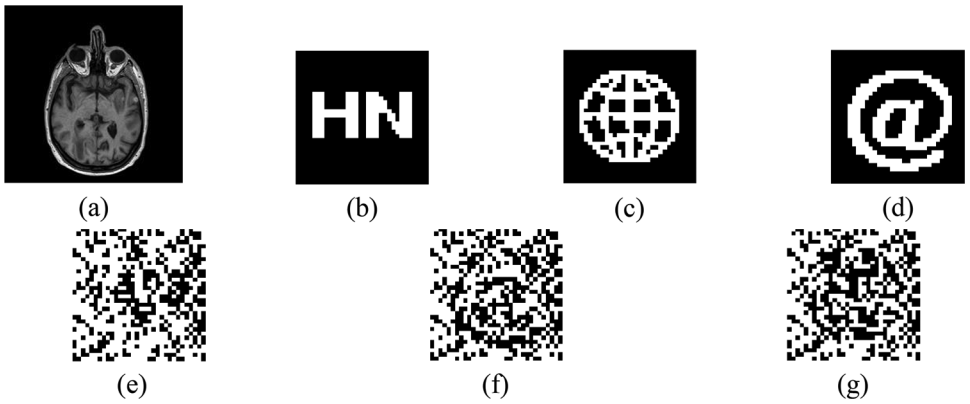


Figure 10: Medical images and watermarks. (a) Original medical image. (b) Original binary watermark 1. (c) Original binary watermark 2. (d) Original binary watermark 3. (e) Encrypted watermark 1. (f) Encrypted watermark 2. (g) Encrypted watermark 3

4.1 Performance Indicators

In our experiments, we used two performance metrics: peak signal-to-noise ratio (PSNR) and normalized correlation coefficient (NC). Among them, PSNR can measure the distortion degree of medical images containing watermarks, and the smaller the PSNR value, the greater the distortion degree of the image. In Eq. (6), I(i, j) denotes the grayscale value of each pixel point in the original image; I′(i, j) denotes the grayscale value of each pixel point in the embedded watermarked image; M and N denote the pixel values of the rows and columns of the medical image.

$$PSNR = 10\lg\left[\frac{MN\max_{i,j}\left(I\left(i,j\right)\right)^2}{\sum_i\sum_j\left(I\left(i,j\right)-I'\left(i,j\right)\right)^2}\right] \tag{6}$$

Meanwhile, to compare the correlation between the original watermark and the extracted watermark, we use the normalized correlation coefficient NC. In Eq. (7), W(i, j) is the original watermark and W′(i, j) is the extracted watermark. in the experiment, when the NC value is not less than 0.5, the algorithm can effectively extract the watermark information; when the NC value is closer to 1, it means that the correlation between the two is higher and the algorithm is more robust against attacks.

$$NC = \frac{\sum_i\sum_j W\left(i,j\right)W'\left(i,j\right)}{\sum_i\sum_j W^2\left(i,j\right)} \tag{7}$$

4.2 The Reliability of the Algorithm

To prove the reliability of the algorithm, it is guaranteed that the extracted feature vectors are representative. We can use the normalized correlation coefficient NC to measure the similarity between different image feature vectors, when the NC value is lower than 0.5, it means that the similarity of different image feature vectors is low and the extracted feature vectors are well representative; on the contrary, it means that the feature vectors are not very representative. In this time, we selected 4 different medical images from inside and outside the test set to test, and Fig. 11 shows the 8 medical images tested, and Table 3 shows the NC values between them.

