Computers, Materials & Continua
DOI: 10.32604/cmc.2023.031445
Article

Tech Science Press

A Multi-Watermarking Algorithm for Medical Images Using Inception V3 and DCT

Yu Fan[1,6], Jingbing Li[1,2,*], Uzair Aslam Bhatti[1,2], Chunyan Shao[1], Cheng Gong[1], Jieren Cheng[3,5] and Yenwei Chen[4]

[1]School of Information and Communication Engineering, Hainan University, Haikou, 570100, China
[2]State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, 570100, China
[3]School of Computer Science and Technology, Hainan University, Haikou, 570100, China
[4]Graduate School of Information Science and Engineering, Ritsumeikan University, Kyoto, 5258577, Japan
[5]Hainan Blockchain Technology Engineering Research Center, Hainan University, Haikou, 570100, China
[6]TJ-YZ School of Network Science, Haikou University of Economics, Haikou, 571127, China
*Corresponding Author: Jingbing Li. Email: jingbingli2008@hotmail.com
Received: 18 April 2022; Accepted: 12 June 2022

Abstract: Medical images are a critical component of the diagnostic process for clinicians. Although the quality of medical photographs is essential to the accuracy of a physician's diagnosis, they must be encrypted due to the characteristics of digital storage and information leakage associated with medical images. Traditional watermark embedding algorithm embeds the watermark information into the medical image, which reduces the quality of the medical image and affects the physicians' judgment of patient diagnosis. In addition, watermarks in this method have weak robustness under high-intensity geometric attacks when the medical image is attacked and the watermarks are destroyed. This paper proposes a novel watermarking algorithm using the convolutional neural networks (CNN) Inception V3 and the discrete cosine transform (DCT) to address above mentioned problems. First, the medical image is input into the Inception V3 network, which has been structured by adjusting parameters, such as the size of the convolution kernels and the typical architecture of the convolution modules. Second, the coefficients extracted from the fully connected layer of the network are transformed by DCT to obtain the feature vector of the medical image. At last, the watermarks are encrypted using the logistic map system and hash function, and the keys are stored by a third party. The encrypted watermarks and the original image features are performed logical operations to realize the embedding of zero-watermark. In the experimental section, multiple watermarking schemes using three different types of watermarks were implemented to verify the effectiveness of the three proposed algorithms. Our NC values for all the images are more than 90% accurate which shows the robustness of the algorithm. Extensive experimental results demonstrate the robustness under both conventional and high-intensity geometric attacks of the proposed algorithm.

Keywords: Inception V3; multi-watermarking; DCT; watermark encryption; robustness

1 Introduction

The rise of technology has opened up a slew of new possibilities for digital content creation and distribution. Web publishing and digital repositories/libraries are only a few examples of the many uses of this technology. However, the most critical matter with these applications is protecting users' data. For digital data, current copyright laws are inadequate, according to experts. Consequently, the protection and enforcement of intellectual property rights for digital media have become a significant concern. As a result, researchers are working to devise new ways to keep copies from being produced. The use of digital watermarking techniques is one attempt that has gained significant attention. Stenciling and watermarking are two different techniques, but they both focus on the message's durability and its ability to withstand removal attacks, such as image manipulations like cropping and filtering. For several different reasons, including copy protection and control, digital watermarking involves embedding information (the "watermark") into digital multimedia content so that it may later be recovered or recognized. As digital content continues to increase at an ever-increasing rate, new watermarking techniques are being developed and commercialized to address some of these difficulties.

Medical images are playing an important role in the field of assisted medical diagnosis and telemedicine. Fast advanced network technology provides a good transmission channel for telemedicine and medical image information sharing, solving the problem of uneven distribution of medical resources, and improving the utilization rate of medical data. At the same time, medical image information sharing also faces problems such as illegal copying and tampering [1]. As an important basis for physicians to access patient information, the security and copyright protection of medical images is particularly important for the patient. Techniques used to protect the copyright of medical images are still required to explore for the security of data.

Digital watermarking technology [2], an effective way for traditional encryption techniques, enables the concealment of information and performs well on copyright protection for medical images [3]. Digital watermarking technology produces encrypted images by embedding watermarks with identification significance (such as author information, product serial number, trademark pattern, etc.) into the digital image without information value loss and usage effect of the digital image. Due to the good concealment, security and robustness, the watermark persists invariability even after various attacks, thereby determining the copyright confirmation of the digital image. As a basis for physicians' diagnosis, medical images are more rigorous and complete. To ensure the accuracy and objectivity of the physician's diagnosis, the copyright information of watermark embedded medical images should be clarified even under medical image attacking. The above-mentioned watermark embedding algorithms are not suitable for the digital watermarking scheme for medical images. Consequently, robust watermarking algorithms for medical images are required for security against different attacks.

The main digital watermarking algorithms can be classified into two types, spatial domain digital watermarking and transform domain digital watermarking. The spatial domain digital watermarking algorithm alters the image pixel directly by embedding the watermark information, which is simple and easy to implement with low robustness. The transform domain digital watermarking is a reversible mathematical transformation of the image before the watermark is embedded, and the watermark information is embedded in the transformed data and then inverted when the watermark is extracted. Compared to the spatial domain watermarking, watermark energy has an even distribution in the

transformed image, making the watermark information more concealed to improve the embedding strength of the watermark information greatly [4].

Cox et al. [5] proposed a spread-spectrum digital watermarking algorithm that first transforms the discrete cosine transform (DCT) of the carrier image and then embeds the watermark information into the low-frequency sub-band, improving the watermark's resistance to compression. Kang et al. [6] proposed a robust watermarking algorithm based on discrete wavelet transform (DWT) against geometric attacks; they introduce a distance measure between the distorted and undistorted images to determine the distortion before the image recovers by reversing the geometric distortion. The watermarking algorithm is resistant to geometric attacks such as rotation, scaling, translation, clipping, cropping, dithering attacks, and linear transformations. Cedillo-Hernandez et al. [7] proposed a robust watermarking algorithm for medical images based on the discrete Fourier transform (DFT), which embeds the watermark into the DFT domain of medical images ensuring the quality of medical images and improving the robustness of the watermark. The above algorithms realized the embedding and extraction of the watermark, but the extraction processes of image features were complex, and the algorithms were less resistant to high-intensity geometric attacks.

The core of digital watermarking technology is image feature extraction; however, the method of extracting data features manually is complicated. Therefore, we can automatically learn the potential attributes of data through deep learning (DL). In recent years, the research of deep learning has become a hot spot again, and its applications are all over the fields of computer vision, natural language processing, speech recognition, and so on. Based on the research on deep learning, Cheng et al. [8] proposed a lightweight multiscale information fusion network (MIFNet), which solved the two problems of accurate segmentation and efficient reasoning and improved the performance of semantic segmentation technology. Among the typical deep learning networks, deep learning models such as convolutional neural networks (CNN) [9], deep residual networks (DRN) [10], generative adversarial networks (GAN) [11], and U-Net [12] have achieved outstanding results in various fields. Adding attention mechanisms with deep learning approaches also increases the performance of classification and recognition [13]. Zhao et al. [14] used cross model attention mechanism for character recognition and show the performance of the machine learning method improves with the attention mechanism. Yuan et al. [15] applied a deep residual network (DRN) to fingerprint liveness detection (FLD) for the first time and proposed an FLD algorithm combining region of interest (ROI) extraction and DRN based on adaptive learning (ALDRN). The experimental results of the algorithm are better than the most advanced FLD method.

Convolutional neural networks (CNN) are a widely used neural network architecture. It is an effective algorithm for automatic learning and recognition of required features. It plays an important role in speech recognition, image detection, and image classification [16]. Leonid et al. [17] realized the classification of elephant sounds through CNN by concatenating parallel convolution layers and then extracting features from different feature sets. Lee [18] used CNN to simulate the structure of the human optic nerve and completed the classification and detection of small moths through automatic learning and recognition. Sudha et al. [19] trained deep CNN VGG-19, which extracted features from 20000 image training sets and extracted features from 5000 image test sets, and achieved automatic labeling and classification of diabetic retinopathy (DR) grades. The sensitivity and accuracy of the algorithm were 82% and 96%, respectively. Rajakumari et al. [20] extracted the features and realized the detection and classification of breast cancer by introducing the reconstructed image into the CNN GoogleNet model. Zhang et al. proposed a 3D watermarking algorithm based on wavelet-based transform with improved security [21] and used a similar approach for soft tissue processing [22].

As mentioned above, a deep learning network has obvious advantages in the automatic extraction and recognition of speech and image features. Therefore, in recent years, the research on digital watermarking technology is also closely combined with deep learning networks. Through the integration of the two technologies, the research in the field of digital watermarking technology has achieved creative results [23]. Jin et al. [24] proposed a digital watermarking algorithm based on CNN, which firstly divides the original image into 8×8 image blocks, and then uses CNN to learn the texture properties and luminance properties of the image and adaptively determine the embedding strength of the watermark, the algorithm balances the invisible rows and robustness of the watermark. Kandi et al. [25] proposed a novel learning-based auto-encoder CNN for image watermarking that outperforms traditional image watermarking techniques in terms of imperceptibility and robustness. Fierro-Radilla et al. [26] proposed a reinforcement learning model to ensure the robustness of watermarking. The learning process consists of three stages: watermark embedding, attack simulation and weight update, and experiments demonstrate that reinforcement learning is more competitive than supervised learning. Hayes et al. [27] applied adversarial neural networks to digital watermarking, and the network model can determine whether an image contains watermarked information. Baluja et al. [28] trained a neural network to hide a full-color image within another image of the same size, the watermarked image has a very good visual effect, and the algorithm can embed not only images of different sizes but also text and audio. Meng et al. [29] and Liu et al. [30] developed an irreversible watermarking scheme using wavelet transform and U-net based machine learning method. Fang et al. [31] proposed an information hiding technique based on adversarial generative networks to effectively secure data in data sharing. Uchida et al. [32] embedded watermarking information in the network model without affecting the performance of the network to ensure the intellectual property of the shared neural network model.

