A Zero-Watermark Hybrid Algorithm for Remote Sensing Images Based on DCT and DFT

SiMing Xing$^{1,*}$, TongYi Li$^{2}$, Jing Liang$^{2}$

$^1$School of Mathematics and Science, TianGong University, Tianjin, China
$^2$School of Computer Science and Technology, TianGong University, Tianjin, China

*Corresponding author: Siming.Xing@tjpu.edu.cn

Abstract. Remote sensing image has significant advantages such as large detection range and fast acquisition speed, so it has been used in military, environmental, meteorological and other fields. In order to improve the robustness of the digital watermarking technology on the premise that the remote sensing image information is not modified, a remote sensing image zero watermarking algorithm based on Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) is proposed in this paper. First of all, the color remote sensing image is converted into grayscale image. The transformed coefficient matrix is obtained by DFT, to the grayed host image. Secondly, in order to compress the amount of information and improve the efficiency of the algorithm, the high frequency coefficient image is transformed by DCT transform. The low frequency coefficient image which is consistent with the size of the watermark image after DCT is selected as the feature image of the host image. After that, the watermark information is scrambled by Arnold transform to improve the security of the watermark information. Finally, the zero-watermark image is obtained by XOR operation between the scrambled watermark information and the feature image. The zero-watermark image is saved in a third-party database for copyright verification. In order to verify the robustness of digital watermarking, this paper carries out sharpening, histogram equalization, Karma transform, noise, filtering and geometric attacks on the host image, and compares it with other algorithms. The NC value between the extracted watermark image and the original watermark image after attacking the host image show that the algorithm has a strong ability to resist common attacks.

Keywords: Zero watermark, Discrete Fourier Transform, Discrete Cosine Transform, Feature Image.

1. Introduction
The rapid development of digital media communication technology has increased the ways of image acquisition, accelerated the speed of image transmission, and brought a lot of convenience to people's life. However, it also leads to the proliferation of image copyright problems such as illegal acquisition and illegal embezzlement. Digital watermarking technology is an effective method to protect the rights of copyright owners. Without affecting the visual effect of the image, the digital watermark
According to the way of watermark embedding, watermarking algorithm can be divided into spatial domain watermarking algorithm and transform domain watermarking algorithm. The spatial domain watermarking algorithm modifies the pixel value of the image directly in the image domain. The main idea of the watermarking algorithm based on transform domain is to transform the host image with certain rules, and then embed the watermark by modifying the image information in the transform domain. Due to the advantages of robustness and imperceptibility of watermark, transform domain watermarking algorithm has been widely studied. At present, there are three main transform domain watermarking algorithms: Discrete Fourier Transform (DFT) [2,3], Discrete Wavelet Transform (DWT) [4,5] and Discrete Cosine Transform (DCT) [6,7].

The main characteristics of digital watermarking are: robustness, imperceptibility, security and capacity. Robustness refers to the ability of digital watermark to resist various attacks. Imperceptibility means that the digital watermark cannot be detected by the human perception system after it is embedded. Coordinating the contradiction between imperceptibility and robustness of watermarking has always been an issue to be considered. Zero watermarking algorithm provides an idea to solve this problem. Zero watermark does not make any changes to the host image. According to the characteristics of the host image, a feature watermark is constructed and stored in a third-party database. If there is a copyright dispute, whether the user is a legitimate authorized user can be determined by implementing watermark detection in a third-party database.

Remote sensing images are mainly including aerial photos and satellite photos. Nowadays, Remote sensing images play an important role in land monitoring and topographic survey, and gradually covered a wide range of fields. Remote sensing image has the characteristics of high acquisition cost, large amount of information, various data types, and image information cannot be destroyed [8].

The non-damage of zero watermark to the host image provides a way for the copyright protection of remote sensing images. The main way to improve the performance of zero watermarking is to enhance the robustness of watermarking. This work proposes a robust zero-watermarking algorithm for remote sensing images based on DFT and DCT. Firstly, perform 8×8 block DFT on the grayscaled host image, and the high frequency coefficients are constructed into coefficient image. In order to further enhance the robustness of the watermarking algorithm, perform DCT on the coefficient image. The feature image is obtained by binarizing the low frequency coefficient image of DCT. XOR the feature image with the watermark image to construct a zero watermark. The experimental results show that the algorithm proposed in this paper has strong anti-attack ability and does not have the problem of false positive.

