# A holographic image robust watermarking algorithm based on DWT-SIFT and neural network model

IOP Conf. Series: Materials Science and Engineering **563** (2019) 052088 doi:10.1088/1757-899X/563/5/052088

# A holographic image robust watermarking algorithm based on DWT-SIFT and neural network model

**J P Pang[1], A L Wang[2], X F Zhu, L Guo, S K Li, K Xin, S X Fan and F P Liu**

[1] Beijing Institute of Graphic Communication, China
[2] Corresponding author A L Wang, 1206517881@qq.com

**Abstract.** In order to improve the robustness of holographic watermarking, we propose a watermarking algorithm combining wavelet transform (DWT) and scale-invariant feature transform (SIFT). And neural network model is applied to digital watermarking technology. Firstly, the watermark image is transformed by Fresnel diffraction to generate hologram, which is divided into 16×16 blocks. And wavelet transform is carried out on each block to obtain the low-frequency information. Then, the feature points of the carrier image are extracted by SIFT, and the 16×16 blocks around the feature points are selected as the embedding areas to realize the embedding of the watermark.Finally, the random coordinates are taken as the input data of the neural network model, and the embedded position coordinates are taken as the output data of the neural network model. The relationship model between coordinates is constructed to achieve the confidentiality of the embedded position. Experimental results show that the watermarking algorithm has good robustness and visibility under the premise of ensuring image quality.

## 1. Introduction

As an effective method to protect image, text and video copyright in network environment, digital watermarking is a very important research direction at home and abroad. Robust watermarking algorithm includes spatial domain and transform domain, according to the difference of watermark embedding domain. At present, the commonly used transforms mainly include discrete cosine transform, discrete wavelet transform, discrete Fourier transform and singular value decomposition, etc[1]. Therefore, how to use different transformations to select the appropriate watermark embedding region is the core problem of watermark algorithm research.

When we select the embedding region, we need to select the region with geometric invariant property. That is, the region can maintain a relatively stable state under conventional processing attack or geometric attack, so as to ensure the strong robustness of watermark. Image features often represent the most essential features of the image, so the embedded region based on image features will not change significantly against geometric attacks[2].

In recent years, information optical holography technology has been introduced into the field of information hiding and digital watermarking and has shown great potential. This is because the optical holographic method can provide us with a variety of encrypted degrees of freedom such as phase, amplitude, diffraction distance, wavelength. And this method has many advantages such as high design freedom, high robustness, difficulty in tearing, natural parallelism, and difficulty in cracking[3]. Therefore, digital holography has a great application prospect in the field of information hiding and digital watermarking.

In this paper, neural network is applied to digital watermarking, and a watermarking algorithm combining DWT and SIFT is proposed.

## 2. Basic theories

### *2.1. Wavelet transform*

DWT is a multiple resolution analysis method for time-scale (time-frequency) signals. For 2-D image signals, the method of filtering in horizontal and vertical directions respectively can be used to realize 2-D wavelet multiple resolution decomposition. After each level of decomposition, it will be decomposed into four sub-graphs, namely, the middle-high frequency detail sub-graph and the low-frequency approximation sub-graph in horizontal, vertical and diagonal directions[4]. The watermark embedded in the texture and edge of the image is not easy to be detected. Therefore, some wavelet coefficients at high frequencies can be modified to embed the watermark information.

### *2.2. Scale-invariant feature transform*

The algorithm of SIFT is an algorithm based on the scale space theory to extract the local features of images. The generation of SIFT feature descriptor is divided into the following four steps[5-6] :

(1)detection of extreme value points in scale space. First, the Difference of Gaussian (DOG) function was built to judge the extreme value of the scale space:

$$D(x,y,\sigma)=(G(x,y,k\sigma)-G(x,y,\sigma))*I(x,y)=L(x,y,k\sigma)-L(x,y,\sigma) \quad (1)$$

Among them, $G(x,y,\sigma)=1/(2\pi\sigma^2)e^{-(x2+y2)/2\sigma2}$, $I(x,y)$ represents the original image, $L(x,y,\sigma)$ represents the scale of the image space, $k$ represents the coefficient of scale change.

And then, compare the value of a pixel $(x, y)$ in $D(x,y,\sigma)$ with the value of 8 adjacent points in the same scale and 9×2 adjacent points in each neighboring scale of the same layer of the image pyramid, and detect all poles as candidate points of key points.