By considering the above studies, we can conclude that watermark algorithms performing directly on the original image cannot avoid affecting the image quality and the watermarks are unstable to geometric attacks. Aiming to address the intolerable problem of the watermark algorithm of medical images, this paper proposes an algorithm based on the combination of CNN Inception V3 and DCT to process the medical image and extract the image feature vectors. The algorithm combines logistic map and hash functions to scrambled encryption of watermarks. The "third party" concept to achieve zero embedding and blind extraction of multiple watermarks is also combined to improve the performance of medical image watermarking techniques.

The main contributions of this research are:

(1) A CNN-based image feature extraction method is proposed, extracting the fully connected layer data (predictions) of the Inception V3 network as processing data and extracting image features through the DCT transform. The algorithm achieves algorithmic innovation by combining deep learning theory with traditional image transformation theory.
(2) Three completely different images (text, graphics, and symbols) were chosen as digital watermarks to enable multiple watermarks embedding and to analyze the robustness of different types of digital watermarks.
(3) The watermark is encrypted using a chaotic system and the key is stored by a third party to improve the security of the watermark.
(4) The extraction of the watermark does not require the original image, enabling zero watermarking and blind extraction.

2 The Fundamental Theory

The theoretical basis of this paper is the combination of the CNN Inception V3 and the traditional transform DCT to achieve the embedding and extraction of digital watermarks of the medical image through watermark encryption techniques.

2.1 Convolutional Neural Networks Inception V3

The Inception V3 network is the most representative CNN in the Inception Net. Inception V1 (GoogLeNet) won the 2014 ILSVRC Challenge. Its parameters were 12 times smaller than the Alex Net network, and the Top5 error rate was reduced to 6.67%. Based on the advantages of fewer network parameters and high accuracy of Inception V1, Inception V3 continuously improves the network, which decomposes the symmetric convolution kernel into two layers of asymmetric convolution kernel in series. This change greatly accelerates the calculation speed, deepens the depth of the network, increases the nonlinearity of the network, reduces the probability of overfitting, and further improves the accuracy of network recognition. Compared with other classical CNN, Alex Net, VGG and Resnet, Inception V3 has fewer parameters and a deeper network, with a faster speed and lower recognition error rate, therefore, this paper selects Inception V3 as the experimental network.

Inception V3 is a pre-trained version of the network trained on more than a million images from the ImageNet database. The pre-trained network can classify images into 1000 object categories. As a result, the network has learned rich feature representations for a wide range of images.

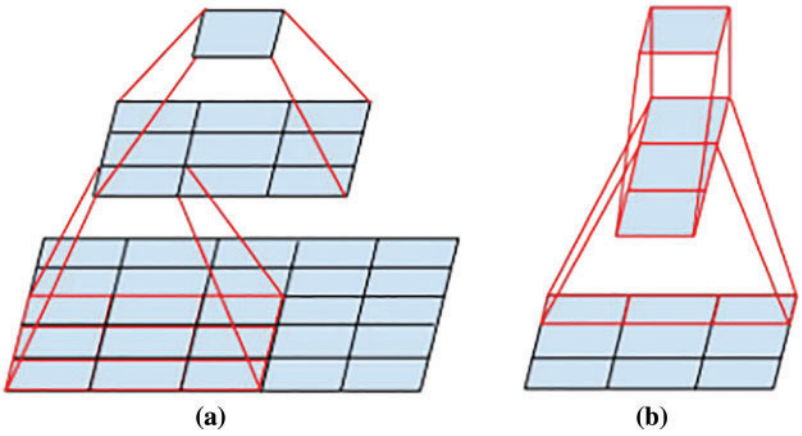

Figure 1: Operation of the convolution kernel. (a) Mini-network replacing the 5×5 convolutions. (b) Decomposing symmetric convolution into asymmetric convolution

The input to the Inception V3 network is an image of $299 \times 299 \times 3$. The network contains three different types of inception modules ($35 \times 35/17 \times 17/8 \times 8$) and two Grid Size Reduction modules. The inception Modules enable autonomous learning of data without manual processing. The Grid Size Reduction modules solve the problem of feature bottlenecks and computational overload and finally achieve image classification recognition by using the softmax function. The most important feature of the Inception V3 network is the splitting of a larger two-dimensional convolutional kernel into two smaller one-bit convolutional kernels, e.g., decomposing a 5×5 convolutional kernel into two 3×3 convolutional kernels (see Fig. 1a), this improves the performance of the network and increases the speed of computation while reducing the cost of computation. In addition, the network decomposes symmetric convolution kernels into asymmetric convolution kernels, such as

splitting the 3×3 convolutional kernels into 1×3 and 3×1 convolutional kernels (see Fig. 1b). The deconvolution kernel approach saves a large number of parameters, speeding up computation while reducing overfitting [33].

On the other hand, to solve the problem of feature representation bottlenecks and excessive computation, two Grid Size Reduction modules were added between each of the three Inception Modules to reduce the size of the feature map by using a parallel two-branch structure (convolution and pooling) (see Fig. 2).

The data used in the proposed algorithm is not the final output data of this network. Still, the fully connected layer data (predictions) is selected for processing, which achieves a high level of feature integration and the data is distinctly representative. Therefore, we choose the fully connected layer as the data source for feature extraction. The Inception V3 network structure is shown in Fig. 3.

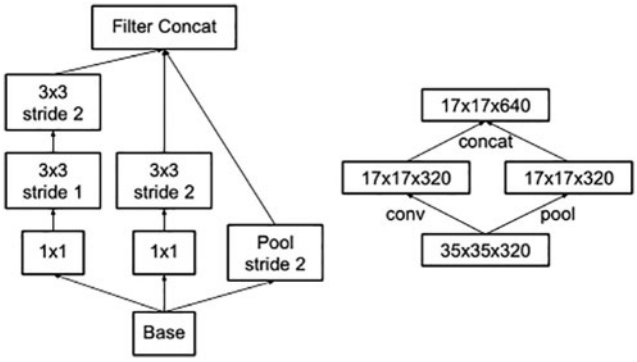

Figure 2: Grid size reduction modules

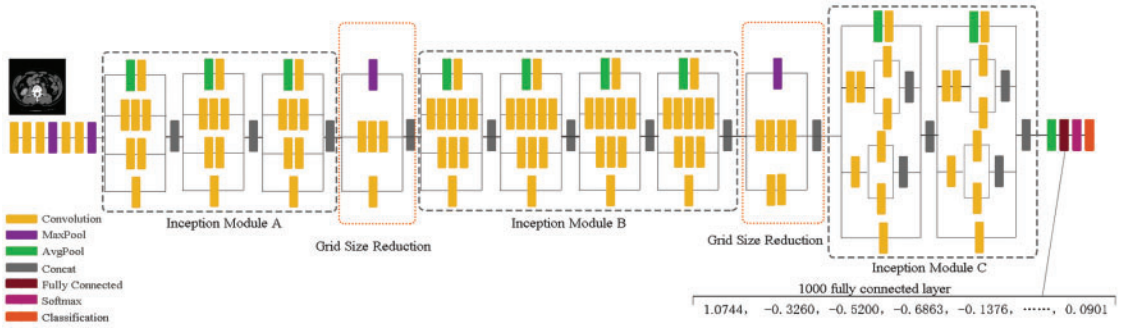

Figure 3: The Inception V3 network structure

2.2 Discrete Cosine Transform

To strengthen the algorithm's resilience to attacks, we execute another DCT transform on the data extracted from the CNN [34]. This concentrates the energy in the image signal, making it easier to retrieve image features. The discrete cosine transform is a separable transform with a cosine function as its transform kernel [35]. The DCT transform can concentrate the majority of the signal's energy in its low-frequency components. DCT can describe the correlation between human speech signals and image signals [36]. Therefore, the DCT was chosen to extract the feature vectors of medical images in this experiment.

For a sequence of length N, its 1D-DCT transformation is as in Eqs. (1) and (2).

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

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

2.3 Logistic Map

To improve the security of the watermark, this paper uses chaotic sequences to encrypt the watermark. The chaos is a seemingly irregular movement, referring to a random-like process that occurs in a deterministic system; with its initial values and parameters, it is possible to generate this chaotic system. The most famous type of chaotic system is Logistic Map.