2. Related works

2.1. Hybrid watermarking algorithm
In order to meet the robustness requirements of digital watermarking, the researchers combine single watermarking algorithm and propose a hybrid digital watermarking algorithm based on transform domain. Ying et al [9] proposed a robust digital watermarking algorithm for color images based on DFT and dual-tree complex wavelet transform (DTCWT). The algorithm divides the image into three channels: Y, U and V, and transforms the host image on different channels. Experiments show that this method has significant advantages in resisting geometric attacks.

With the continuous development of intelligent algorithms, particle swarm optimization algorithm [10] and machine learning [11] also have some applications in digital watermarking.

2.2. Zero watermarking algorithm
Medical images and remote sensing images contain important information, and the security and protection of their information put forward higher requirements for digital watermarking algorithms. Liu et al. [12] firstly encrypt medical images through DWT, DCT and chaotic maps. Secondly, the
encrypted image is transformed by SIFT-DCT transform, and 32 bits are selected as the feature sequence in the transformed coefficients. Finally, zero watermark is generated by distinguishing the feature sequence of the encrypted watermark image and the host image. The watermarking algorithm shows good robustness to common attacks.

Wang [13] proposed a zero-watermarking algorithm for color images against rotation attacks based on Nonsubsampled Pyramidde Composition and DCT.

2.3. Zero watermarking algorithm for remote sensing image

In order to protect the copyright of remote sensing image without modifying remote sensing image data, zero watermarking is introduced into the digital watermarking algorithm of remote sensing image. Zhao et al. [14] uses Nonsubsampled Contourlet Transform to decompose the grayed host image, and then divides the low frequency subband into block DCT transform. The feature image of the host image is constructed according to the stable relationship of direct current coefficient on the average value of each block and all blocks after DCT. Atoany [15] proposed a robust zero watermarking algorithm based on convolution neural network (CNN) and depth learning algorithm for remote sensing images with less distortion. The characteristic images constructed by Li et al. [16] are the low-frequency coefficient image after the DWT of the host image and the logarithmic polar mapping image of the host image.

The robustness of the above algorithm is passable, but the ability to resist some attacks does not meet the requirements of copyright protection. In this paper, a robust zero watermarking algorithm is proposed for remote sensing images.

3. Preliminaries

3.1. Discrete Fourier transform (DFT)

Discrete Fourier transform (DFT) converts the image signal from time domain to frequency domain, that is, the gray distribution function of the image is transformed into the frequency distribution function. The amplitude and phase parts can be obtained by DFT decomposition. DFT is widely used in image enhancement, denoising, edge detection, feature extraction and so on. The DFT transform formula of an image of \( MN \times MN \) size is as follows:

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

(1)

Where \( F(u, v) \) is the result of discrete Fourier transform of image matrix \( f(x, y) \), and \( u \) and \( v \) can be used to determine the frequency of sine and cosine.

3.2. Discrete cosine transforms (DCT)

Discrete cosine transform (DCT) is one of the commonly used transforms in image watermarking, which is separable and energy-concentrated. Separability means that two-dimensional DCT can be divided into two one-dimensional DCT transforms. After DCT transform, the energy of the image is mainly concentrated in the low frequency part, so embedding the watermark in the low frequency component of DCT has good stability. DCT transform is widely used in image processing and data compression, such as common JPEG still image coding, MJPEG, MPEG dynamic coding and other standards. The formula of DCT transform is as follows.

\[
C(k, l) = \frac{1}{\sqrt{M \times N}} \alpha(k) \alpha(l) \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m, n) \cos \left( \frac{(2m+1)k\pi}{2M} \right) \cos \left( \frac{(2n+1)l\pi}{2N} \right)
\]  

(2)
\[ \alpha(k) = \alpha(l) = \begin{cases} \sqrt{2} & \text{if } k, l = 0 \\ 1 & \text{else} \end{cases} \] (3)

The inverse DCT is:

\[ x(m, n) = \frac{1}{\sqrt{M \times N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \alpha(k) \alpha(l) x(m, n) \times \cos \left( \frac{(2m+1)k\pi}{2M} \right) \cos \left( \frac{(2n+1)l\pi}{2N} \right) \] (4)

3.3. Arnold transform

Arnold transform realizes image scrambling through finite elementary matrix transformation of image matrix. After the Arnold transform, the pixels of the image will be redistributed, and the image will become disorganized, so as to realizing the hiding of image information [17]. The Arnold transform is periodic, and the continuous transformation of the image can finally restore the original image. This characteristic of Arnold transform can realize the encryption and decryption of the image. The Arnold transform formula of the M-order image is:

\[ \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \mod(M) \] (5)

Where \( n \) is the degree of the current transformation, \((x_n, y_n), (x_{n+1}, y_{n+1})\) is the position of the corresponding pixel before and after the transformation respectively.