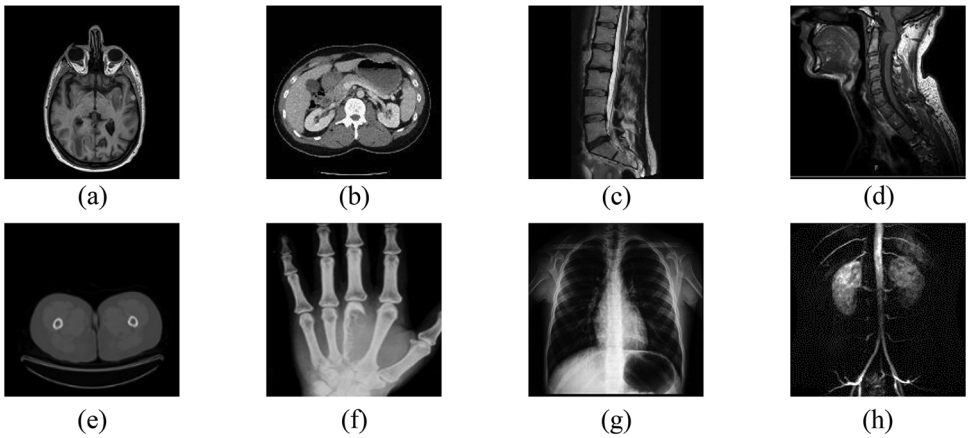


Figure 11: Different medical images. (a) Brain. (b) Abdomen. (c) Spine 1. (d) Spine 2. (e) Breast. (f) Hand. (g) Chest. (h) Lung

Table 3: NC value between different images

Image	Brain	Abdomen	Spine 1	Spine 2	Breast	Hand	Chest	Lung
Brain	1.00	0.06	−0.12	−0.06	0.43	−0.02	0.08	0.31
Abdomen	0.06	1.00	0.06	0.25	−0.13	0.33	0.00	0.25
Spine 1	−0.12	0.06	1.00	0.06	0.20	0.28	0.18	0.20
Spine 2	−0.06	0.25	0.06	1.00	−0.25	0.33	0.39	0.00
Breast	0.43	−0.13	0.20	−0.25	1.00	−0.11	−0.23	0.37
Hand	−0.02	0.33	0.28	0.33	−0.11	1.00	0.02	0.29
Chest	0.08	0.00	0.18	0.39	−0.23	0.02	1.00	0.16
Lung	0.31	0.25	0.20	0.00	0.37	0.29	0.16	1.00

The data in Table 3 shows that the absolute values of NC values between different images are less than 0.5, and the NC values between the same images are all 1. Therefore, the medical image feature vectors extracted by the trained network are representative and can distinguish between different images, indicating that the algorithm is reliable.

4.3 The Result of the Attack Experiment

In this simulation experiment, we tested conventional and geometric attacks of different intensities, respectively, and selected three types of watermark information. The original watermark is shown in Fig. 10 above. Meanwhile, in the experimental results, "NC1" represents the NC value after the original watermark 1 attack, "NC2" represents the NC value after the original watermark 2 attacks, and "NC3" represents the NC value after the original watermark 3 attacks.

4.3.1 Conventional Attacks

In the conventional attacks, we tested three attacks of Gaussian noise, JPEG compression, and median filtering, respectively. As can be seen from Table 4, when the JPEG compression strength reaches 5%, the NC values of the three extracted watermarks are more than 0.9; meanwhile, two

strengths of the median filter attack were tested, and the NC values are greater than 0.8; in addition, when the Gaussian noise attack reaches 14%, the NC values are 0.59, 0.58 and 0.58, respectively, and the watermark information can still be effectively recovered, Fig. 12 shows some experimental effects. Therefore, the proposed algorithm can effectively resist conventional attacks, especially in JPEG compression attacks with strong robustness.

Table 4: PSNR and NC values under conventional attacks

Attacks	Intensity	PSNR (dB)	NC1	NC2	NC3
Gaussian noise (%)	2	19.02	0.91	0.94	0.94
	5	15.27	0.86	0.87	0.88
	10	12.56	0.78	0.84	0.83
	14	11.30	0.59	0.58	0.58
JPEG compression (%)	5	24.47	0.91	0.94	0.94
	10	29.46	0.91	0.94	0.94
	20	31.77	1.00	1.00	1.00
	30	33.27	1.00	1.00	1.00
Median filter (5 times)	[3, 3]	29.53	0.91	0.93	0.93
	[7, 7]	24.06	0.81	0.87	0.87