(2)After the initial feature points are determined, the feature points are screened to eliminate the points of low contrast and unstable edge response. The size of the principal curvature is calculated by using the 2-by-2 Hessian matrix H to filter:

$$H=\begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \quad (2)$$

If the extreme point satisfies the following formula, the extreme point is retained, otherwise the point will be excluded.

$$\frac{Tr(H)^2}{Det(H)}<\frac{\alpha+\beta}{\alpha\beta} \quad (3)$$

Among them, $\alpha$ is the eigenvalue when H takes the maximum modulus, $\beta$ is the eigenvalue when H takes the minimum modulus, $Tr(H)$ is the sum of eigenvalues, $Det(H)$ is the value of the h determinant.

(3)Direction matching. The key idea of SIFT feature descriptor to obtain rotation invariant is to count the gradient direction distribution characteristics of the neighborhood of key points, take the gradient direction with the largest energy as its main direction, and introduce the concept of auxiliary direction to enhance the robustness of the algorithm.

(4)Description of feature points. Firstly, the scale and direction are calculated in the 16×16 neighborhood of the feature point, and the 16×16 neighborhood is divided into 4×4 sub-blocks. In this way, there are 16 blocks in the neighborhood of each feature point and each center point of 4×4 blocks has eight directions, so 128 directions can be obtained as the direction vector of 1×128 feature points. Finally, the length of feature vectors is normalized.

### *2.3. Neural network*

The basic principle of BP network model to process information is: the input signal acts on the output node through the intermediate node (hidden layer point), and then generates the output signal through non-linear transformation. Each sample of the network training includes an input vector *X* and a desired output *t*, a deviation between the network output value *Y* and the expected output value *t*, by adjusting the connection strength values of the input node and the hidden layer node, and the hidden layer node and the output node, The strength of the connection and the threshold value cause the error to fall in the direction of the gradient. After repeated training, with the minimum error of the corresponding network parameters (weights and threshold), the training is to stop. At this time, the trained neural network can process the non-linear transformation information with the smallest output error for the input information of similar samples[7].

## 3. Watermark Embedding and Extraction

### *3.1. Watermark embedding*

The specific steps of watermark embedding are as follows:

(1)Select the watermark image to generate a hologram by Fresnel diffraction transform, then perform 16*16 partitioning, and perform first-order wavelet decomposition to obtain low-frequency coefficient *CA1*;

(2)Select the carrier image, extract the feature points with SIFT, and filter the feature points: select the feature points with the scale between 2-8 (more stability), and the distance between the feature points is less than 22*sqrt (2) to prevent the embedding areas from overlapping. Select the high-frequency coefficients of the first-order wavelet decomposition around the feature points that meet the conditions as the embedded region. Embed according to the following embedding formula, and save the position coordinates (*x, y*) of the feature points;

$$cD1=CD1+CA1*0.02 \tag{4}$$

(3)Carry out inverse wavelet transform to obtain an carrier image with watermark;

(4)In order to ensure the confidentiality and security of the embedded position coordinates, the random coordinates are used as the input data of the neural network model, and the position coordinates are embedded as the output data of the neural network model. BP neural network model is used to train the relationship model between the random coordinates and the embedded position coordinates.

The watermark embedding process is shown in the following figure:

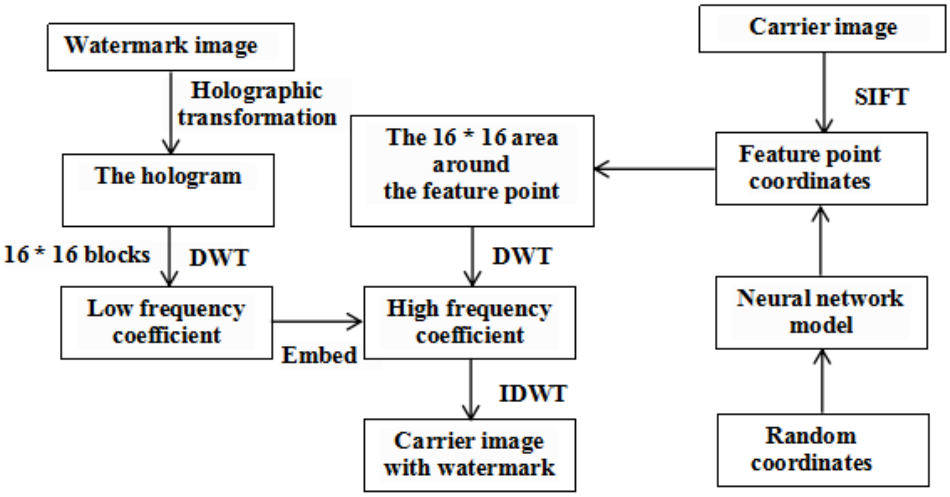


Figure 1. Watermark embedding process

### *3.2. Watermark extraction*

The specific steps of watermark extraction are as follows:

