Wavelet Tree Quantization for Copyright Protection Watermarking

Shih-Hao Wang and Yuan-Pei Lin, *Member, IEEE*

***Abstract*—This paper proposes a wavelet-tree-based blind watermarking scheme for copyright protection. The wavelet coefficients of the host image are grouped into so-called super trees. The watermark is embedded by quantizing super 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 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.**

***Index Terms*—Blind watermarking, copyright protection, quantization, wavelet.**

I. Introduction

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.

There are several important issues in watermarking systems, including visual distortion, robustness, the access of original data, etc [1]. In most cases, it is required that a watermark be invisible to maintain secrecy and the commercial value of products. For the application of this paper, copyright protection, a high level of robustness is essential. Through the insertion of watermarks, ownership can be proved even when the copies are altered or modified. The watermark are embedded without imposing perceptible artifacts on the images. Only with the secret key can the watermark information can be extracted. A watermarking technique is referred to as *blind* if the original image is not needed for extraction [2]–[4]; it is not blind if the original image is used in extraction [5], [6]. In some cases, 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 [7], [8] that for resolving rightful ownership, a blind watermarking approach is preferred. Two crucial requirements for watermark detection are proposed in [8]. 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 function to map a valid key to a pseudorandom sequence which is independent of the host images. The detection confidence is quantified using false positive detection probability.

In [9], Cox *et al.* invent the idea of using spread spectrum for embedding watermarks in the discrete cosine transform (DCT) domain. The host image is viewed as a communication channel, while the watermark as a signal to be transmitted. The watermark message is inserted throughout the perceptually important part of the signal spectrum. Security and robustness are obtained using Gaussian-noise like watermarks. The watermark cannot 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 [10].

In [11], 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 two parts to embed a watermark bit. High-frequency DCT coefficients in the compressed bitstream are selectively discarded to produce an energy difference in the two parts of the same macroblock, where the energy difference is determined by the watermark bit. 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 adjusting the three factors, appropriate marking systems are obtained for different applications. This method performs well in attacks such as pixel shifting and StirMark [12], [13]. As the embedding process is done in the compressed domain, it can also be applied in real-time processing.

An image-adaptive watermarking scheme for perceptually invisible watermarks are considered in [14]–[16]. According to the characteristics of the host image, a visual model can be incorporated in watermarks embedding. In [17] and [18], the so-called cocktail watermarking is proposed. Complementary modulation rules, positive modulation, 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. In [19], the watermark is also 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.

Manuscript received January 15, 2002; revised October 6, 2003. The work was supported in part by NSC 90-2213-E-009-108, NSC 90-2213-E-002-097, and the Lee and MTI Center for Networking Research. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Gopal Pingali.

The authors are with the Department of Electronics Engineering, National Chiao Tung University, Hsinchu 300, Taiwan, R.O.C. (e-mail: shwang.ee90g@nctu.edu.tw; ypl@cc.nctu.edu.tw).

Digital Object Identifier 10.1109/TIP.2004.823822

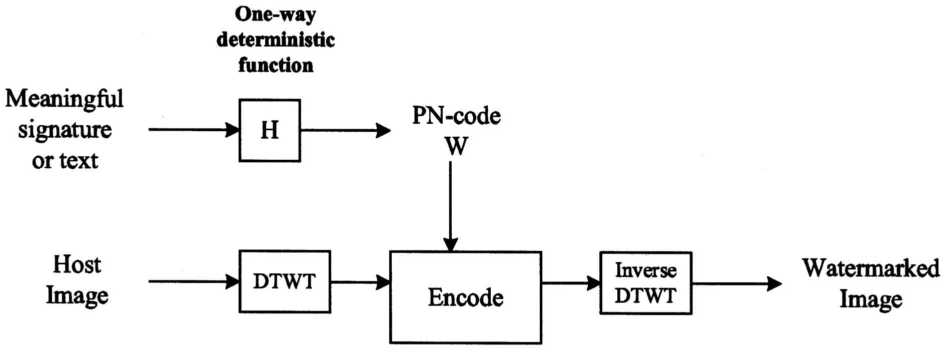


Fig. 1. Block diagram of the proposed encoder.

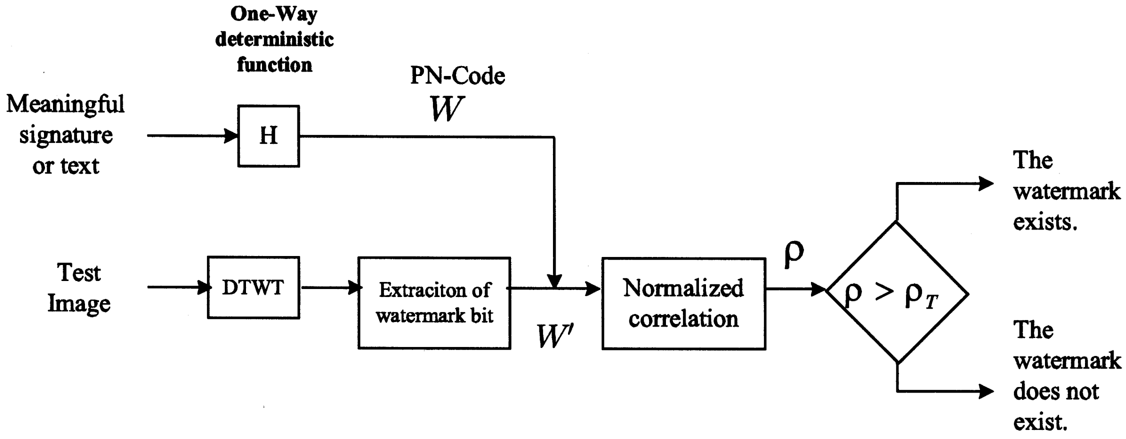

One-Way deterministic function
PN-Code W
Meaningful signature or text
H
Test Image
DTWT
Extraciton of watermark bit
W'
Normalized correlation
ρ
ρ > ρ_T
The watermark exists.
The watermark does not exist.

Fig. 2. Block diagram of the proposed decoder.