It is a non-linear mapping given by Eq. (3).

$$X_{k+1} = \mu \cdot X_k \cdot (1 - X_k) \tag{3}$$

k is the number of iterations, $X_k \in (0, 1)$, The growth parameter$\mu \in (0, 4]$, when$3.5699456 < \mu \leq 4$, the logistic map gets a chaotic state and the chaotic sequence can be used as an ideal key sequence. Different studies used the logistic map for encryption of information, Szegedy et al. scrambled the row and column for each pixel in the input image using two 1-D discrete for watermark encryption, similarly [33]. Dai et al. also used logistic mapping for generating encrypted watermark sequences for improving the security of medical images [34]. Therefore, Logistic mapping is one of the key factors in securing the image with better security. In the chaotic encryption of the medical images and the watermark, the initial values of the chaos are set to 0.135 and 0.2, respectively.

3 The Proposed Watermarking Algorithm

This study proposed a watermarking algorithm based on a CNN Inception V3 combined with DCT, generating a key sequence using chaotic encryption during the watermarking process. We found that in most of the relevant literature on watermarks, whether single watermark or multi watermark, the content of watermark information used is mostly text type. To test the robustness of the algorithm based on Inception V3 and DCT from multiple angles and all aspects, we use multiple watermarking schemes where the watermark information includes three types of text, graphics and symbols to achieve zero watermarking and blind extraction in the following experiments.

The algorithm consists of five parts: Inception V3-based feature extraction, watermark encryption, watermark embedding, watermark extraction and watermark decryption. First, the original medical images are convolved and pooled using the Inception V3 network to obtain the fully connected layer data (predictions). Then, a global discrete cosine transform is applied to the fully connected layer data and the low-frequency data is selected from the matrix obtained by DCT as the visual feature vector of the medical image. Finally, a new feature sequence based on perceptual hashing was found in the DCT domain to participate in the watermark operation. In the design of the algorithm, watermark technology is combined with chaotic encryption, cryptography and the third-party concept, which not only allows the digital watermark to resist conventional and geometric attacks but also makes the algorithm robust. Meanwhile, the use of multiple watermarks also enhances the security of medical image transmissions, protecting the privacy of patients.

3.1 Medical Image Feature Extraction

The flowchart of the proposed algorithm is presented in Fig. 4; we start processing the images in two directions: the original medical image and the original watermarks. On the one hand, original medical image is first resized to 299×299 image $I(i,j)$ as the input of the Inception V3 network. After the initial medical image has been convolved and pooled by 3 Inception Modules and 2 Grid Size Reduction Modules, the fully connected layer (predictions) data $E(i)$ of the InceptionV3 convolutional network is selected. Finally, DCT transform was then performed on the fully connected layer data for a vector $V_m(i,j)$ conforming to human visual features, founded in the transformation domain. To process watermark images, first, a chaotic sequence $X(j)$ based on the initial value x_0 is generated, then binarizing the chaotic sequence to generate the binary encryption matrix $k(n)$, at last, the binary encryption matrix $k(n)$ is operated with the watermark $W(i,j)$ to obtain the encrypted watermark $BW(i,j)$. When watermarks need to be embedded, using the hash function on the encrypted watermark $BW(i,j)$ and the visual feature vector $V_m(i,j)$ of the image, meanwhile binary logic sequences $Key(i,j)$ are generated. These binary logic sequences $Key(i,j)$ can be stored in a third-party platform.

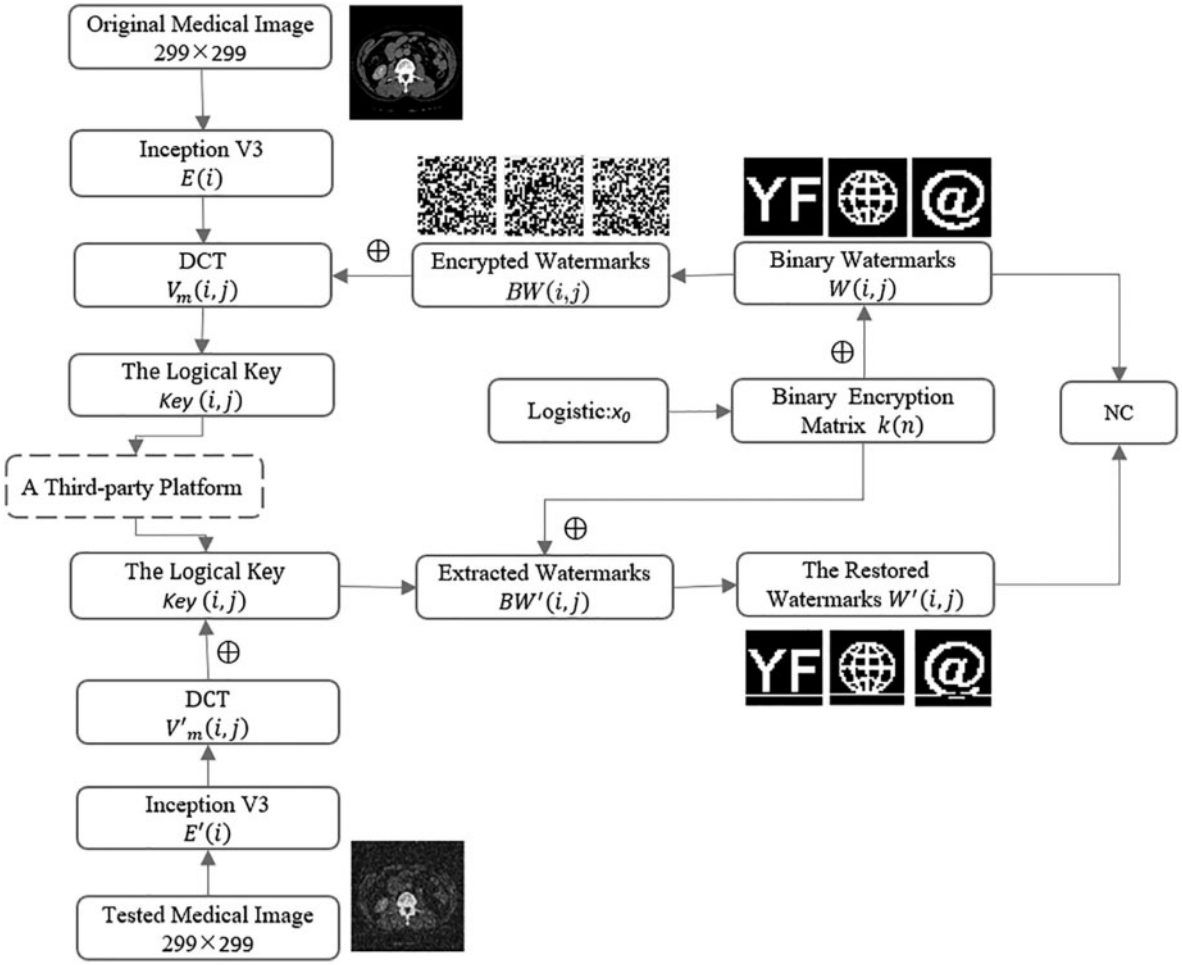

Figure 4: Flowchart of the proposed algorithm

When testing, the same method was performed. Extract the visual feature vector $V'_m(i,j)$ of the tested medical image, the binary logic sequences $Key(i,j)$ is obtained from the third party, and to obtain the extracted watermarks $BW'(i,j)$ by the feature vector $V'_m(i,j)$ and the $Key(i,j)$. The chaotic sequences $X(j)$ and the encryption matrixes $k(n)$ were generated using the same initial value x_0 as the above method. Then, the restored watermarks $W'(i,j)$ were obtained by hashing $k(n)$ and $BW'(i,j)$.

To verify whether the extracted features using the specified algorithm are valid, this experiment randomly selects a medical gray-scale image of 512×512 pixels which Inception V3 and DCT transform, and different types of attacks are carried out on the medical image (as shown in Fig. 5). In this paper, we selected 32 bits of low-frequency data and replaced data greater than or equal to 0 with 1, and the other data with 0. Tab. 1 lists the low-frequency coefficients of the medical image under different attacks. To exemplify this, we have selected the top 10 data ($O(1,1) \sim O(1,10)$) in Tab. 1. As can be seen from Tab. 1, after Inception V3 and DCT transformation, we find that the values change significantly, but their symbols remain largely unchanged; the sequences of all the attacked images are almost identical to the original images. Therefore, the experiment proves that the image features extracted by the proposed algorithm are effective.

