Discrete wavelet transform processing system based on digital watermarking algorithm

Miao Shi*
School of Tianjin University of Technology, Tianjin, China

*Corresponding author e-mail: shimiao@tjut.edu.cn

Abstract. This paper introduces the concept of multimedia digital watermarking and summarizes the current technology status. This paper summarizes the research status and basic principle of digital watermarking. The advantages of digital watermarking algorithm based on wavelet transform are analyzed. The proposed algorithm combines Arnold scrambling method and DWT transform multi-resolution characteristics, and adopts linear and different embedding strength methods. Effectively improve the security of the watermark. According to the classification results, different intensity watermarking components are embedded into the DCT low frequency coefficients of different image blocks. Experimental results show that this algorithm has strong masking and robustness, and the watermarking realized by using the proposed algorithm has good robustness against common image processing and noise interference.

1. Introduction

1.1. Basic principle of digital watermarking algorithm
Digital watermarking is an effective supplement to solve the problem of copyright protection. It confirms the ownership of raw data by embedding secret information -- watermarks -- into the data. Mainly used in: 1) detection of illegally copied media data; 2) Identification of media ownership; 3) Anti-copy protection of media; 4) Identification of authenticity of original media. For digital images, watermarking can be divided into invisible and visible.

The basic principle of digital watermarking is to embed the watermark information as identification data into the protected host data, making the watermark in the host data imperceptible and secure. The usual watermarking algorithm includes three basic aspects: watermarking generation, embedding and extraction, and involves the selection of watermarking, watermarking verification and watermarking based on visual characteristics and other key technologies.

1.2. Generating watermark Signals can be divided into meaningless and meaningful watermark signals.
Watermark encoding can be seen as superimposing a weak signal (watermark) under a strong background (original image). As long as the superimposed signal is below the contrast sensitivity threshold, the visual system cannot detect the presence of the signal. The generation of meaningless watermark signal is usually based on the pseudo-random number generator or chaotic system, and the generated watermark signal often needs further transformation to adapt to the needs of watermark
embedding algorithm. Significant watermark signals include binary image, gray image and color image. Meaningful images can be directly embedded into the carrier data as watermarks, but in order to enhance the security of watermarks, it is generally necessary to encrypt and preprocess watermarks, including the use of M-sequence spread spectrum, bit decomposition of watermark signals and the use of scrambled images to preprocess watermarks.

From the point of view of digital communication, the embedding of watermark can be understood as adding a narrowband signal in a broadband channel with spread spectrum communication technology, which will involve the embedding method, embedding location and embedding information and other issues. Since the change of the sense-important component is more likely to affect the visual effect, some algorithms adopt a compromise method to embed the watermark in the intermediate frequency component. Wavelet watermarking embedding algorithm firstly the two-dimensional signal wavelet transform of the original image, the watermark information embedded into the high-frequency subband of wavelet decomposition can meet the requirements of concealment, but increase the decomposition level can produce very big effect to the human visual, meanwhile the watermark embedding coefficient of low frequency or high frequency coefficients are hard to satisfy both perceptual and robustness requirements. The robustness of watermark is related not only to the embedding position but also to the strength of watermark. The effective way to solve this problem is to use the visual characteristics of human eyes to achieve self-adaptation.

1.3. Watermark extraction and detection
Watermark extraction and detection is a weak signal detection problem in noisy channel, the ultimate purpose is to judge whether the watermark signal exists or to extract the watermark. From the perspective of signal processing, the robustness and invisibility of watermarks are contradictory. Orthogonal transformation methods in signals, DFT-based method and DWT-based method, are used to judge and detect the extracted and original watermarks. The watermark can be determined by output a 0 or 1 decision. If C is the correlation detection function, W is the original watermark, W’ is the extracted watermark, K is the key, and d is the decision threshold then:

\[ C(W, W', K, d) = \begin{cases} 1 & \text{Existence} \\ 0 & \text{Inexistence} \end{cases} \]

2. Based on wavelet digital watermarking algorithm
Practice shows that has a higher scan recognition accuracy in with a lower percentage of dot. In the dense area due to the expansion of the dot scan recognition rate is low, the wavelet transform will become a major technology. Because wavelet has good time-frequency characteristics, and wavelet transform is similar to some characteristics of human visual system, embedding watermarking in wavelet domain is one of the hot spots in watermarking research.

