BLIND WATERMARKING USING WAVELET TREE QUANTIZATION*

Shih-Hao Wang[1] *and Yuan-Pei Lin*[2**]

[1]Dept. of Electronics Engr., National Chiao Tung Univ., Taiwan
[2]Dept. of Electrical and Control Engr., National Chiao Tung Univ., Taiwan
**E-mail : ypl@cc.nctu.edu.tw

ABSTRACT

This paper proposes a blind watermarking scheme using wavelet tree quantization. The wavelet coefficients of the host image are grouped into wavelet trees and each watermark bit is embedded using two trees. The trees are so quantized that they exhibit a large enough statistical difference, which will later be used for watermark extraction. Each watermark bit is embedded in all frequency bands, which renders the mark more resistant to attacks that remove certain frequency components. Also, the embedding is spread throughout a relatively large spatial region, which yields more robustness against spatial domain geometric attacks. Examples of various attacks will be given to demonstrate the robustness of the proposed technique.

1. INTRODUCTION

There are several important issues in watermarking systems, including visual distortion, robustness, the access of original data, etc. For the application of copyright protection, very high level of robustness is essential. A watermarking technique is referred to as *private* if the extraction of watermark requires the original image. It is *blind* if the original image is not needed for extraction. When the original data is not easy to obtain, or when we do not know which copy is the original one, it is necessary to use blind watermarking. It is demonstrated in [1] that blind watermarking is necessary for resolving rightful ownership. Two crucial requirements for watermark detection are proposed in [1]. First, a registered ID or a meaningful signature should be used as a valid secret key. The other is the adoption of a certified one-way deterministic host function to map the valid key to a pseudo-random sequence. The detection confidence is quantified based on the measure of false positive detection probability.

In previous works, Langelaar *et al.* [2] proposed a blind method called differential energy watermarking. A macroblock which consists of DCT blocks is divided into 2 parts to embed a watermark bit. High frequency DCT coefficients in the compressed bit stream are selectively discarded to produce an energy difference in the two parts of the same macroblock. In [3], the authors proposed an image-adaptive watermarking scheme by incorporating a visual model for embedding perceptually invisible watermark with according to the characteristics of the host image. In [4], watermark is embedded in wavelet coefficients. Each watermark bit is embedded by quantizing a single wavelet coefficient out of a set of coefficients corresponding to a particular spatial region. In [5], the authors use the so called scalar Costa scheme for blind watermarking. The watermark bit is used to generate a dither for uniform scalar quantization of most image and the watermark is embedded by adding the scaled quantization noise back to the host. In [6], complementary modulation rules, positive and negative modulation, are applied on wavelet coefficients for watermark embedding. If the attack causes "negative" distortion, the positive one will survive, and vice versa. Superior performance over existing blind schemes is demonstrated.

In this paper, we propose a new wavelet tree based blind watermarking scheme. The wavelet coefficients of the host image are grouped into wavelet trees. Each watermark bit is embedded using two wavelet trees. The trees are so quantized that they exhibit a large enough statistical difference, which will later be used for watermark extraction. A binary decision is made based on the extracted watermark to prove ownership, and false positive detection probability is used to quantify the detection confidence. As the tree marking technique spreads the watermark throughout the low to high frequency part of wavelet trees, it will be more resistant against attacks that remove certain frequency components. Furthermore, the tree marking approach is based on wavelet trees which encompass a relatively large spatial region and yield more robustness against geometric attacks, such as pixel shifting up to 12 pixels, global rotation up to 1 degree and StirMark [7]. The proposed tree quantization watermarking technique is also resistant against various common attacks as will be demonstrated in the examples.

2. TREE QUANTIZATION WATERMARKING

In the proposed tree watermarking scheme, the host image is transformed into wavelet coefficients using DWT (discrete wavelet transform). The wavelet coefficients are grouped into wavelet trees. The watermark sequence W is a binary PN (+1 and -1) sequence of watermark bits, and $W=\{w_m\}$ for $m = 1, 2, ..., N_w$, where N_w is the length of watermark.

*This work is supported by NSC 90-2213-E-009-108, Taiwan, R.O.C.

0-7803-7304-9/02/$17.00 C2002 IEEE

The sequence can be generated by mapping a meaningful signature or text through a certified one-way deterministic function [1]. Each watermark bit is embedded using two randomly chosen wavelet trees. Depending on the value of the watermark bit, one of the two trees is quantized with respect to a quantization index. The index is such that the two trees exhibit a large enough statistical difference, which will later be extracted for the decision of the underlying watermark bit. After the decoder, the extracted watermark sequence W^e is compared with the stored watermark sequence W. We will compute the normalized correlation between the stored watermark W and the extracted one W^e. If the correlation is above a chosen threshold, we determine that the watermark exists. The choice of threshold depends on the desired false positive probability as we will see later.