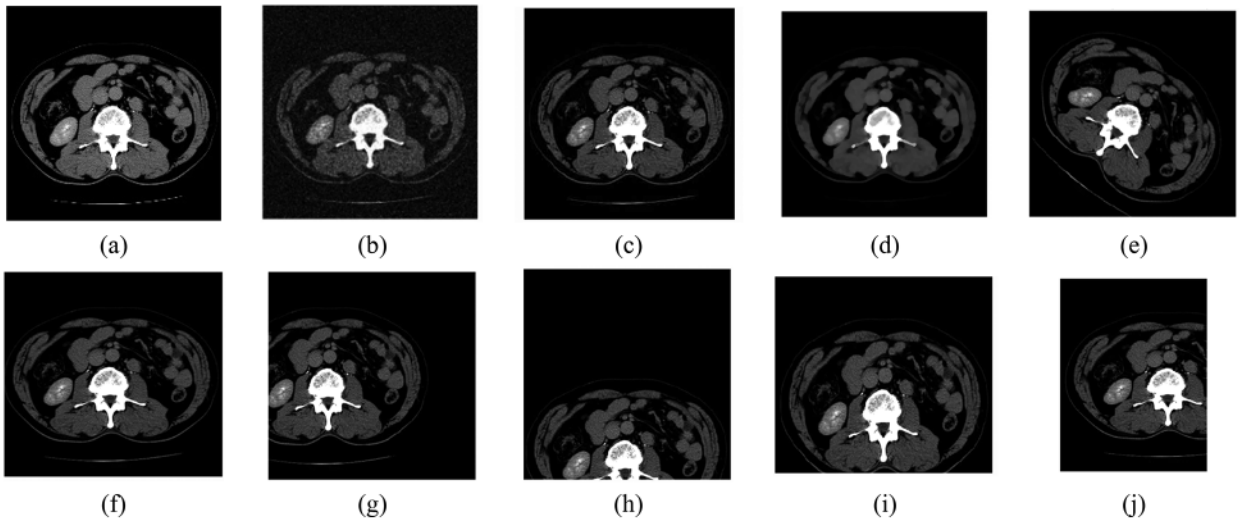

Figure 5: Different attacks on the abdomen. (a) Original image. (b) Gaussian noise (16%). (c) JPEG compression (21%). (d) Median filter [3 × 3] (15times). (e) Rotation (clockwise, 40°). (f) Scaling (×1.5). (g) Translation (28%, left). (h) Translation (35%, down). (i) Cropping (30%, Y direction). (j) Cropping (32%, X direction)

We randomly selected other medical images to test the same algorithm, as shown in Fig. 6, and verified the value of the normalized correlation coefficient, as show in Tab. 2, that the NC values of the different images obtained using the feature vector selected with the above method are all less than 0.5, and their NC values are 1.00. These results are consistent with human visual features. Therefore, we can use the low-frequency coefficients of medical images based on the CNN Inception V3 and the traditional DCT transform as their feature vectors.

Table 1: Changes of Inception V3 and DCT coefficients under different attacks for the medical images

Image processing	PSNR (dB)	O (1, 1)	O (1, 2)	O (1, 3)	O (1, 4)	O (1, 5)	O (1, 6)	O (1, 7)	O (1, 8)	O (1, 9)	O (1, 10)	Sequence of coefficient signs	NC
Original image	/	−1.23898	−7.91148	−3.74813	1.154251	0.646601	−1.94961	−2.77929	1.556383	0.144174	1.6805359	0001100111	1.0
Gaussian noise (2%)	19.12	−1.30063	−12.4179	−6.73767	3.145781	1.076835	−0.17014	−5.55097	1.967321	0.168225	2.6991644	0001100111	1.0
JPEG compression (35%)	33.96	−1.20436	−7.62404	−4.26336	1.544986	0.554832	−1.20787	−3.33877	1.988583	0.026068	2.5266697	0001100111	1.0
Median filter [3, 3] (35 times)	29.02	−1.27199	−9.55575	−4.00191	3.074254	2.001256	0.523326	−3.24354	1.686682	0.217292	1.2284669	0001110111	0.75
Rotation (clockwise, 40°)	15.03	−1.28436	−9.82873	−3.75639	1.758381	1.936239	−0.61681	−1.29868	0.81516	0.364847	0.8412921	40001100111	1.0
Scaling (×8.0)	/	−1.21921	−8.00264	−4.62872	1.753362	0.093074	−1.05737	−3.48623	2.065893	0.304405	2.0755959	0001100111	1.0
Translation (21%, left)	12.79	−1.26796	−6.52771	−4.61591	1.846608	0.737819	−0.63933	−2.97566	1.335132	0.130301	1.5306479	0001100111	1.0
Translation (35%, down)	11.87	−1.16118	−6.05354	−3.5574	2.754599	1.973892	1.545179	−1.08467	1.437165	0.203135	1.8267167	0001110111	0.83
Cropping (19%, Y direction)	/	−1.29197	−6.14289	−0.89311	1.059037	0.040989	−0.62871	−0.59192	1.486014	0.332596	0.3324622	50001100111	1.0
Cropping (32%, X direction)	/	−1.22588	−10.2754	−4.97074	3.529296	1.907433	−0.12879	−3.65184	2.703147	0.564717	2.5739105	0001100111	1.0

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

Image	Abdomen	Neck	Wrist	Coronary artery	Internal auditory canal	Lumbar spine	Foot	Shoulder
Abdomen	1.00	0.31	0.24	0.19	0.12	0.12	0.37	0.31
Neck	0.31	1.00	0.04	0.13	0.31	0.18	0.31	0.13
Wrist	0.24	0.04	1.00	0.32	−0.14	−0.01	0.24	0.19
Coronary artery	0.19	0.13	0.32	1.00	0.19	−0.06	0.31	0.13
Internal auditory canal	0.12	0.31	−0.14	0.19	1.00	0.12	0.25	0.31
Lumbar spine	0.12	0.18	−0.01	−0.06	0.12	1.00	0.37	0.31
Foot	0.37	0.31	0.24	0.31	0.25	0.37	1.00	0.44
Shoulder	0.31	0.13	0.19	0.13	0.31	0.31	0.44	1.00

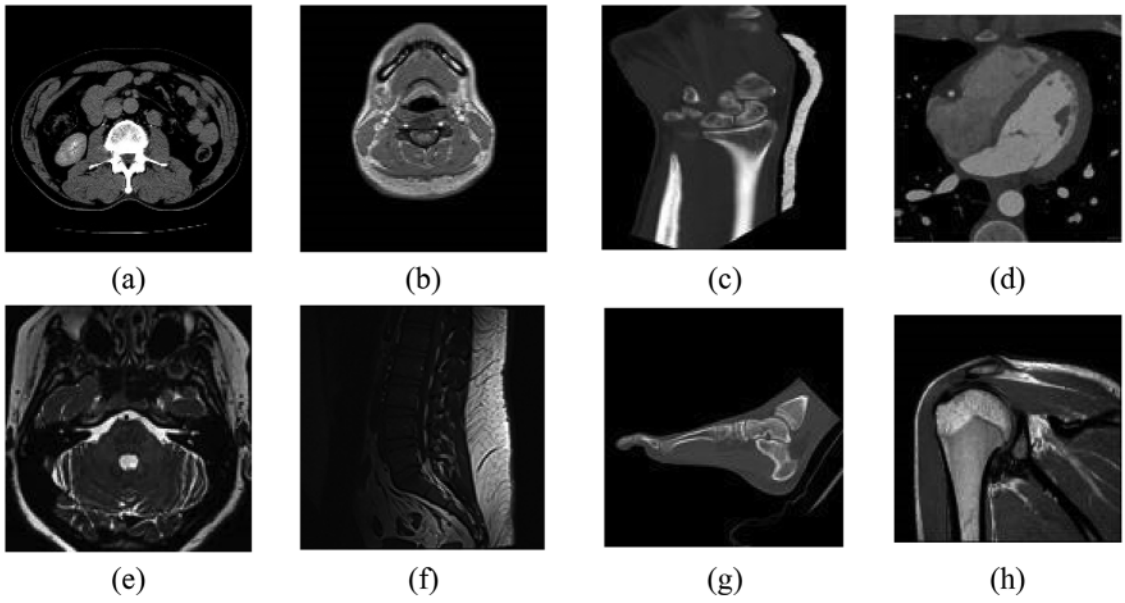

Figure 6: The tested images. (a) Abdomen. (b) Neck. (c) Wrist. (d) Coronary artery. (e) Internal auditory canal. (f) Lumbar spine. (g) Foot. (h) Shoulder

3.2 Watermarks Encryption

To ensure the security of the watermark, the watermark is scrambled and encrypted before it is embedded, as shown in Fig. 7.

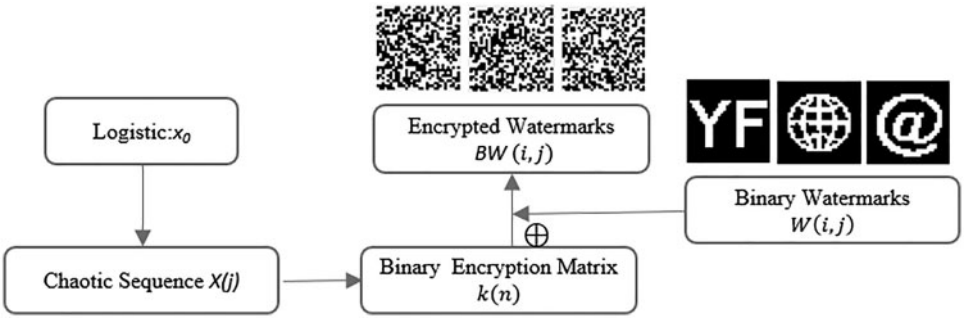

Figure 7: Watermarks encryption process

Step1: Generate a chaotic sequence $X(j)$ based on the initial value $x_0 = 2$, $\mu = 4$, Binarization of the chaotic sequence $X(j)$, When the value of $X(j)$ is greater than 0.5, it is "1", the rest is "0", and a binary encryption matrix $k(n)$ is generated.

