A Discrete Wavelet Transform Based Robust Watermarking for Copyright Protection

WEN-TZENG HUANG 1, SUN-YEN TAN 2, YUAN-JEN CHANG 3, CHIN-HSING CHEN 3

1 Department of Computer Science and Information Engineering
Mingsin University of Science and Technology
No.1, Xinxing Rd., Xinfeng Hsinchu 30401, Taiwan, R.O.C.
wthuang@must.edu.tw

2 Department of Electronic Engineering
National Taipei University of Technology
No. 1, Sec. 3, Chung-hsiao E. Rd., Taipei, 10608, Taiwan, R.O.C.
sytan@ntut.edu.tw

3 Department of Management Information Systems
Central Taiwan University of Science and Technology
No.666, Buzih Road, Beitun District, Taichung City 40601, Taiwan, R.O.C.
{ronchang, chchen}@ctust.edu.tw

Abstract: - Digital watermarking is a simple and effective way to provide copyright protection. This paper proposes a robust and blind watermarking scheme for static images. It utilizes discrete wavelet transform and applies three coding methods according to the different characteristics of band coefficients: lattice code based on the communication principle, modification of insignificant coefficients based on the just-noticeable distortion of the human visual model, and quantization index modulation based on singular value decomposition. Together, these methods embed a watermark while maintaining image fidelity. The experimental results prove that the proposed method is robust against frequency-based and time domain geometric attacks.

Key-Words: - Digital watermark, Discrete wavelet transform, Copyright protection, Watermark Extraction Procedure, Watermark Verification.

1 Introduction

Intellectual property is thoroughly protected by law to ensure that the rights of original authors are not violated by others. However, while all materials that take time and effort to produce qualify for protection, it is becoming increasingly difficult to prove who created a given work in the current digital era. Due to the rapid development of information and computer technologies, more and more information is presented in digital form, which is very easy to duplicate, store, and revise. The Internet also makes digital materials easy to distribute. In addition, digital works can be pirated, and any signatures or other markings used to identify them can be easily altered. This has led to an “epidemic” of unauthorized materials being spread via the Internet without the consent of the original authors, which in many cases has caused huge damage to the owners of such works. Therefore, it is important to develop different methods for enhancing the protection of intellectual property. Digital watermarks are one such technique [1]. Watermarking technology can be used to hide discernible copyright information in target media efficiently and cheaply, and if a problem arises, one can retrieve the information to prove who the legal owner is.

The paper is organized as follows: In Section 2, we review the digital watermark. Then, in Section 3, we describe our proposed watermarking scheme. In Section 4, experimental results are presented. Finally, a conclusion is given in Section 5.

2 Digital watermark

In 1997, Cox et al. [2] proposed using the spread spectrum of communication to embed a digital watermark in an image. It utilizes random serial numbers generated by Gaussian-spreading numeric code, and then uses these numbers as alternating (AC) parameters for a discrete cosine transform (DCT) function. This method successfully resists
common media/digital attacks. However, it requires
information from the original image to retrieve the
watermark; that is, it is a non-blind watermark. In
using coefficients derived from discrete wavelet
transform (DWT). In this scheme, all wavelet
coefficients are grouped into “data trees” that are
further organized into a larger structure called a super
tree. This method requires no information from the
original image; that is, it is a blind watermark. The
virtue of this method is that it can detect the
watermark even after attacks such as image
compression and space filtering. However, some
degradation of image quality occurs. In 2006, Yu and
Liu [4] proposed a blind marking method that uses
the error ranges of DCT and inverse DCT to define an
embedding threshold for modifying watermark
coefficients.