In this paper, we propose a wavelet-based blind watermarking scheme for the application of copyright protection. The wavelet coefficients of the host image are grouped into so-called super trees. Watermark bits are also embedded by quantizing wavelet coefficients, similar to [19], but here all the coefficients in super trees are quantized. The trees are so quantized that they exhibit a large enough statistical difference. The resulting difference between quantized and unquantized trees will later be used for watermark extraction. Using the disparity between super trees to extract the watermark is similar to the method in [11], which uses energy difference between macroblocks for watermark extraction. A binary decision is made based on the extracted watermark to prove ownership. A false positive detection probability is used to quantify the detection confidence. The tree marking technique spreads the watermark in wavelet coefficients of perceptual importance. The watermark will be more resistant against attacks that remove certain frequency components. Furthermore, the tree-marking approach is based on wavelet trees, which encompass large spatial areas. This yields more robustness against geometric attacks such as pixel shifting and image rotation. The proposed watermarking technique is also resistant against various common attacks as will be demonstrated in the examples. These include nongeometric attacks, e.g., lossy signal compression, histogram modification, etc., and geometric attacks that introduce small geometric distortions. Some preliminary results of this paper can be found in [20].

This paper is organized as follows. In Section II, the proposed watermarking scheme for copyright protection is introduced. We derive the maximum likelihood decoder in Section III. The extraction algorithms are given in Section IV. In Section V, the performance of the proposed watermarking method is evaluated by applying various attacks on watermarked images, including nongeometric and geometric attacks. A conclusion is given in Section VI.

II. Watermarking Using Tree Quantization

In the proposed tree watermarking scheme, the host image is transformed into wavelet coefficients using a discrete-time wavelet transform (DTWT). The watermark is embedded in the wavelet coefficients. The wavelet coefficients are grouped into so called super trees. Each watermark bit is embedded using two super trees. Depending on the value of the watermark bit w_n, one of the super trees is quantized with respect to a quantization index q_n. The index is such that the two super trees exhibit a large enough statistical difference, which will later be extracted for the decision of w_n.

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 [8]. 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

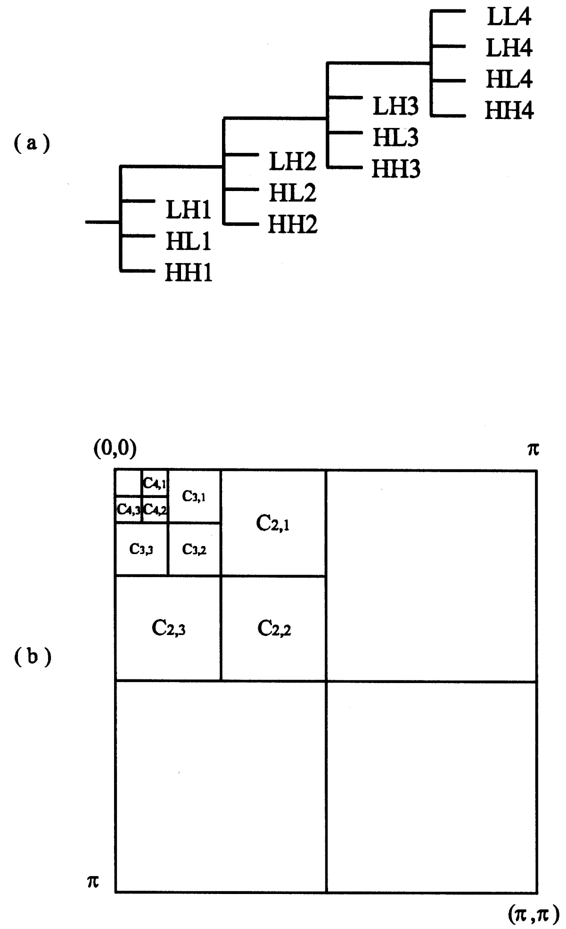


Fig. 3. (a) A four-level wavelet decomposition and the resulting 13 subbands. (b) The 13 frequency bands corresponding to the subbands in (a).

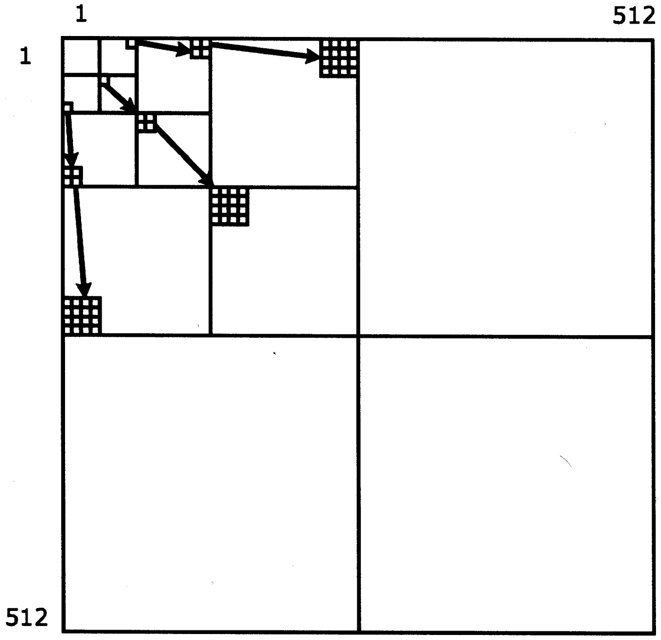


Fig. 4. Illustration of grouping wavelet coefficients that correspond to the same spatial area.

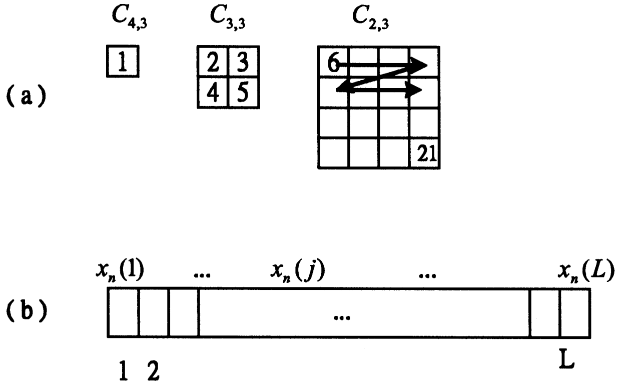


Fig. 5. (a) A group of wavelet coefficients with one coefficient from $C_{4,3}$, 4 coefficients from $C_{3,3}$, and 16 coefficients from $C_{2,3}$. (b) A super tree obtained by combining two groups of wavelet coefficients.

exists. The choice of the threshold depends on the desired false positive probability.

For the convenience of illustration, we will use a discrete time wavelet transform of four levels (see [21] and the references therein for details of wavelet transforms). A 512×512 image will be used as an example. With a four-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 pseudorandom manner. A pseudorandom 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.

