Expert Systems with Applications 36 (2009) 11509–11516

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

A blind watermarking method using maximum wavelet coefficient quantization

Wei-Hung Lin [a], Yuh-Rau Wang [b,*], Shi-Jinn Horng [a,c], Tzong-Wann Kao [d], Yi Pan [e]

[a] Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan
[b] Department of Computer Science and Information Engineering, St. John's University, Taipei, Taiwan
[c] Department of Electronic Engineering, National United University, Miao-Li, Taiwan
[d] Department of Electronic Engineering, Technology and Science Institute of Northern Taiwan, Taipei, Taiwan
[e] Department of Computer Science, Georgia State University, Atlanta, GA 30302-4110, USA

ARTICLE INFO

Keywords:
Watermark
Blind
Copyright protection
Maximum coefficient quantization
Wavelet

ABSTRACT

This paper proposes a blind watermarking algorithm based on maximum wavelet coefficient quantization for copyright protection. The wavelet coefficients are grouped into different block size and blocks are randomly selected from different subbands. We add different energies to the maximum wavelet coefficient under the constraint that the maximum wavelet coefficient is always maximum in a block. The watermark is embedded the local maximum coefficient which can effectively resist attacks. Also, using the block-based watermarking, we can extract the watermark without using the original image or watermark. Experimental results show that the proposed method is quite robust under either non-geometry or geometry attacks.

1. Introduction

The rapid growth of the Internet and digital media manifests itself in widespread public forms such as the digital image, the MPEG, and so on, because digital media are easy to copy and transmit. Many researchers are aware of the issues of copyright protection, image authentication, proof of ownership, etc. Hence, there are many solutions that have been proposed. The watermarking technique is one of the solutions. This technique embeds information so that it is not easily perceptible; that is, the viewer cannot see any information embedded in the contents. A watermarking technique is referred to as blind if the original image and watermark are not needed during extraction (Chen, Horng, & Lee, 2005; Dugad, Ratakonda, & Ahuja, 1998; Ganic & Eskicioglu, 2004; Inoue, Miyazaki, & Yamamoto, 1998; Tsai, Yu, & Chen, 2000). There are several important issues in the watermarking system. First, the embedded watermark should not degrade the quality of the image and should be perceptually invisible to maintain its protective secrecy. Second, the watermark must be robust enough to resist common image processing attacks and not be easily removable; only the owner of the image ought to be able to extract the watermark. Third, the blindness is necessary if it is difficult for us to obtain the original image and watermark.

Spread spectrum communication is robust against many types of interference and jamming (Pickholtz, Schilling, & Milstein, 1982). In the following paragraphs, we will briefly review some proposed watermarking approaches which are based on the frequency domain (discrete cosine transform (DCT) and discrete wavelet transform (DWT)). Cox, Kilian, and Leighton (1996, 1997) suggested inserting the watermark into the perceptually significant portion of the whole DCT-transformed image, wherein a predetermined range of low frequency components excludes the DC component. This watermarking scheme has been shown to be robust against common attacks, such as compression, filtering, cropping, etc. Kwon, Kim, and Park (1999) embedded the watermark in the variable DCT block size. The block size is determined according to the characteristics of the region in the spatial domain. Langelaar and Lagendijk (2001) proposed a blind watermarking approach called differential energy watermarking. A set of several 8×8 DCT blocks are composed and divided into two parts to embed a watermark bit. The high frequency DCT coefficients in the JPEG/MPEG stream are selectively discarded to produce energy differences in the two parts of the same set.

Although different watermarking approaches are proposed, the DWT approach remains one of the most effective and easy to implement techniques for image watermarking (Meerwald & Uhl, 2001). The most important issue in DWT-based image watermarking is how to choose the coefficients to be embedded. In Dugad et al. (1998), Kim and Moon (1999), Kwon, Ban, and Ha (2001), Wang, Chen, and Cheng (2000), Wang and Huo (1997), and Wang, Su, and Kuo (1998), the watermark is embedded the significant coefficient which is selected from the wavelet coefficients. Wang

* Corresponding author.
E-mail addresses: D9515013@mail.ntust.edu.tw (W.-H. Lin), yrwang@mail.sju.edu.tw (Y.-R. Wang), horngsj@yahoo.com.tw (S.-J. Horng), tkao@tsint.edu.tw (T.-W. Kao), pan@cs.gsu.edu (Y. Pan).

0957-4174/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2009.03.060

et al. (1998) proposed a watermarking method, according to multi-threshold wavelet coding (MTWC) (Wang & Kuo, 1997); the successive subband quantization (SSQ) was adopted to search for the significant coefficients. The watermark is added by quantizing the significant coefficient in the significant band using different weights. Davoine (2000) proposed two watermarking methods. One is the watermark embedded by modifying the triplets of significant coefficients, according to a sequence of information bits. The other considers rectangular blocks of coefficients, and each block is used to embed one watermark bit.