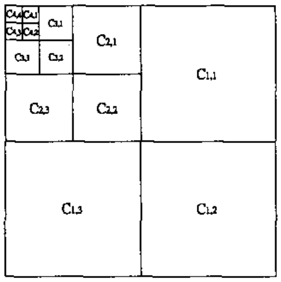

Figure 1: Wavelet decomposition and its subbands.

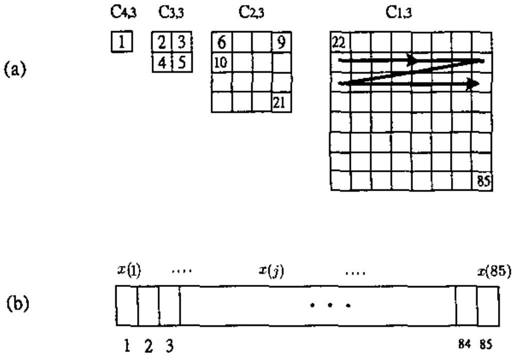

Figure 2: (a) The 85 coefficients of a wavelet tree; (b) ordered coefficients of the a wavelet tree.

2.1. Watermark insertion

For convenience, we will use 4-level wavelet transform of a 512×512 image as an example. With 4-level decomposition, we have 13 subbands as shown in Fig. 1. The coefficients are grouped according to wavelet trees except the coefficients of LL band ($C_{4,4}$). We will use the coefficients in subband $C_{4,1}$, $C_{4,2}$, $C_{4,3}$ as roots to form wavelet trees. At the forth level, the subbands, $C_{4,1}$, $C_{4,2}$, $C_{4,3}$ have 32^2 coefficients, and there are total $3 \times 32^2 = 3072$ trees. Each tree consists of 1+4+16+64=85 coefficients as shown in Fig. 2(a). The coefficients are in the order of parent to children. For coefficients in the subbands of the same level, a raster scanning order is followed as shown in Fig. 2(a). The j-th coefficient of a tree is denoted by

$$x(j), \quad 1 \leq j \leq 85$$

We can obtain the binary representation of the 85 coefficients in each tree. With the coefficients expressed in binary representation, the bits of the coefficients form a two dimensional array as shown in Fig. 3, each entry equal to 0 or 1. The most significant bitplane (MSB) is denoted by $2^{p_{max}}$, and the least significant bitplane (LSB) is denoted by $2^{p_{min}}$. Excluding the sign bit, there are total N_p bits where

$$N_p = 85(p_{max} - p_{min} + 1).$$

We order these bits using a raster scan of the two-dimensional array in Fig. 3, left to right, and top to bottom.

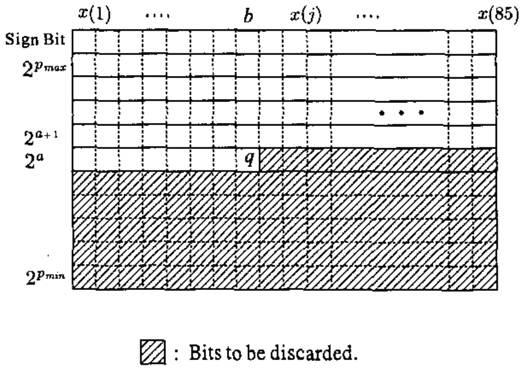

Figure 3: A tree quantization with respect to a quantization index q.

For a watermark sequence W of N_w bits, the embedding of each bit is performed independently. It suffices to explain the encoding of one bit; a sequence of N_w watermark bits can be encoded by repeating the procedure N_w times. For each bit w to be embedded, we choose 2 trees, say tree A and tree B, $1 \leq A, B \leq 3072$ in a pseudo random manner known to the encoder and the decoder. One of tree A or tree B will be quantized depending the watermark bit to be embedded. We discuss the quantization of a tree next.

Tree quantization. Let us consider the quantization of a tree with respect to a given quantization index q, with $1 \leq q \leq N_p$. The choice of q will be discussed later. The coordinate of q in the tree array is (a, b) as shown in Fig. 3. All the bits after the quantization index will be discarded. The discarded bits are shown as shaded area in Fig. 3. After the quantization, the LSB of the j-th coefficient becomes 2^{a-1} if $j \leq b$ and the LSB of the j-th coefficient become 2^a if $j > b$. Let $round(x)_i$ denote the rounding of a number x to the 2^i bitplane. The quantization of $x(j)$ with respect to q, denoted by $Q\left(x\left(j\right)\right)_q$, is given by

$$Q\left(x\left(j\right)\right)_q = \begin{cases} round(x(j))_a, & \text{if } j \leq b \\ round(x(j))_{a+1}, & \text{otherwise} \end{cases} \quad (1)$$