Super trees: We further combine the coefficients of every two groups together to form super trees $\mathcal{T}_n$, for $n = 1, \ldots, 1536$, each with $L = 42$ coefficients. An example of a super tree is shown in Fig. 5(b). Each watermark bit is embedded using two super trees. The maximum number of watermark bits that can be embedded is thus $1536/2 = 768$. Let the watermark length be $N_w (< 768)$ and let the jth coefficient of the nth tree be denoted by

$$x_n(j) \quad \text{for} \quad 1 \leq j \leq L \quad \text{and} \quad 1 \leq n \leq 2N_w.$$

We quantize all the coefficients to integers and express the coefficients in binary representation, then the bits of the coefficients form a two dimensional array as shown in Fig. 6(a), each entry equal to 0 or 1. The least-significant bitplane (LSB) is 2^0, and the most significant bitplane (MSB) is denoted by 2^p. Excluding the sign bit, there are a total of $N_p = L(p+1)$ bits. We order

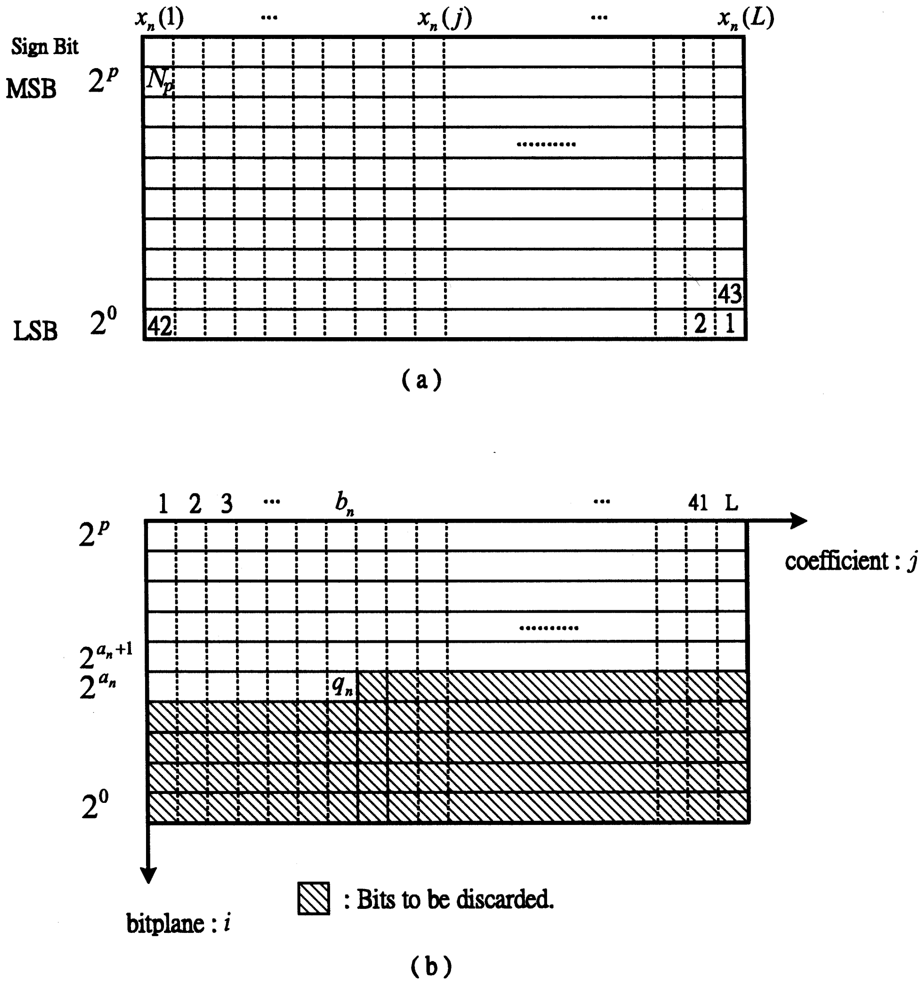


Fig. 6. (a) Binary representation of the coefficients in the nth super tree. (b) Quantization of the nth super tree with respect to a quantization index q_n.

these bits using a raster scan of the two-dimensional array in Fig. 6(a), right to left, and bottom to top. The super trees will be quantized depending the watermark bit to be embedded.

Quantization of super trees: Let us consider the quantization of the nth tree with respect to a given quantization index q_n, with $1 \leq q_n \leq N_p$. The choice of q_n will be discussed later. The coordinate of q_n in the array is (a_n, b_n) as shown in Fig. 6(b). All the bits below the quantization index will be discarded. The discarded bits are shown as shaded area in Fig. 6(b). After quantization, the LSB of the jth coefficient becomes a_n if $j \leq b_n$ and the LSB of the jth coefficient become $(a_n + 1)$ if $j > b_n$. Let $round(x)_i$ denote the rounding of a number x to the ith bitplane. The quantization of $x_n(j)$ with respect to q_n, denoted by $Q[x_n(j)]_{q_n}$, is given by

$$Q[x_n(j)]_{q_n} = \begin{cases} \text{round}(x_n(j))_{a_n}, & j \leq b_n \\ \text{round}(x_n(j))_{a_n+1}, & \text{otherwise.} \end{cases} \tag{1}$$

Therefore the quantization step size $\Delta_n(j)$ is given by

$$\Delta_n(j) = \begin{cases} 2^{a_n}, & j \leq b_n \\ 2^{a_n+1}, & \text{otherwise.} \end{cases} \tag{2}$$

The quantization error of the jth coefficient with respect to q_n is

$$e_n(j) = Q[x_n(j)]_{q_n} - x_n(j).$$

The total quantization error of the nth tree with respect to q_n is

$$\mathcal{E}_n(q_n) = \sum_{j=1}^{L} |e_n(j)|. \tag{3}$$

The value of q_n is an index of the number of bits discarded in quantization. The larger q_n is, the larger is the number of bits discarded.

Embedding of watermark bits: We use two trees $\mathcal{T}_{2n-1}$ and $\mathcal{T}_{2n}$ to embed the nth 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 cannot 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 $w_n = -1$, $\mathcal{T}_{2n-1}$ is quantized with respect to q_n. If $w_n = 1$, $\mathcal{T}_{2n}$ is quantized with respect to q_n. When all the

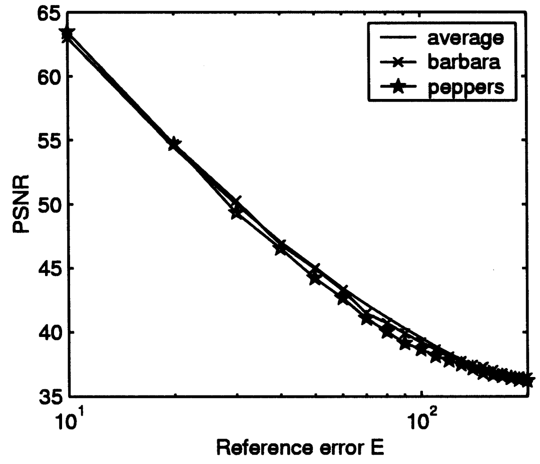


Fig. 7. PSNR of watermarked images as a function of the reference error $\mathcal{E}$.