Some researches embed a watermark using block-based DWT. Huang and Yang (2004) proposed a watermarking algorithm based on the DWT. The original image is separated into m blocks, with each of size $n \times n$; then every block is decomposed into a wavelet domain. The watermark is embedded in the wavelet coefficients in the middle and lower subbands of a block in each image. Khelifi, Bouridane, and Kurugollu (2005) proposed an adaptive blind watermarking technique based on the DWT. The original image is separated into non-overlapping blocks classified as uniform or non-uniform blocks using a JND-based classifier. The watermark is embedded in the high subband of each block which is transformed into the DWT according to its classification. Zhang, Wang, and Wen (2004) divided the original image into $n \times n$ blocks and transformed these into a DWT domain. The watermark is embedded by using the mean and the variance of a subband to modify the wavelet coefficient of a block. Hsieh, Tseng, and Huang (2001) proposed a watermarking method based on the qualified significant wavelet tree (QSWT). Wang and Lin (2004) proposed a wavelet-based blind watermarking scheme and each watermark bit is embedded using two trees. One of the two trees is quantized with respect to a quantization index, and both trees exhibit a large statistical difference between the quantized tree and the unquantized tree; the difference can later be used for watermark extraction. Li, Liang, and Niu (2006) improved Wang and Lin's (2004) method, adding the Human Visual System (HVS) to effectively resist geometric attack. Lien and Lin (2006) improved Wang and Lin's (2004) method by using four trees to represent two watermark bits in order to improve visual quality. One of the four trees is quantized according to the binary value of the two embedded watermark bits. Wu and Huang (2007) improved Wang and Lin's method using minimum mean to extract the watermark. Tsai and Lin (2007) proposed a structure based wavelet tree quantization. A super-tree which consists of four wavelet trees is divided into five subblocks. Each subblock is separated into two areas, namely up and low. According to a watermark bit, one of the two areas in each subblock is quantized. But these methods (Li et al., 2006; Lien & Lin, 2006; Tsai & Lin, 2007; Wang & Lin, 2004; Wu & Huang, 2007) cannot effectively resist low-pass filtering such as median filtering or Gaussian filtering.

Previous researches (Dugad et al., 1998; Hsieh et al., 2001; Temi, Choomchuay, & Lasakul, 2005; Wang et al., 2000, 1998; Wang & Huo, 1997) use significant coefficients which are selected from global coefficients are showed that can effectively resist attacks. The problem is that the order of extracting significant coefficients in the extraction process should be exactly the same as those in the embedding process. So, they were unsuitable for the blind watermarking, especially for the attacked watermarked image. For this reason, in this paper, we use the local maximum wavelet coefficient quantization; the wavelet coefficients of a host image are grouped into blocks of variable size. We embed a watermark in different subbands and every block will be used to embed either the watermark bit 0 or bit 1. By adjusting the local maximum wavelet coefficient and maintaining the maximum wavelet coefficient always maximum to present a binary watermark, we embed a watermark bit 1 by increasing the energy of the local maximum wavelet coefficient in a block and embed a watermark bit 0 by decreasing the energy of the local maximum wavelet coefficients in a block. In the extraction process, if we subtract the energy from the local maximum coefficient in a block, and the resulting value is still the maximum in the block, then the block has been embedded with a watermark bit 1; otherwise, the block has been embedded the watermark bit 0. Experimental results show that the proposed method decreases the distortion of the host image and is effectively robust against JPEG compression, low-pass filtering and Gaussian noise, and the PSNR value of a watermarked image is greater than 40 dB.

This paper is organized as follows: In Section 2, we briefly introduce the scan order of wavelet coefficients and the block base significant coefficient. The proposed method is described in Section 3. The experimental results and experimental analysis are given in Section 4. Finally, the conclusions are summed up in Section 5.

2. The scan order of wavelet coefficients and the block-based significant coefficient

2.1. The scan order of wavelet coefficients

A host image of size I_W by I_H is transformed into wavelet coefficients using the L-level discrete wavelet transform (DWT). With an L-level decomposition, we have $3 \times L + 1$ subbands. The LL_L frequency band is found to be unsuitable to be modified since it is a low frequency band which contains important information about an image and easily causes image distortions. Embedding a watermark in the HH_L, $HH_{L-1}, \ldots, HH_1$ subbands is also not suitable, since the subbands can easily be eliminated, for example by lossy compression. In Shapiro (1993), the significant wavelet coefficients are transmitted by the significant frequency subbands. The significant subbands must be transmitted in the order of LL_L, LH_L, HL_L, HH_L, LH_{L-1}, HL_{L-1}, $HH_{L-1}, \ldots$, LH_1, HL_1, and HH_1 as shown in Fig. 1. According to the characteristics of this scan order, we embed the watermark bits into the LH_L and HL_L subbands. Fig. 2 illustrates the watermark embedding procedure using 3-level DWT, and Fig. 3 illustrates the extraction procedure.

2.2. The block-based significant coefficient

As mentioned in Section 1, watermarking is more robust when the watermark bits are embedded in the significant coefficients of the whole frequency domain. But it is not easy to use blind detection to find the permutations in the original order of the significant coefficients. Although there are many block-based watermarking methods are proposed, these methods cannot efficiently resist

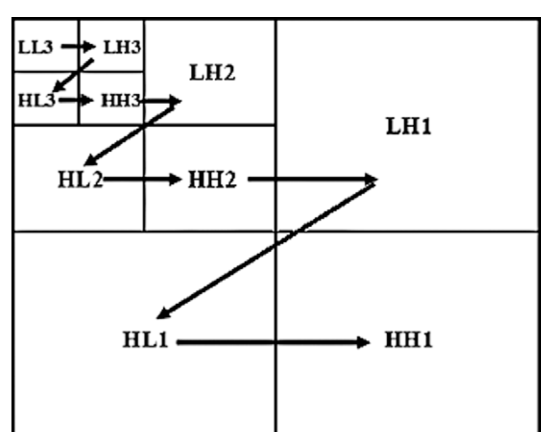


Fig. 1. Transmission of wavelet subbands by scan order.

