A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection

Liu Ping Feng, Liang Bin Zheng, Peng Cao
School of Information and Mechanical Engineering
Beijing Institute of Graphic Communication
Beijing, China
e-mail: lpfeng@yahoo.cn

Abstract—Digital watermark technology is used to protect the legal owner’s copyrights. We propose a blind watermarking algorithm combination of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). The watermark is scrambled by Arnold and embedded in a spread spectrum pattern using pseudo random. The block-based DCT transform of DWT LL sub-band is computed and the pseudo random sequence of the watermark bits are embedded in the mid frequency coefficients of the corresponding DCT blocks. Using DWT prior to DCT to provide better imperceptibility and higher robustness against signal processing attacks. Experimental evaluation results show that combining the two transforms improved the performance of the watermarking algorithm based solely on DCT transform.

Keywords—Arnold; spread spectrum; DWT; DCT; watermarking attacks;

I. INTRODUCTION

With the advent of digital technologies, the digital distribution through Internet is a common practice, but certain problems have risen along with it. The main problem is copyright control because piracy of digital media becomes so easy. Digital watermark technology is used to protect the legal owner’s copyrights. It is usually embedded in digital media invisible copyright watermarks, including the author signature, ownership and publication identification. The embedded watermark can be extracted and used to resolve copyright disputes. However, many image attacks have been used to sabotage the embedded watermarks. In order to protect the copyright effectively, watermarking must has a good robustness, meanwhile, without reducing imperceptibility.

The Discrete Wavelet Transform (DWT) is widely applied to image watermarking applications because of its excellent spatial localization and multi-resolution properties. In general, most of the image energy is concentrated at the lower frequency sub-bands and therefore embedding watermarks in the low frequency sub-bands could increase robustness significantly, however, may degrade the image significantly.

The block-based DCT transform segments an image non-overlapping blocks and applies DCT to each block. The watermark is embedded by modifying the mid frequency coefficients so that the visibility of the image will not be affected.

In this paper, we propose a DWT-DCT based digital watermarking algorithm that can resist various watermark attacks. Rather than embedding the watermark to the DCT mid frequency coefficients, we use a DWT beforehand. To improve the security and robustness further, the watermark is scrambled and embedded in a spread spectrum pattern.

II. DCT-DWT BASED BLIND WATERMARKING ALGORITHM

The main purpose for embedding the watermark in the transform domain is the resulting dispersion of the watermark in the spatial domain, hence it becomes very difficult to remove the watermark from the image. We combined DWT with DCT to provide the embedded watermark higher imperceptibility yet more energy.

A. Watermark generation

The embedded watermark in the algorithm is a meaningful two value image, and it is scrambled first. Watermark scrambling can eliminate pixels of spacing relativity, the robustness against image cropping operation will be improved. In addition, after the watermark processed by scrambling algorithm, even if some attacker can detect the watermark signal, he cannot recover the original watermark without the scrambling algorithm. Even if achieving the scrambling algorithm, he still does a great deal of test to recover the original watermark. In this way, the watermark security can be strengthened further[1].

Arnold transform is chosen as scrambling method for watermark signal in the algorithm because of its intuitionistic, simple, periodic and easy to use. For digital square image, discrete Arnold mapping can be done as in (1):

\[
\begin{pmatrix}
x' \\
y'
\end{pmatrix} = \begin{pmatrix}
1 & 1 \\
1 & 2
\end{pmatrix} \begin{pmatrix}
x \\
y
\end{pmatrix} \mod N
\]

\(32 \times 32\) Original watermark and scrambled one for 10 times using Arnold are showed in Figure 1. It is hard to recognize the scrambled watermark image. Because of Arnold transform of periodicity, the original image will be recovered[2].

Figure 1. Original watermark(32 x 32) and scrambled watermark
The basic idea of spread spectrum watermarking for digital image involves the addition of a pseudo random signal to the image that is below the threshold of perception and that cannot be identified and thus removed without knowledge of the parameters of the watermarking algorithm. The pseudo random signal behaves as watermark for the image[3][4]. Let \( M \) be the number of the block-based DCT mid frequency coefficients. Generate two uncorrelated pseudo random sequences by a key \( k_2: p_{n0} \) and \( p_{n1} \). Number of elements in each pseudo random sequences is equal to \( M \). To ensure watermark information well-proportioned, not affect average brightness of image, pseudo random sequence \( \{0,1\} \) is mapped to \( \{-1,1\} \), namely \( 0 \rightarrow 1, 1 \rightarrow -1 \).

To extract watermark from a host image, receiver must have the same pseudo random sequence that was used in embedding process. The secret key to generate pseudo random sequence is \( k_2 \).

**B. Watermark Embedding**

Watermarking process is started by applying the DWT to the original image, and subsequently applying the DCT to the DWT sub-bands. The watermark embedding procedure is represented in Figure 2.

1. The Original image is decomposed four bands denoted by LL, LH, HL and HH at level 1 in DWT domain. The sub-band LL represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the finescale of DWT coefficients.
2. Divide the sub-band LL into 8 x 8 blocks, and apply DCT to each block. The watermark is not applied to all block DCT values, but is applied only to the mid frequency DCT coefficients using mask shown in Figure 3.
3. Scramble the watermark signal with Arnold algorithm for \( k_1 \) times and gain the scrambled watermark. Scrambled times \( k_1 \) can be see as the secret key.
4. Embed the scrambled watermark in the mid frequency coefficients of the DCT transformed block, then embedding is done as follows:
   - If the watermark bit is 0 then
     \[ X' = X + \alpha \cdot p_{n0} \]  
   - If the watermark bit is 1 then
     \[ X' = X + \alpha \cdot p_{n1} \]

   \( \alpha \) is the intensity factor of embedded.