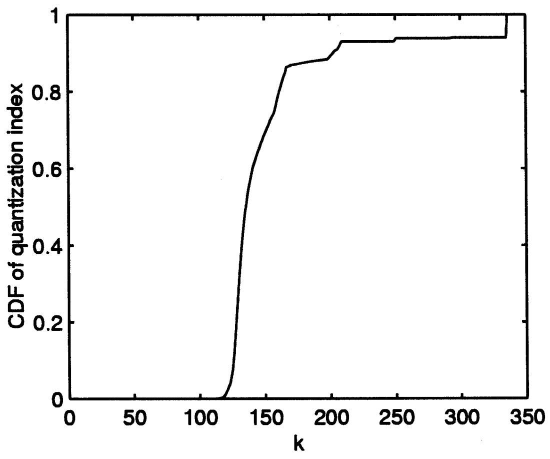


Fig. 8. CDF of the quantization index.

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. A summary of the embedding procedure is given next.

```
Embedding Procedure
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 pseudorandom manner using the seed generated in step 1. Combine every 2 groups to form super trees
   $\mathcal{T}_k, k = 1,\ldots,2N_w$. Set $n = 1$.
3. Set $q_n = 1$, $\mathcal{E}_{2n-1}(1) = 0$ and $\mathcal{E}_{2n}(1) = 0$.
4. while (($\mathcal{E}_{2n-1}(q_n)$ < $\mathcal{E}$ or < $\mathcal{E}$) and $q_n < q_{\max}$)
     Compute $\mathcal{E}_{2n-1}(q_n)$ and $\mathcal{E}_{2n}(q_n)$ using (3). Set $q_n = q_n + 1$.
5. Quantize $\mathcal{T}_{2n-1}$ if $w_n = -1$. Quantize $\mathcal{T}_{2n}$ if $\mathrm{w_n} = 1$. Set $n = n + 1$.
6. Go to step 2 if $n < N_w$.
7. Pass the modified wavelet coefficients through the inverse DTWT. Quantize the pixel values to integers
   between 0 and $2^b - 1$ to obtain a watermarked image.
```

Remarks: The reference error $\mathcal{E}$ provides a tradeoff between the strength of the watermark and quality of the watermarked image. The larger $\mathcal{E}$ is, the more heavily quantized are the super trees; using a larger $\mathcal{E}$ trades signal-to-noise ratio (SNR) quality of the image for more robustness of the watermark. In Fig. 7, we plot the peak signal-to-noise ratio (PSNR) as a function of $\mathcal{E}$ for the images Barbara and Peppers. We also show the average PSNR of 12 commonly used images from [22]. For $40 <$ PSNR < 60, PSNR decreases approximately linearly with the $\log_{10} \mathcal{E}$. The references errors corresponding to $\mathrm{PSNR} = 40\,\mathrm{dB}$ and $\mathrm{PSNR} = 60\,\mathrm{dB}$ are, respectively, $\mathcal{E} = 12$ and $\mathcal{E} = 70$. For a desired PSNR between 40 and 60 dB, linear interpolation can be used to get a good estimate of $\mathcal{E}$. For $\mathcal{E} = 100$ and $q_{\max} = 336$, we show in Fig. 8 the empirical cumulative distribution function (cdf) of the quantization index by averaging over the 12 images. We can see that most quantization indices are between 100 and 200, i.e., in the 2^3, 2^4 and 2^5 bitplanes.

III. Designs of Watermark Decoders

Through the embedding process in Section II, a statistical difference between quantized and unquantized super trees is embedded. We will first discuss such a difference. Then we will see how the difference can be used for the maximum likelihood detection of watermarks.

To see there is a difference between quantized and unquantized super trees, let us pass a watermarked image through DTWT. The wavelet coefficients are grouped into super trees in the same manner as is done in encoding. The binary representation of each super tree again gives rise to a two-dimensional array of bits like the one in Fig. 6(a). We quantize all the super trees with respect to the corresponding quantization index q_n and compute new quantization errors $e'_n(j)$. Now the requantization errors of the super trees that had been quantized earlier and the super trees that had not bee quantized earlier have different statistical behaviors. For those trees that had been quantized earlier, the new errors $e'_n(j)$ will be close to 0. However, for those that had not been quantized earlier, the new errors $e'_n(j)$ will be relatively more uniformly distributed.

To be more specific, we define the empirical cdf of the magnitude of normalized requantization errors as

$$f(y) = \mathrm{Prob}\left[\left|\frac{e'_n(j)}{\Delta_n(j)}\right| < y\right] \tag{4}$$

where $\Delta_n(j)$ is the quantization step size as given in (2). The empirical cdf, based on 12 commonly used images obtained from [22], is plotted in Fig. 9(a) for trees that were quantized and for trees that were not quantized in the embedding procedure. Compared to a quantized tree, the distribution of a unquantized tree has more probability mass around 0. For example, when $y = 0.1$, $f(y)$ is 0.99 for quantized trees and 0.4 for unquantized trees. Thus, when a coefficient has $e'_n(j)$ satisfying, e.g., $|e'_n(j)/\Delta_n(j)| < 0.1$, it is more likely that it belongs to a unquantized tree. The curves in Fig. 9 are obtained by averaging over 12 images. The empirical cdfs of individual images are very similar. Notice that for the cdf of a quantized tree in Fig. 9(a), not all the probability mass is at 0. This is because additional