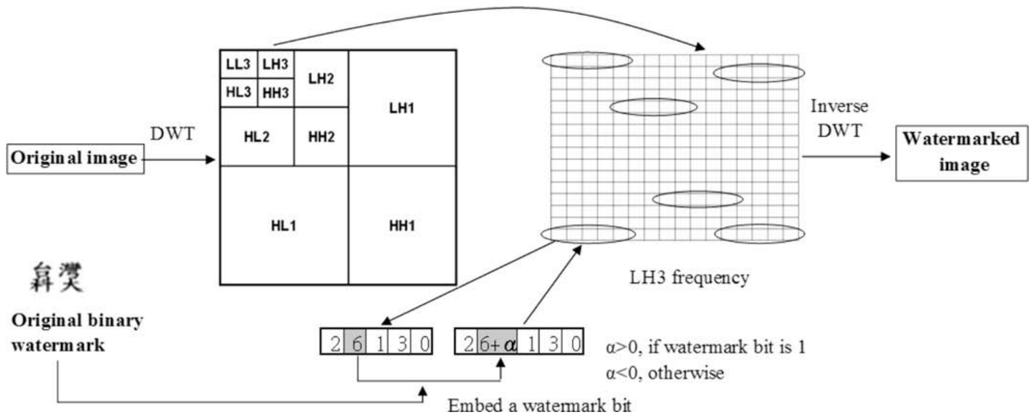


Fig. 2. The watermark embedding procedure: embed a watermark bit by quantizing the maximum wavelet coefficient in a block.

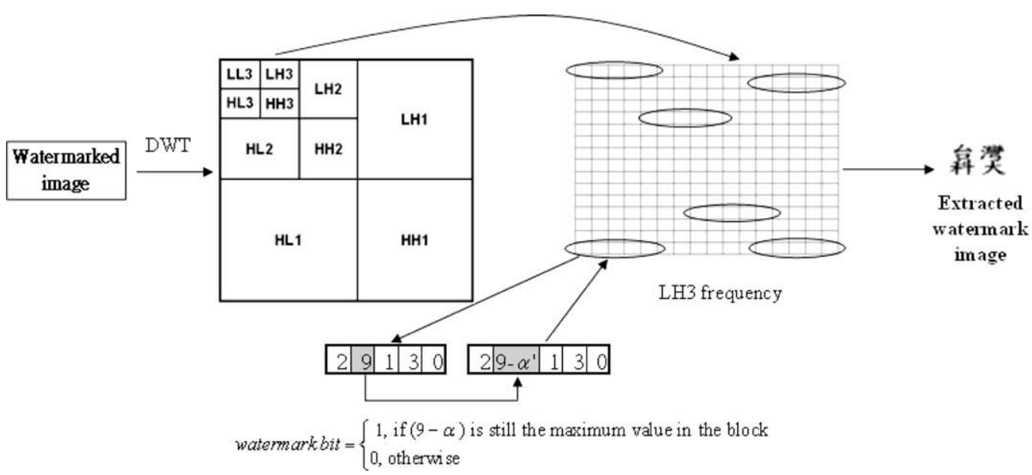


Fig. 3. Watermark extraction procedure.

attacks, since a watermark bit is embedded in the coefficient of a block of size $n \times n$ and the significant coefficients are not considered. To solve the above problems, we group the variable number of the wavelet coefficients from the LH_L and HL_L subbands into a block, each of $Blocks_N$ blocks (see Algorithm 1), then we quantize the maximum coefficient of the block to embed a watermark bit.

Algorithm 1.

$I_L = \left\lfloor I_W/2^L \times I_H/2^L \right\rfloor$.
$AvailCoeff = I_L$.
$J = 1$.
While $(I_L - N_{B,j} >= 0)$ {
  $N_{B,j} \in \{2,3,\ldots,(I_L/N_w)\}$.
  $Blocks_N = Blocks_N + 1$; initially, $Blocks_N = 0$.
  $AvailCoeff = I_L - N_{B,j}$.
  j++;
}

where I_L is the number of wavelet coefficients in the L-level subband; for example, the LH_L subband totally has I_L wavelet coefficients, as does the HL_L subband. I_W and I_H are the width and height of the host image, respectively. N_w denotes the number of watermark bits which are embedded. $N_{B,j}$ denotes the block size of these blocks. $N_{B,j}$ is an integer which ranges from 2 to N_B, where N_B denotes the maximum number of wavelet coefficients in a block, $2 \leqq N_B \leqq (I_L/N_w)$. To avoid $Blocks_N < N_w$ and to assure that there are enough blocks for embedding watermark bits, N_B must be less than or equal to I_L/N_w. For example, if we set $N_B = 7$, then $2 \leqq N_{B,j} \leqq N_B = 7$. Both LH_L and HL_L subbands use the same $N_{B,j}$ to construct a block. Hence, we define

$$Block_{r,j} = N_{B,j} \text{ for } r \in \{0,1\} \text{ and } 1 \leqq j \leqq Blocks_N, \tag{1}$$

where $r = 0$ denotes the LH_L subband and $r = 1$ denotes the HL_L subband. In the jth block, the LH_L subband has $N_{B,j}$ wavelet coefficients as the HL_L subband. When embedding a watermark bit, either $Block_{0,j}$, or $Block_{1,j}$ is used. In the next section, we will use these blocks to embed the watermark.