4.3.2 Geometric Attacks

Since resistance to geometric attacks is an important part of the current need to be addressed, we tested multiple groups of attacks, including rotation, scaling, translation, and shear attacks, respectively, in this time. From Table 5, we can see that the algorithm can effectively extract watermarks under five different geometric attacks, and their NC values are all greater than 0.5. Among them, when the rotation attack reaches 45 degrees, the NC values of all three watermarks exceed 0.8; meanwhile, when the Y-axis shear strength reaches 45%, the NC values of their extracted watermarks are 0.72, 0.72 and 0.74, respectively, and the watermark information can be effectively recovered. Therefore, the algorithm can well solve the problem of resistance to geometric attacks, especially in rotation, scaling, and translation with good robustness. Fig. 13 shows some experimental effects.

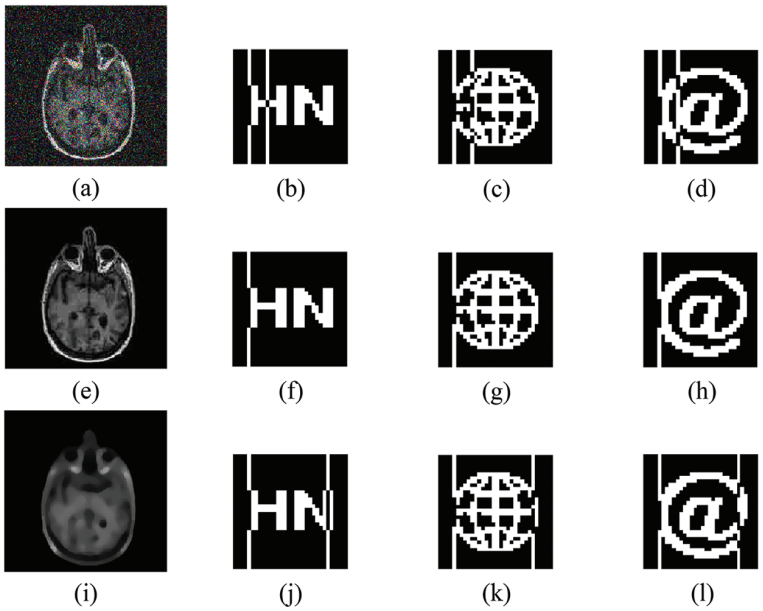


Figure 12: Under conventional attacks. (a) Gaussian noise 5%. (e) JPEG compression 10%. (i) Median filter [7,7] (5 times). (b–d) are all three watermarks extracted with Gaussian noise at 5%. (f–h) are all three watermarks extracted with JPEG compression at 10%. (j–l) are all three watermarks extracted with median filter [7,7] (5 times)

Table 5: PSNR and NC values under geometric attacks

Attacks	Intensity	PSNR (dB)	NC1	NC2	NC3
Rotation (clockwise) (°)	5	18.44	1.00	1.00	1.00
	10	16.30	1.00	1.00	1.00
	20	15.81	0.91	0.93	0.92
	40	14.75	0.87	0.84	0.86
	45	14.73	0.87	0.84	0.86
Scaling factor	0.2	—	0.91	0.94	0.94
	0.5	—	1.00	1.00	1.00
	2.0	—	1.00	1.00	1.00
	3.0	—	1.00	1.00	1.00
Left translation (%)	5	14.86	1.00	1.00	1.00
	15	14.02	1.00	1.00	1.00
	30	13.14	0.95	0.93	0.94
	40	12.77	0.86	0.87	0.88
Cropping ratio (%) (Y direction)	10	—	1.00	1.00	1.00
	27	—	1.00	1.00	1.00
	40	—	0.76	0.81	0.80
	45	—	0.72	0.72	0.74

(Continued)

Table 5: Continued

Attacks	Intensity	PSNR (dB)	NC1	NC2	NC3
Cropping ratio (%) (X direction)	5	—	1.00	1.00	1.00
	15	—	1.00	1.00	1.00
	30	—	0.95	0.93	0.94
	40	—	0.72	0.72	0.72

