Digital Holographic Watermarking Algorithm Based on DWT-DCT

Zhiyue Liu, Anling Wang*, Kuang Xin, Fuping Liu, Xiaofeng Zhu, Yajing Li, Zichao Yu
Information Engineering, Beijing Institute of Graphic Communication, China
535920925@qq.com
*wanganling@bigc.edu.cn

Abstract. In order to improve the robustness and invisibility of watermarking, a digital holographic watermarking algorithm based on DWT-DCT is proposed. First, the watermark image is generated into a digital hologram to improve the security and non-tearability of the watermark, and the I1 image is selected as the watermark image to be embedded. Perform discrete wavelet transform on the original carrier image to extract its low-frequency coefficients; secondly, the low-frequency coefficients are subjected to DCT transformation, and finally the watermark information is embedded in the high-frequency coefficient matrix after DCT, thereby completing the watermark information embedding. This algorithm combines the transformation characteristics of DWT and DCT, makes up for each other's shortcomings, and makes digital watermarking more robust and invisible. In order to verify the anti-attack ability of this algorithm, different attack tests were performed on the watermark image. The results show that this algorithm is robust against simple linear attacks and noise attacks.

1. Introduction
With the gradual development of the Internet, digital watermarking, as an effective means of copyright protection of multimedia digital products, has become a research focus in the field of information security in recent years. Using digital watermarking technology to protect the copyright of images, texts, and videos in the network environment is a very important means [1]. In recent years, digital image watermarking technology has made great progress. The embedding of watermarking is usually realized in three fields: spatial domain, transform domain and compressed domain. This paper realizes the hiding of watermark information in the transform domain, combines the respective advantages of DCT and DWT, makes up for their respective shortcomings, and uses the method of combining DWT and DCT to carry out the algorithm design of digital watermarking. Take the watermark image to generate holograms I1, I2, I3, I4, and perform discrete wavelet transformation on the original carrier image to extract its low-frequency coefficients; secondly, perform DCT transformation on the low-frequency coefficients, and embed the watermark information into the DCT according to a certain embedding strength The high frequency part. This algorithm effectively guarantees the robustness, integrity and concealment of the watermark information, and can resist a certain degree of noise attacks and linear attacks.
2. Basic principles of the algorithm

2.1. Principle of Digital Hologram
This technology uses photoelectric technology, replaces traditional photosensitive materials with digital cameras, and uses image sensors without focusing optics to record interference fringes. The reconstruction of the image of the object uses diffraction theory to propagate the wave field back from the image sensor plane to the object plane. Form a hologram [2]. The original image is transformed into a hologram as watermark information to increase the security of watermark information. In the unknown sampling number, sampling interval and reference light wavelength, even if the hologram is obtained, the watermark information cannot be reconstructed, thereby increasing the security performance of its information transmission [3].

In the experiment, Matlab programming was used to realize the hologram generation process and reconstruction process. After obtaining the required holographic watermark, the inverse Fourier transform is used to complete the reconstruction of the hologram, and the reconstructed watermark image can be obtained. The figure below shows the four generated holograms I1, I2, I3, and I4.

![Fig.1 Original watermark image](image1)

![Fig. 2 Hologram I1](image2)

![Fig. 3 Hologram I2](image3)

![Fig. 4 Hologram I3](image4)

![Fig. 5 Hologram I4](image5)

2.2. Digital Holographic Watermarking Algorithm Based on DWT-DCT
DWT can quickly decompose image information into low-frequency components, horizontal components, vertical components and diagonal components. Among them, the low frequency part is the best approximation to the minimum resolution and minimum scale of the original image [4].
Embedding the watermark in the low-frequency part of the image can resist attack operations such as filtering and compression processing, and can extract the watermark quickly and effectively to ensure the robustness of the watermark; but the embedded watermark will affect the original image to a certain extent and reduce the image The invisibility of the watermark [5].

If the DCT transformation is performed on the information obtained above, the important visual information of the image can be concentrated in a small part of the transformed coefficients, and the image can be divided into low-frequency, intermediate-frequency and high-frequency regions according to the image energy [6]. Embedding watermark information into the high frequency part after DCT can improve the invisibility of image watermark.

Based on the respective advantages of DCT and DWT, a combination of DCT and DWT is used to develop digital watermarking algorithms. First perform DWT on the original image carrier to extract low-frequency coefficients; then perform DCT on it, embed the watermark information into the high-frequency part after DCT transformation, so that the energy is evenly distributed on all pixels of the image, which can balance the invisibility and invisibility of the watermark. Robustness has certain practical value.

### 2.3. Embedding and Extraction of Digital Holographic Watermark Image

Combining the characteristics of Fourier transform holographic technology and DWT-DCT transform, a Fourier holographic watermarking algorithm based on DWT-DCT transform domain is proposed, which makes digital watermarking more robust and invisible.

The embedding process of holographic watermark, the implementation process is shown in the figure below. The specific expression is: (1) Four-step phase shift method is used for the watermark image to generate four digital holograms I1, I2, I3, and I4. The obtained I1 information is the watermark information to be embedded. In this way, the non-tearability and strong robustness of the holographic watermark image can be realized. (2) Prepare a gray-scale host image. (3) Perform wavelet decomposition on the grayscale carrier image, perform DCT transformation on the low-frequency coefficient part LP, and extract the high-frequency coefficient matrix. (4) Perform DCT transformation on the hologram I1 generated in the first step and embed it in the high-frequency coefficient matrix; (5) Perform inverse DCT and inverse DWT transformation on the coefficient matrix added with watermark information to obtain an image containing watermark.