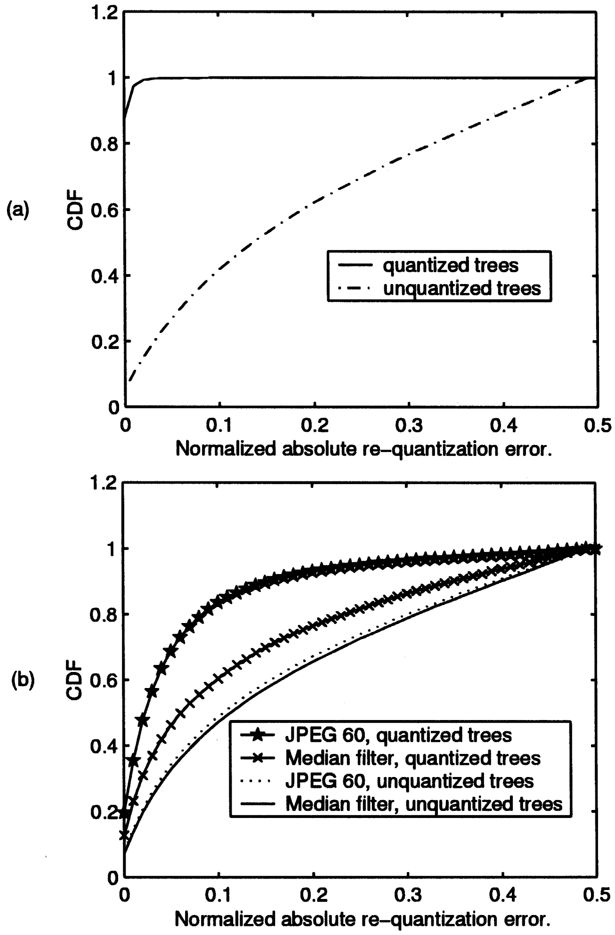


Fig. 9. CDF of the magnitude of normalized quantization error $|e'_n(j)/\Delta_n(j)|$: (a) without attacks and (b) with attacks.

errors are introduced in the spatial domain when the output of the inverse DTWT is quantized (step 7 of the embedding procedure).

In the presence of attacks, new quantization errors continue to have such a difference. Fig. 9(b) shows the empirical cdfs for two types of attacks, JPEG compression with a quality factor of 60 and median filtering of size 2 by 2. In either case, the cdf of a quantized super tree is above that of a unquantized super tree, i.e., $f_{\text{quantized}}(y) > f_{\text{unquantized}}(y)$. This property will be used for watermark decoding.

Maximum likelihood detection: For the extraction of watermark bits, we first compute the wavelet coefficients of the image (possibly attacked). For the nth bit to be decoded, the watermark decoder examines 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., $f_{\text{quantized}}(\epsilon) > f_{\text{unquantized}}(\epsilon)$ for some ϵ, where $f(y)$ is the cdf defined in (4). Let $f_{\text{quantized}}(\epsilon) = p_0$ and $f_{\text{unquantized}}(\epsilon) = p_1$ with $p_0 > p_1$. Let the number of coefficients in $\mathcal{T}_{2n-1}$ that satisfy $|e'_{2n-1}(j)/\Delta_{2n-1}(j)| < \epsilon$ be N_{2n-1}, and similarly let the number of coefficients in $\mathcal{T}_{2n}$ that satisfy $|e'_{2n}(j)/\Delta_{2n}(j)| < \epsilon$ be N_{2n}. Then

$$Prob[\mathcal{H}_0 \text{ is true}] = \binom{L}{N_{2n-1}} p_0^{N_{2n-1}}(1-p_0)^{L-N_{2n-1}} \times \binom{L}{N_{2n}} p_1^{N_{2n}}(1-p_1)^{L-N_{2n}}$$

$$Prob[\mathcal{H}_1 \text{ is true}] = \binom{L}{N_{2n-1}} p_1^{N_{2n-1}}(1-p_1)^{L-N_{2n-1}} \times \binom{L}{N_{2n}} p_0^{N_{2n}}(1-p_0)^{L-N_{2n}}.$$

We can verify that the ratio of the two can be rewritten as

$$\frac{Prob[\mathcal{H}_0 \text{ is true}]}{Prob[\mathcal{H}_1 \text{ is true}]} = \alpha^{N_{2n-1}-N_{2n}}, \text{ where}$$

$$\alpha = \frac{p_0(1-p_1)}{p_1(1-p_0)}.$$

As $p_0 > p_1$, we have $\alpha > 1$. Therefore, hypothesis $\mathcal{H}_0$ is more likely if $N_{2n-1} > N_{2n}$ and $\mathcal{H}_1$ is more likely if $N_{2n-1} < N_{2n}$.

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 is 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 given in Section IV.

IV. Watermark Extraction

In the extraction process, we first compute the wavelet coefficients of the image for which the existence of a watermark sequence is in question. The watermark bits are extracted one by one. The maximum likelihood decoder derived in Section III implies that to determine the sign of the nth watermark bit, we only need to see which of $\mathcal{T}_{2n-1}$ and $\mathcal{T}_{2n}$ has more coefficients whose normalized quantization errors are bounded between $-\epsilon$ and ϵ. Although the decoder does not have q_n, an estimate can be obtained using the reference error $\mathcal{E}$. For the decoding of w_n, we find the smallest index q'_n such that $\mathcal{E}_{2n-1}(q'_n) \geq \mathcal{E}$ or $\mathcal{E}_{2n}(q'_n) \geq \mathcal{E}$. Quantizing $\mathcal{T}_{2n-1}$ and $\mathcal{T}_{2n}$ with respect to q'_n, we have quantization errors given by

$$e'_\ell(j) = x'_\ell(j) - Q[x'_\ell(j)]_{q'_n}, \text{ where } \quad \ell = 2n-1, 2n$$

where $x'_\ell(j)$ denotes the jth coefficient of the ℓth super tree. Let the coordinates of q'_n be (a'_n, b'_n). The quantization step size is $\Delta'_n(j) = 2^{a'_n}$ for $j \leq b'_n$ and $\Delta'_n(j) = 2^{a'_n+1}$ for $j > b'_n$.

We compute the number of coefficients in $\mathcal{T}_{2n-1}$ that have $|e'_{2n-1}(j)/\Delta'_{2n-1}(j)| < \epsilon$ and the number of coefficients in $\mathcal{T}_{2n}$ that have $|e'_{2n}(j)/\Delta'_{2n}(j)| < \epsilon$. Denote these two numbers by N_{2n-1} and N_{2n}. The value of ϵ is chosen to be 0.1, as discussed in Section III. We determine the extracted bit w'_n by comparing N_{2n-1} and N_{2n}

$$w'_n = \begin{cases} -1, & \text{if } N_{2n-1} > N_{2n} \\ 1, & \text{otherwise.} \end{cases} \tag{5}$$

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

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

where N_w is the number of watermark bit embedded. The coefficient is bounded by $-1 \leq \rho(W, W') \leq 1$. 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

$$\rho(W, W') = \frac{\sum_m w_m w'_m}{N_w}. \tag{6}$$

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

Let $P_E = \text{Prob}(w_m \neq w'_m)$. Using this expression, the probability of false positive error P_{fp} can be computed by [19],

$$P_{\text{fp}} = \sum_{k=((\rho_T+1)/2)N_w}^{N_w} \binom{N_w}{k} P_E^{N_w-k} (1 - P_E)^k.$$

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.

```
Extraction Procedure
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 pseudorandom manner using the
 seed generated in step 1. Combine every 2 groups
to form super trees $\mathcal{T}_k$, $k = 1, \ldots, 2N_w$. 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 $\mathcal{E}_{2n}(q'_n)$ using (3).
 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 $\rho$
 using (6).
8. If $\rho$ is above the threshold $\rho_T$, the watermark
$W$ exists; otherwise, it does not exist.
```

Fig. 10. Original image of Lenna.