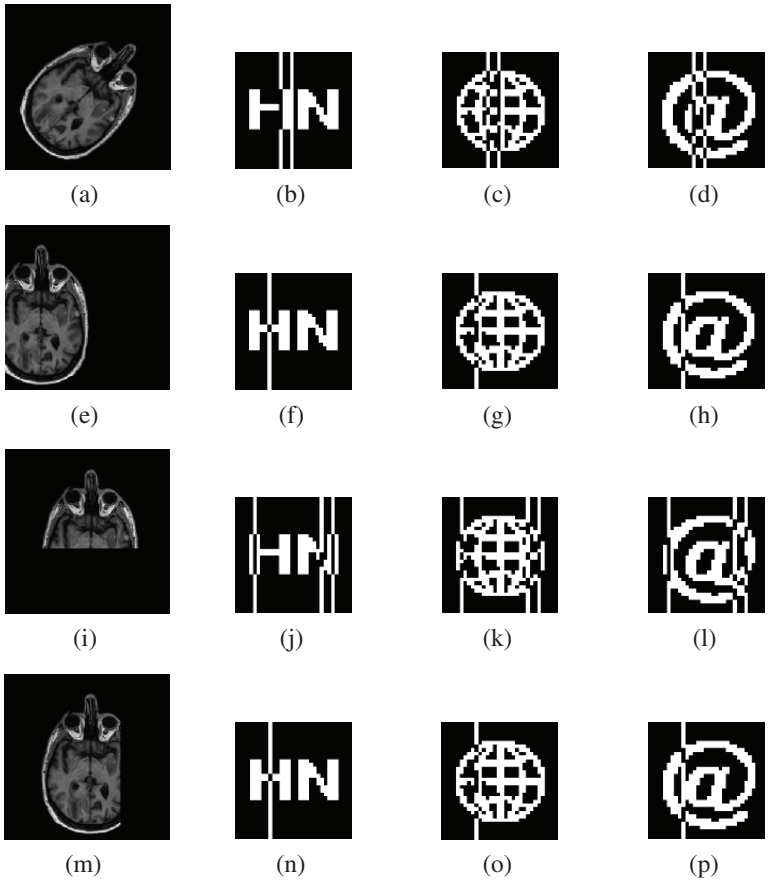


Figure 13: Under geometric attacks. (a) Clockwise rotation (45°). (e) Left translation 30%. (i) Cropping ratio 40% (Y direction). (m) cropping ratio 30% (X direction). (b–d) are the three watermarks extracted under clockwise rotation (45°). (f–h) are the three watermarks extracted under left translation 30%. (j–l) are the three watermarks extracted under a cropping ratio 40% (Y direction). (n–p) are the three watermarks extracted under a cropping ratio 30% (X direction)

4.4 Algorithms Comparison

To better verify the robustness of the proposed algorithm, we compare it with a part of existing classical watermarking algorithms. In the experimental process, we selected the same size of brain map and text "HN" watermark information for testing to maintain uniformity. Then, we compared with the existing algorithms KAZE-DCT [30], Zernike-DCT [31], Inception V3-DCT [32], and DWT-DCT. As can be seen, from both Table 6 and Fig. 14, the performance of the proposed algorithm is similar to the other four algorithms in conventional attacks; in geometric attacks, although the algorithm performs slightly lower than the DWT-DCT algorithm in downshift attacks, it significantly outperforms the existing algorithms in most geometric attacks, especially in comparison with the algorithm using pre-trained Inception V3, the proposed paper based on GoogLeNet transfer learning based watermarking scheme in this paper has superior performance. Thus, the proposed algorithm is generally better than the existing algorithms and has good robustness in both conventional and geometric attacks.