Then, the quantization error of the tree with respect to the quantization index q is,

$$\mathcal{E}\left(q\right) = \sum_{j=1}^{85} \left| \, Q\left(x\left(j\right)\right)_q - x\left(j\right) \, \right|$$

If $w = -1$, tree A is quantized with respect to q. If $w = +1$, tree B is quantized with respect to q. The quantized index q is chosen in the following manner. It is the index such that $\mathcal{E}_A\left(q\right) \geq \mathcal{E}_0$ and $\mathcal{E}_B\left(q\right) \geq \mathcal{E}_0$ where $\mathcal{E}_0$ is an appropriately chosen quantity called reference error. As two trees are used for embedding one bit, the maximum number of bits that can be embedded is half of the total number of trees 3072, i.e. 1536 bits.

2.2. Watermark extraction and detection

As each watermark bit is encoded independently, each bit is decoded independently. For each watermark bit to be extracted, the two corresponding wavelet trees are inspected. We examine which one is statistically more similar to a quantized tree. When we determine which tree was quantized earlier in the embedding process, the sign of the watermark bit is determined accordingly. Even when the images are attacked, the coefficient of the trees bearing the watermark are more likely to be close to the quantized value given in eq. (1). For example, suppose in embedding process $w = -1$ and the coefficients of A are quantized with respect to q. All the coefficients in A will be replaced with the quantized value $Q\left(x\left(j\right)\right)_q$. The coefficients in tree B will be more uniformly distributed. Therefore, tree A will have more coefficients close to the quantized values than tree B. Conversely, if $w = 1$ and the coefficients of B are quantized, then tree B will have more coefficients close to quantized value than A. Therefore the quantized and unquantized trees have a statistical difference.

For the decoding of a watermark bit w, we find the largest quantization index q^e such that $\mathcal{E}_A\left(q^e\right) \geq \mathcal{E}_0^e$ or $\mathcal{E}_B\left(q^e\right) \geq \mathcal{E}_0^e$, where $\mathcal{E}_0^e$ is the reference error for extraction. Let the coordinate of q^e be (a^e, b^e). For each watermark bit embedded in tree A and B, we determine which one is a quantized tree with respect to q^e. In particular, a coefficient $x^e(j)$ is a watermark coefficient if

$$\left| x_m^e(j) - Q\left(x^e(j)\right)_{q^e} \right| \leq \begin{cases} 2^{(a^e-1)}, & \text{if } j \leq b^e \\ 2^{(a^e)}, & \text{otherwise} \end{cases}$$

We use majority rule in the decision of each watermark bit. We count the number of watermark coefficients in tree A and B. Let the number be respectively N_A and N_B. We determine the extracted bit w^e by comparing the number of quantized coefficients in A and B.

$$Q\left(w^e\left(j\right)\right)_q = \begin{cases} -1, & \text{if } N_A(q^e) > N_B(q^e) \\ +1, & \text{otherwise} \end{cases}$$

For the application of copyright protection and proof of ownership, a binary decision is made based on the extracted watermark sequence W^e and the owner's watermark sequence W. We use the normalized correlation coefficient to quantify the correlation between the original watermark and the extracted one:

$$\rho\left(W, W^e\right) = \frac{\sum\limits_{m=1}^{N_w} w_m w_m^e}{N_w},$$

We choose a threshold ρ_T. The existence decision is "Yes" if $\rho\left(W, W^e\right) \geq \rho_T$ and "No" if $\rho\left(W, W^e\right) < \rho_T$. Let $P_E = Prob\left(w_m \neq w_m^e\right)$, using this expression the probability of false positive error P_{fp} can be computed by[4],

$$P_{fp} = \sum_{k=\frac{\rho_T+1}{2}N_w}^{N_w} \binom{N_w}{k} P_E^{N_w-k}\left(1 - P_E\right)^k$$

Consider the case $N_w = 1536$ as in our 4 level wavelet decomposition of a 512×512 image. For $\rho_T = 0.1$, 0.15, and 0.2, the corresponding P_{pf} is respectively 4.67×10^{-5}, 1.76×10^{-9}, 1.93×10^{-15}.

Remarks.

The idea of embedding watermark in statistical difference between wavelet trees is in essence similar to differential energy watermarking [2] in the sense that both detection rely on the statistical difference of groups of coefficients in the frequency domain. However there are important differences. In [3], high frequency components in DCT blocks are removed and the statistical difference lies in the tail energy of the DCT blocks. In tree marking, the statistical difference lies in the least significant bits of the trees. The watermark is embedded in wavelet coefficients of all frequency bands throughout the spatial region corresponding to the tree. The tree marking technique has more robustness against attacks that remove certain frequency components and also geometric attacks.

