Remote Sensing Image Zero Watermarking Algorithm Based on DFT

Liang Jing1,*, Zhentao Sun2, Kexin Chen3, Xue Wen4, Xinyi Cheng5

1School of Computer Science and Technology, TianGong University, Tianjin, 300387, China
2School of Electrical and Electronic Engineering, TianGong University, Tianjin, 300387, China
3School of Mathematics and Science, TianGong University, Tianjin, 300387, China
4School of Computer Science and Technology, TianGong University, Tianjin, 300387, China
5School of Mathematics and Science, TianGong University, Tianjin, 300387, China

*Corresponding author: liangjing@tjpu.edu.cn

Abstract. This paper proposes a remote sensing image zero-watermark algorithm based on DFT, which can be used to protect the rights and interests of digital image copyright owners. First, the high frequency part after DCT transformation is binarized to obtain the characteristic image. Second, block DFT processing the host image. The high frequency part after DFT and the characteristic image are XORed to complete the watermark embedding. In order to test the performance of the watermark, an attack was carried out on the image embedded with the watermark. In order to extract the watermark from the attacked image, the high-frequency part of the data extracted from the attacked image is XORed again with the result of the first XOR. Compare the extracted watermark with the embedded watermark, and calculate its NC value. Most of the NC values are close to 1, indicating that the algorithm is robust. In addition, the PSNR values of the attacked image and the original image are also calculated. The experimental results show that the watermark obtained by the algorithm in this paper has strong invisibility and robustness.

Keywords: Discrete Fourier Transform, Remote Sensing Image, Zero Watermark.

1. Introduction and Motivation

With the increasing of image applications, images are illegally stolen, and unauthorized use is more and more frequent. In order to protect the rights and interests of image copyright owners, digital watermarking technology, which belongs to the field of information hiding, has emerged. Digital watermarking technology requires that watermark should have the characteristics of security, invisibility and robustness. Invisibility is mainly to ensure that the original image does not affect the normal use after embedding watermark, and it is not easy to be found by others and destroyed maliciously. The main purpose of robustness is to ensure that the watermark will not be damaged in a large area in the process of transmission and normal use, or after malicious attacks.
The early digital watermarking technology directly modifies the pixel value of the image. Although this algorithm is simple, the ability of watermark to resist attacks is weak, and the performance of watermark is poor. After that, the digital watermarking technology in transform domain is proposed. Several common transformation methods include Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), etc. The image is transformed from the time domain to the frequency domain by the transform method. The pixel value is modified in the frequency domain, and then the watermark is embedded by the inverse transform. This algorithm enhances the performance of the watermark, but still modifies the image information. Zero in zero watermarking means that the original image is not modified. The zero-watermark technology constructs the watermark by extracting the features of the original image, which has good invisibility and robustness.

Remote sensing image is mainly obtained by means of aerial photography, which is related to people's livelihood and other important fields. It is of great significance to protect the security of remote sensing images. On the other hand, considering the particularity of remote sensing image, we should avoid modifying the original image information when embedding watermark. In this work, zero watermark technology is used to protect the copyright information of remote sensing image.

2. Related Works
Early research on digital watermarking is basically embedding the watermark in the time domain [1-2]. As the problem of information security becomes more and more serious, the research on digital watermarking is getting deeper and deeper. The digital watermarking algorithm in the transform domain gradually appeared. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and other transformation methods have certain advantages, so they are widely used. In order to achieve higher requirements on the invisibility and robustness of the watermark, a watermark algorithm combining two or more transformation methods is proposed. Ali M [7] et al. combined SVD with lossless and symmetrical DCT, Feng LP et al. [8] combined DWT and DCT and proposed a blind watermarking algorithm. Singh D et al. [9] combined DCT, DWT and SVD, and the experimental results showed that the algorithm is more robust and invisible.

Zero watermark was proposed relatively late, but due to its unique performance, zero watermark has been widely used in many studies. Combining zero-watermarking with transformation methods and cellular automata, many high-performance watermarking algorithms have been obtained. Shakeri M and Jamzad M et al. [10] first performed wavelet transformation on the normalized image, and then used cellular automata to filter the low-frequency sub-images. Rawat S and Raman B et al. [11] combined Fourier transform and encryption technology to propose a better zero-watermark algorithm. It can be seen that the application of the zero-watermark algorithm is very flexible. This paper proposes a zero-watermark algorithm with high robustness and invisibility based on DFT.