3. The proposed method

3.1. The preprocess

In the previous section, we have $Blocks_N$ blocks in LH_L and HL_L subbands. In order to decrease the probability that the watermark may be tampered with, each time we must select a block from either $Block_{0,j}$ or $Block_{1,j}$ to embed a watermark bit. We define

$$E = \{e_j | e_j \in \{0,1\}, 1 \leqslant j \leqslant Blocks_N\}, \tag{2}$$

where

$$BlockQue = \{BlockQue_j | Block_{r,j}, r = e_j, 1 \leqslant j \leqslant Blocks_N\}. \tag{3}$$

If $e_j = 0$, then $Block_{0,j}$ is selected; otherwise $Block_{1,j}$ is chosen. Hence, the selected blocks form a set of blocks called *BlockQue*. We shuffle the *BlockQue* blocks in a pseudorandom manner. A pseudorandom order of the numbers from $Blocks_1$ to $Blocks_N$ can be obtained by repeating two random numbers $\lfloor Blocks_N/2 \rfloor$ times; each time we generate two random numbers by using the same seed and taking modulo ($Blocks_N$ +1). Note that we use these two generated random numbers to denote the indices of two blocks. Then the corresponding two blocks indexed by these two generated random numbers are exchanged. For example, if the two generated random numbers are 123 and 33, then block 123 and block 33 are exchanged. A binary watermark W of size N_w ($\leqq Blocks_N$) bits will be embedded. We represent each watermark bit as either 1 or 0. Now, we invoke a pseudorandom function to shuffle N_w bits by using different seeds. According to the watermark bits embedded later, we select N_w non-overlapping blocks from *BlockQue* and compute the average local maximum coefficient of all the N_w blocks using Eq. (4).

$$Mean_{embed} = \frac{1}{N_w}\sum_{i=1}^{N_w} M_i, \tag{4}$$

where

$$M_i = \begin{cases} \max_i, & \text{if } i\text{th watermark bit is } 1, \\ \max_i \times T_1, & \text{otherwise.} \end{cases}$$

$Mean_{embed}$ denotes the average value of the local maximum wavelet coefficients in all N_w blocks; $\max_i$ is the local maximum wavelet coefficient of the ith block, $1 \leqq i \leqq N_w$. The value of $\max_i \times T_1$ will be explained later.

3.2. Watermark embedding

Two types of techniques are proposed for embedding a pre-defined watermark into an image. One is pseudo random Gaussian sequence; the other is binary image or gray image. The former is used for objective detection, the latter is used for subjective detection (Potdar, Han, & Chang, 2005). In this paper, in order to subjectively verify the ownership of an image by extracting a watermark, a binary logo image is used. The watermark bit is either 1 or 0. In the proposed method, the magnitude of the local maximum wavelet coefficient is increased if the watermark bit is 1; otherwise, the magnitude of the local maximum wavelet coefficient is decreased. Each time we embed a watermark bit, we seek the local maximum wavelet coefficient $\max_i$ and the local second maximum wavelet coefficient $\sec_i$. Since we only alter the local maximum wavelet coefficient, if the watermark bit is 1, the remaining coefficients are unchanged. This characteristic can be used in the extraction process. We compute the average coefficient value avg_i of the ith block excluding the local maximum wavelet coefficient $\max_i$. The later value will be referred to in order to quantize the local maximum wavelet coefficient. Hence we quantize $\max_i$ with a reference value α_i which is represented as

$$\alpha_i = Maximum\{|avg_i|, |Mean_{embed} \times T_q|\}. \tag{5}$$

Originally, we use avg_i to quantize $\max_i$, but sometimes the value of avg_i is too close to zero or negligible, which may cause error in the watermark extraction process. Hence we must take both avg_i and $Mean_{embed}$ into consideration. Let T_q be a scale parameter. If the value of $|\text{avg}_i|$ is less than $Mean_{embed} \times T_q$, the reference value α_i is set to $Mean_{embed} \times T_q$; otherwise, it is set to $|\text{avg}_i|$. Finally, if a block is embedded with a watermark bit 1, the $\max_i$ is quantized as

$$\max_i^{new} = \max_i + \alpha_i, \tag{6}$$

where $\max_i^{new}$ is the new value of $\max_i$.

Otherwise, the block is embedded with a watermark bit 0, and the $\max_i$ is quantized as

$$\max_i^{new} = \max_i - \alpha_i, \tag{7}$$

where $\alpha_i = \max_i \times (1 - T_1)$.

Clearly, Eq. (7) can be rewritten as

$$\max_i^{new} = \max_i \times T_1.$$

Suppose that $\max_i^{new} < \sec_i$, $\sec_i$ is then quantized as

$$\sec_i^{new} = \sec_i \times T_2, \tag{8}$$

where $\sec_i^{new}$ is the new value of $\sec_i$. Both T_1 and T_2 are threshold values; in the experiment, we set $T_1 = 0.1$, and $T_2 = 0.3$. By reducing the values of $\max_i$ and $\sec_i$, the accuracy in the extraction process can be increased, although the value of $\max_i \times T_1$ is still less than the value of $\sec_i \times T_2$.

In Fig. 4, we plot the peak signal-to-noise ratio (PSNR) (see Eq. (14)) for the selected Baboon, Lena and Peppers images (512×512 pixels, 8 bits/pixel) with different T_q values, ranging from 0.1 to 1, where $T_1 = 0.1$, $T_2 = 0.3$, $N_w = 512$, and we use 3-level DWT. We also show the average PSNRs of other 12 commonly used images obtained from Petitcolas (1997). Fig. 4 shows that the larger the T_q is, the more robust the watermark will be; however, in the meanwhile, the image distortion increases as well. The issue is how to tradeoff between the robustness and the quality of the images. In the experiment, if we set $T_q = 0.7$, then the corresponding PSNRs of all the images are greater than 40 dB.

