行政院國家科學委員會專題研究計畫　成果報告

著作權保護小波樹浮水印(2/2)

計畫類別：個別型計畫
計畫編號：NSC94-2213-E-009-038-
執行期間：94 年 08 月 01 日至 95 年 08 月 31 日
執行單位：國立交通大學電機與控制工程學系(所)

計畫主持人：林源倍

報告類型：完整報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 95 年 8 月 10 日

行政院國家科學委員會專題研究計畫成果報告

著作權保護小波樹浮水印
Wavelet Tree Quantization for Copyright Protection Watermarking
計畫編號：NSC 93-2213-E-009-115-
執行期限：93年8月1日至95年7月31日

主持人：林源倍　國立交通大學電機與控制工程學系
email: ypl@mail.nctu.edu.tw

1 摘要

We proposed a blind watermarking scheme using wavelet tree quantization. With the use of wavelet trees, each watermark bit is embedded in all frequency bands. The wavelet coefficients of the host image are grouped into wavelet trees and each watermark bit is embedded using two trees. Each watermark bit is embedded in perceptually important frequency bands, which renders the mark more resistant to frequency based attacks. Also, the watermark is spread throughout large spatial regions. This yields more robustness against time domain geometric attacks. Examples of various attacks will be given to demonstrate the robustness of the proposed technique.

Keywords: wavelet tree, watermark, copyright protection

2 緣由與目的

There has been great interest in applying watermarks to digital multimedia data for copyright protection, copy protection, image authentication, proof of ownership, etc. Watermarking techniques apply minor modifications to the original data in a perceptually invisible or almost invisible manner with the modifications bearing the watermark information. By detecting the existence of these modifications, we can prove the ownership and even trace an illegal copy source.

The idea of using spread spectrum for embedding watermarks in the DCT domain is proposed in [3], Cox *et al.*. The watermark is embedded in the spectrum that is perceptually important. The watermark can not be destroyed without damaging the watermarked image. It is not a blind watermarking scheme as the original image is required for watermark extraction. The spread spectrum method can be generalized to embed watermarks in wavelet coefficients for images as well as video [4].

In [5], a method called differential energy watermarking (DEW) is proposed by Langelaar and Langendijk. A macroblock which composes of several 8×8 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. This scheme has three parameters: the number of 8×8 DCT blocks in a macroblock, JPEG quantization stepsize, and a minimal cutoff index for watermarking. By ad-

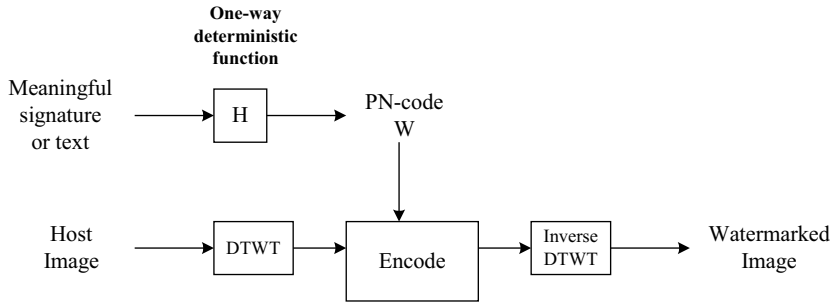

圖 1: Block diagram of the proposed encoder.

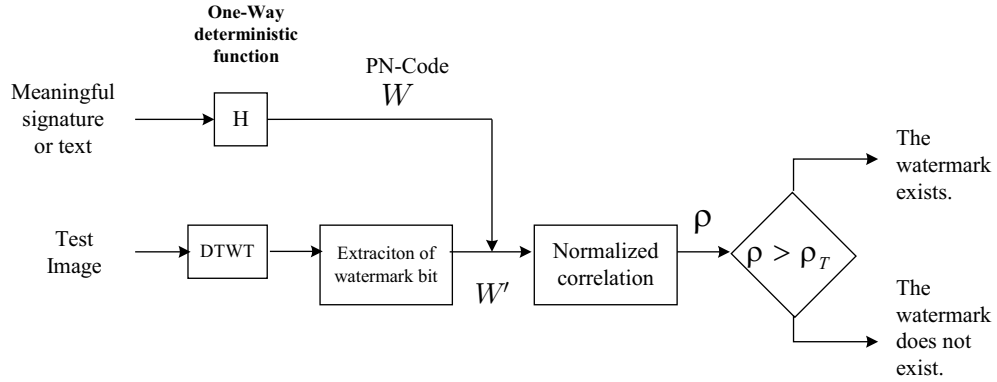

圖 2: Block diagram of the proposed decoder.