4. The Algorithm

Based on DCT and DFT, this paper proposes a zero-watermarking algorithm for remote sensing image. In this section, Baboon (128x128) is used as the watermark image to show the algorithm of this work.

4.1. Zero-watermark generation

4.1.1. Construct feature image. Firstly, the original host image is grayscale processed. The RGB image is converted into grayscale image to reduce the amount of data and improve the processing speed. The principle of image graying is as follows:

\[ \text{Gray} = \sqrt{R^2 + (1.5G)^2 + (0.6B)^2} \] (6)

Secondly, perform DFT on the grayed host image, to get the high frequency part which represents the details of the image and the low frequency part that represents the outline information of the image.

In order to enhance the robustness of the watermark, the DCT is computed on the high frequency coefficient image after DFT. DCT concentrates most of the energy of the image on the upper left corner of the transformed coefficient matrix. The coefficient matrix which is consistent with the size of the watermark is selected from the upper left corner, and the mean value is used as the threshold for binarization. The binarized image is used as the feature image of the host image.

4.1.2. Processing watermark image. In order to improve the security of the watermark, Arnold transform is used to scramble the binary watermark image. The number of scrambles is used as the key Key. The purpose of scrambling is that even if the feature information of the image is extracted correctly, the original watermark image cannot be restored without grasping the key. Figure 1 shows the course of processing the original watermark image.
Figure 1. Watermark Image Processing. (a) Original watermark image. (b) Watermark after gray processing. (c) Scrambled watermark image.

The zero watermark can be obtained by XOR operation between the final feature image and the watermark image.

The overall process of constructing a zero-watermark image is as follows:
Step1. If the host image $I$ is a RGB image or a color image, convert it to a grayscale image $I_G$.
Step2. Perform DFT on $I_G$ to obtain the corresponding DFT coefficient $DFT$.
Step3. Perform block DCT on the high frequency part of $DFT$ to get DCT coefficient $DCT$.
Step4. In order to make the size of the feature image consistent with that of the watermark image, the $m \times n$ part of the upper left corner of the $DCT$ is extracted as the feature image $Feature$ of the host image.
Step5. Select the mean value as the threshold value to perform binarization processing on $Feature$, and mark the image after binarization as $Feature'$.
Step6. After binarizing the original watermark image $W$ of size $m \times n$, perform Arnold transform according to the key $Key$ to obtain the scrambled watermark image $W_A$.
Step7. The zero-watermark image $zero_{watermarking}$ is obtained by XOR operation between the feature image $Feature'$ and $W_A$. The zero watermark is saved in the third-party database for copyright verification.

4.2. Watermark extraction

Extracting the watermark image needs to use the zero-watermark image saved in the third-party database. Firstly, extract the feature image from the attacked host image. Then the extracted watermark image can be obtained by XORing the feature image with the zero-watermark stored in the third-party database.

The specific algorithm flow of extracting watermark image is as follows:
Step1. Enter image $I'$ to be detected, which is the host image after attack.
Step2. Perform DFT on the image $I'$ to get the coefficient matrix $DFT'$.
Step3. Perform DCT on the high-frequency part in $DFT'$, and get the DCT coefficient $DCT'$.
Step4. Extract the low-frequency part $low_{DCT'}$ from $DCT'$.
Step5. Binarize the $low_{DCT'}$ with the mean value as the threshold to obtain the image $Feature'$.
Step6. Perform XOR on $Feature'$ and zero watermarking image $zero_{watermarking}$ to get the extracted watermark image $W_G$.
Step7. Perform Arnold transformation on $W_G$ according to the key $Key$ to obtain $W_G'$. Compare the similarity between the original watermark image and $W_G'$ to complete copyright verification.
5. Experimental Results
The experimental samples used in this section are mainly 20 color remote sensing images. Figure 2 shows the image data set of this article, and the number and size of the image are given at the bottom of each image.

![Image data set](image.png)

**Figure 2.** Image data set.

5.1. Evaluation index
In this work, the performance of digital watermarking is quantitatively evaluated by Normalized Correlation (NC).