Discrete cosine transform is a global transform from image space to frequency space while discrete wavelet transform is a local transform. Using wavelet transform to decompose the original image or video sequence into multi-band sub-image can adapt to the visual characteristics of human eyes and make the watermark embedding and detection can be divided into multiple levels Wavelet transform domain digital watermarking method has the advantages of both time-space method and DCT transform domain method. The key of this method lies in its unique screening method combined with the characteristics of the printing process this screening method can be effectively used. Discrete wavelet transform is characterized by its ability of multi-scale analysis. Due to the global nature of discrete cosine transform the error of any data in the transform space will affect every pixel in the image. In the process of multi-layer net adding, the black dot at is exactly in the area with small percentage of dot. Embedding watermark information in these areas can ensure the reliability of data recovery during extraction.
2.1. Discrete wavelet transform

Digital watermarking in wavelet domain is one of the research hotspots. On the one hand, the wavelet theory itself is increasingly perfect and mature, on the other hand, the wavelet multi-resolution analysis method is increasingly widely used, especially in the field of information processing.

The definition of discrete wavelet can be expressed by the following formula:

$$\psi_{m,n}(t) = \psi\left( \frac{t-nb_0}{a_0^m} \right) \frac{1}{\sqrt{a_0^m}} \psi\left( a_0^{-m} t - nb_0 \right)$$  \hspace{1cm} (2)

Generally, $m$ is selected, where $n$ is an integer $a_0 > 1$, $b_0 > 0$. The corresponding discrete wavelet transform can be defined by the following formula

$$\langle f, \psi_{m,n} \rangle = a_0^{-m} \int_{-\infty}^{\infty} f(t) \psi\left( a_0^{-m} t - nb_0 \right) dt$$  \hspace{1cm} (3)

The reconstruction formula of $f(t)$ is:

$$f(t) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \langle f, \psi_{m,n} \rangle \psi_{m,n}(t)$$  \hspace{1cm} (4)

2.2. Watermarking encryption technology

Scrambling technology is an image encryption technology; it uses the characteristics of digital array of digital image to scramble the position or color of pixels in the image into a chaotic image so as to achieve the purpose of unrecognizable original image. Arnold transform is the most common scrambling technique; it realizes the scrambling of images by changing pixel coordinates. For images of size Arnold transform is defined as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod} N$$  \hspace{1cm} (5)

Where $(x, y)$ represents the position of a pixel of the image matrix without transformation $(x', y')$ represents the new position after transformation; mod represents the remainder operation. After the gray value is moved to position $(x', y')$, the Arnold transformation of pixel $(x, y)$ is completed.

2.3. Watermarking encryption technology

(1) The original carrier image is decomposed by two-dimensional discrete wavelet transform to obtain four subgraphs; (2) Select the appropriate watermark image to conduct Arnold scrambling transformation on binary watermark image; (3) The scrambled watermark image is decomposed by two-dimensional discrete wavelet transform to obtain four subgraphs. (4) Linear embedding is carried out for the low frequency part and high frequency part after wavelet decomposition of the original carrier image respectively with different embedding intensity values:

$$\begin{pmatrix} I_{L}' \\ I_{H}' \end{pmatrix} = \begin{pmatrix} 1 + \alpha L_w \\ 1 + \beta H_w \end{pmatrix}$$  \hspace{1cm} (6)

Where, and are the low-frequency and high-frequency parts of the decomposed image of the original carrier respectively; $I_{L}'$ is the transformed watermark part to be embedded; $\alpha$ and $\beta$ are the embedding intensity of low frequency and high frequency, respectively. And are respectively the low and high frequency parts after watermark embedding; (5) The four new wavelet coefficients are inverted by 2d discrete wavelet inverse transform to obtain the image containing watermark information.
2.4. Evaluation Criteria

Two important criteria for performance evaluation of digital watermarking algorithms are transparency and robustness. The evaluation of the transparency of the watermark can be measured by subjective observation or quantitative measurement however, it is not accurate to judge the quality change only by subjective observation in some cases, quantitative distortion detection is required. At present, the commonly used distortion detection methods mainly include: (1) The calculation formula of peak signal to noise ratio (PSNR) is as follows:

$$PSNR = 10 \log_{10} \frac{255^2}{\sum_{m=1}^{M} \sum_{n=1}^{N} (f(m,n) - f'(m,n))^2}$$  \hspace{1cm} (7)

(2) The correlation coefficient (NC) means the similarity between the original watermark and the detected watermark the calculation formula is as follows:

$$NC = \frac{\sum_{m,n} f(m,n)f(m,n)}{\sum_{m,n} f^2(m,n)}$$  \hspace{1cm} (8)

(3) Where, and respectively represent the original image and the embedded image M, and n represents the image size.