Remarks:

1) The parameter reference error $\mathcal{E}_0$ is used in encoding and decoding. It is a quantity that the attacker can probably get a good estimate of. However, even if $\mathcal{E}_0$ is known, the attacker cannot easily identified which are quantized trees without the secret key. This is because DTWT of the image yields only wavelet groups and the attacker does not know how the groups are combined to form super trees. Furthermore, there are two super trees corresponding to every watermark bit and these two trees are compared to determine which has been quantized earlier. The attacker has no knowledge of which two trees should be compared without the secret key.
2) We have used a four-level wavelet decomposition for illustration. More levels of decomposition can also used. With more levels of decomposition, each tree contains more coefficients, leading to more robustness, but the maximum length of the watermark decreases, which affect false positive probability. The number of decomposition gives a tradeoff between robustness and false positive probability.
3) In the proposed marking scheme, the human visual system (HVS) can be easily incorporated to improve the visual quality of watermarked images [23], [24]. The wavelet coefficients can be properly scaled according HVS before tree quantization so that the quantization imposes less perceptual quality loss.
4) We can also apply the tree marking method to data hiding. A data bit stream can be embedded in the same way a watermark sequence is embedded.

V. Examples

We will use three images for experiments Lenna, Goldhill, and Peppers, which are obtained from [22]. The images are of size of 512 by 512. For brevity, only the Lenna image is shown. The original image of Lenna is shown in Fig. 10.

Fig. 11. Watermarked Lenna with $\mathrm{PSNR} = 38.2\ \mathrm{dB}$.

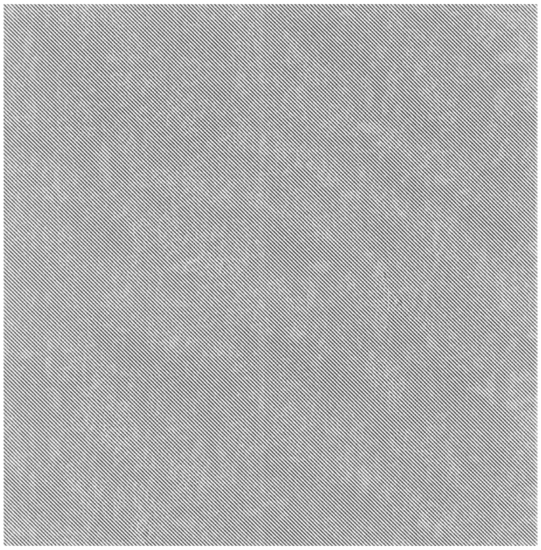


Fig. 12. Error image obtained by subtracting the watermarked Lenna from the original version.

TABLE I
CORRELATION COEFFICIENT ρ AND WATERMARK EXISTENCE UPON ATTACKS OF JPEG COMPRESSION WITH QUALITY FACTOR 30, 40, 50, 70, 90. (a) LENNA. (b) GOLDHILL. (c) PEPPERS

JPEG	30	40	50	70	90
ρ	0.15	0.23	0.26	0.57	1
Existence	N	Y	Y	Y	Y

(a)

JPEG	30	40	50	70	90
ρ	0.23	0.52	0.71	0.93	1
Existence	Y	Y	Y	Y	Y

(b)

JPEG	30	40	50	70	90
ρ	0.34	0.54	0.70	0.97	1
Existence	Y	Y	Y	Y	Y

(c)

TABLE II
CORRELATION COEFFICIENT ρ AND WATERMARK EXISTENCE UPON ATTACKS OF SPIHT COMPRESSION WITH BITRATE 0.3–0.7.
(a) LENNA. (b) GOLDHILL. (c) PEPPERS

Bitrate	0.3	0.4	0.5	0.6	0.7
PSNR	33.1	34.3	34.6	35.2	36.7
ρ	0.21	0.41	0.85	0.83	0.85
Existence	N	Y	Y	Y	Y

(a)

Bitrate	0.3	0.4	0.5	0.6	0.7
PSNR	31.7	32.4	32.9	33.2	34.1
ρ	-0.06	0.02	0.23	0.27	0.35
Existence	N	N	Y	Y	Y

(b)

Bitrate	0.3	0.4	0.5	0.6	0.7
PSNR	33.13	33.6	34.4	34.7	34.9
ρ	0.36	0.66	0.65	0.71	0.85
Existence	Y	Y	Y	Y	Y

(c)

We use a four-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 PSNRs of, respectively, 38.2, 38.7, and 39.8 dB. The watermarked Lenna is shown in Fig. 11. The difference image of the original Lenna and the watermarked version are shown in Fig. 12. The distortion due to watermarking is mostly on the edges. We consider both nongeometric and geometric attacks. Nongeometric processing includes low-pass filtering, lossy compression, histogram modification, sharpening, etc. Geometric distortion includes rotation, scaling, and pixel shifting. With watermark length $N_w = 512$, the correlation threshold ρ_T is chosen to be 0.23 for a false positive probability of $P_{\mathrm{fp}} = 1.03 \times 10^{-7}$. In the following experiments, when the PSNR of an attacked image is computed, it is obtained by subtracting the attacked image from the original version. The details of the attacks used and the corresponding results are given next.