Table 6: Comparison between different algorithms

Attacks	Intensity	Ref. [30] (NC1)	Ref. [31] (NC2)	Ref. [32] (NC3)	DWT-DCT (NC4)	Proposed (NC5)
Gaussian noise (%)	2	0.63	0.94	0.76	0.95	0.91
	5	0.53	0.72	0.63	0.95	0.86
	10	0.41	0.67	0.59	0.82	0.78
JPEG compression (%)	5	0.69	0.93	0.77	0.96	0.91
	10	0.80	0.72	0.82	1.00	0.91
	15	0.62	1.00	0.80	1.00	**1.00**
Rotation (clockwise) (°)	3	0.80	0.91	0.91	0.88	**1.00**
	15	0.46	0.50	0.67	0.62	**0.91**
	35	0.66	0.45	0.58	0.29	**0.78**
Scaling factor	0.2	0.23	0.21	0.67	0.92	0.91
	0.6	0.54	0.87	1.00	0.92	**1.00**
	1.2	0.79	0.91	1.00	0.96	**1.00**
Left translation (%)	1	1.00	0.84	0.94	0.95	**1.00**
	5	1.00	0.33	0.91	0.42	**1.00**
	8	1.00	0.24	0.87	0.27	**1.00**
Downward translation(%)	3	1.00	1.00	0.91	0.93	0.81
	10	0.62	0.76	0.76	0.80	0.78
Cropping ratio (%) (Y direction)	8	0.88	0.91	0.91	0.87	**1.00**
	22	0.68	0.57	0.59	0.78	**1.00**
	40	0.54	0.45	0.81	0.54	0.76