The extraction process of the watermark is the reverse process of embedding. The DCT and DWT transform are performed to extract the watermark information. After I1 is obtained, the digital holographic watermark is reconstructed, and finally the extracted watermark image is obtained.

![Fig. 6 Watermark embedding algorithm flow](image-url)
2.4. Watermark quality evaluation index

In order to evaluate the quality of the watermark image more objectively and verify the invisibility and robustness of the watermark information, the peak signal-to-noise ratio (PSNR) index is often used to objectively evaluate the similarity between the original carrier image and the watermarked image, and the NC value is used. The index makes an objective evaluation of the similarity between the original watermark and the extracted watermark. The larger the PSNR value and NC value, the better. It is generally believed that when the PSNR value is greater than 28dB and the NC value is greater than 0.75, the watermarking algorithm is effective.

The formula of peak signal-to-noise ratio PSNR is as follows [7]:

$$PSNR = 10 \times \log_{10}(\frac{(2^n-1)^2}{MSE})$$

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

The NC value formula is as follows:

$$NC = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} W(x, y) - W'(x, y)}{\sqrt{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} W^2(x, y) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} W'^2(x, y)}}$$
The PSNR value of the watermark image and the original carrier image obtained by using the algorithm in this paper is 37.9862, and the watermark algorithm is effective. In order to further verify the robustness of the watermark algorithm, an attack test was carried out on the embedded watermark image.

3. Watermark attack test experiment

3.1. Shear attack
Cut 3/4 of the embedded watermark image and keep 1/4 of it, and finally the watermark image can be successfully reconstructed:

Through this algorithm, the watermark image can be reconstructed even after the image has been cut attack, and the calculated NC value is 0.9662. It is concluded that the reconstructed image and the original watermark image have a high similarity. It can be seen that this attack did not cause obvious damage to the watermark, and this algorithm has a better defense effect against cutting attacks.

3.2. Spin attack
Rotate the watermarked image 90 degrees clockwise, and finally successfully reconstruct the watermark image:

Through this algorithm, the watermark image can be reconstructed even after the image is rotated and attacked, and the calculated NC value is 0.9533. It is concluded that the reconstructed image and the original watermark image have a high similarity. It can be seen that this attack did not cause obvious damage to the watermark, and this algorithm has a better resistance to rotation attacks.

3.3. Noise attack
Add salt and pepper noise to the watermarked image, and finally successfully reconstruct the watermarked image:
Through this algorithm, the watermark image can be reconstructed even after the image is attacked by salt and pepper noise, and the calculated NC value is 0.9558. It is concluded that the reconstructed image and the original watermark image have a high similarity. It can be seen that this attack did not cause obvious damage to the watermark, and this algorithm has a better resistance to salt and pepper noise attacks.

3.4. Translation attack
Translate the grayscale image after embedding the watermark, the translation data is $a=200$, $b=200$ (at the same time, the image is translated to the right and down by 200 unit coordinates), and finally the watermark image is successfully reconstructed:

Through this algorithm, the watermarked image can be reconstructed even after the image undergoes a translation attack, and the calculated NC value is 0.9737. It is concluded that the reconstructed image and the original watermark image have a high similarity. It can be seen that this attack did not cause obvious damage to the watermark, and this algorithm has a better defense against translation attacks.

4. Conclusion
This paper combines digital holographic watermarking and DWT-DCT technology, and proposes a digital holographic watermarking algorithm based on the DWT-DCT transform domain, which makes the watermark highly invisible and safe. And through watermark embedding and extraction simulation experiments and robust attack experiments, it is verified that the algorithm in this paper has strong robustness to image processing operations such as cropping, translation, rotation and salt and pepper noise, and improves the security of information transmission in practical applications.

Acknowledgments
This work was financially supported by the key project of Beijing Institute of Graphic Communication, the deepening project of the Beijing University Student Research and Training Program in 2019. (03150120001/003)
References

[1] Zhang Wenzhao, Wu Wei. Image fusion algorithm based on wavelet transform [J]. Jiangsu Science and Technology Information, 2013(20): 52-53. (in Chinese).

[2] Kong Lingjun, Nie Peng. A holographic watermarking technology based on DWT-DCT transform domain [J]. Photonics-Laser, 2016, 27(02): 198-202. (in Chinese).

[3] Li Shike. Research on anti-distortion holographic watermarking algorithm based on image feature points [D]. Beijing Institute of Graphic Communication, 2020. (in Chinese).

[4] Lin Guoqiang. Application of Computational Holography Technology in Encryption Field [D]. Xiamen University, 2018. (in Chinese).

[5] Huang Fuying, Tang Zhenhua, Qin Tuanfa. Color image watermarking algorithm based on digital hologram and transform domain [J]. Laser Journal, 2018, 39(04): 86-89. (in Chinese).

[6] Paulius Palevicius, Loreta Saunoriene, Maosen Cao, Minvydas Ragulskis. Time-averaged computer generated holography for the estimation of torsional amplitudes of oscillating microdevices [J]. Optics Communications, 2019, 439.

[7] Liu Bo. Research on digital holographic image watermark encryption processing [D]. Harbin University of Science and Technology, 2018. (in Chinese).