Step2: The binary encryption matrix $k(n)$ and the binary watermark $W(i,j)$ are operated by the hash function, such as shown in Eq. (4), then we obtain the encrypted watermarks $BW(i,j)$.

$$BW(i,j) = W(i,j) \oplus k(n) \tag{4}$$

3.3 Watermarks Embedding

Step3: Using Eq. (5) to calculate the image feature matrix $V_m(i,j)$ and the encrypted watermark $BW(i,j)$, the watermark can be embedded into the medical image, and the logical key $Key(i,j)$ can be obtained at the same time.

$$Key(i,j) = BW(i,j) \oplus V_m(i,j) \tag{5}$$

Step4: Save the logical key $Key(i,j)$ to a third-party platform. When it is necessary to extract the watermark of the tested image, we can apply for logical key $Key(i,j)$ from the third-party platform.

Fig. 8 shows the watermark embedding process.

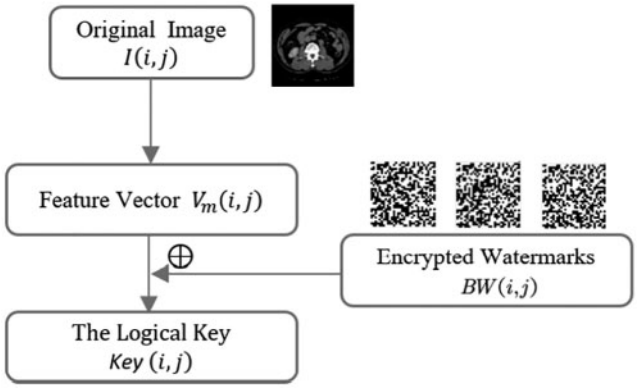

Figure 8: Watermarks embedding process

3.4 Watermarks Extraction

Step5: Extraction of features $V'_m(i,j)$ of the tested image using the same method as the extraction of components of the original medical image.

Step6: The encrypted watermark $BW'(i,j)$ is extracted by Eq. (6).

$$BW'(i,j) = V'_m(i,j) \oplus Key(i,j) \tag{6}$$

The algorithm only requires the $Key(i,j)$ when removing the watermark and does not need the participation of the original image. Therefore, it is a zero watermarking extraction algorithm.

Fig. 9 shows the extraction process of the watermark.

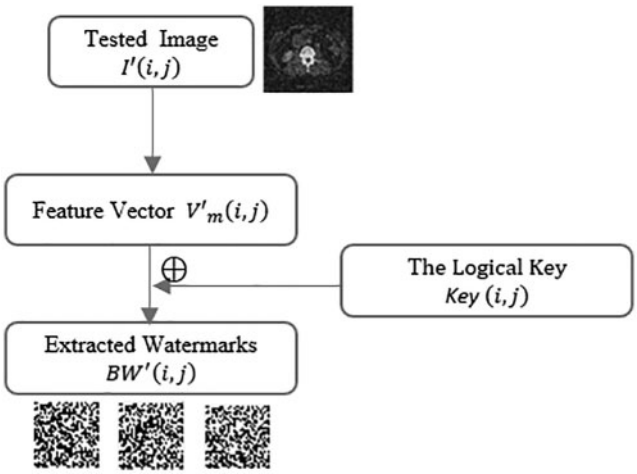

Figure 9: Watermarks extraction process

3.5 Watermarks Decryption

Step7: Using the same method as watermark encryption, the same binary encryption matrix $k(n)$ is obtained.

Step8: Inverse the scramble watermarking image using Eq. (7). The watermark decryption process is shown in Fig. 10.

$$W'(i,j) = BW'(i,j) \oplus k(n) \tag{7}$$

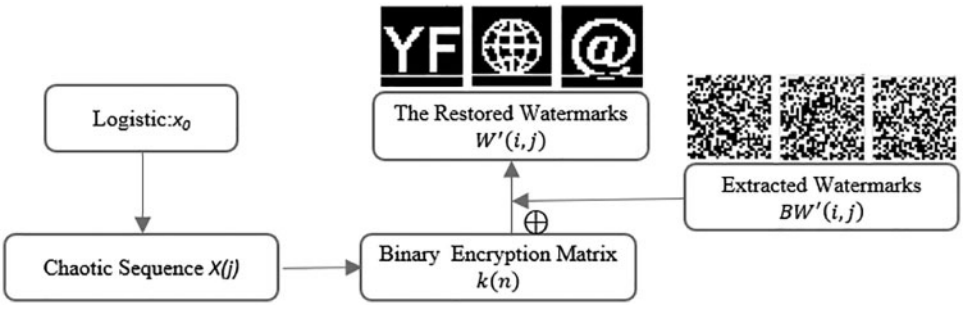

Figure 10: Watermarks decryption process

Determine the watermark information and clarify the medical image ownership by calculating the correlation coefficients NC between $W(i,j)$ and $W'(i,j)$.

4 Experimental Results

This experiment used Matlab 2019a as the test platform and selected an abdominal CT image as the study object. We choose three different types of images as watermarks (as shown in Fig. 11). Verify the robustness of the algorithm from multiple perspectives. Fig. 12 shows the encrypted watermarks effect. The encrypted watermarks change greatly and are completely unrecognizable to the naked eye, which improves the security of the watermark information.

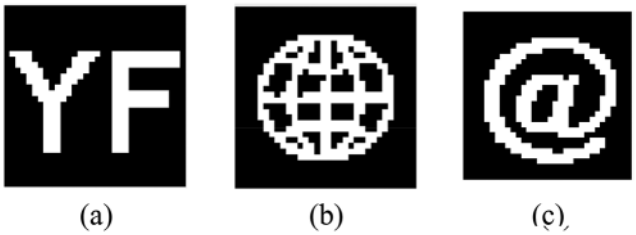

Figure 11: Binary watermark. (a) Binary watermark 1-text. (b) Binary watermark 2-graphic. (c) Binary watermark 3-symbol

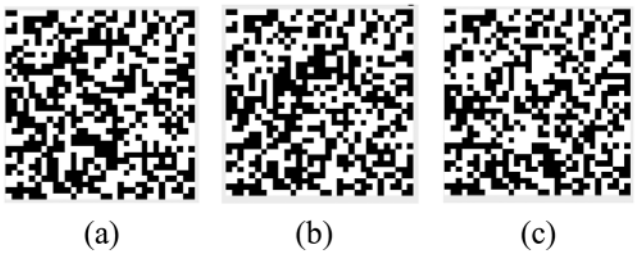

Figure 12: Encrypted watermark. (a) Encrypted watermark 1-text. (b) Encrypted watermark 2-graphic. (c) Encrypted watermark 3-symbol

4.1 Evaluation Criteria

Calculating the NC value between the watermark extracted from the tested image and the original watermark (NC value between 0 and 1), we evaluate the robustness of the algorithm using NC values [37]. The NC value is calculated as shown in Eq. (8). $W(i,j)$ represents the original watermark, and $W'(i,j)$ was the extracted watermark. $\overline{W(i,j)}$ was the mean of $W(i,j)$, $\overline{W'(i,j)}$ was the mean of $W'(i,j)$. The algorithm has the best robustness when the NC value is 1. The embedded watermark can still be extracted when the NC value is greater than 0.5, so we consider the algorithm to be robust when the NC value [38] is greater than 0.5.

$$NC = \frac{\sum_i \sum_j \left(W(i,j) - \overline{W(i,j)}\right)\left(W'(i,j) - \overline{W'(i,j)}\right)}{\sqrt{\left(\sum_i \sum_j \left(W(i,j) - \overline{W(i,j)}\right)^2\right)\left(\sum_i \sum_j \left(W'(i,j) - \overline{W'(i,j)}\right)^2\right)}} \tag{8}$$

The peak signal-to-noise ratio is the ratio of the maximum possible power of a representative signal and the destructive noise power that affects its representation accuracy. PSNR value indicates

the degree of distortion of the image, the larger the value, the smaller the image distortion [38]. The PSNR is calculated as shown in Eq. (9). $I(i,j)$ and $I'(i,j)$ are the pixel values of each point of the image I and I' respectively, MAX_I is the maximum possible pixel value of the image, if the pixel value of each point is represented by B-bit binary, then $MAX_I = 2^B - 1$. To facilitate the operation, the image is usually taken as a square, that is, $M = N$ [39].

$$PSNR = 10\lg\frac{MN \cdot MAX_I^2}{\sum_i \sum_j (I(i,j) - I'(i,j))^2} \tag{9}$$

Fig. 13 shows that the medical images were not changed when the medical images were not attacked; the NC value of the watermark information extracted from the original image is 1. The following conventional and geometric attacks are used to verify the robustness of the algorithm.

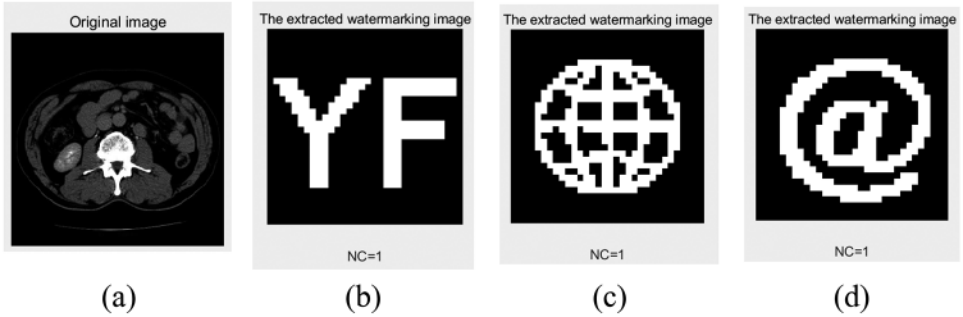

Figure 13: The extracted watermarks without attack. (a) Extracted watermark 1. (b) Extracted watermark 2. (c) Extracted watermark 3

4.2 Conventional Attacks

4.2.1 Gaussian Noise Attacks

As shown in Fig. 14 and Tab. 3, we added different levels of Gaussian noise to the watermarked images, and the NC values for the three extracted watermarks were 0.66, 0.66 and 0.72 when the Gaussian intensity was 20%, and from all data, the NC values for the two types of watermarks (text and graphic) were lower than the symbolic watermark. When the Gaussian noise intensity reaches 30%, the watermark information can still be extracted well.