justing the three factors, appropriate marking systems are obtained for different applications. This method performs well in attacks such as pixel shifting and StirMark [6, 7]. As the embedding process is done in the compressed domain, it can also be applied in real-time processing.

We proposed a wavelet based watermarking scheme for the application of copyright protection. In the application of copyright protection, a watermark is embedded in a host image using a watermark encoder. The watermark can later be extracted using a watermark decoder to prove ownership. The watermark decoder gives a binary decision on the existence of the watermark by comparing the extracted watermark and the owner's watermark. In addition, for the watermarking scheme to be useful, the method should be a blind one, meaning the original image is not used in the watermark extraction process.

We will use the tree marking technique to embed watermark bits in wavelet coefficients based on their perceptual importance. When the attacked image is so that there are clearly distortions, there is no need resorting to watermarks to show ownership. As the tree marking approach is based on wavelet trees, which encompass large spatial areas, more robustness against geometric attacks such as pixel shifting and image rotation can be expected. We will investigate the embedding of watermark bits by quantizing wavelet trees. The trees should be so quantized that they exhibit a large enough statistical difference. The resulting difference between quantized and unquantized trees will

allow for watermark extraction at a later time.

3 結果與討論:

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. Fig. 1 illustrates the embedding procedure. The watermark W is a binary PN sequence of ± 1. The seed of the sequence can be generated by mapping a meaningful signature or text through a certified one-way deterministic function [2]. Fig. 2 illustrates the extraction procedure. After a watermark W' is extracted, it is compared with the owner's watermark W, and a normalized correlation coefficient between the stored watermark W and the extracted one W' is computed. If the correlation is above a chosen threshold, we determine that the watermark exists. The choice of the threshold depends on the desired false positive probability. In particular the normalized correlation coefficient that quantifies the correlation between the original watermark and the extracted one is,

$$\rho\left(W, W'\right) = \frac{\sum_{m=1}^{N_w} w_m w'_m}{\sqrt{\sum_{m=1}^{N_w} w_m^2 \sum_m w_m'^2}},$$

where N_w is the number of watermark bit embedded. The coefficient is bounded by $-1 \leq \rho\left(W, W'\right) \leq 1$. Since the watermark is a binary sequence of ± 1, we have

$$\sum_{m=1}^{N_w} w_m^2 = \sum_{m=1}^{N_w} (w'_m)^2 = N_w$$

The normalized correlation coefficient can also be written as

$$\rho\left(W, W'\right) = \frac{\sum_m w_m w'_m}{N_w} \qquad (1)$$

We choose a threshold ρ_T. The existence decision is "Yes" if $\rho\left(W, W'\right) \geq \rho_T$ and "No" if $\rho\left(W, W'\right) < \rho_T$.

Let $P_E = Prob\left(w_m \neq w'_m\right)$. Using this expression the probability of false positive error P_{fp} can be computed by [**?**],

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

The false positive probability depends on P_E, N_w, and ρ_T. In the case that the underlying image is not a watermarked copy, it is reasonable to assume $P_E = 0.5$. Let $N_w = 768$. For $\rho_T = 0.15$, 0.20, and 0.25, the corresponding P_{fp} is respectively 1.61×10^{-5}, 1.5×10^{-8}, 2.14×10^{-12}. Given a false positive probability, we can choose an appropriate ρ_T to meet the requirement.