3.3. The decoder design

In the proposed method, an original image or an original watermark logo is not required for the extraction process. In the preprocess stage of the extraction process, we generate *BlockQue* from the watermarked image the same as in the embedding process. We shuffle the blocks using the same seed as used in the embedding process. During the embedding process, the energy α_i is added to the local maximum wavelet coefficient. When the value of α_i is subtracted from the local maximum wavelet coefficient $\max_i'$ of a watermarked image, if the value of $\max_i'$ is still the local maximum in a block, there is a high probability that the block has been embedded a watermark bit 1. Therefore, it is very important to find the suitable α_i value.

In Eq. (5), α_i is obtained from either avg_i or $Mean_{embed} \times T_q$. There are two conditions if the block is embedded with a watermark bit 1. One is that α_i is set to avg_i. Since the value of avg_i is unchanged, the value of α_i can be found, and the watermark bit 1 can be extracted in the extraction process. The other condition is that α_i is set to $Mean_{embed} \times T_q$. In the extraction process, the value of $Mean_{embed}$ cannot be obtained, hence the value of α_i also cannot be obtained. To extract the watermark, we must use another value to substitute for $Mean_{embed} \times T_q$.

Here, some values are calculated in a process that is similar to the embedding process. In Eq. (9), the average maximum wavelet coefficient of the watermarked image is obtained.

$$Mean_{extract} = \frac{1}{N_w}\sum_{i=1}^{N_w} \max_i'. \tag{9}$$

In Eq. (5), the value of α_i is not added to $Mean_{embed}$ when the block has an embedded watermark bit 1. So the value of $Mean_{extract}$ is larger than $Mean_{embed}$. Then, the value of $Mean_{block}$ in all N_w blocks is computed by Eq. (10).

$$Mean_{block} = \frac{1}{N_w}\sum_{i=1}^{N_w} |avg_i'|, \tag{10}$$

where avg_i' is the average coefficient value of the ith block excluding $\max_i'$. If avg_i' is negative, the value is transformed using the absolute value. Finally the value of α_i' is obtained by Eq. (11).

$$\begin{aligned} \alpha_i' &= (|Mean_{block}| + \sigma_1 + \sigma_2), \\ \sigma_1 &= \max_i'/Mean_{extract}, \\ \sigma_2 &= avg_i'/Mean_{block}, \end{aligned} \tag{11}$$

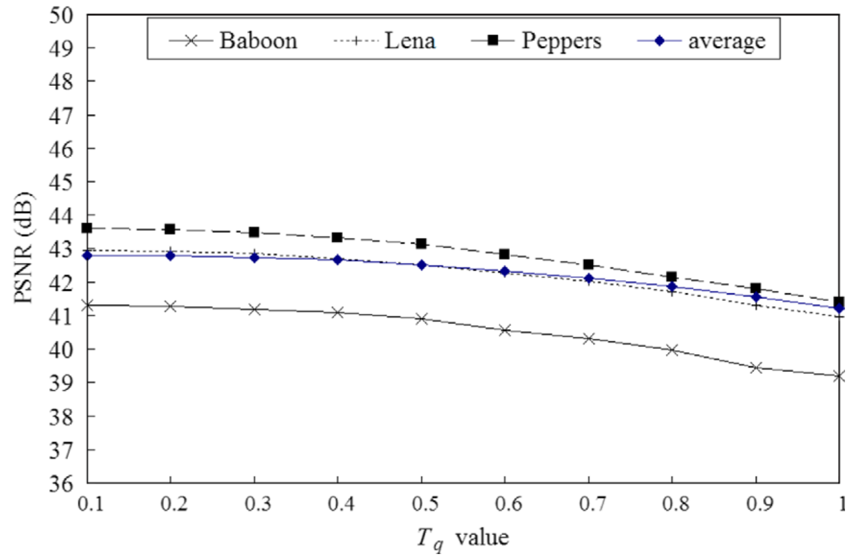


Fig. 4. The T_q value vs. PSNR.

where σ_1 and σ_2 are biased. The value σ_1, which is obtained from the block embedded with a watermark bit 1, is greater than the value σ_1 which is obtained from the block embedded with a watermark bit 0 in the extraction process. The above is also the case applied for σ_2, since the value of $\sec_i$ is somewhere between $\max_i$ and avg_i; if avg'_i is obtained from the block embedded with a watermark bit 1, then it will be greater than the value of avg'_i which is obtained from the block embedded with a watermark bit 0 in the extraction process.

3.4. Watermark extraction

Eq. (11) is rearranged as follows:

$$\alpha'_i = Maximum\{|avg'_i|, |Mean_{block}| + \sigma_1 + \sigma_2\}. \tag{12}$$

The watermark can be obtained by Eq. (13).

$$watermarkbit = \begin{cases} 1, & \text{if } (\max'_i - \alpha'_i) \geqslant \sec'_i, \\ 0, & \text{otherwise}. \end{cases} \tag{13}$$

If after the value of α'_i is subtracted from $\max'_i$, the remainder value of $\max'_i$ is still the local maximum in the ith block (i.e., $\max'_i - \alpha'_i$ is greater than or equal to $\sec'_i$), then the block is embedded with a watermark bit 1. Otherwise, the block is embedded with a watermark bit 0. By using Eqs. (11)–(13) on the remaining $N_w - 1$ blocks, the watermark image can be extracted.