(1)Take the random coordinates as the input data of the trained neural network model, and obtain the coordinates of the corresponding embedded position;

(2)Then select the 16×16 neighborhood around the coordinate of the carrier image to perform wavelet transform to obtain the high frequency coefficient *CD1*. At the same time, select the 16×16 neighborhood around the coordinates of the carrier image embedded with watermark to perform wavelet transform to obtain high frequency coefficient *cD1*;

(3)Extract the embedded low frequency coefficients according to the following extraction formula, carry out inverse wavelet transform to obtain block hologram, and combine these blocks to obtain a complete hologram;

$$CA1=(cD1-CD1)/0.02 \tag{5}$$

(4)The hologram is inversely transformed to obtain watermark information.

The process of watermark extraction is shown as follows:

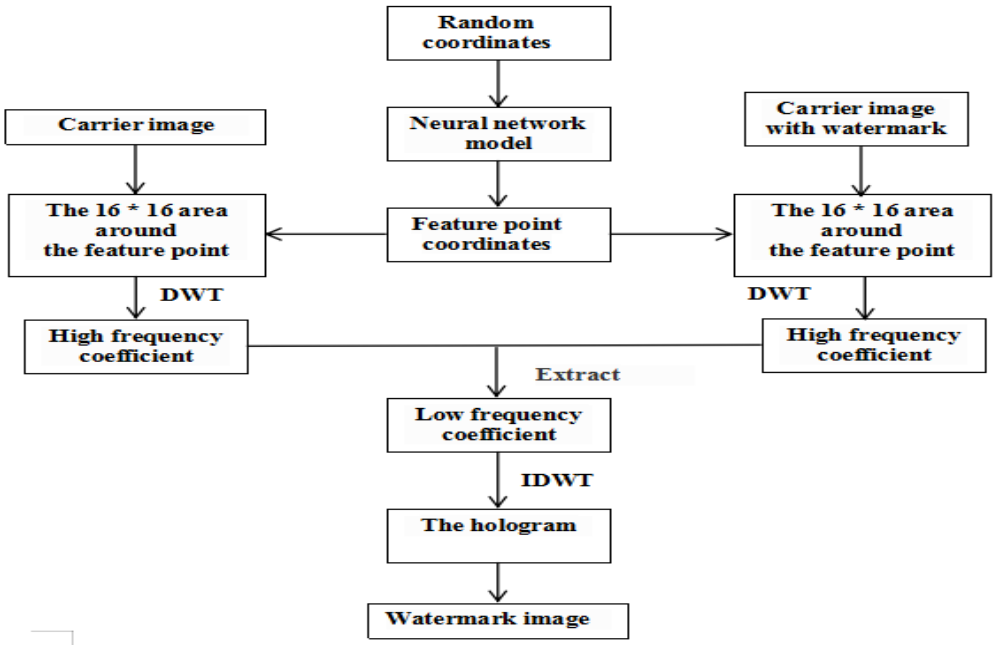


Figure 2. Watermark extraction process

## 4. Algorithm Implementation and Analysis

### *4.1. Watermark embedding and extraction examples*

(1)The original watermark image of 256×256 (Figure. 3) is selected to generate a hologram by Fresnel diffraction transform (Figure. 4). The feature points of the extracted carrier image (Figure. 5) are shown in Figure. 6. Then The hologram is embedded in the carrier image according to the designed embedding method to obtain a carrier image with watermark (Figure. 7). Then, the feature point coordinates are used as the output data of the neural network model, and the random coordinates are used as the input data of the neural network model to train the relational model.