For the convenience of illustration, we will use a discrete time wavelet transform of 4 levels (see [9] and the references therein for details of wavelet transforms). A 512×512 image will be used as an example. With a 4-level decomposition (Fig. 3(a)), we have 13 frequency bands as shown in Fig. 3(b). We will use the coefficients in bands labeled as $C_{i,j}$ in Fig. 3(b) for watermarking. The coefficients in high frequency bands are not used as they often contain little energy. If we place the 13 subband images in their corresponding slots in Fig. 3(b), we get a 512×512 array of wavelet coefficients in Fig. 4. We group the coefficients corresponding to the same spatial location together (Fig. 4). Fig. 5(a) shows an example of a group with one coefficient from $C_{4,3}$, 4 coefficients from $C_{3,3}$ and 16 coefficients from $C_{2,3}$. There are 21 coefficients in each group. Coefficients of the same group correspond to various frequency bands of the same spatial location. The total number of groups is equal to the number of coefficients in $C_{4,1}$, $C_{4,2}$ and $C_{4,3}$, each of which has 32^2 coefficients. There are a total of $3 \times 32^2 = 3072$ groups. We order the groups in a pseudo-random manner. A pseudo-

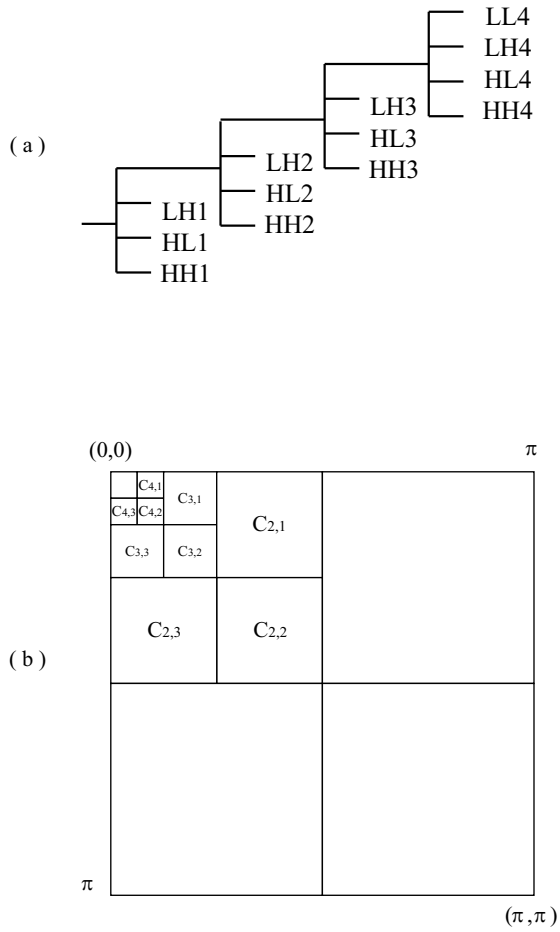

圖 3: (a) A four-level wavelet decomposition and the resulting 13 subbands; (b) the 13 frequency bands corresponding to the subbands in (a).

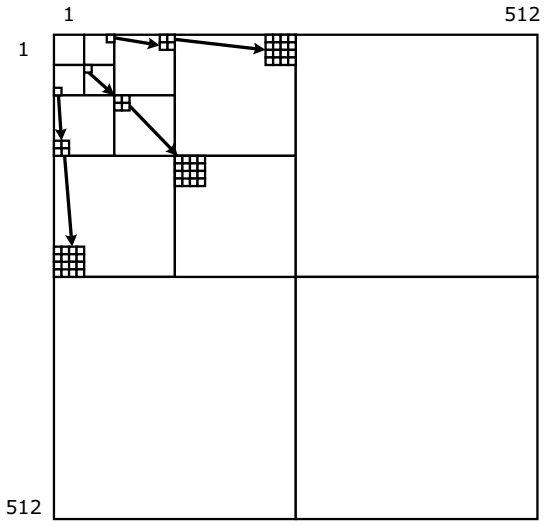

圖 4: Illustration of grouping wavelet coefficients that correspond to the same spatial area.