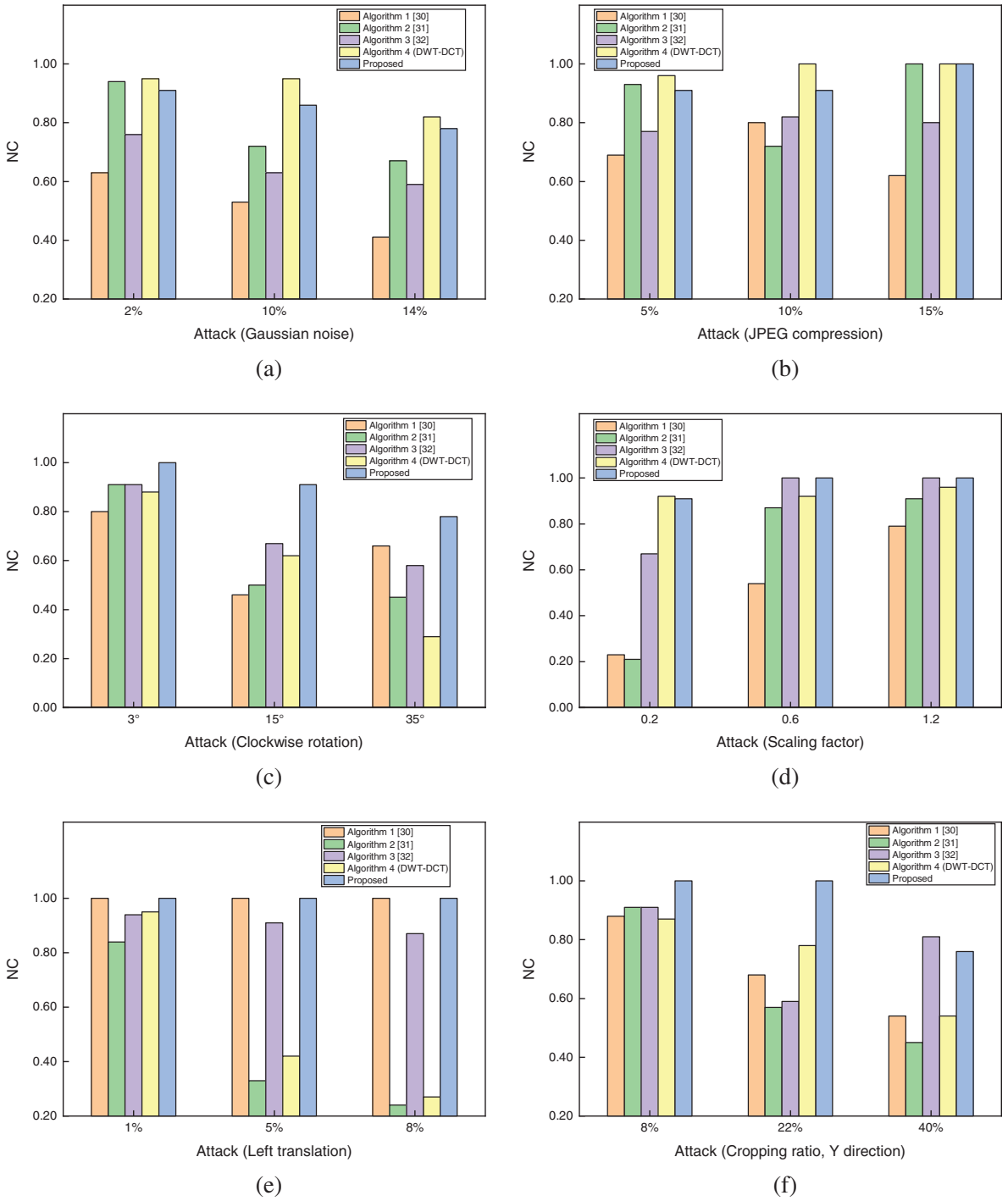


Figure 14: Comparison of the NC values of the proposed algorithm with the three existing algorithms under different attacks. (a) Gaussian noise attack. (b) JPEG compression attack. (c) Rotation attack (clockwise). (d) Scaling attack. (e) Left translation attack. (f) Cropping attack (Y direction)

5 Conclusions

In this paper, we propose a robust multi-watermarking algorithm for medical images based on GoogLeNet and Henon Map, which combines neural networks, chaotic encryption, and zero-watermarking techniques. First, the GoogLeNet network is migrated to learn with the constructed medical training sample set, and then the trained network is used to extract the feature vectors of medical images; meanwhile, to further improve the security of watermark information, we choose a two-dimensional chaotic Henon Map system with higher security performance to perform chaotic encryption on the watermark; among them, for watermark embedding and extraction, we embed simultaneously Three different types of watermark information are embedded and extracted, which can be used to test the reliability of the algorithm from multiple perspectives. Finally, the obtained feature vectors are combined with the encrypted watermark, thus completing the zero watermark embedding and blind extraction. The experimental results show that the algorithm has good robustness against both conventional and geometric attacks, especially in geometric attacks, and also achieves the embedding and extraction of multiple watermark information, so the algorithm has good applicability. Of course, the algorithm still has a lot of room for improvement, and future work will focus on optimizing our feature extraction network to improve the performance of the algorithm continuously.

Acknowledgement: 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 ZDYF2021SHF Z093, the Hainan Provincial Natural Science Foundation of China under Grants 2019RC018 and 619QN246, and the postdoctor research from Zhejiang Province under Grant ZJ2021028.

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 ZDYF2021SHF Z093, 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] O. Ayaad, A. Alloubani, E. A. ALhajaa, M. Farhan, S. Abuseif *et al.,* "The role of electronic medical records in improving the quality of health care services: Comparative study," *International Journal of Medical Informatics*, vol. 127, no. 1, pp. 63–67, 2019.

[2] 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.

[3] M. J. Vidya and K. V. Padmaja, "Enhancing security of electronic patient record using watermarking technique," *Materials Today: Proceedings*, vol. 5, no. 4, pp. 10660–10664, 2018.

[4] T. F. Li, J. B. Li, J. Liu, M. X. Huang, Y. W. Chen *et al.,* "Robust watermarking algorithm for medical images based on log-polar transform," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, pp. 1–11, 2022.

[5] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, no. 3, pp. 72–80, 2020.

[6] A. F. Qasim, F. Meziane and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Computer Science Review*, vol. 27, pp. 45–60, 2018.

