Research on Digital Watermarking Technology Based on Discrete Wavelet Transform

Dingying Tan, Huiling Liu, Huili Wang, Min Zou and Pingping Chen*

School of Medical Information Engineering, Guangzhou University of Chinese Medicine, Guangzhou, China

*Corresponding author

Abstract. By using the advantages of discrete wavelet transform in digital watermark embedding, extraction and detection, a corresponding basic model was established. Using MATLAB as a tool for simulation experiments, the experimental results show that the discrete wavelet transform can extract the watermark signal under the common JPEG compression, noise, shear and rotation, filtering and other attacks, and has high robustness.

Keywords: Digital watermarking; Discrete wavelet transform; Robustness.

1. Introduction

In recent years, people have made remarkable theoretical and technical achievements in the research of digital image watermarking problems. A large number of watermarking algorithms and watermark attack methods have been proposed. These studies have theoretically and technically ensured the better development of digital watermarking technology[1-2]. There are generally three types of frequency domain algorithms: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). This paper is mainly based on the discrete wavelet algorithm of digital image watermarking algorithm.

2. Process Based on DWT Digital Watermarking Technology

Digital watermarking technology is to make full use of the data redundancy and visual redundancy of multimedia information to embed watermark information into multimedia information through a certain algorithm, thereby forming an effective Means of copyright protection and copyright authentication of digital products. A complete digital watermarking system generally includes two modules, namely watermark embedding and watermark extraction and detection.

![Figure 1. Flow chart of the complete digital watermarking system.](image-url)
2.1. Watermark Embedding

Before embedding a watermark, a watermark must be generated first. The generation of a watermark signal is usually based on a pseudo-random number generator or a chaotic system, or some meaningful data, such as: serial number, image, text information, etc. The generated watermark signal often needs further to adapt to the watermark embedding algorithm. The original watermark signal can also be specified in advance, and the watermark signal can be appropriately transformed or not transformed before the watermark is embedded, and the key can be generated during the watermark addition process.

The watermark embedding process \cite{3} is shown in figure 2 and its function is to embed the watermark signal into the original data. In the watermark embedding process, the selection of the watermark, the embedding position, the infiltration intensity, and the type of wavelet base selected will affect the performance of the watermark system.

![Figure 2. Watermark embedding process.](image)

The watermark embedding system inputs watermark information, carrier information, and keys. Watermarks can be any form of data, such as text, images, and data.

2.2. Watermark Extraction and Detection

The watermark extraction process \cite{4} is responsible for extracting watermark information from the watermark carrier data, and the watermark detection process is used to determine whether a certain data contains the specified watermark.

Watermark extraction and detection algorithms are generally divided into two categories: blind watermark detection extraction and non-blind watermark detection extraction. Non-blind detection extraction is more reliable and robust than blind detection extraction, but blind watermark detection extraction has more advantages in computing efficiency and application scope.

![Figure 4. Watermark extraction process.](image)
Figure 5. General block diagram of wavelet transform digital watermark extraction.

Figure 6. Watermark detection process.

Figure 4 and figure 6 are the watermark extraction and detection process diagrams respectively. Figure 5 is the general block diagram of the digital watermark extraction based on wavelet transform. The carrier information can not be required in the extraction process.

2.3. Attacks on Embedded Watermark Images
The attack methods of embedded watermark images mainly use different degrees of noise, compression, shearing, rotation, scaling and other attacks to detect the resistance of the DWT algorithm to these attacks, thereby verifying the robustness of the DWT algorithm. The working principle of the above attacks is to attack the watermark image, and the watermark is extracted after the attack, and the similarity of the watermark is compared with the watermark that has not been attacked (NC value). The stronger the ability of DWT, on the other hand, the closer the absolute value of NC value is to 0, the weaker the ability of DWT algorithm to resist attacks.

Figure 7. Attack and comparison flowchart.

3. Experimental Results and Analysis Based on DWT Digital Watermarking Technology

3.1. Experimental Test Environment
MATLAB integrates DCT, DWT and other functions. It has rich wavelet functions and processing functions, and provides image processing toolbox, wavelet analysis toolbox, and digital signal processing toolbox. For example, we can call wfilters to obtain the specified wavelet decomposition and comprehensive filter coefficients. At the same time, it can be well applied to digital image processing technology.
3.2. Watermark Embedding and Extraction
Two sets of images were used in this experiment, one set was a 1024 × 1024 gray image woman as the original carrier image for watermark embedding, and the other set was 512 × 512 gray image lena as the original carrier image for watermarking embedding. Note: The size of the watermark is one quarter of the original image, and the length and width are the original image. In general, if the PSNR index is above 30db, the watermark is not perceptible [5]. The PSNR value in this experiment is 38.879 db.

The watermark is embedded into the original image through a watermark embedding program to obtain a watermark image. By comparison analysis, there is basically no difference between the embedded watermark image and the original carrier image. At the same time, the extracted watermark is the same as the original watermark. It means that the embedded watermark has good invisibility and will not affect the carrier.

3.3. Attacks on Watermarked Images

3.3.1. JPEG Lossy Compression. The two sets of watermark images are subjected to JPEG lossy compression with different quality factors, and then watermark extraction is performed. It is shown as the following table:

| IMAGE | IMAGE | IMAGE | IMAGE | IMAGE | IMAGE | IMAGE |
|-------|-------|-------|-------|-------|-------|-------|
| One   | One   | Two   | Two   | Two   | Two   | Two   |
| JPEG compression | 10 | 20 | 5 | 10 | 15 | 20 |
| NC value | 0.92 | 0.99 | 0.90 | 0.97 | 0.99 | 1 |

It can be seen from the experimental results that when the watermarked image embedded by the DWT algorithm faces a JPEG compression attack and the image compression factor is above 30, the watermarked image can be clearly extracted. It is shown that the proposed algorithm is robust against JPEG compression attacks.