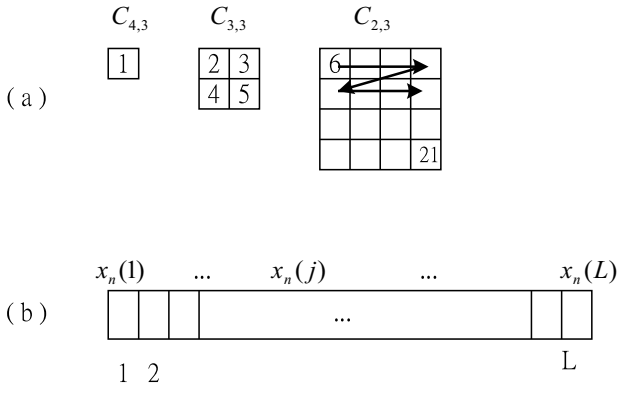

圖 5: (a) A group of wavelet coefficients with one coefficient from $C_{4,3}$, 4 coefficients from $C_{3,3}$ and 16 coefficients from $C_{2,3}$. (b) A super tree obtained by combining two groups of wavelet coefficients.

random order of the numbers from 0 to 3071 can be obtained by repeatedly generating random numbers and taking modulo 3072. If a number between 0 and 3071 has appeared already, the number is discarded. We do this until we have a set of numbers from 0 to 3071. The random numbers can be generated using the same seed in generating the watermark W.

We use two trees to embed the n-th watermark bit w_n. For this, we find the smallest quantization index q_n such that $\mathcal{E}_{2n-1}(q_n) \geq \mathcal{E}$ and $\mathcal{E}_{2n}(q_n) \geq \mathcal{E}$, where $\mathcal{E}$ is some appropriately chosen quantity called reference error. To

maintain the quality of watermarked images, we can constrain the maximum value of q_n to be a pre-determined value q_{max}, known to both the encoder and the decoder. If we can not find $q_n \leq q_{max}$ such that $\mathcal{E}_{2n-1}(q_n) \geq \mathcal{E}$ and $\mathcal{E}_{2n}(q_n) \geq \mathcal{E}$, the index q_{max} will be used as the quantization index. If $w_n = -1$, the first tree is quantized with respect to q_n. If $w_n = 1$, the second tree is quantized with respect to q_n. When all the watermark bits are embedded, we apply the inverse DTWT on the new wavelet coefficients. The output of the inverse DTWT is quantized to have integer values between 0 and $2^b - 1$, where b is the number of bits per pixel of the original host image.

Maximum likelihood detection. For the extraction of watermark bits, we first compute the wavelet coefficients of the image (possibly attacked). For the n-th bit to be decoded, the watermark decoder exams the corresponding two super trees $\mathcal{T}_{2n-1}$ and $\mathcal{T}_{2n}$. It determines which one is more likely to be a quantized tree and thus determines the sign of the watermark bit. There are two hypotheses,

$$\mathcal{H}_0 : \mathcal{T}_{2n-1} \text{ is a quantized tree,}$$

$$\mathcal{H}_1 : \mathcal{T}_{2n} \text{ is a quantized tree.}$$

Because $w_n = \pm 1$ with equal probability, the two hypotheses are equally likely. We will use maximum likelihood detection.

The decoder quantizes super trees $\mathcal{T}_{2n-1}$ and $\mathcal{T}_{2n}$, and compute new quantization errors $e'_n(j)$. The new errors of the coefficients that had been quantized in the embedding process is more likely to be around 0 and the normalized error $e'_n(j)/\Delta_n(j)$ has more probability mass around 0, i.e., $f_{quantized}(\epsilon) > f_{unquantized}(\epsilon)$ for some ϵ, where $f(y)$ is the CDF defined in (**??**). Let $f_{quantized}(\epsilon) = p_0$ and $f_{unquantized}(\epsilon) = p_1$ with $p_0 > p_1$. We have found that a maximum likelihood decision can be easily obtained by inspecting which super tree has more coefficients with normalized errors bounded between $-\epsilon$ and ϵ. The threshold ϵ be chosen to be a number for which there is a wider gap between p_0 and p_1. In most of our experiments, p_0 and p_1 are reasonably separated when $\epsilon = -0.1$. The details of watermark extraction procedure is give in the next section. The extraction procedure can be summarized as followed

1. Generate a seed by mapping a signature/text through a one-way deterministic function. Obtain a PN sequence W of length N_w using the seed.