4. Experimental results

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between an attacked image and the original image. For the sake of completeness, we list the PSNR formula as follows:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{I_H \times I_W} \sum_{x=0}^{I_H-1} \sum_{y=0}^{I_W-1} [f(x,y) - g(x,y)]^2} dB, \tag{14}$$

where I_W and I_H are the height and width of the image, respectively. $f(x, y)$ and $g(x, y)$ are the values located at coordinates (x, y) of the original image, and the attacked image, respectively.

After extracting the watermark, the normalized correlation coefficient (NC) is computed using the original watermark and the extracted watermark to judge the existence of the watermark and to measure the correctness of an extracted watermark. It is defined as

$$NC = \frac{1}{w_h \times w_w} \sum_{i=0}^{w_h-1} \sum_{j=0}^{w_w-1} w(i,j) \times w'(i,j), \tag{15}$$

where w_h and w_w are the height and width of the watermark, respectively. $w(i, j)$ and $w'(i, j)$ are the watermark bits located at coordinates (i, j) of the original watermark and the extracted watermark. Here $w(i,j)$ is set to 1 if it is watermark bit 1; otherwise, it is set to -1. $w'(i, j)$ is set in the same way. So the value of $w(i, j) \times w'(i, j)$ is either -1 or 1.

We used three images for the experiments, namely Lena, Goldhill, and Peppers (512×512 pixels, 8 bits/pixel). They were obtained from Petitcolas (1997). We predetermine the scale parameter T_q at 0.7, $L = 3$, and the threshold values T_1 and T_2 as 0.1 and 0.3, respectively. The PSNRs of the three watermarked images (Lena, Goldhill, and Peppers) are 42.02, 42.58, and 42.53 dB, respectively. For brevity, only the Peppers image is shown. Fig. 5 shows the original image and the binary watermark. Fig. 6 shows the unattacked watermarked image and the extracted result.

Here we consider both geometric and nongeometric attacks. The tools of the Stirmark benchmark (Petitcolas, 1997) and PhotoImpact 11 software (Ulead Systems, Inc., 2005) are used to simulate these attacks. Nongeometric attacks include JPEG compression, low-pass filtering, histogram equalization, and sharpening.

(a) (b)

Fig. 5. (a) The original image of Peppers of size 512×512 and (b) the original binary watermark of size 32×16.

Fig. 6. (a) Watermarked Peppers with PSNR=42.53 dB. (b) The extracted watermark with NC = 1.

JPEG is one of the most frequently used formats on the Internet and in digital cameras. The JPEG quality factor is a number between 0 and 100 and associates a numerical value with a particular compression level. When the quality factor is decreased from 100, the image compression is improved, but the quality of the resulting image is significantly reduced. Varied quality factors (Petitcolas, 1997) are applied in the experiments, and the results are shown in Table 1. The proposed method can detect the existence of a watermark through quality factors greater than 20. The results show that the value of NC is still greater than 0.67.

For other nongeometric attacks (Petitcolas, 1997), for example median filters, Gaussian filter, average filters, sharpening, and histogram equalization, the resulting images are blurred or sharpened at the edge (Gonzalez & Woods, 2002), and shown in Table 2. The proposed method can effectively resist attacks such as median filter with a mask of size 5×5, or average filter with a mask of size 5×5. For geometric attacks, rotation, scaling, Gaussian noise and cropping are used. The rotational attacks are performed by rotating an image at a small angle, scaling the rotated image, and cropping the scaled image to the original image size (Petitcolas, 1997). For a pixel-based watermarking system, although an image is rotated in a small degree, the positions of pixels will be shifted. It is then difficult to recover the original image from a rotational image. The result of grouping coefficients into blocks for a rotation image will be quite different from that of the original image. Though the rotation attack does not cause the image serious visual distortion, it will cause errors in the watermark extraction process. The results are shown in Table 3. The attack of scaling is performed by first shrinking an image of pixels 512×512 to 256×256 via PhotoImpact 11 software, and then open the above image of pixels 256×256 to resize them back to pixels 512×512. The resulting extracted watermark is shown in Table 3. The noise variation is varied from 1 to 3 with the step size of 1; for the cropping attack, an image of 1/4 size is cropped via PhotoImpact 11 software, and each cropped pixel is replaced with 255, hence the size of the cropped image is still 512×512; the results are also shown in Table 3.

4.1. Experimental analysis

We compare the proposed method to Wang and Lin's (2004), Li et al.'s (2006), and Lien and Lin's (2006) methods using the Lena image; the results are shown in Table 4. Their watermarking approaches are blind and their methods are based on wavelet-tree quantization. Although Lien improves on Wang and Lin's (2004) approach to watermarked image quality, our method's PSNR is higher than Lien's. Moreover, our proposed method is better than theirs in robustness.

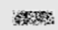
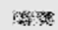
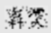
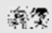
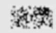
Table 1
Normalized correlation coefficients (NC) after attacked by JPEG compression with the quality factors (QF) 10, 15, 20, 25, 30, 35, 40, 50, 60, 70, 80, 90, and 100 on (a) Lena, (b) Goldhill, and (c) Peppers.