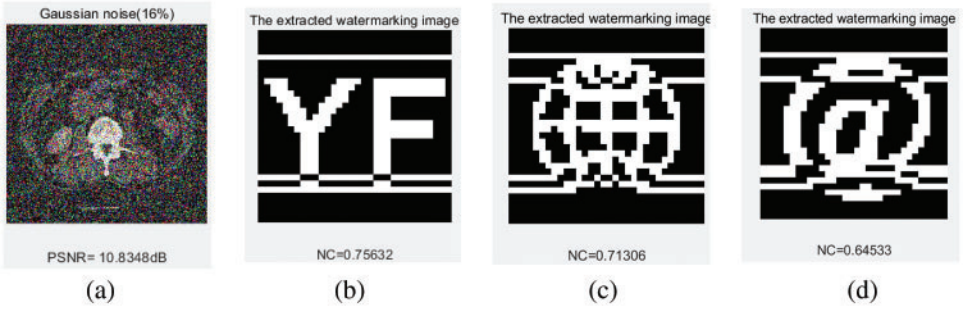

Figure 14: Under Gaussian noise attacks. (a) Gaussian noise level of 16%. (b) The extracted watermark 1 with a Gaussian noise level of 16%. (c) The extracted watermark 2 with a Gaussian noise level of 16%. (d) The extracted watermark 3 with a Gaussian noise level of 16%

Table 3: PSNR and NC values after Gaussian noise attacks

Gaussian noise (%)	2	4	8	16	20	30
PSNR (dB)	19.12	16.28	13.51	10.83	10.08	8.81
NC1	0.90	0.82	0.69	0.76	0.66	0.53
NC2	0.92	0.79	0.64	0.71	0.66	0.60
NC3	0.92	0.79	0.70	0.65	0.72	0.66

4.2.2 JPEG Attacks

JPEG compression, as an international standard, is widely used in images compression processing, and JPEG attacks are often used in the watermarking field. As shown in Fig. 15 and Tab. 4, the NC values of the three watermarks extracted are 0.72, 0.77 and 0.77 when the compression quality reaches 35%, with the graphic and symbol watermarks having better extraction quality than the text.

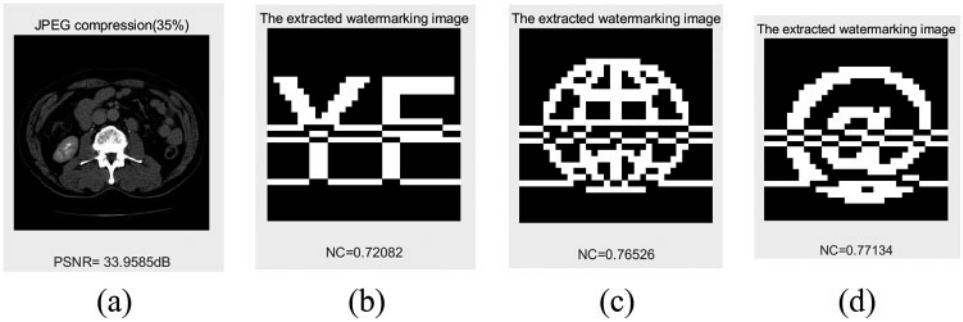

Figure 15: Under JPEG attacks. (a) Compression quality set to 30%. (b) The extracted watermark 1 under compression quality set to 30%. (c) The extracted watermark 2 under compression quality set to 30%. (d) The extracted watermark 3 under compression quality set to 30%

Table 4: PSNR and NC values after JPEG attacks

Compression quality (%)	1	7	14	21	28	35
PSNR (dB)	24.88	28.62	31.00	32.37	33.27	33.96
NC1	0.41	0.40	0.60	0.60	0.66	0.72
NC2	0.48	0.47	0.63	0.64	0.70	0.77
NC3	0.49	0.48	0.65	0.64	0.70	0.77

4.2.3 Median Filter Attacks

We applied the [3 × 3] and [5 × 5] median filtering attacks to the watermarked image, the NC values of the watermark information were greater than 0.66 when the median filtering parameter was [3 × 3] and the number of filtering repetitions was 35, and the data are shown in Fig. 16 and Tab. 5. The NC values of the three types of watermarked information-text, graphic and symbol-increase sequentially under the median filtering attack.

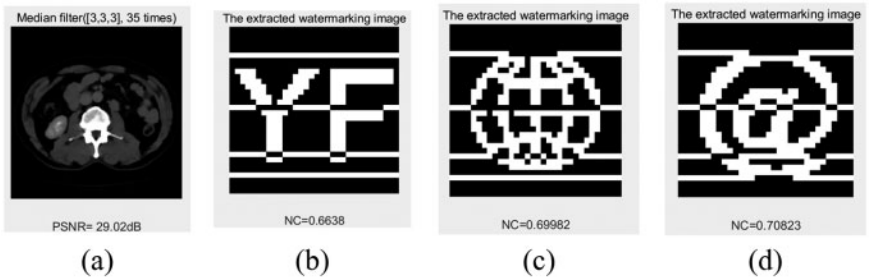

Figure 16: Under Median Filter attacks. (a) Median Filter [3 × 3] with 35 repetitions. (b) The extracted watermark 1 under median filter [3 × 3] with 35 repetitions. (c) The extracted watermark 2 under median filter [3 × 3] with 35 repetitions. (d) The extracted watermark 3 under median filter [3 × 3] with 35 repetitions

Table 5: PSNR and NC values after Median filter attacks

Median filter	[3 × 3]			[5 × 5]		
Repeat times	3	15	35	3	15	35
PSNR (dB)	31.26	29.55	29.02	26.67	24.32	23.47
NC1	0.63	0.60	0.66	0.51	0.54	0.54
NC2	0.66	0.63	0.70	0.54	0.58	0.63
NC3	0.64	0.64	0.71	0.52	0.60	0.64

4.3 Geometrical Attacks

4.3.1 Rotation Attacks

The images with watermark information are rotated in different directions and at different angles, and it can be found in Fig. 17 and Tab. 6 (Negative is counterclockwise, positive is clockwise) that the algorithm is more robust against rotation attacks. When the image is rotated 40° clockwise, the watermark NC values exceed 0.90, and when rotated 80° counterclockwise, the watermark NC values are approximately 0.70. The robustness of the three types of watermarks is generally consistent.

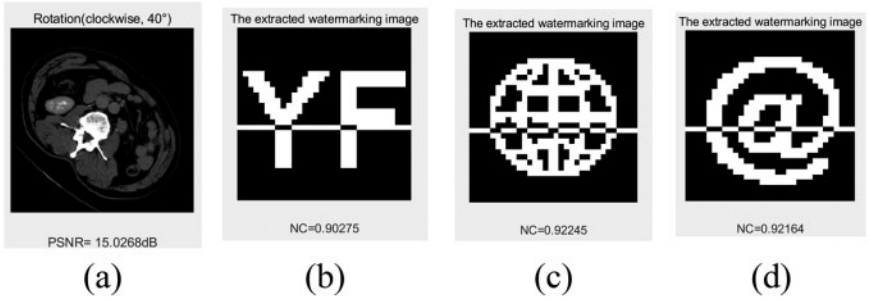

Figure 17: Under rotation attacks. (a) Rotation (clockwise) 40°. (b) The extracted watermark 1 under rotation (clockwise) 40°. (c) The extracted watermark 2 under rotation (clockwise) 40°. (d) The extracted watermark 3 under rotation (clockwise) 40°

Table 6: PSNR and NC values after rotation attacks

Rotation	−80°	−40°	−16°	−8°	8°	16°	40°	80°
PSNR (dB)	13.80	15.03	16.22	17.89	17.89	16.21	15.03	13.81
NC1	0.69	0.72	0.60	0.57	0.71	0.64	0.90	0.82
NC2	0.70	0.78	0.66	0.63	0.77	0.69	0.92	0.88
NC3	0.70	0.78	0.65	0.62	0.78	0.69	0.92	0.84

4.3.2 Scaling Attacks

The image was attacked using different scaling factors; when the scaling factor was as small as 0.5, the NC value of the extracted watermarks was 0.83 on average, and the watermarks could be identified. When the scaling factor reached 1.2, the NC values of the extracted watermarks were above 0.90. Fig. 18 and Tab. 7 show these data and part of the attack images.