Compression: JPEG [25] is one of the most used compression technique, and is often an unintentional attack. Quality factors of 30, 40, 50, 70, 90 are used, and the results are tabulated in Table I. The proposed methods can detect the existence of watermarks for quality factors greater than 40. Usually for

TABLE III
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. (c) PEPPERS

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)

TABLE IV
CORRELATION COEFFICIENT ρ AND WATERMARK EXISTENCE UPON ATTACKS OF PIXEL SHIFTING, TYPE-I: CIRCULAR SHIFT AND TYPE-II: LINE DELETION FOLLOWED BY DUPLICATION OF ADJACENT LINES ON THE IMAGE EDGE. (a) LENNA. (b) GOLDHILL. (c) PEPPERS

(a)

Pixel shift	5	6	7	8	9	10
Type I, ρ	0.28(Y)	0.34(Y)	0.29(Y)	0.81(Y)	0.26(Y)	0.19(N)
Type II, ρ	0.27(Y)	0.33(Y)	0.27(Y)	0.82(Y)	0.25(Y)	0.17(N)

(b)

Pixel shift	5	6	7	8	9	10
Type I, ρ	0.36(Y)	0.35(Y)	0.41(Y)	0.84(Y)	0.29(Y)	0.21(N)
Type II, ρ	0.37(Y)	0.31(Y)	0.43(Y)	0.85(Y)	0.25(Y)	0.20(N)

(c)

Pixel shift	5	6	7	8	9	10
Type I, ρ	0.32(Y)	0.34(Y)	0.29(Y)	0.92(Y)	0.29(Y)	0.26(Y)
Type II, ρ	0.34(Y)	0.33(Y)	0.31(Y)	0.91(Y)	0.28(Y)	0.27(Y)

images with a quality factor lower than 40, there are visible artifacts. In this case it is apparent that the image has been distorted without resorting to a watermark detector. We also consider the attack of SPIHT compression [26] (Table II). The embedded watermark can be detected when PSNR falls to around 34 dB.

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 III. The embedded watermarks survive all these attacks.

Pixel shifting: Two types of pixel shifting are considered. Type-I is a circular shift and type-II is a deletion of lines followed by duplication of the adjacent lines. The results given in Table IV show that the proposed watermark can resist a shift of up to nine pixels. Usually, a shift of ten pixels with either type may cause visible difference.

TABLE V
CORRELATION COEFFICIENT ρ AND WATERMARK EXISTENCE UPON ATTACKS OF ROTATION, FOLLOWED BY SCALING AND CROPPING TO THE ORIGINAL SIZE. (a) LENNA. (b) GOLDHILL. (c) PEPPERS

(a)

Rotation	0.25	0.5	0.75	1.0	-0.25	-0.5	-0.75	-1.0
ρ	0.37	0.29	0.26	0.24	0.32	0.23	0.24	0.16
Existence	Y	Y	Y	Y	Y	Y	Y	N

Unit of rotation : degree (a positive degree for a clockwise rotation and a negative degree for a counterclockwise rotation)

(b)

Rotation	0.25	0.5	0.75	1.0	-0.25	-0.5	-0.75	-1.0
ρ	0.33	0.24	0.21	0.15	0.38	0.27	0.25	0.14
Existence	Y	Y	N	N	Y	Y	Y	N

(c)

Rotation	0.25	0.5	0.75	1.0	-0.25	-0.5	-0.75	-1.0
ρ	0.41	0.30	0.26	0.17	0.39	0.25	0.25	0.16
Existence	Y	Y	Y	N	Y	Y	Y	N

Rotation and scaling: This is done by rotating the image by a small angle, scaling the rotated image, and cropping the scaled image to the original image size. Although this kind of attacks does not cause serious visual distortions, they can still severely affect watermark extraction, especially for those pixel-based watermarking systems. The results given in Table V show the watermark can resist a rotation of up to 0.75°.

Multiple watermarking: A would-be attacker may know the scheme using which the image is watermarked, but does not have the key of the watermark. The attacker may apply one or more watermarks using the same tree quantization technique in an attempt to confuse the detector or to destroy the embedded watermark. Table VI gives of the results when the images are attacked through multiple watermarking. The watermark can be detected when the PSNR of the attacked images is around 29 dB.

Bitplane removal: In the proposed tree quantization method, the bits are embedded by removing LSBs of super trees. The attacker does not know how the wavelet groups are combined to form super trees and does not have the quantization index q_n with respect to which the nth tree is quantized. One possible attack is to remove from all the wavelet coefficients a few least significant bitplanes. Table VII shows the results when the least significant k bitplanes are removes, $k = 1, 2, \ldots, 5$. The watermark can still be detected when four bitplanes are removed. In this case, PSNR falls below 25 dB.

In Table VIII, we compare the proposed method with that in [19] using the image Peppers. The watermarked images in both cases are around 41.5 dB. The two methods have comparable performance in the tests of median filtering, Gaussian filtering, and histogram equalization. In the test of JPEG compression, the method in [19] shows more robustness; the watermark survives the attack of JPEG compression with a quality factor of 35. However, we can see that the proposed method is significantly more robust against geometric attacks; it can resist a much larger pixel shift and rotation.

TABLE VI
CORRELATION COEFFICIENT ρ AND WATERMARK EXISTENCE UPON ATTACKS OF MULTIPLE WATERMARKING. (a) LENNA. (b) GOLDHILL. (c) PEPPERS

Number of watermarks	1	2	3	4
ρ	0.65	0.41	0.27	0.11
PSNR	35.50	32.78	29.35	28.05
Existence	Y	Y	Y	N

(a)

Number of watermarks	1	2	3	4
ρ	0.79	0.45	0.31	0.18
PSNR	35.26	31.50	29.71	28.57
Existence	Y	Y	Y	N

(b)

Number of watermarks	1	2	3	4
ρ	0.80	0.53	0.31	0.22
PSNR	34.53	31.99	30.19	28.81
Existence	Y	Y	Y	N

(c)

TABLE VII
CORRELATION COEFFICIENT ρ AND WATERMARK EXISTENCE UPON ATTACKS OF REMOVING LEAST SIGNIFICANT k BITPLANES, FOR $k = 1, 2, \ldots, 5$. (a) LENNA. (b) GOLDHILL. (c) PEPPERS

Number of bitplanes removed	1	2	3	4	5
ρ	1	1	0.99	0.52	0.11
PSNR	36.81	34.72	30.41	24.28	18.47
Existence	Y	Y	Y	Y	N

(a)

Number of bitplanes removed	1	2	3	4	5
ρ	1	1	0.97	0.38	0.14
PSNR	36.07	33.72	28.87	22.72	16.18
Existence	Y	Y	Y	Y	N

(b)

Number of bitplanes removed	1	2	3	4	5
ρ	.99	0.96	0.90	0.64	0.14
PSNR	35.97	33.64	28.76	22.71	16.93
Existence	Y	Y	Y	Y	N

(c)

TABLE VIII
COMPARISON OF THE PROPOSED WATERMARKING METHOD AND THE METHOD OF [19]

Attacks \ Watermark Existence	Ref [19]	Proposed
Median filter (3x3)	Yes	Yes
Gaussian Filter	Yes	Yes
Histogram equalization	Yes	Yes
JPEG (QF= 35)	Yes	*No*
JPEG (QF=50)	Yes	Yes
Pixel shift of 2 pixels (Type I)	*No*	Yes
Pixel shift of 8 pixels (Type I)	*No*	Yes
Rotation (d egree : 0. 3)	*No*	Yes
Rotation (d egree : 0. 5)	*No*	Yes

VI. CONCLUSIONS

In this paper, we proposed a wavelet-based watermarking technique by quantizing the so-called super trees. Each watermark bit is embedded in various frequency bands and the information of the watermark bit is spread throughout large spatial regions. As a result, the watermarking 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 the removal of the high-pass band in low-pass processing, and the removal of high-pass details in JPEG compression. It is also robust to time domain attacks such as pixel shifting and rotation. In addition to copyright protection, the proposed watermarking scheme can also be applied to data hiding or image authentication.