2. Compute wavelet coefficients of a host image of b bits/pixel. Group the coefficients, and order the groups in a pseudo-random manner using the seed generated in step 1. Combine every 2 groups to form super trees $\mathcal{T}_k$, $k = 1, \cdots, 2N_w$. Set $n = 1$.

3. Set $q'_n = 1$, $\mathcal{E}_{2n-1}(1) = 0$ and $\mathcal{E}_{2n}(1) = 0$.

4. while ($(\mathcal{E}_{2n-1}(q'_n) < \mathcal{E}$ and $\mathcal{E}_{2n}(q'_n) < \mathcal{E})$ and $q'_n < q_{max}$) Compute $\mathcal{E}_{2n-1}(q'_n)$ and $\mathcal{E}_{2n}(q'_n)$. Set $q'_n = q'_n + 1$.

5. Compute N_{2n-1} and N_{2n}. If $N_{2n-1} > N_{2n}$, $w'_n = -1$; otherwise $w'_n = 1$.

6. Go to step 2 if $n < N_w$.

7. Compute normalized correlation coefficient ρ using equation (1).

8. If ρ is above the threshold ρ_T, the watermark W exists; otherwise, it does not exist.

Examples We will use 3 images for experiments, Lenna, Goldhill, and Peppers. The images are of size of 512 by 512. We use a 4-level wavelet decomposition and a watermark sequence of length 512. The reference error $\mathcal{E}$ is 100 and the largest quantization index $q_{max} = 336$. The three watermarked images have PSNR respectively 38.2, 38.7, 39.8 dB. With watermark length $N_w = 512$, the correlation threshold ρ_T is chosen to be 0.23 for a false

Attack	Median filter (2x2)	Median filter (3x3)	Median filter (4x4)	Sharpening	Gaussian filter
ρ	0.38	0.51	0.23	0.46	0.64
Existence	Y	Y	Y	Y	Y

(a)

Attack	Median filter (2x2)	Median filter (3x3)	Median filter (4x4)	Sharpening	Gaussian filter
ρ	0.35	0.56	0.24	0.39	0.56
Existence	Y	Y	Y	Y	Y

(b)

Attack	Median filter (2x2)	Median filter (3x3)	Median filter (4x4)	Sharpening	Gaussian filter
ρ	0.46	0.71	0.25	0.62	0.74
Existence	Y	Y	Y	Y	Y

(c)

表格 1: Correlation coefficient ρ and watermark existence upon attacks of Median filter (2×2, 3×3, 4×4), Gaussian filtering, and sharpening; (a) Lenna, (b) Goldhill, and (c) Peppers.

positive probability of P_{fp}=1.03×10^{-7}. We consider common signal processing attacks. These include linear and nonlinear filtering, for example median filters, Gaussian filter, histogram modification and sharpening. After these attacks, the images are blurred or sharpened on the edges. The results are given in Table. 1. We can see from the table that the embedded watermarks have successfully survived all these attacks.

參考文獻

[1] N. Kaewkamnerd, and K. R. Rao, "Wavelet based image adaptive watermarking scheme," *IEEE Electronics Letters,* vol. 36, pp. 312-313, Feb. 2000.

[2] 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.

[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673-1687, Jan. 1997.

[4] W. Zhu, Z. Xiong, and Y.-Q. Zhang, "Multiresolution watermarking for images and video," *IEEE Transactions on Circuit and System,* vol. 9, pp. 545-550, 1999.

[5] 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.

[6] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Attacks on copyright marking systems," *2nd workshop on information hiding, vol. 1525 of lecture Notes in Computer Science*, April 1998.

[7] F. A. P. Petitcolas, "Weakness of existing watermark scheme," Oct. 1997.

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

[9] M. Vetterli and J. Kovacevic, *Wavelets and subband coding*, Prentice Hall 1995.

[10] W. B. Pennebaker, and J.L. Mitchell, *JPEG: Still image data compression standrad*," New Yrok: Van Nostrand Reinhold, 1993.

[11] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuits and Systems for Video Technology,* vol. 6, pp. 243-250, June 1996.