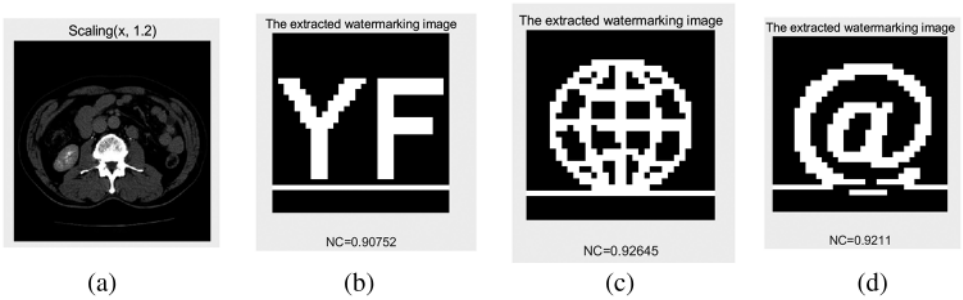

Figure 18: Under scaling attacks. (a) Scaling factor 1.2. (b) The extracted watermark 1 under scaling factor 1.2. (c) The extracted watermark 2 under scaling factor 1.2. (d) The extracted watermark 3 under scaling factor 1.2

Table 7: PSNR and NC values after scaling attacks

Scaling factor	0.5	0.8	1.2	2.4	4.0	8.0
NC1	0.81	0.81	0.91	0.81	0.81	0.81
NC2	0.84	0.87	0.93	0.87	0.87	0.87
NC3	0.85	0.84	0.92	0.84	0.84	0.84

4.3.3 Translation Attacks

Fig. 19 and Tab. 8 show the experimental data of the algorithm against translation attacks. The NC value of the watermarked image is greater than 0.91 when the image is shifted 21% horizontally to the left, the NC value is greater than 0.70 when the image is shifted 21% to the right or up, the robustness of graphic and symbol watermarks outperforms text watermark in all three directions of translation attack. The NC value of the watermarks are between 0.52 and 0.57 when the image is shifted vertically downwards by 21%. In addition, we found that when the image moves down 35%, the NC value of the watermark image is better than 14%, 21% and 28%. We speculate that the main

reason for this is that more invalid features in the image are removed. The watermark can be extracted accurately from the images after the above attacks, so the watermarking algorithm has strong resistance to translation attacks.

Table 8: PSNR and NC values after translation attacks

Distance (%)		7	14	21	28	35
Left	PSNR (dB)	14.80	13.38	12.79	12.49	12.41
	NC1	0.76	0.82	0.91	0.82	0.76
	NC2	0.79	0.85	0.93	0.85	0.79
	NC3	0.78	0.85	0.92	0.85	0.79
Right	PSNR (dB)	14.85	13.44	12.88	12.48	12.31
	NC1	0.66	0.57	0.70	0.72	0.63
	NC2	0.71	0.59	0.77	0.78	0.70
	NC3	0.69	0.57	0.77	0.77	0.70
Up	PSNR (dB)	14.99	13.30	12.28	11.68	11.35
	NC1	0.69	0.67	0.72	0.62	0.47
	NC2	0.72	0.71	0.76	0.66	0.50
	NC3	0.71	0.71	0.77	0.66	0.52
Down	PSNR (dB)	15.08	13.39	12.38	11.92	11.87
	NC1	0.83	0.68	0.52	0.49	0.77
	NC2	0.86	0.71	0.57	0.58	0.79
	NC3	0.85	0.69	0.55	0.56	0.78

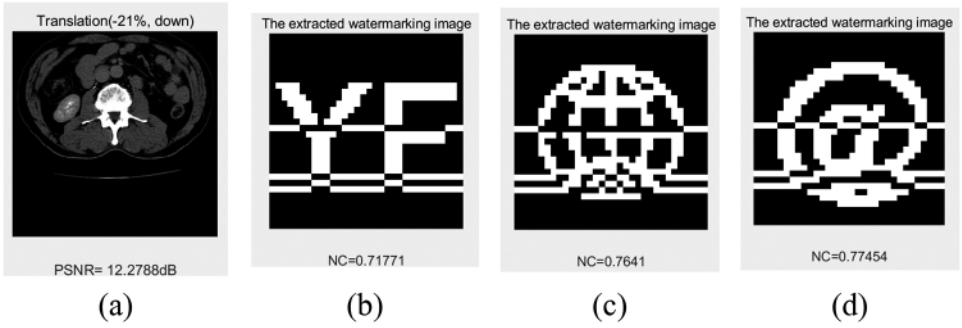

Figure 19: Under-up translation attacks. (a) up distance 21%. (b) The extracted watermark 1 under up distance 21%. (c) The extracted watermark 2 under up distance 21%. (d) The extracted watermark 3 under up distance of 21%

4.3.4 Cropping Attacks

To verify the cropping attack resistance of the algorithm, we design cropping attacks to the images from both horizontal and vertical directions, with cropping attack strength from 8% to 50%. When cropping 32% of the medical image along the X-axis, the NC values of the extracted watermarks are greater than 0.82 and the watermarks are very clear. When clipping 19% of the medical image along

the Y-axis, the NC values are between 0.75 and 0.78, at which point the graphic watermark NC value is higher than the other two types of watermarks. The data of cropping attacks is shown in Fig. 20 and Tab. 9.

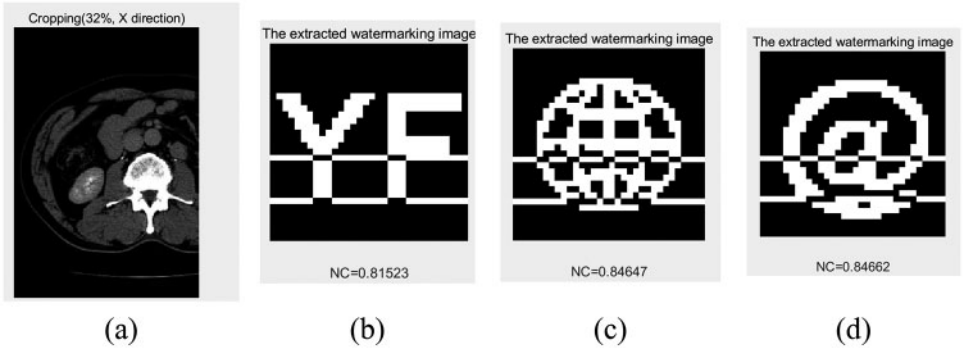

Figure 20: Under cropping attacks. (a) Cropping 32%, X direction. (b) The extracted watermark 1 under 32% cropping. (c) The extracted watermark 2 under 32% cropping. (d) The extracted watermark 3 under 32% cropping

Table 9: PSNR and NC values after cropping attacks

Cropping (%)		8	10	15	19	32	35
Y direction	NC1	0.81	0.80	0.74	0.75	0.59	0.63
	NC2	0.85	0.84	0.78	0.78	0.63	0.66
	NC3	0.84	0.84	0.77	0.77	0.63	0.64
Cropping (%)		5	8	10	19	25	32
X direction	NC1	0.69	0.82	0.76	0.65	0.67	0.82
	NC2	0.72	0.85	0.78	0.71	0.71	0.85
	NC3	0.71	0.84	0.77	0.70	0.70	0.85

4.4 Comparison with Other Algorithm

The proposed algorithm combines a CNN with DCT to design a set of medical image digital watermarking research schemes. To further, verify the advantages and disadvantages of the algorithm, this paper selects a traditional algorithm for comparison. Tab. 10 lists the comparison results of the proposed algorithm with SIFT-DCT [40]. It can be seen that the performance of the algorithm proposed in this paper is better than the SIFT-DCT algorithm in all high-intensity geometric attacks. In conventional attacks, the performance of the proposed algorithm is better than SIFT-DCT in Gaussian noise attack but weaker than SIFT-DCT in JPEG compression attack. Compared with the three different watermark types selected in the experiment, the robustness of graphic watermark is the best, the symbol watermark is the second, and the robustness of text watermark is the weakest. Experiments show that the algorithm based on a CNN and DCT has good performance.

Table 10: Comparison of the SIFT-DCT algorithm

Attacks	Parameter	SIFT-DCT	Proposed algorithm		
		NC	NC1 (text)	NC2 (graphic)	NC3 (symbol)
Gaussian noise	15%	0.60	0.60	**0.71**	**0.65**
JPEG compression	30%	0.90	0.68	0.71	0.71
Rotation (clockwise)	8°	0.51	**0.71**	**0.77**	**0.78**
	10°	0.60	**0.81**	**0.85**	**0.84**
Scaling	×1.5	0.79	**0.81**	**0.85**	**0.84**
	×3.0	0.65	**0.81**	**0.85**	**0.84**
Cropping (X-direction)	25%	0.72	0.67	0.71	0.70
	30%	0.66	**0.76**	**0.78**	**0.77**

In future we will use LSTM and graph based methods to improve the encryption and decryption process [41]. Hybrid approaches for securte watermarking are proved to be a better way to increase robustness and security against geometric attacks [42,43].

5 Conclusions

This article presents a multi-watermarking technique based on Inception V3 and DCT that combines deep learning and classical transforms. A CNN is firstly used to automatically extract the fully connected layer coefficients (predictions) of the medical image. Then, the DCT transform is applied to extract features. To protect the security of the watermarks, the watermarks are scrambled and encrypted using the logistic map system. This algorithm uses a hash function to implement a zero-watermarking technique by storing the key through a third platform, achieving blind extraction of the watermarks during watermarks extraction. To verify the feasibility of the algorithm and promote its generalization using, three different types of watermarks (text, image, symbol) were selected for this experiment. The experimental data shows that the algorithm is more robust to conventional attacks and performs better than traditional watermarking algorithms against geometric attacks. Therefore, the algorithm is important for the medical field, where image quality is very demanding.