3. Experimental results and discussion

3.1. Watermark Embedding

The digital watermarking image is embedded in the specified position to observe the image, and it can be seen that the watermark image is not visible image quality has not changed. Carry out wavelet transform on the carrier image containing watermark extract the digital watermark image at the specified position observe the image and it can be seen that the digital watermark image is complete image quality changes little Calculate the correlation coefficient between extracted watermark and original watermark NC, NC = 0.9785.

3.2. Test of distortion ability against spatial geometric attack

Because the watermark image to publish attack may be limited by many ways violators may try to removed from the watermark image watermark to analyze the performance of this watermarking algorithm against attack we under several typical form of attack on the algorithm robustness analysis table 1 is the experimental results of several kinds of typical attacks figure 3 is in all kinds of typical means of attack Extract the watermark. It can be seen from the data in the table that the algorithm has strong robustness to several typical attacks and that the algorithm in this paper has certain advantages. The degree of distortion of the watermark information and the image quality of the watermark image are measured by the similarity ratio (NC) and peak signal-to-noise ratio (PSNR) The similarity ratio of an $M \times N$ image is defined as Formula (9):
\[ NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} A(i,j)B(i,j)}{\left( \sum_{i=1}^{M} \sum_{j=1}^{N} A(i,j)^2 \right)^{1/2} \left( \sum_{i=1}^{M} \sum_{j=1}^{N} B(i,j)^2 \right)^{1/2}} \]  

(9)

Where is the original binary watermark image, is the detected binary watermark image. Peak signal to noise ratio (PSNR) is defined as follows:

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

(10)

### Table 1. Similarity ratio and peak signal to noise ratio under several typical attack modes

| attack pattern       | parameter | In this paper, methods | YU method |
|----------------------|-----------|------------------------|-----------|
|                      |           | NC | PSNR/dB | NC | PSNR/dB |
| No attack            |           | 1  | 46.1411 | 1  | 39.6480 |
| unpitched sound      | gauss     | 0.001 | 0.9768 | 29.5762 | 0.9696 | 39.5325 |
|                      | impulse   | 0.005 | 0.9581 | 25.1677 | 0.9369 | 25.1543 |
|                      | mid-value | 0.003 | 0.9142 | 18.8914 | 0.8937 | 19.0183 |
|                      | norbert wiener | 0.005 | 0.9509 | 30.8686 | 0.9292 | 30.4781 |
|                      | JPEG      | 0.005 | 0.9594 | 32.3726 | 0.9652 | 32.2308 |
|                      | Compress  | 0.005 | 0.9391 | 31.0414 | 0.9017 | 30.7633 |
|                      | cut       | 0.005 | 0.9968 | 9.7531 | 0.9798 | 9.7514 |

The experimental results of the robustness test of the embedding method in this paper show that the embedding method based on wavelet multifraction decomposition is not only invisible to the digital watermark image but also has strong robustness.

### 4. Summarize

The proposed algorithm combines Arnold scrambling method with the characteristics of wavelet domain simulation experiment and robustness analysis results show that the algorithm can hide watermark information well effectively improve the security of watermarking. The robustness of digital watermarking algorithm is tested by acoustic, filtering, rotation, shearing and compression attack tests and various attack tests are analyzed and evaluated by different evaluation criteria to verify the feasibility and effectiveness of the proposed algorithm.

### Acknowledgments

Thank you for helping my teachers, classmates and parents during my writing. Your help is indispensable for me to complete my thesis. I will always bear this in mind!

### References

[1] H. M. Ozaktas D. Mendlovic. Fractional Fourier optics [J]. J. Opt. Soc. Amer. A 1995 (12): 743-751.
[2] A. W. Lohmann. Image rotation wigner rotation and the fractional Fourier transform [J]. J. Opt. Soc. 1993 (10): 2181-2186.
[3] S.-C. Pei M.-H. Yeh. A novel method for discrete fractional Fourier transform computation [J]. IEEE 2001 585-588.
[4] W.-L. Hsue S.-C. Pei. The Multiple-Parameter Discrete Fractional Fourier Transform and Its Application [J]. IEEE ICASSP2006: 416-419.