3. Analysis of Travel Strength in Cities
3.1. Discrete Fourier Transform (DFT)
DFT is one of the commonly used transformation methods to transform image signals from time domain to transform domain. DFT transforms the gray distribution function of the image into the frequency distribution function of the image, and the frequency of the image is an index that characterizes the severity of the gray change in the image. Due to the nature of the Fourier function, DFT has separability, periodicity, symmetry and translation invariance. The formula for two-dimensional DFT is:

\[
F(u, v) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)e^{-2\pi j \left(\frac{ux}{M} + \frac{vy}{N}\right)}
\]
Among them, \( M \times N \) is the size of the host image, and \( f(x, y) \) is the pixel value at the point \((x, y)\).

The inverse transformation of the two-dimensional DFT is to transform the frequency distribution function of the image into the gray distribution function, that is, to transform the image from the frequency domain to the spatial domain. The corresponding formula is:

\[
f(u, v) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v)e^{2\pi i \left( \frac{ux}{M} + \frac{vy}{N} \right)}
\]

3.2. Indicators for measuring watermark performance

In order to judge the performance of the watermark, the indicators Peak signal-to-noise Ratio (PSNR) and Normalized correlation (NC) to measure the performance of the watermark are introduced. The PSNR value reflects the degree of distortion of the image. The calculation formula is:

\[
PSNR = 10 \times \log_{10} \left( \frac{255^2}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I'(i, j) - I(i, j))^2} \right)
\]

The NC value can reflect the similarity between two images, and its calculation formula is:

\[
NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} I'(i, j) \ast I(i, j)}{\sum_{i=1}^{m} \sum_{j=1}^{n} I^2(i, j)}
\]

4. Algorithm flow

4.1. Feature image extraction

The zero watermark is mainly constructed by extracting the characteristic information of the host image. Choosing Discrete Cosine Transform (DCT) can make most of the information of the original host image concentrate on a few transform coefficients. Therefore, in this work, DCT is used to extract feature images. After selecting the high frequency part of the DCT, binarize it to get the corresponding watermark image. In this paper, 100 remote sensing images are selected as experimental objects. Here, the images of No. 067 and No. 069 are taken as examples to show the corresponding characteristic images.
4.2. **Embedding of watermark**

After the feature image is obtained, the feature image needs to be embedded in the host image. Take the 64*64 high-frequency part of the upper left corner of the image after DFT processing for embedding. Here shows the high-frequency part of the image after the DFT of the 067 and 069 images.

![High Frequency Part Image after DFT](image)

**Figure. 2** High Frequency Part Image after DFT

The watermark embedding result is obtained by XORing the high frequency part information with the characteristic image, and the corresponding expression is:

$$xor_{ij} = feature_{ij} \oplus h_{ij}$$

The results of the first exclusive OR of images 067 and 069 are:

![Result of Embedding Watermark](image)

**Figure. 3** Result of Embedding Watermark
4.3. Watermark Extraction

Attack the image embedded with the watermark. The attack types selected in this article mainly include image enhancement processing and image scaling. The attacked image is processed into 8x8 blocks, and the 64x64 high-frequency data in the upper left corner is extracted. In order to extract the watermark from the attacked image, this part of the high-frequency data is XORed again with the result of the first XOR. The formula for extracting the watermark is:

\[ x_{ij} = x_{ij} \oplus h_{ij} \]

Among them, \( x_{ij} \) is the result of the first XOR, and \( h_{ij} \) is the high-frequency data extracted from the attacked image.

4.4. Summary

The algorithm flow of DFT based remote sensing image zero watermarking algorithm is as follows:

- Step 1: The original image is processed by 8 × 8 block DFT, and the high frequency data part of 64 × 64 on the upper left is extracted.
- Step 2: XOR the high frequency data with the binary watermark to get the first XOR result \( F_1 \).
- Step 3: Attack the original image.
- Step 4: The attacked image is divided into 8 × 8 blocks, and the high frequency data of 64 × 64 in the upper left corner is extracted.
- Step 5: XOR this part of high frequency data with \( F_1 \) to get the second XOR result \( F_2 \), which is the extracted watermark.

5. Experimental Result

5.1. Some experimental results

In order to measure the anti-attack performance of the watermark, the watermark extracted from the attacked image is compared with the embedded watermark. In this work, we use the embedded watermark and the NC value of the extracted watermark to test the performance of the watermark.