3.3.2. Noise Attack. Common noise attacks include salt and pepper noise and Gaussian noise. An important indicator for evaluating the robustness of digital watermarking algorithms is the resistance of digital watermarking to noise attacks. In the experiment, different pepper and salt noise and Gaussian noise (mean is 0) are added to the images that have been embedded with watermarks. The experimental results are shown in the following tables:

| IMAGE | IMAGE | IMAGE | IMAGE | IMAGE | IMAGE | IMAGE |
|-------|-------|-------|-------|-------|-------|-------|
| One   | One   | One   | Two   | Two   | Two   | Two   |
| Salt and pepper noise | 0.01 | 0.02 | 0.03 | 0.01 | 0.02 | 0.03 |
| NC value | 0.99 | 0.98 | 0.93 | 1 | 0.98 | 0.96 |

| IMAGE | IMAGE | IMAGE | IMAGE | IMAGE | IMAGE | IMAGE |
|-------|-------|-------|-------|-------|-------|-------|
| One   | One   | One   | Two   | Two   | Two   | Two   |
| Gaussian noise | 0.01 | 0.02 | 0.03 | 0.01 | 0.02 | 0.03 |
| NC value | 0.96 | 0.88 | 0.87 | 0.96 | 0.87 | 0.87 |
According to the above experimental results, it can be known that even if the watermarked image embedded by the DWT algorithm is attacked by strong noise, it can still clearly extract the watermarked image. It indicates that this algorithm is highly robust against attacks by Gaussian noise and salt and pepper noise.

3.3.3. Rotation and Scaling Attack. Scaling attack and rotation attack are the most commonly used geometric attacks by watermark attackers, so the watermarking algorithm should have a certain resistance to scaling attack and rotation attack. In the experiment, one set of watermarked images were counter-clockwise 30 degrees, 60 degrees and 90 degrees of rotation, respectively. The embedded watermark image of the two images is scaled 1/4, and then the watermark is extracted. The results are shown in the following table:

| IMAGE | IMAGE One | IMAGE One | IMAGE One | IMAGE Two |
|-------|-----------|-----------|-----------|-----------|
| Attack type | Rotate 30° | Rotate 60° | Rotate 90° | Zoom 1/4 |
| NC value | 0.85 | 0.82 | 0.85 | 0.94 |

It can be seen from the experimental results that although the extracted watermark is not complete, it can be clearly identified visually.

3.3.4. Filter Attack. Image filtering can well protect the detailed information of the signal (edge, sharpening, etc.) while filtering out noise. We use Gaussian low-pass filtering and median filtering to process embedded watermark images, and then extract the watermark. The results are shown as below:

| IMAGE | IMAGE One | IMAGE One | IMAGE One | IMAGE Two |
|-------|-----------|-----------|-----------|-----------|
| Attack type | Gaussian low-pass filtering | Median filtering | Gaussian low-pass filtering | Median filtering |
| NC value | 0.61 | 0.65 | 0.58 | 0.64 |

Figure 8. (a) Median filtering attack on image one (b) Extracted watermark.

Figure 9. (a) Gaussian low-pass filtering attack on image two. (b) Extracted watermark image.

Figure 10. (a) Median filtering attack on image two (b) Extracted watermark.
It can be known from the experiment that although the watermark extracted in the figure is incomplete, it can be visually recognized. This shows that the algorithm has a certain resistance to the filtering process.

4. Conclusion
This paper combines the DWT digital watermarking algorithm of the human visual system HVS model in the wavelet domain and proves it through a large number of simulation experiments. The DWT algorithm used in this paper can well resist JPEG compression attacks, noise attacks, scaling attacks and rotation for digital watermark attacks, including attacks and filtering attacks. This algorithm has good robustness against various watermark attacks. Therefore, it can be concluded that the proposed algorithm is an excellent image digital watermarking algorithm with large embedding information, imperceptibility and robustness.

Acknowledgments
This work was financially supported by Guangzhou University of Chinese Medicine, grant number: A3-0433-181-427-037, Innovation and entrepreneurship education project of Education Bureau of Guangzhou Municipal, grant number:2019KC103 and Research project of innovation and entrepreneurship education reform of undergraduate colleges and universities in Guangdong Province, grant number:2018A010920.

References
[1] Hui CHEN. A Digital WATERMARKING Algorithm with High Efficiency Based on DWT and LSB[C]. Advanced Science and Industry Research Center. Proceedings of 2019 International Conference on Artificial Intelligence, Control and Automation Engineering(AICAЕ 2019),Advanced Science and Industry Research Center: Science and Engineering Research Center,2019:494-498.
[2] Podilchuk, C.I, Delp, E.J. Digital watermarking: algorithms and applications[J]. IEEE Signal Processing Magazine, 18(4):33-46.
[3] Li Haiyang. Anti-Noise Image Watermarking Processing Based on Discrete Wavelet Transform[J]. Informatization Research,2019,45(05):23-26.
[4] LIU Yan, ZHOU Li. Digital image embedding and extracting method based on wavelet transform domain[J].Journal of Shenyang University of Technology,2019,41(01):68-72.
[5] Tu Gang, Chen Zhendong, Wang Yiju. Research on an Image Digital Watermarking Algorithm[J].Bulletin of Science and Technology,2018,34(05):222-226.