3. EXPERIMENT RESULTS

The 512 × 512 image *Lenna* is used for our experiments. We use 4-level wavelet decomposition and a watermark sequence of length 1024. For watermark length equal to 1024, the correlation threshold ρ_T is chosen to be 0.17 for a false positive probability P_{fp}=2.11x10^{-8} [4]. The watermarked image in this example has PSNR=38.9dB which is suggested in [7] for a quality if no perceptually visible artifacts. A different PSNR may be chosen for different applications. We consider both non-geometric and geometric attacks. For non-geometric attacks, JPEG is one of the most used compression technique, and is often an unintentional attack. Quality factor of 40, 50, 70, 90 are used, and the results are shown in Table 1(a). The proposed methods can detect the existence of watermark for quality factor greater than 40. Usually for images with quality factor smaller than 40, there are visible artifacts. Even if the detector fails to confirm the existence of the watermark, it is apparent that the image has been distorted. The results of attacks using SPIHT compression are shown in Table 1(b). For other non-geometric attacks, including linear and nonlinear filtering the results are given in Table 1(c). The watermark survives all these attacks. For geometric attacks, rotation or pixel shifting are often taken into consideration. This attack of rotation is performed by rotating the image by a small angle, scaling the rotated image, and cropping the scaled image to the original image size [7]. The results given in Table 1(d) can resist rotation up to 1 degree. The pixel shifting attack is applied by circular shift to the column of the image. The results shown in Table 1(e) can resist pixel shifting up to 12 pixels. Combination of these attacks, like StirMark are proven to be very effective for confusing watermark detectors [7]. When the attack of StirMark with random bending [7] is used, the proposed watermark also survives as listed in Table 1(c).

4. CONCLUSION

In this paper, we proposed a wavelet based watermarking technique by quantizing wavelet trees. The tree marking method embed each watermark bit in all frequency bands of a particular tree and the information of the watermark bit is spread throughout a relatively large spatial region. As a result, the tree marking technique is robust to attacks in both frequency and time domains. The results in this paper demonstrate that, it is robust to frequency based attacks, for example removal of highpass band in the lowpass processing and removal of highpass details in JPEG compression. It is also robust to time domain attacks such as pixel shifting and StirMark with random bending.

5. REFERENCES

[1] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Transactions on Image Processing*, vol. 8, pp. 1534-1548, Nov. 1999.

[2] Gerrit C. Langelaar and Reginnald L. Langendijk, "Optimal differential energy watermarking of DCT encoded images and video,"*IEEE Transactions on Image Processing*, vol. 10, pp. 148-158, Jan. 2001.

[3] C.I. Podilchuk, W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Comm.*, vol. 12, pp. 525-539, May 1998.

[4] D. Kundur and D. Hatzinakos, "Digital watermarking, using multiresolution wavelet decomposition," *Proc. IEEE ICASSP*, vol. 5, pp. 2969-2972, 1998.

[5] J.J. Eggers, J.K. Su, and B. Girod, "Robustness of a blind image watermarking scheme," *Proc. IEEE ICIP* , pp. 17-20, Sep. 2000.

[6] C.S. Lu, S.K. Huang, C.J. Sze, and H.Y. Liao, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, vol. 2, pp. 209-224, Dec. 2000.

[7] F.A.P. Petitcolas, "Weakness of existing watermark scheme," October, 1997. http://www.cl.cam.ac.uk/~fapp2/watermarking/image-watermarking.

JPEG	40	50	70	90
ρ	0.20	0.26	0.43	0.98

(a)

Bitrate	0.5	0.6	0.7
ρ	0.19	0.23	0.4

(b)

Attack	Median filter (2x2)	Median filter (3x3)	Median filter (4x4)	Gaussian filter
ρ	0.30	0.34	0.23	0.33
Attack	StirMark with bending	Histogram Equalizatio	Histogram stretching	Sharpening
ρ	0.18	0.91	0.97	0.38

(c)

Rotation	0.5	0.75	1.0	-0.5	-0.75	-1.0
ρ	0.31	0.25	0.21	0.28	0.24	0.20

Rotation Unit : degree(+ : clockwise, - : counterclockwise)

(d)

Pixel shif	7	8	9	10	11	12
ρ	0.29	0.47	0.25	0.37	0.17	0.26

(e)

Table 1: Correlation coefficient ρ and watermark existence upon attacks: (a)JPEG compression with quality factor 40, 50, 70, 90; (b)SPIHT compression with bitrate 0.5-0.7; (c)Median filter (2x2, 3x3, 4x4), Gaussian filtering, StirMark with random bending, histogram equalization and stretching, sharpening; (d)Rotation followed by scaling and cropping to the original size (e)Circular pixel shifting.