Take the original pictures No. 067 and 069 as examples to show the results of its NC value:
| Attack name                  | 67 | 69  |
|-----------------------------|----|-----|
| Gaussian filter [2, 2]      | 0.858 | 0.9146 |
| Gaussian filter [3, 3]      | 0.8389 | 0.9241 |
| Gaussian filter [5, 5]      | 0.8198 | 0.9125 |
| Gaussian filter [7, 7]      | 0.8193 | 0.909 |
| Gaussian filter [9, 9]      | 0.8196 | 0.9084 |
| median filtering [2, 2]     | 0.8618 | 0.9226 |
| median filtering [3, 3]     | 0.8326 | 0.9228 |
| median filtering [5, 5]     | 0.8093 | 0.8704 |
| median filtering [7, 7]     | 0.7823 | 0.8599 |
| median filtering [9, 9]     | 0.7695 | 0.8419 |
| Wiener filtering [2, 2]     | 0.905 | 0.9218 |
| Wiener filtering [3, 3]     | 0.9055 | 0.9104 |
| Wiener filtering [5, 5]     | 0.8966 | 0.8642 |
| Wiener filtering [7, 7]     | 0.9007 | 0.8571 |
| Wiener filtering [9, 9]     | 0.8966 | 0.8433 |
| Average filter [2, 2]       | 0.858 | 0.9146 |
| Average filter [3, 3]       | 0.8101 | 0.902 |
| Average filter [5, 5]       | 0.7593 | 0.865 |
| Average filter [7, 7]       | 0.7688 | 0.834 |
| Average filter [9, 9]       | 0.7484 | 0.8316 |
| sharpen amount 2            | 0.9656 | 0.9491 |
| sharpen amount 3            | 0.976 | 0.9492 |
| sharpen amount 5            | 0.9853 | 0.9662 |
| sharpen amount 7            | 0.9905 | 0.9743 |
| sharpen amount 9            | 0.9951 | 0.9735 |
| histogram equalization 128 bit | 0.9047 | 0.9506 |
| histogram equalization 64 bit | 0.9025 | 0.9231 |
| histogram equalization 32 bit | 0.9033 | 0.8855 |
| histogram equalization 16 bit | 0.9014 | 0.8579 |
| histogram equalization 8 bit | 0.8768 | 0.8361 |
| Gamma transform attack 3    | 0.9919 | 0.9885 |
| Gamma transform attack 2    | 0.9787 | 0.9883 |
| Gamma transform attack 0.75 | 0.9698 | 0.9868 |
| Gamma transform attack 0.5  | 0.9335 | 0.9783 |
| Gamma transform attack 0.25 | 0.9084 | 0.9713 |
| salt-and-pepper noise 0.01  | 0.7774 | 0.8921 |
| salt-and-pepper noise 0.03  | 0.7834 | 0.7298 |
| salt-and-pepper noise 0.05  | 0.639 | 0.6961 |
| salt-and-pepper noise 0.1   | 0.6432 | 0.6699 |
| salt-and-pepper noise 0.12  | 0.6336 | 0.6723 |
| Speckle noise 0.001         | 0.9696 | 0.8376 |
| Speckle noise 0.005         | 0.9171 | 0.7732 |
| Speckle noise 0.007         | 0.9041 | 0.7673 |
| Speckle noise 0.009         | 0.8844 | 0.7647 |
| Speckle noise 0.011         | 0.8771 | 0.7489 |
It can be seen from the data in the above table that most of the NC values are above 0.9, and some of the NC values are close to 1, indicating that the watermark is basically not damaged after being attacked. Therefore, in the process of continuous image dissemination, the watermark generated by this algorithm can be used as a sign of copyright information. The watermark has high anti-attack performance, and the information contained in the watermark will not be affected after basic attacks.

5.2. Algorithm robustness test

In order to test the robustness of the watermark, the PSNR value of the attacked image and the original image is calculated. Taking images 067 and 069 as examples, the results are shown as follows:

| Attack name             | PSNR Value of Image 067 | PSNR Value of Image 069 |
|------------------------|--------------------------|-------------------------|
| Gaussian noise attack 0.005 | 0.7079                  | 0.678                   |
| Gaussian noise attack 0.01  | 0.6652                  | 0.6805                  |
| Gaussian noise attack 0.015 | 0.6681                  | 0.6751                  |
| Gaussian noise attack 0.02  | 0.6671                  | 0.6738                  |
| Gaussian noise attack 0.025 | 0.6498                  | 0.6641                  |
| image scaling 2 times    | 0.9436                  | 0.9703                  |
| image scaling 4 times    | 0.9466                  | 0.9708                  |
| image scaling 5 times    | 0.9473                  | 0.9708                  |
| image scaling 8 times    | 0.9468                  | 0.9708                  |
| image scaling 10 times   | 0.9468                 | 0.9708                  |