[7] H. Tao, L. Chongmin, J. M. Zain and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014.
[8] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Information*, vol. 11, no. 2, pp. 110, 2020.
[9] F. Regazzoni, P. Palmieri, F. Smailbegovic, R. Cammarota and I. Polian, "Protecting artificial intelligence IPs: A survey of watermarking and fingerprinting for machine learning," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 2, pp. 180–191, 2021.
[10] R. H. Meng, Q. Cui and C. S. Yuan, "A survey of image information hiding algorithms based on deep learning," *Computer Modeling in Engineering & Sciences*, vol. 117, no. 2, pp. 425–454, 2018.
[11] V. L. Cu, T. Nguyen, J. C. Burie and J. M. Ogier, "A robust watermarking approach for security issue of binary documents using fully convolutional networks," *International Journal on Document Analysis and Recognition*, vol. 23, no. 3, pp. 219–239, 2020.
[12] J. Abraham and V. Paul, "An imperceptible spatial domain color image watermarking scheme," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 1, pp. 125–133, 2019.
[13] A. Tiwari and M. Sharma, "A survey of transform domain based semifragile watermarking schemes for image authentication," *Journal of the Institution of Engineers*, vol. 93, no. 3, pp. 185–191, 2012.
[14] Z. H. Yuan, Q. T. Su, D. C. Liu and X. T. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *The Visual Computer*, vol. 37, no. 7, pp. 1867–1881, 2021.
[15] R. A. Alotaibi and L. A. Elrefaei, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)," *Applied Computing and Informatics*, vol. 15, no. 2, pp. 191–202, 2019.
[16] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake and H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging," *Signal, Image and Video Processing*, vol. 9, no. 5, pp. 1163–1178, 2015.
[17] I. Assini, A. Badri, K. Safi, A. Sahel and A. Baghdad, "A robust hybrid watermarking technique for securing medical image," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 3, pp. 169–176, 2018.
[18] K. Hu, X. C. Wang, J. P. Hu, H. F. Wang and H. Qin, "A novel robust zero-watermarking algorithm for medical images," *The Visual Computer*, vol. 37, no. 9, pp. 2841–2853, 2021.
[19] B. W. Wang, J. W. Shi, W. S. Wang and P. Zhao, "Image copyright protection based on blockchain and zero-watermark," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 2188–2199, 2022.
[20] S. Sinha, A. Singh, R. Gupta and S. Singh, "Authentication and tamper detection in tele-medicine using zero watermarking," *Procedia Computer Science*, vol. 132, no. 4, pp. 557–562, 2018.
[21] J. Liu, J. B. Li, K. Zhang, U. A. Bhatti and Y. Ai, "Zero-watermarking algorithm for medical images based on dual-tree complex wavelet transform and discrete cosine transform," *Journal of Medical Imaging and Health Informatics*, vol. 9, no. 1, pp. 188–194, 2019.
[22] L. X. Cao, Y. C. Liang, W. Lv, K. Park, Y. Miura *et al.,* "Relating brain structure images to personality characteristics using 3D convolution neural network," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 3, pp. 338–346, 2021.
[23] S. K. Jafarbigloo and H. Danyali, "Nuclear atypia grading in breast cancer histopathological images based on CNN feature extraction and LSTM classification," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 4, pp. 426–439, 2021.
[24] 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*, Cancun, Mexico, pp. 1–5, 2019.
[25] 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, no. 18, pp. 1–12, 2021.

[26] C. Szegedy, W. Liu, Y. Q. Jia, P. Sermanet and S. Reed, "Going deeper with convolutions," in *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, Boston, USA, pp. 1–9, 2015.
[27] M. Hénon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics*, vol. 50, no. 1, pp. 94–102, 1976.
[28] S. Kumar, P. Singh and M. Ranjan, "A review on deep learning based pneumonia detection systems," in *Proc. ICAIS*, Coimbatore, India, pp. 289–296, 2021.
[29] K. Ton, H. Jaap and O. Job, "Issues with digital watermarking and perceptual hashing," *Multimedia Systems and Applications IV*, vol. 4518, pp. 189–197, 2001.
[30] C. Zeng, J. Liu, J. B. Li, J. R. Cheng, J. J. Zhou *et al.,* "Multi-watermarking algorithm for medical image based on KAZE-DCT," *Journal of Ambient Intelligence and Humanized Computing*, vol. 32, no. 9, pp. 1–9, 2022.
[31] 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, no. 5, pp. 1–8, 2021.
[32] Y. Fan, J. B. Li, U. A. Bhatti, C. Y. Shao, C. Gong *et al.,* "A multi-watermarking algorithm for medical images using inception v3 and dct," *Computers, Materials & Continua*, vol. 74, no. 1, pp. 1279–1302, 2023.