The normalized correlation coefficient is able to measure the degree of similarity between the images. The robustness of the digital watermark can be tested by calculating the NC value between the extracted watermark and the original watermark. The calculation formula of NC value is:

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

Where \( m \times n \) represents the size of the watermark image, \( W, W' \) represents the embedded watermark and the extracted watermark respectively.

5.2. Parameter Setting
Before carrying out the experiment, some experimental parameters need to be set. The main parameters used in this algorithm are the block size of DFT, the threshold of binarization after DFT and the times of Arnold scrambling. Considering the efficiency of time and space and the accuracy of the results, the block size of DFT is set to 8×8, the mean value as the threshold, and the times of Arnold scrambling is 5.

Before the XOR operation between the feature image of the host image and the watermark information, it is necessary to binarize the feature image. For the threshold in binarization, the mean, median, mode, 3/4 digits and 1/4 digits are selected to test. Table 1 shows the average NC values of 20 images. It can be seen from the table 1 that the average NC of all test images is the lowest when the mean is used as the threshold, which verifies the rationality of the mean as the threshold.

| Threshold | Average | Median | Mode | Quarter digit | Three-quarter digits |
|-----------|---------|--------|------|---------------|----------------------|
| NC value  | 0.956   | 0.728  | 0.912| 0.931         | 0.828                |

Table 1. Robustness results of images under different thresholds.
5.3. Noise Attack and Filtering Attack

In order to test the performance of watermark, compare the similarity between the original watermark information and the watermark extracted from the attacked host image. The types of attacks selected are:

| Attack type            | Image 4 | Image 7 | Image 10 | Image 11 | Image 14 |
|------------------------|---------|---------|----------|----------|----------|
| Low-pass Gaussian filtering |         |         |          |          |          |
| μ = 2×2                | 0.986   | 0.991   | 0.984    | 0.970    | 0.981    |
| μ = 3×3                | 0.990   | 0.993   | 0.988    | 0.978    | 0.989    |
| μ = 5×5                | 0.988   | 0.992   | 0.986    | 0.975    | 0.986    |
| μ = 7×7                | 0.988   | 0.991   | 0.986    | 0.975    | 0.986    |
| μ = 9×9                | 0.988   | 0.991   | 0.986    | 0.975    | 0.986    |
| Median filtering       |         |         |          |          |          |
| μ = 2×2                | 0.986   | 0.991   | 0.983    | 0.969    | 0.981    |
| μ = 3×3                | 0.989   | 0.993   | 0.988    | 0.977    | 0.988    |
| μ = 5×5                | 0.982   | 0.988   | 0.982    | 0.970    | 0.982    |
| μ = 7×7                | 0.980   | 0.985   | 0.978    | 0.956    | 0.976    |
| μ = 9×9                | 0.978   | 0.983   | 0.973    | 0.951    | 0.968    |
| Wiener filtering       |         |         |          |          |          |
| μ = 2×2                | 0.993   | 0.992   | 0.993    | 0.986    | 0.991    |
| μ = 3×3                | 0.993   | 0.994   | 0.993    | 0.987    | 0.991    |
| μ = 5×5                | 0.987   | 0.989   | 0.991    | 0.982    | 0.987    |
| μ = 7×7                | 0.984   | 0.986   | 0.989    | 0.978    | 0.984    |
| μ = 9×9                | 0.982   | 0.983   | 0.989    | 0.974    | 0.981    |
| Average filtering      |         |         |          |          |          |
| μ = 2×2                | 0.986   | 0.991   | 0.984    | 0.970    | 0.981    |
| μ = 3×3                | 0.981   | 0.985   | 0.980    | 0.969    | 0.980    |
| μ = 5×5                | 0.973   | 0.976   | 0.974    | 0.953    | 0.968    |
| μ = 7×7                | 0.969   | 0.970   | 0.967    | 0.944    | 0.957    |
| μ = 9×9                | 0.964   | 0.964   | 0.961    | 0.937    | 0.948    |
| salt-and-pepper noise  |         |         |          |          |          |
| σ = 0.01               | 0.959   | 0.946   | 0.960    | 0.941    | 0.941    |
| σ = 0.03               | 0.918   | 0.893   | 0.916    | 0.890    | 0.878    |
| σ = 0.05               | 0.876   | 0.879   | 0.874    | 0.849    | 0.835    |
| σ = 0.1                | 0.809   | 0.843   | 0.865    | 0.829    | 0.823    |
| σ = 0.12               | 0.805   | 0.828   | 0.848    | 0.811    | 0.801    |
| Speckle noise          |         |         |          |          |          |
| σ = 0.001              | 0.990   | 0.989   | 0.989    | 0.985    | 0.986    |
| σ = 0.005              | 0.975   | 0.979   | 0.975    | 0.965    | 0.972    |
| σ = 0.007              | 0.970   | 0.975   | 0.973    | 0.956    | 0.967    |
| σ = 0.009              | 0.966   | 0.968   | 0.968    | 0.953    | 0.962    |
| σ = 0.011              | 0.962   | 0.966   | 0.964    | 0.946    | 0.955    |
| Gaussian noise         |         |         |          |          |          |
| σ = 0.005              | 0.942   | 0.907   | 0.943    | 0.918    | 0.917    |
| σ = 0.01               | 0.902   | 0.843   | 0.902    | 0.874    | 0.867    |
| σ = 0.015              | 0.865   | 0.834   | 0.870    | 0.843    | 0.834    |
| σ = 0.02               | 0.839   | 0.804   | 0.839    | 0.815    | 0.828    |
| σ = 0.025              | 0.812   | 0.801   | 0.813    | 0.805    | 0.811    |
In this section are filtering attacks and noise attacks. Take image 7 as the host image. Figure 3 shows the visualization result of the host image after being attacked by filtering and noise. Table 2 shows the NC value of the image 4, 7, 10, 11, 14 as the host image.