Table 2 PSNR Value of Image 067 and 069
| Noise Type                      | PSNR Value 1 | PSNR Value 2 |
|-------------------------------|--------------|--------------|
| Salt-and-pepper noise 0.01    | 25.0479      | 25.0537      |
| Salt-and-pepper noise 0.03    | 20.1186      | 20.163       |
| Salt-and-pepper noise 0.05    | 17.9065      | 17.9327      |
| Salt-and-pepper noise 0.1     | 14.878       | 14.9961      |
| Salt-and-pepper noise 0.12    | 14.1563      | 14.1608      |
| Speckle noise 0.001           | 40.274       | 38.2449      |
| Speckle noise 0.005           | 33.3233      | 31.3506      |
| Speckle noise 0.007           | 31.8772      | 29.9263      |
| Speckle noise 0.009           | 30.7873      | 28.8234      |
| Speckle noise 0.011           | 29.959       | 27.9633      |
| Gaussian noise attack 0.005   | 23.0758      | 23.1726      |
| Gaussian noise attack 0.01    | 20.1964      | 20.2807      |
| Gaussian noise attack 0.015   | 18.5651      | 18.6529      |
| Gaussian noise attack 0.02    | 17.4807      | 17.5151      |
| Gaussian noise attack 0.025   | 16.6357      | 16.6449      |
| Image scaling 2 times         | 37.1475      | 36.1354      |
| Image scaling 4 times         | 37.3678      | 36.3591      |
| Image scaling 5 times         | 37.3838      | 36.3757      |
| Image scaling 8 times         | 37.3782      | 36.3699      |
| Image scaling 10 times        | 37.3786      | 36.3703      |

It can be seen that the PSNR values under most attacks are within the ideal range of 20-30, so the watermark is more robust. Since histogram equalization and Gamma transformation conflict with PSNR in principle, the PSNR value under histogram equalization and Gamma transformation is not shown here.

6. Conclusions and Prospects

6.1. Conclusions

Based on DFT, this paper proposes a zero-watermarking algorithm for remote sensing image. Firstly, the feature image of the host image is extracted by DCT. Secondly, the host image is embedded into the feature image after DFT. Attack the image embedded watermark to verify the performance of the watermark. The experimental results show that the watermark obtained by the algorithm can well resist the basic attacks, and has strong robustness and invisibility.

Acknowledgements

In this article, only common attack types are tested, and no test results are given for combined attacks.

References

[1] Bruyndoncky O, Quisquater JJ, Marq B, Spatial method for copyright labeling of digital images [C]. In: Proc. IEEE Workshop on Nonlinear Signal Processing. Lausanne, 1995, 456-459.
[2] Bender W, Gruhl D, Morimoto N, Techniques for data hiding. Proceedings of the SPIE on Storage and Retrieval for Image and Video Databases III, 1995, (2420):164-173.
[3] Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. AEU-Int J Electron C 68(3): 244–253
[4] Hsu CT, Wu JL (1999) Hidden digital watermarks in images. IEEE Trans Image Process 8(1): 58–68.
[5] Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2012) Robust
digital image watermarking using interest points and DFT domain. In: 35th IEEE
international conference on telecommunications and signal processing (TSP), pp 715–719

[6] Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise
masking. IEEE Trans Image Process 10(5):783–791

[7] Ali M, Ahn CW, Pant M (2014) A robust image watermarking technique using SVD and
differential evolution in DCT domain. Optik-International Journal for Light and Electron
Optics 125(1): 428–434

[8] Feng LP, Zheng LB, Cao P (2010) A DWT-DCT based blind watermarking algorithm for
copyright protection. In: Third IEEE international conference on computer science and
information technology (ICCSIT), vol 7, pp 455–458

[9] Singh D, Singh SK (2017) DWT-SVD and DCT based robust and blind watermarking scheme
for copyright protection. Multimed Tools Appl 76(11): 13001–13024

[10] Shakeri M and Jamzad M, A Robust Zero-Watermark Copyright Protection Scheme Based on
DWT and Image Normalization [C]// International Conference on Advances in Image and
Video Technology,2012: 359-370.

[11] Rawat S and Raman B. A blind watermarking algorithm based on fractional Fourier transform
and visual cryptography [J].Signal Processing,2012,92(6): 1480-1491.