1. Perform inverse DCT on each block after its mid frequency coefficients have been modified to embed the watermark bits.
2. Perform the inverse DWT on the DWT transformed image, including the modified coefficient sets, to produce the watermarked host image.

**C. Watermark Extraction**

The combined DWT-DCT algorithm is a blind watermarking algorithm and thus the watermark could be extracted without the original host image. The extraction procedure is described as follows.

1. Apply DWT to decompose the watermarked image into four non-overlapping sub-bands: LL, LH, HL, and HH.
2. Divide the sub-band LL into 8x8 blocks, and apply DCT to each block.
3. Extract the mid frequency coefficients of each DCT transformed block, and calculate the correlation between the mid frequency coefficients and the pseudo random sequences \( p_{n0} \) and \( p_{n1} \). If the correlation with the \( p_{n0} \) was higher than the correlation with \( p_{n1} \), then the extracted watermark bit is considered 0, otherwise the extracted watermark bit is considered 1.
4. Reconstruct the scrambled watermark using the extracted watermark bits, and then recover the watermark with Arnold algorithm from the scrambled watermark using \( k_2 \).

**III. EXPERIMENTAL EVALUATION RESULTS**

We program the DWT-DCT watermarking algorithm above using MATLAB 2008a, and then the watermarked image is tested with some typical attacks such as Gaussian white noise, median filtering, cropping, resizing, and JPEG compression. The test image is a 512 x 512 gray image ‘lena.bmp’ shown in Figure 4, and watermark is a 32 x 32 binary image shown in Figure 1. We use \( \alpha = 10 \) for the intensity factor of embedded watermark.

To determine the degradation of the original image, we use the peak signal to noise ratio PSNR. PSNR presents the...
distortion caused by the watermarking. PSNR is defined using the following equation:

\[ PSNR = 10 \log_{10} \left( \frac{X^2}{MSE} \right) \]  

(4)

In the previous equation (4), \( X \) is the maximum fluctuation in the images. \( MSE \) is the mean square error and defined as in (5):

\[ MSE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (I_i - I'_i)^2}{MN} \]  

(5)

Where \( I \) and \( I' \) are the original and the watermarked one, respectively. The image is not influenced when \( PSNR > 30dB \) [5].

We measured the similarity between the original watermark and the extracted watermark using the correlation factor \( sim \) given below [6]:

\[ sim = \frac{\sum_{i=1}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2 \sum_{i=1}^{N} \hat{w}_i^2}} \]  

(6)

Where \( N \) is the number of pixels in watermark, \( w \) and \( \hat{w} \) are the original and extracted watermarks respectively. The correlation factor \( sim \) may take values between 0 to 1. If exact matches occur, then \( sim = 1 \).

Figure 5 (a) shows the watermarked image and extracted watermark where no attack done. The watermarked image has PSNR=37.7160dB, and there is no distinct differences between these two images in vision impression. Similarity between original watermark and extracted watermark is 0.9906.

We have tested robustness of the proposed scheme against various attacks using common image processing. The first attack applied is Gaussian white noise of mean zero and variance 0.01 to the watermarked image. The second attack is median filtering of the watermarked image using 3-by-3. The third attack is cropping 25% of watermarked image. The forth attack is resizing from size to 1/2 and then to 2. The fifth attack is JPEG compression, and the Quality of the JPEG compression is 50%. Figure 5 (b) –(f) shows the extracted watermarks for DCT only based algorithm after applying the same attacks above respectively, and the parameter (e.g. the DCT block size, the intensity factor, etc.) is the same as above.

The watermarked image using the DCT only based algorithm has PSNR=31.6954dB where no attack done, and it is shown in Figure 6(a). The PSNR value of the DWT-DCT based algorithm is 37.7160dB forenamed, and is better than of the DCT only based algorithms. This indicates that improvement in imperceptibility can be achieved by applying DCT on a DWT transformed LL sub-band. Figure 6(b)–(f) shows the extracted watermarks for DCT only based algorithm after applying the same attacks above respectively, and the parameter (e.g. the DCT block size, the

Figure 6. Watermarked image and extracted watermark using DCT only based algorithm

The correlation factor values \( sim \) given in Figure 5 and Figure 6 show clearly that DWT-DCT based algorithm outperforms DCT only based algorithm with respect to robustness against the median filtering, cropping, resizing and JPEG compression attacks.

As illustrated in Figure 5(f) and Figure 6(f), the extracted watermark cannot be recognized under JPEG compress with 50% Quality using DCT only based algorithm, while it is well done using DWT-DCT based algorithm. Experiments evaluation results show that the extracted watermark cannot be recognized using DCT only based algorithm under JPEG compression lower than 75% Quality. But using DWT-DCT based algorithm proposed, the extracted watermark can be identified above 20% Quality. This is due to the fact that the DCT is the core component of the JPEG compression [6], and therefore applying DCT only at a whole image degraded the quality of the embedded watermark greatly.

IV. CONCLUSION

In this paper, we have proposed a DWT-DCT based blind watermarking algorithm for copyright protection. The combination of the two transforms improved the watermarking performance compared to DCT only watermarking approach. And the watermark is scrambled and embedded in a spread spectrum pattern to improve the security and robustness further. Experiment evaluation results show that the proposed algorithm is robust against typical attacks such as Gaussian white noise, median filtering, cropping, resizing, JPEG compression, and the imperceptibility of the watermarked image is acceptable.

ACKNOWLEDGMENT

This paper is supported by Scientific Research Common Program of Beijing Municipal Commission of Education, No.KM200710015011; Talent Recommended Foundation of
REFERENCES