REFERENCES

[1] G. C. Langelaar, I. Setyanwn, and R. L. Lagendijk, "Watermarking digital image and video data, a state-of-the-art overview," *IEEE Signal Processing Mag.*, pp. 20–46, Sept. 2000.

[2] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet based scheme for watermarking images," in *Proc. IEEE ICIP*, vol. 2, 1997, pp. 4–7.

[3] H. Inoue, A. Miyazaki, A. Yamamoto, and T. Katsura, "A digital watermark based on the wavelet transform and its robustness on image compression," in *Proc. IEEE ICIP*, vol. 2, 1998, pp. 391–395.

[4] M.-J. Tsai, K.-Y. Yu, and Y.-Z. Chen, "Wavelet packet and adaptive spatial transformation of watermark for digital images authentication," in *Proc. IEEE ICIP*, vol. 1, 2000, pp. 450–453.

[5] N. Kaewkamnerd and K. R. Rao, "Wavelet based image adaptive watermarking scheme," *Electron. Lett.*, vol. 36, pp. 312–313, Feb. 2000.

[6] C.-T. Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," *IEEE Trans. Circuits Syst. II*, vol. 45, pp. 1097–1101, Dec. 1997.

[7] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitation, attacks, and applicaitons," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 573–586, May 1998.

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

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

[10] W. Zhu, Z. Xiong, and Y.-Q. Zhang, "Multiresolution watermarking for images and video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 9, pp. 545–550, June 1999.

[11] G. C. Langelaar and R. L. Langendijk, "Optimal differential energy watermarking of DCT encoded images and video," *IEEE Trans. Image Processing*, vol. 10, pp. 148–158, Jan. 2001.

[12] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. 2nd Workshop on Information Hiding*, vol. 1525, Lecture Notes in Computer Science, Apr. 1998 .

[13] F. A. P. Petitcolas. (1997) Weakness of existing watermark scheme. [Online]. Available: http://www.cl.cam.ac.uk/~fapp2/watermarking/image-watermarking

[14] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Select. Areas Commun.*, vol. 12, pp. 525–539, May 1998.

[15] Y.-S. Kim, O.-H. Kown, and R.-H. Park, “Wavelet based watermarking method for digital images using the human visual system,” in *Proc. IEEE ISCAS*, vol. 4, 1999, pp. 80–83.

[16] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual watermarks for digital images and video,” *Proc. IEEE*, vol. 87, pp. 1108–1126, July 1999.

[17] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. Liao, “Cocktail watermarking for digital image protection,” *IEEE Trans. Multimedia*, vol. 2, pp. 209–224, Dec. 2000.

[18] C. S. Lu and H. Y. Liao, “Multipurpose watermarking for image authentication and protection,” *IEEE Trans. Image Processing*, vol. 10, pp. 1579–1592, Oct. 2001.

[19] D. Kundur and D. Hatzinakos, “Digital watermarking, using multiresolution wavelet decomposition,” in *Proc. IEEE ICASSP*, vol. 5, 1998, pp. 2969–2972.

[20] S.-H. Wang and Y.-P. Lin, “Blind watermarking using wavelet tree quantization,” in *Proc. IEEE ICME*, vol. 1, 2002, pp. 589–592.

[21] M. Vetterli and J. Kovacevic, *Wavelets and Subband Coding*. Englewood Cliffs, NJ: Prentice-Hall, 1995.

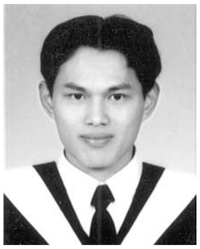
[22] USC SIPI—The USC-SIPI Image Database [Online]. Available: http://sipi.usc.edu/services/database/Database.html

[23] I. Höntsch, L. J. Karam, and R. J. Safranek, “A perceptually tuned embedded zerotree image coder,” in *Proc. IEEE ICIP*, vol. 1, 1997, pp. 41–44.

[24] A. B. Watson, G. Y. Yang, A. Solomon, and J. Villasenor, “Visibility of wavelet quantization noise,” *IEEE Trans. Image Processing*, vol. 6, pp. 1164–1175, Aug. 1997.

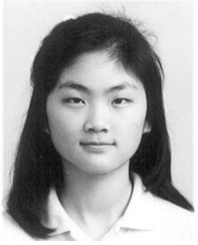
[25] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standrad*. New York: Van Nostrand, 1993.

[26] A. Said and W. A. Pearlman, “A new, fast, and efficient image codec based on set partitioning in hierarchical trees,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, pp. 243–250, June 1996.



Shih-Hao Wang was born in Tainan, Taiwan, R.O.C., in 1977. He received the B.S. degree in power mechanical engineering from National Tsing-Hua University, Hsinchu, Taiwan, in 1999 and the M.S. degree in electrical and control engineering from National Chiao Tung University, Hsinchu, in 2001, where he is currently pursuing the Ph.D. degree in the Institute of Electronics Engineering.

His research interests are digital watermarking, video signal processing, and VLSI implementation.



Yuan-Pei Lin (S’93–M’97) was born in Taipei, Taiwan, R.O.C., in 1970. She received the B.S. degree in control engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1992, and the M.S. and Ph.D. degrees, both in electrical engineering, from California Institute of Technology, Pasadena, in 1993 and 1997, respectively.

She joined the Department of Electrical and Control Engineering, National Chiao Tung University, in 1997. Her research interests include digital signal processing, multirate filter banks, and digital communication with emphasis on multicarrier systems.

Dr. Lin is currently an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and an Associate Editor for *Multidimensional Systems and Signal Processing*.