WAVELET-BASED WATERMARKING FOR DIGITAL IMAGES

Prapon Rakpratanporn, Punya Thitimajshima, and Yuttapon Rangsanseri

Department of Telecommunications Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
Tel: (66-2)326-9967, Fax: (66-2)326-9086
Email: ktpunya@kmitl.ac.th, kryutta@kmitl.ac.th

ABSTRACT

In this paper, we propose a method of digital image watermarking using discrete wavelet transform. The watermark, generated by pseudo-random sequence is added to all high-frequency coefficients that are above a given threshold. By comparing the correlation between the wavelet coefficients of a possibly corrupted watermarked image and the watermark with a threshold, the embedded watermark can be detected. Experimental results are given to illustrate the robustness against smoothing, cropping, and JPEG compression.

1. INTRODUCTION

The growth of high-speed computer networks and that of the Internet has become the part of the future business communication. Since the digital information can be easily duplicated and distributed, the intellectual property of the sensitive or critical digital information is an important issue for copyright protection. One approach to protect multimedia data is called digital watermarking. Digital watermarking is the imperceptible marking of multimedia data to "brand" ownership.

In order to be effective, an imperceptible watermark should meet the following requirements [1].

Unobtrusiveness: The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

Unambiguousness: Retrieval of it should unambiguously prove the identity of the data owner.

Readily extractable: The data owner or an independent control authority should easily extract it.

Robustness: The watermark must be difficult to remove for an attacker trying to counterfeit the copyright of the data.

Image watermarking techniques proposed in the literature can be classified into two categories: spatial domain approach [2] or transform domain approach [1,3,4,5]. The spatial domain watermarking scheme is generally fast and simple, but it doesn't guarantee that the watermarking would be robust against noises and JPEG compression as the transform domain methods. Many schemes have found that the transform domain approach has some advantages because most of the signal processing operations can be well characterized in the frequency domain, and several good perceptual models are developed in the frequency domain.

In this paper, we propose a technique in frequency domain approach based on wavelet transform that does not requires the original image for watermark detection. Furthermore, the robustness of the watermarking will be analyzed. Finally, we will investigate the limitations of the watermarking techniques and discuss further research issues.
2. THE PROPOSED ALGORITHM

The overall of the watermarking process consists of two main steps: watermark insertion and watermark detection.

2.1 Watermark Insertion

Figure 1 shows a block diagram of the watermark insertion process. First, the original image \( I \) is decomposed by using discrete wavelet transform (DWT) until the scale \( N \). We obtain multiresolution representation (MRR) \( LH_n, HL_n, HH_n \) (\( n = 1,2,\ldots, N \)) and multiresolution approximation (MRA) \( LL_N \). We leave out the low pass sub-band \( (LL_N) \) and pick all coefficients in the other sub-bands which are above a given threshold \( (T_i) \). The watermark \( X \) is a matrix of the same dimension as the image, and the elements \( x_i \) are given by the pseudo random sequence whose probability law has a uniform distribution of zero mean and unit variance. The watermark is inserted into the image by:

\[
V'_i = V_i + \alpha |V_i|x_i
\]  

(1)

where \( i \) runs over all DWT coefficients whose magnitude is greater than a threshold \( T_1 \). \( V_i \) and \( V'_i \) denote respectively the DWT coefficient of the original and watermarked image and \( \alpha \) is a scaling parameter. Finally, we reconstruct the watermarked image \( I' \) using the inverse DWT.

2.2 Watermark Detection

Figure 2 shows the overall process of watermark detection. The detection process is composed of DWT of watermarked image. We choose all the high-pass coefficients above \( T_2 > T_1 \) and correlate them with the original copy of the watermark. We use \( T_2 = 50 \) and \( T_1 = 40 \) [5] \( (T_1 \) is the threshold used for watermark insertion). \( T_2 \geq T_1 \) is necessary because we should not compute correlation over coefficients to which we have not added any watermark. We choose \( T_2 \) to be strictly larger than \( T_1 \) for robustness since some coefficients, which were originally below \( T_1 \), may become greater than \( T_1 \) due to image manipulation.

![Figure 1 Watermark insertion process.](image1)

![Figure 2 Watermark detection process.](image2)
We calculate the correlation $z$ between the DWT coefficients of the corrupted watermarked image and a possibly different watermark $Y$ is computed as:

$$z = \frac{1}{M} \sum_{i} |\tilde{v}_i| y_i$$  \hspace{1cm} (2)

If the similarity value is greater than a threshold value $S$ in equation (3), it is possible to determine whether a given watermark is present.

$$S = \frac{a}{2M} \sum_{i} |\tilde{v}_i|$$  \hspace{1cm} (3)

where $M$ is the number of coefficients where the watermark is inserted.

Figure 3 Experimental results on Lena image. (a) Original image. (b) Watermarked image. (c) Absolute difference between the original image and the watermarked image. (d) Detector response of the detector to 1000 randomly generated watermarks.
3. EXPERIMENTAL RESULTS

Figure 3(a) shows the original "Lena" image and Figure 3(b) shows the watermarked image with the parameter $\alpha = 0.2$, the wavelet filter used is Daubechies 8 taps with $N = 3$. We can see that the watermark image is not distinguishable from the original image. Figure 3(c) illustrates the absolute value of difference between the original image and the watermarked image. We see that most of the watermark is added in edge regions of the image. Figure 3(d) shows the response $z$ of the watermark detector to 1000 randomly generated watermarks. The dotted line showed the threshold $S$, we find that the positive response to the correct watermark is much stronger than the response to incorrect watermarks.

The robustness capability is very critical for watermark. We tested the robustness

(a)  

(b)  

Figure 4 Attack by filtering. (a) Watermarked image smoothed with a 3x3 median filter. (b) Corresponding detector response.

(a)  

(b)  

Figure 5 Attack by cropping. (a) Watermarked image after cropping. (b) Corresponding detector response.
of the watermarking with some attacks such as median filtering, cropping, and JPEG compression. Figures 4 and 5 show the results of watermark detection after smoothing with 3x3 median filter and 50% cropping respectively. The robustness against JPEG compression is illustrated in Figure 6 and 7 when the watermarked image was compressed with quality factors of 10% and 50% respectively. In all cases the detector responses are still well above the threshold.

4. CONCLUSIONS
We have presented a wavelet-based watermarking for digital image. We found that the DWT-based watermarking technique can be used to embed information into the image and does not require the original image for watermarking detection. The watermark is still robust under several attacks such as compressing, smoothing and cropping. Furthermore, we will investigate the tolerance of the other attack, such as D/A and A/D conversion.
REFERENCES