Figure 3. Watermark image

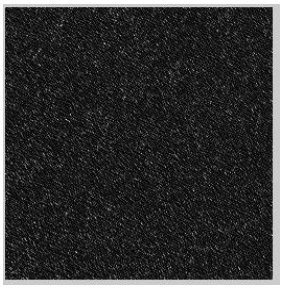

Figure 4. The hologram

Figure 5. Carrier image

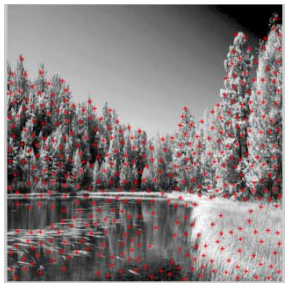

Figure 6. Carrier image feature point

Figure 7. Carrier image with watermark

The PSNR of the embedded image that shown in the experimental results reaches 63.7379, which guarantees the quality of the carrier image.

(2)Take the random coordinates as the input data of the neural network relation model, obtain the coordinates of the correct embedding position, extract the hologram (Figure. 8) according to the designed extraction method, and then recover the watermark image (Figure. 9).

Figure 8. The extracted hologram

Figure 9. The recovered watermark image

From the results, we can know that the NC value of the extracted watermark image is 0.9904, which is almost indistinguishable from the original watermark image.

4.2. *Robust detection of carrier image with watermark*

(1)Tailoring test

The carrier image with watermark is cropped 1/2 and 3/4, and then the hologram is extracted to restore the watermark image.

Figure 10. Cropped 1/2 image

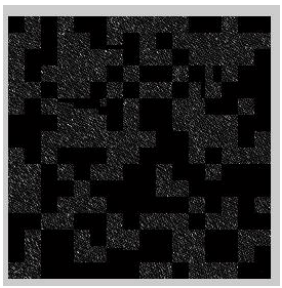

Figure 11. Extracted hologram

Figure 12. Recovered watermark image

Figure 13. Cropped the 3/4 image

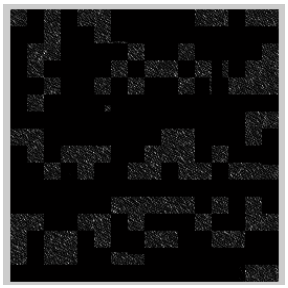

Figure 14. Extracted the hologram

Figure 15. The recovered watermark image

According to the NC value of the experimental results, the NC value of the watermark image recovered after cutting 1/2 was 0.8697. The NC value of watermark image after cutting 3/4 is 0.7431. The larger the proportion of image cutting is, the less clea r the reconstructed watermark image will be. However, the watermark image can still be recovered after cutting 3/4, indicating that the watermark image has a strong anti-cutting ability.

(2)Noise test

The salt-and-pepper noise with a variance of 0.01 is added to the carrier image with watermark (Figure. 16) , and then the hologram (Figure. 17) is extracted to recover the watermark image (Figure. 18).

Figure 16. The image of salt and pepper noise

Figure 17. The extracted hologram

Figure 18. The recovered watermark image

## 5. Conclusion

Aiming at the robustness of watermark, this paper mainly proposes the method of the combination of wavelet transform and SIFT to select the embedding region of watermark. In order to ensure the accuracy of the extracted watermark , the embedded position coordinates need to be preserved, which increases the possibility of being attacked. So this article combined with the neural network model, the embedding position coordinates as model output data, and the random coordinates as model input data. This training relationship model ensures the security of coordinates. At the same time, the attack test of the carrier image with watermark is carried out. PSNR and NC values obtained from the experimental results show that the watermark has good invisibility and robustness.

## Acknowledgment

The authors thank all the Editor and the anonymous referees for their constructive comments and valuable suggestions, which are helpful to improve the quality of this paper. This paper is supported by the BIGC Project(Ec201803, Ea201806, Ed201802), Beijing Higher Education Improvement Program(PXM2017_014223_000063).

**References**

[1] Zhang X Q, Hu Z, Tang T G and Zhang J L 2018 Digital image watermarking technology research *Computer programming skills and maintenance* pp 135-137
[2] Wang Q L 2009 Research on digital watermarking technology based on image features(Northwest Normal University)
[3] Liang J 2013 Image encryption based on phase recovery algorithm (Nangjing Normal University)
[4] Pu Y K and Cong S 2009 An improved image compression method based on wavelet transform and its application *Tech review* pp 28-32
[5] Feng L P 2013 *Digital copyright protection technology and its application* (Beijing: Publishing House of Electronics Industry) pp 318-322
[6] Li Y Y, Zhang Y F, Cheng X and Sun Y B 2019 Robust watermarking algorithm based on DWT optimal multiple subgraph and SIFT geometric correction Computer application research
[7] Yuan B Q, Cheng G and Zhen L G 2018 Basic principles of BP neural network *Digital communication world* pp 28-29