QF	10	15	20	25	30	35	40	50	60	70	80	90	100
(a) Lena													
NC	0.34	0.55	0.67	0.74	0.82	0.85	0.90	0.96	0.95	0.97	0.99	0.99	1.00
EXtracted watermark													
(b) Goldhill													
NC	0.30	0.58	0.69	0.77	0.81	0.84	0.88	0.90	0.95	0.96	0.97	0.98	1.99
EXtracted watermark													
(c) Peppers													
NC	0.35	0.53	0.72	0.81	0.86	0.90	0.93	0.96	0.96	0.97	0.99	0.99	1.00
EXtracted watermark													

Table 2
Normalized correlation coefficients (NC) after attacked by median filter (3×3, 5×5, 7×7), Gaussian filtering, average filtering attacks (3×3, 5×5, 7×7), sharpening, and histogram equalization of the three test images. (a) Lena, (b) Goldhill, and (c) Peppers.

Neogeometric attacks	Median filter			Gaussian filter	Average filter			Sharpening	Histogram equalization
	(3×3)	(5×5)	(7×7)		(3×3)	(5×5)	(7×7)		
(a) Lenna									
NC	0.90	0.76	0.53	0.88	0.95	0.80	0.47	0.97	0.79
EXtracted watermark									
(b) Goldhill									
NC	0.85	0.66	0.37	0.93	0.91	0.76	0.48	0.95	0.68
EXtracted watermark									
(c) Peppers									
NC	0.92	0.75	0.46	0.92	0.94	0.76	0.43	0.96	0.89
EXtracted watermark									

Table 3
Normalized correlation coefficients (NC) after attacked by scaling 256 × 256, cropping 1/4, Gaussian noise added by variations from 1 to 3, and rotation flow by scaling and cropping to the original size of the three test images.

Geometric attacks	Scaling	Cropping	Gaussian noise			Rotation			
			Variance 1	Variance 2	Variance 3	Degree 0.25	Degree 0.3	Degree −0.25	Degree −0.3
(a) Lenna									
NC	0.88	0.66	0.81	0.62	0.34	0.59	0.45	0.60	0.52
Extracted watermark									
(b) Goldhill									
NC	0.84	0.65	0.85	0.54	0.32	0.54	0.44	0.51	0.44
Extracted watermark									
(c) Peppers									
NC	0.88	0.64	0.90	0.59	0.46	0.65	0.55	0.61	0.55
Extracted watermark									

(a) Lena, (b) Goldhill, and (c) Peppers.

Table 4
Comparing the proposed method with Wang and Lin's (2004), Li et al.'s (2006), and Lien and Lin's (2006) methods.

Attacks \ NC	Wang and Lin (2004) (PSNR = 38.2 dB)	Li et al. (2006) (PSNR = 40.6 dB)	Lien and Lin (2006) (PSNR = 41.54 dB)	Proposed method (PSNR = 42.02 B)
Median filter (3 × 3)	0.51	0.35	0.79	0.90
Median filter (4 × 4)	0.23	0.26	0.51	0.76
Median filter (7 × 7)	NA	NA	NA	0.53
JPEG (QF = 10)	NA	0.15	0.17	0.34
JPEG (QF = 20)	NA	0.34	0.61	0.67
JPEG (QF = 30)	0.15	0.52	0.79	0.82
JPEG (QF = 50)	0.28	0.52	0.89	0.96
JPEG (QF = 70)	0.57	0.63	0.97	0.97
JPEG (QF = 90)	1	0.78	1	0.99
Sharpening	0.46	0.38	0.88	0.97
Gaussian filter	0.64	0.70	0.84	0.88
Rotation (degree: 0.25°)	0.37	0.46	0.53	0.59
Rotation (degree: −0.25°)	0.32	0.50	0.47	0.60
Cropping 1/4	NA	0.61	0.92	0.66
Scaling 256 × 256	NA	0.35	0.79	0.88

Unit of rotationt: degree (+: clockwise; −: counter clockwise).

5. Conclusion

In this paper, a blind watermarking method based on the DWT using maximum wavelet coefficient quantization is proposed. The proposed method is different from the block-based or wavelet-tree based methods which are discussed in Section 1. In order to achieve the secrecy of embedding watermark, we use variable blocks size and embed a watermark bit using different subbands which are selected randomly from two subbands. As a result, in the proposed method the watermarked images look lossless in comparison to the original images and the watermark can effectively resist common image processing attacks, especially by JPEG compression (with a quality factor greater than 20) and low-pass filter. Moreover, the proposed method is more robust in resisting common attacks such as median filter 5 × 5, average filter 5 × 5, and Gaussian noise with a variation of less than 2. In addition to copyright protection, the proposed scheme can also be applied to data hiding and image authentication.

Acknowledgement

This work was partially supported by National Science Council of Taiwan under the Contract Numbers NSC-97-2221-E-129-007 and NSC-97-2221-E-239-022.

References

Chen, T. H., Horng, G., & Lee, W. B. (2005). A publicly verifiable copyright-proving scheme resistant to malicious attacks. *IEEE Transactions on Industrial Electron, 52*(1), 327–334.

Cox, I. J., Kilian, J., Leighton, T., et al. (1996). Secure spread spectrum watermarking for images, audio and video. In *Proceedings of the IEEE ICIP*, Lausanne, pp. 243–246.

Cox, I. J., Kilian, J., Leighton, F. T., et al. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing, 6*(12), 1673–1687.

Davoine, F. (2000). Comparison of two wavelet based image watermarking schemes. In *International Conference on Image Processing*, Vancouver, pp. 682–685.