Acknowledgement: This work was supported in part by Key Research Project of Hainan Province under Grant ZDYF2021SHFZ093, the Natural Science Foundation of China under Grants 62063004 and 62162022, the Hainan Provincial Natural Science Foundation of China under Grants 2019RC018, 521QN206 and 619QN249, the Major Scientific Project of Zhejiang Lab 2020ND8AD01, and the Scientific Research Foundation for Hainan University (No. KYQD(ZR)-21013).

Funding Statement: The authors received no specific funding for this study.

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

References

[1] J. Hu, H. H. Chen and T. W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Computer Standards & Interfaces*, vol. 32, no. 5–6, pp. 274–280, 2010.

[2] U. A. Bhatti, L. Yuan, Z. Yu, J. B. Li and K. Zhang, "Hybrid watermarking algorithm using clifford algebra with arnold scrambling and chaotic encryption," *IEEE Access*, vol. 8, pp. 76386–76398, 2020.

[3] C. K. Tan, J. C. Ng, X. Xu, C. L. Poh, Y. L. Guan *et al.,* "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, no. 3, pp. 528–540, 2011.

[4] M. J. Sahraee and S. Ghofrani, "A robust blind watermarking method using quantization of distance between wavelet coefficients," *Signal Image & Video Processing*, vol. 7, no. 4, pp. 799–807, 2013.

[5] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in *Proc. of 3rd IEEE Int. Conf. on Image Processing*, Lausanne, Switzerland, vol. 3, pp. 243–246, 2002.

[6] X. Kang, J. Huang and Y. Q. Shi, "An image watermarking algorithm robust to geometric distortion," in *Int. Workshop on Digital Watermarking*, Seoul, Korea, pp. 212–223, 2002.

[7] 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.

[8] J. Cheng, X. Peng, X. Tang, W. Tu and W. Xu, "MIFNet: A lightweight multiscale information fusion network," *International Journal of Intelligent Systems*, pp. 1–26 2021. https://doi.org/10.1002/int.22804.

[9] N. Loris, G. Stefano and B. Sheryl, "Ensemble of convolutional neural networks for bioimage classification," *Applied Computing & Informatics*, vol. 17, no. 1, pp. 19–35, 2018.

[10] X. Li, L. Ding, W. Li and C. Fang, "FPGA accelerates deep residual learning for image recognition," in *2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conf.*, Chengdu, China, pp. 837–840, 2017.

[11] J. Cheng, Y. Yang, X. Tang, N. Xiong, Y. Zhang *et al.,* "Generative adversarial networks: A literature review," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 12, pp. 4625–4647, 2020.

[12] O. Ronneberger, P. Fischer and T. Brox, "U-Net: Convolutional networks for biomedical image segmentation," in *Int. Conf. on Medical Image Computing and Computer-Assisted Intervention*, Istanbul, Turkey, pp. 234–241, 2015.

[13] S. Zhao, M. Hu, Z. Cai, Z. Zhang, T. Zhou *et al.,* "Enhancing Chinese character representation with lattice-aligned attention," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–10, 2021. https://doi.org/10.1109/TNNLS.2021.3114378.

[14] S. Zhao, M. Hu, Z. Cai and F. Liu. "Dynamic modeling cross-modal interactions in two-phase prediction for entity-relation extraction," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–10, 2021. https://doi.org/10.1109/TNNLS.2021.3104971.

[15] C. Yuan, Z. Xia, X. Sun and Q. J. Wu, "Deep residual network with adaptive learning framework for fingerprint liveness detection," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 12, no. 3, pp. 461–473, 2019.

[16] J. Cheng, J. Liu, X. Xu, D. Xia, L. Liu *et al.,* "A review of Chinese named entity recognition," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 6, pp. 2012–2030, 2021.

[17] T. T. Leonid and R. Jayaparvathy, "Classification of elephant sounds using parallel convolutional neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1415–1426, 2022.

[18] S. Lee, "A study on classification and detection of small moths using cnn model," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 1987–1998, 2022.

[19] V. Sudha and T. R. Ganeshbabu, "A convolutional neural network classifier vgg-19 architecture for lesion detection and grading in diabetic retinopathy based on deep learning," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 827–842, 2021.

[20] R. Rajakumari and L. Kalaivani, "Breast cancer detection and classification using deep cnn techniques," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1089–1107, 2022.

[21] X. Zhang, W. Zhang, W. Sun, X. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.
[22] X. R. Zhang, X. Sun, W. Sun, T. Xu and P. P. Wang, "Deformation expression of soft tissue based on BP neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1041–1053, 2022.
[23] B. Isac and V. Santhi, "A study on digital image and video watermarking schemes using neural networks," *International Journal of Computer Applications*, vol. 12, no. 9, pp. 1–6, 2011.
[24] C. Jin and S. Wang, "Applications of a neural network to estimate watermark embedding strength," in *Eighth Int. Workshop on Image Analysis for Multimedia Interactive Services*, Santorini, Greece, pp. 68–68, 2007.
[25] H. Kandi and D. Mishra, "Exploring the learning capabilities of convolutional neural networks for robust image watermarking," *Computers & Security*, vol. 65, pp. 247–268, 2017.
[26] 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 *7th Int. Workshop on Biometrics and Forensics (IWBF) IEEE*, Sassari, Italy, pp. 1–5, 2019.
[27] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," *Advances in Neural Information Processing Systems*, vol. 30, 2017.
[28] S. Baluja and Google, "Hiding images in plain sight: Deep steganography," *Advances in Neural Information Processing Systems*, vol. 30, pp. 2066–2076, 2017.
[29] L. Meng, L. Liu, G. Tian and X. Wang, "An adaptive reversible watermarking in IWT domain," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 711–735, 2021.
[30] L. Liu, L. Meng, Y. Peng and X. Wang, "A data hiding scheme based on U-Net and wavelet transform," *Knowledge-Based Systems*, vol. 223, pp. 107022, 2021.
[31] Y. Fang, J. Liu, J. Li, J. Cheng, J. Hu *et al.,* "Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT,". *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 16863–16879, 2022.
[32] Y. Uchida, Y. Nagai, S. Sakazawa and S. Satoh, "Embedding watermarks into deep neural networks," in *Proc. of the 2017 ACM on Int. Conf. on Multimedia Retrieval*, Guangzhou, China, pp. 269–277, 2017.
[33] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, Las Vegas, USA, pp. 2818–2826, 2016.
[34] Q. Dai, J. Li, U. A. Bhatti, J. Cheng and X. Bai, "An automatic identification algorithm for encrypted anti-counterfeiting tag based on DWT-DCT and Chen's Chaos," in *Int. Conf. on Artificial Intelligence and Security*, New York, USA, pp. 596–608, 2019.
[35] C. Zeng, J. Liu, J. Li, J. Cheng, J. Zhou *et al.,* "Multi-watermarking algorithm for medical image based on KAZE-DCT," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–9, 2022.
[36] K. A. Al-Afandy, O. S. Faragallah, E. S. M. El-Rabaie, F. E. Abd El-Samie and A. Elmhalawy, "A hybrid scheme for robust color image watermarking using DSWT in DCT domain," in *2016 4th IEEE Int. Colloquium on Information Science and Technology (CiSt)*, Tangier, Morocco, pp. 444–449, 2016.
[37] Z. Zeeshan, U. A. Bhatti, W. H. Memon, S. N. Ali, S. A. Nizamani *et al.,* "Feature-based multi-criteria recommendation system using a weighted approach with ranking correlation," *Intelligent Data Analysis*, vol. 25, no. 4, pp. 1013–1029, 2021.
[38] K. A. Al-Afandy, O. S. Faragallah, E. S. M. EL-Rabaie, F. E. Abd El-Samie and A. ELmhalawy, "Efficient color image watermarking using homomorphic based SVD in DWT domain," in *2016 Fourth Int. Japan-Egypt Conf. on Electronics, Communications and Computers (JEC-ECC)*, Cairo, Egypt, pp. 43–47, 2016.
[39] T. Li, J. Li, J. Liu, M. 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. 1, pp. 1–11, 2022.
[40] J. Liu, J. Li, Y. Chen, X. Zou and U. A. Bhatti, "A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain," *Computers. Materials & Continua*, vol. 61, no. 1, pp. 363–378, 2019.

[41] X. Wu, J. Li, U. A. Bhatti and Y. W. Chen, "Logistic map and contourlet-based robust zero watermark for medical images," *Innovation in Medicine and Healthcare Systems, and Multimedia*, vol. 145, pp. 115–123, 2019.

[42] C. Gong, J. Li, U. A. Bhatti, M. Gong, J. Ma *et al.,* "Robust and secure zero-watermarking algorithm for medical images based on Harris-SURF-DCT and Chaotic Map," *Security and Communication Networks*, vol. 2021, 2021. https://doi.org/10.1155/2021/3084153.

[43] U. A. Bhatti, Z. Yu, J. Chanussot, Z. Zeeshan, L. Yuan *et al.,* "Local similarity-based spatial-spectral fusion hyperspectral image classification with deep CNN and gabor filtering," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 60, pp. 1–15, 2021.