Filtering attacks include Gaussian low-pass filtering, median filtering, Wiener filtering and Average filtering. Noise attacks include salt and pepper noise, speckle noise and Gaussian noise. These attacks have caused varying degrees of damage to the visual effect of the image. Among them, salt and pepper noise and Gaussian noise damage the image the most. However, from the NC value of 20 images, 80% of the NC value is greater than 0.95. The results show that the extracted watermark is not greatly affected, which indicating that the algorithm is robust to filtering and noise attack.

**Figure 3.** Attack Results of noise and Filtering. (a) The original image. (b) Attacked by Gaussian low-pass filtering. (c) Attacked by median filter. (d) Attacked by Wiener filtering. (e) Attacked by Average filtering. (f) Attacked by salt and pepper noise. (g) Attacked by speckle noise. (h) Attacked by Gaussian noise.

5.4. Geometric Attack

The geometric attacks used in this paper include cropping and rotation. Figure 4 shows the visualization results under geometric attacks. When cutting 25% and 35% in the upper left corner, the corresponding NC values are 0.953 and 0.953. When the center is cut by 25% and 35%, the NC values are 0.991 and 0.989. Since the construction of zero watermark information mainly uses the upper left corner coefficient image of the host image after DCT, the NC value after clipping in the upper left corner is less than that after clipping in the center. The NC values under the four parameters are greater than 0.95, indicating that the watermarking algorithm is robust to general clipping.

**Figure 4.** Geometric Attack Results.

In the rotation attack experiment, the host image is rotated 5° and 10° clockwise and counterclockwise. Rotation results in the dislocation between the position of the extracted watermark and the watermark information. With the increase of the rotation angle, the more error information is
extracted at the position where the watermark is constructed, which leads to the decrease of the NC value. When the rotation angle is 10 degrees, the NC value is still above 0.8, indicating that the algorithm has a strong ability to resist rotation attacks.

5.5. Other Attacks

Other types of attacks selected in this paper are sharpening, histogram equalization and gamma correction. Figure 5 shows the watermark image extracted from the host image after being attacked. When the sharpening intensity increases from 3 to 7, the NC value of the image decreases from 0.978 to 0.955. The NC value is still greater than 0.95 under the strong sharpening attack, which indicates that the algorithm in this paper is robust to the sharpening attack.

With the decrease of the number of equalization bits in the histogram, the contrast of the image decreases, and the similarity between the image and the original host image is lower. Under 16-bit histogram equalization, the NC value of the watermark image is still greater than 0.85. For gamma transformation, the gamma values of less than 1 and greater than 1 are tested respectively. When the gamma values are 1.1 and 1.2, the NC values are 0.994 and 0.989 respectively, indicating that the extracted watermark is hardly affected when the low gray value is extended. When the gamma values are 0.9 and 0.8, the NC values are 0.987 and 0.981 respectively, indicating that the watermarking algorithm in this paper can resist the expansion of high gray values.