Dugad, R., Ratakonda, K., & Ahuja, N. (1998). A new wavelet-based scheme for watermarking images. In *IEEE ICIP*, Chicago, IL, pp. 419–423.

Ganic, E., & Eskicioglu, A. M. (2004). Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In *International Multimedia Conference on Multimedia and Security*, Magdeburg, pp. 166–174.

Gonzalez, R. C., & Woods, R. E. (2002). *Digital image processing* (2nd ed.). Prentice-Hall.

Hsieh, M., Tseng, D., & Huang, Y. (2001). Hiding digital watermarks using multiresolution wavelet transform. *IEEE Transactions on Industrial Electronics, 48*(5), 875–882.

Huang, J., & Yang, C. (2004). Image digital watermarking algorithm using multiresolution wavelet transform. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, pp. 2977–2982.

Inoue, H., Miyazaki, A., Yamamoto, A., et al. (1998). A digital watermark based on the wavelet transform and its robustness on image compression. In *Proceedings of the IEEE ICIP*, Chicago, pp. 391–395.

Khelifi, F., Bouridane, A., Kurugollu, F., et al. (2005). An improved wavelet-based image watermarking technique. In *Proceedings of the IEEE AVSS*, Como, 2005, pp. 588–592.

Kim, J. R., Moon, Y. S. (1999). A robust wavelet-based digital watermarking using level-adaptive thresholding. In Proceedings of the IEEE ICIP, Kobe, pp. 226–230.

Kwon, S. G., Ban, S. W., Ha, I.-S., et al. (2001). Highly reliable digital watermarking using successive subband quantization and human visual system. In *Proceedings of IEEE ISIE*, Pusan, pp. 205–209.

Kwon, O. H., Kim, Y. S., & Park, R. H. (1999). A variable block-size dot-based watermarking method. *IEEE Transactions on Consumer Electronics, 45*(4), 1221–1229.

Langelaar, G. C., & Lagendijk, R. L. (2001). Optimal differential energy watermarking of DCT encoded images and video. *IEEE Transactions on Image Processing, 10*(1), 148–158.

Lien, B. K., & Lin, W. H. (2006). A watermarking method based on maximum distance wavelet tree quantization. In *19th Conference on Computer Vision, Graphics and Image Processing*, pp. 269–276.

Li, E., Liang, H., & Niu, X. (2006). An integer wavelet based multiple logo-watermarking scheme. In *Proceedings of the IEEE WCICA*, pp. 10256–10260.

Meerwald, P., & Uhl, A. (2001). A survey of watermark-domain watermarking algorithms. In *Proceedings of the SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, pp. 505–516.

Petitcolas, F. A. P. (1997). *Weakness of existing watermark scheme*. Available from: <http://www.petitcolas.net/fabien/watermarking/stirmark/index.html>.

Pickholtz, R., Schilling, D., & Milstein, L. (1982). Theory of spread-spectrum communications – A tutorial. *IEEE Transactions on Communication, 30*(5), 855–884.

Potdar, V. M., Han, S., & Chang, E. (2005). A survey of digital image watermarking techniques. In *Proceedings of the IEEE INDIN*, pp. 709–716.

Shapiro, J. M. (1993). Embedded image coding using zerotrees of wavelet coefficients. *IEEE Transactions on Signal Processing, 41*(12), 3445–3462 [see also IEEE Transactions on Acoustics, Speech, Signal Processing].

Temi, C., Choomchuay, S., & Lasakul, A. (2005). A robust image watermarking using multiresolution analysis of wavelet. In *Proceedings of the IEEE ISCIT*, pp. 623–626.

Tsai, M. J., & Lin, C. L. (2007). Constrained wavelet tree quantization for image watermarking. In *Proceedings of the IEEE ICC Glasgow*, Scotland, pp. 1350–1354.

Tsai, M. J., Yu, K. Y., & Chen, Y. Z. (2000). Wavelet packet and adaptive spatial transformation of watermark for digital images authentication. In *Proceedings of the IEEE ICIP*, Vancouver, BC, pp. 450–453.

Ulead Systems, Inc., PhotoImpact 11 software.

Wang, H. J., Huo, C. C. J. (1997). A multi-threshold wavelet coder (MTWC) for high fidelity image compression. In *Proceedings of the IEEE ICIP*, Santa Barbara, pp. 652–655.

Wang, H. J., & Kuo, C. C. J. (1997). High fidelity image compression with multithreshold wavelet coding (MTWC). In *SPIE's Annual Meeting-Application of Digital Image Processing XX*, San Diego, 1997, pp. 383–392.

Wang, Y. P., Chen, M. J., & Cheng, P. Y. (2000). Robust image watermark with wavelet transform and spread spectrum techniques. In *Thirty-Fourth Asilomar Conference on Signals*. *Systems and Computers* (pp. 1846–1850). Pacific Grove.

Wang, S. H., & Lin, Y. P. (2004). Wavelet tree quantization for copyright protection watermarking. *IEEE Transactions on Image Processing, 13*(2), 154–165.

Wang, H. J., Su, P. C., & Kuo, C. C. J. (1998). Wavelet-based digital image watermarking. *Optics Express, 3*(12), 491–496.

Wu, G. D., & Huang, P. H. (2007). Image watermarking using structure based wavelet tree quantization. In *ICIS*, Melbourne, Australia, pp. 315–319.

Zhang, G., Wang, S., & Wen, Q. (2004). An adaptive block-based blind watermarking algorithm. In *Proceedings of the IEEE ICSP*, pp. 2294–2297.