![Figure 5. Other Attack Experiment Results.](image)

5.6. Comparative experiment with other algorithms

In order to quantitatively measure the advantages of this algorithm, images 4,10,11 are used as host images to compare with other algorithms.

![Figure 6. Compare results with conventional algorithms.](image)
5.6.1. Compared with conventional algorithms. Firstly, the conventional algorithms: DFT, DCT are compared with the algorithm in this work. Figure 6 shows the NC values of the above algorithms under noise, filtering, geometry and other attacks.

As can be seen from the figure 6, the DCT+DFT hybrid algorithm is better than the single algorithm. The NC value can reach more than 95% under most attacks, and the curve trend is the most stable. For a single algorithm, the NC value of DCT algorithm under partial attack is close to 0.5, so the extracted watermark image may not be recognized.

5.6.2. Compared with previous literature. This section compares the robustness of the algorithm proposed in reference [18] and reference [19] with that of this algorithm under filtering, noise, cropping and rotation attacks. Although the algorithms in references [18] and [19] can resist noise and filtering attacks, they are not robust to geometric attacks. As can be seen from table 3, the robustness of this algorithm in cropping and rotation attacks is much higher than that in references [18] and [19]. The algorithm in this work also has some advantages under filtering and noise attacks.

| Attack type                  | This method | Method in paper [18] | Method in paper [19] |
|------------------------------|-------------|----------------------|----------------------|
| Median filtering             | 0.991       | 0.810                | 0.843                |
| Low-pass Gaussian filtering  | 0.991       | 0.980                | 0.980                |
| Salt and Pepper noise        | 0.946       | 0.890                | 0.885                |
| Shearing (upper left 25%)    | 0.953       | 0.500                | 0.564                |
| Shearing (middle 25%)        | 0.991       | 0.480                | 0.386                |
| Rotation (5°)                | 0.882       | 0.420                | 0.452                |

5.7. False Positive Test

Compared with other watermarking algorithms, zero watermarking algorithm is prone to false positive problem. This section tests whether the algorithm of this work can solve the false positive problem.

Step1. The original watermark image is binarized to get the watermark image $W(x, y)$.

Step2. Using the algorithm of constructing feature image in this paper, extract the feature image $Feature_i$ of each host image $I_i$ in the data set.

Step3. Select an image $I_s$ from the data set as the host image, and construct the zero-watermark _zero watermarking of the image $I_s$.

Step4. Except for the selected image $I_s$, the feature image $Feature_i$ of each image and the _zero watermarking of $I_s$ are subjected to XOR operation to obtain the extracted image $extract_i$.

Step5. Perform the Arnold inverse transform on $extract_i$ to obtain the watermark image $image_i$.

Step6. The NC value $NC_i$ between each watermark image $image_i$ and the original watermark is calculated in turn. If $NC_i$ is greater than 0.8, it means that when $I_s$ is selected as the host image, the $i-th$ image has a false positive problem.

Assuming that when $I_s$ is selected as the host image to construct zero watermark, a total of $FP_s$ images in the data set have false positive problems. The formula for calculating the false positive rate $FPR_s$ of the image $I_s$ is

$$FPR_s = \frac{FP_s}{count} - 1$$

Where $count$ is the total number of images in the data set.
Figure 7 shows the FPR value of the data set image. The average FPR of 20 images is 0.063 as the final total FPR value. Therefore, the probability of false positive problem of the zero-watermark constructed by this algorithm is very small, which makes the accuracy of copyright verification very high.

![Figure 7. False positive test results.](image)

6. Conclusions
In this paper, a zero-watermarking algorithm for remote sensing images is proposed based on DCT and DFT. The innovation of this algorithm lies in: (1) The host image is not modified. (2) The watermarking algorithm has high robustness. (3) The possibility of the false positive problem is very small.

In the experiment of testing the performance of the algorithm, after the host image is attacked with high intensity, even if the image is visually unrecognizable, the algorithm in this paper can still extract the feature image with high accuracy. For all kinds of attacks, the increase in attack intensity has little effect on the visual effect of the extracted watermark. Experimental results show that the watermark has good invisibility and high robustness.

References
[1] Yang HY, Wang XY, Niu PP, Wang AL, "Robust color image watermarking using geometric invariant quaternion polar harmonic transform," ACM Transactions on Multimedia Computing Communications and Applications, vol. 11, no. 3, Article 40, pp.1-26, 2015.
[2] Jyotsna Singh,Parul Garg,Alok Nath De. Multiplicative watermarking of audio in DFT magnitude [J]. Multimedia Tools and Applications,2014,71(3), 1431-1453.
[3] Matthieu Urvo, Dalila Goudia,Florent Autrusseau. Perceptual DFT Watermarking With Improved Detection and Robustness to Geometrical Distortions.[J]. IEEE Trans. Information Forensics and Security,2014,9(7), 1108-1119.
[4] Tanya Koohpayeh Araghi,Azizah Abd Manaf. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD[J]. Future Generation Computer Systems,2019,101, 1223-1246.
[5] Huda Karajeh, Tahani Khatib,Lama Rajab, Mahmoud Maqableh. A robust digital audio watermarking scheme based on DWT and Schur decomposition[J]. Multimedia Tools and Applications,2019,78(13), 18395-18418.
[6] Satendra Pal Singh,Gaurav Bhatnagar. A new robust watermarking system in integer DCT domain [J]. Journal of Visual Communication and Image Representation,2018,53, 86-101.
[7] Yih-Kai Lin, Cheng-Hsing Yang,Jinn-Tsong Tsai. More secure lossless visible watermarking by DCT [J]. Springer US,2018,77(7), 8579-8601.
[8] Guanghui Yuan, Qi Hao. Digital Watermarking Secure Scheme for Remote Sensing Image Protection [J]. China communications, 2020,17(04): 88-98

[9] Ying Qi Chao, Lin Jing Zhi, Qian Zhen Xing, Xu Hai Sheng, Zhang Xin Peng. Robust digital watermarking for color images in combined DFT and DT-CWT domains [J]. Mathematical biosciences and engineering : MBE, 2019, 16(5):4788-4801.

[10] Shen Yuxin, Tang Chen, Xu Min, Chen Mingming, Lei Zhenkun. A DWT-SVD based adaptive color multi-watermarking scheme for copyright protection using AMEF and PSO-GWO [J]. Expert Systems With Applications, 2021, 168, 114414.

[11] Seyed Mostafa Pourhashemi, Mohammad Mosleh, Yousof Erfani. A novel audio watermarking scheme using ensemble-based watermark detector and discrete wavelet transform [J]. Neural Computing and Applications, 2020, (prepublish).

[12] J. Liu, J. Li, Y. Chen, X. Zou, J. Cheng et al. A Robust Zero-Watermarking Based on SIFT-DCT for Medical Images in the Encrypted Domain [J]. Computers, Materials & Continua, 2019, 61(1), 363-378.

[13] R. Wang, H. Shaocheng, P. Zhang, M. Yue, Z. Cheng and Y. Zhang. "A Novel Zero-Watermarking Scheme Based on Variable Parameter Chaotic Mapping in NSPD-DCT Domain," in IEEE Access, vol. 8, pp. 182391-182411, 2020, doi: 10.1109/ACCESS.2020.3004841.

[14] S. Zhao Jie, Li Yawen, Yang, Binfeng, Wu Xiaoyun. Active Forensics Method Based On Local Features for Remote Sensing Images [J]. Journal of Environmental Protection and Ecology, 2019, 20(3): 1470-1478.

[15] 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," 2019 7th International Workshop on Biometrics and Forensics (IWBF), Cancun, Mexico, 2019, pp. 1-5, doi: 10.1109/IWBF.2019.8739245.

[16] Li Jing, Yadong Zhang and Guanyu Chen, "Zero-watermarking for copyright protection of remote sensing image," 2008 9th International Conference on Signal Processing, Beijing, China, 2008, pp. 1083-1086, doi: 10.1109/ICOSP.2008.4697317.

[17] Information on https://www.jianshu.com/p/39727dbaffd9

[18] Ming Li, Jinhua Zhang, Wenying Wen. Cryptanalysis and improvement of a binary watermark-based copyright protection scheme for remote sensing images [J]. Optik - International Journal for Light and Electron Optics, 2014, 125(24), 7231-7234.

[19] Peng Zhu, Fei Jia, Junliang Zhang. A copyright protection watermarking algorithm for remote sensing image based on binary image watermark[J]. Optik - International Journal for Light and Electron Optics, 2013, 124(20), 4177-4181.