3 Proposed watermarking scheme

Lattice Coding

We employ lattice coding [5], which assumes
that reference vectors point to elements. The result of
N elements derived from the lattice code can be
taken as a set of N reference vectors and a set of
integer N elements, as shown in equation (1), where
w_v is a set of reference vectors, z is a set of integers,
and w_r is an approach (dithered index modulation,
[6][7]) to find integers between the vector v and
reference vector. To calculate each integer, the length
of the vector that projects to w_r is first calculated, as
shown in equation (2). Then this vector length is
divided by the length of the reference vector w_r to
obtain the closest integer to the quotient, as shown in
equation (3). To encode with external information,
we first need to define the total number of symbols S
that are to be encoded, represented as m[i], where
(1 ≤ i ≤ N) and N is the total number of messages.
After adding external information, the closest integer
between vector v and the reference vector w_r is
determined as shown in equation (4).

\[ w_m = \sum_{i=1}^{N} z[i] w_r \]  

(1)

\[ l[i] = \frac{v \cdot w_r}{|w_r|} \]  

(2)

\[ z[i] = \left[ \frac{l[i]}{|w_r|} + 0.5 \right] = \frac{v \cdot w_r}{|w_r|} + 0.5 \]  

(3)

\[ z_m[i] = S \left[ \frac{l[i]}{|w_r|} \frac{|m[i]|}{S} + 0.5 \right] + m[i] \]  

(4)

To adjust embedding robustness, we multiply the
reference vector by a robustness parameter \( \beta \),
modifying (4) to become equation (5).

After calculating \( z_m[i] \), the reference vector of the
embedded watermark can be derived using equation
(6). Adding the results to the original image blocks
embeds the watermarks.

\[ z_m[i] = 2 \left[ \frac{l[i}/|w_r| - m[i]}{2} + 0.5 \right] + m[i] \]  

(5)

\[ w_a = \beta z_m[i] w_r \]  

(6)

Equation (7) is used to retrieve a watermark
using lattice coding. The equation uses the integer z
to determine the bit value of the embedded
watermark. If z is odd then the watermark bit is 1;
otherwise it is 0.

\[ z = \frac{v \cdot w_r}{\beta (w_r \cdot w_r)} + 0.5 \]  

(7)

Adjustment Coefficients Based on DWT
Domain Just-Noticeable Distortion

In this section, we describe watermarking that
uses just-noticeable distortion (JND), which
determines threshold values in the wavelet subbands,
HL2 and LH2, and then uses them to embed
watermarks [8][9][10]. The purpose of JND is to
adjust the gray level or coefficient to the maximum
value that cannot be detected by the human eye [8]. It
is based on four factors related to the noise sensitivity
of the human eye: background luminance, edge
proximity, band sensitivity, and texture masking.

Equations (8)–(11) calculate the JND value
from four input parameters, where \( r \), \( s \), \( x \), and \( y \) [ represent the scale \( r \in \{0,1,2,3\} \) and
wavelet band \( s \in \{LL, LH, HL, HH\} \) of the
wavelet transform, based on the x and y
coordinates of the wavelet coefficients, and \( \alpha \) is a constant. Equation (9) is based on the mathematical
model of the Human Vision System (HVS), which
images content under different frequencies. This equation defines changes in luminance and hue, based on the sensitivity of the human eye, in different wavelet transform levels and wavelet bands. Equation (10) is based on Weber’s law [11] and assumes that human eyes are less sensitive to changes in noise when viewing an object against a bright background. Equation (11) assumes that human eyes are less sensitive to noise changes against high-density textures. The sum of the luminance variable in the low-frequency band and the edge variance in the high-frequency band determines the texture of an image [12].

\[
JND(r, s, x, y) = \alpha \cdot \text{frequency}(r, s) \cdot \text{bright}(r, x, y) \cdot \text{texture}(r, x, y)^{0.034}
\]

\[
frequency(r, s) = \begin{cases} 
\sqrt{2}, & \text{if } s = \text{HH} \\
1, & \text{otherwise} 
\end{cases}
\]

\[
bright(r, x, y) = 3 + \frac{1}{256} \sum_{i=1}^{2} \sum_{j=1}^{2} I^{|L^L}_{r} (i+x, j+y)
\]

\[
texture(r, x, y) = \sum_{k=0}^{L^L} \sum_{i=1}^{L^H} \sum_{j=1}^{L^H} \left( \frac{I^{|L^L}_{r,s} (i+ \frac{x}{2^k}, j+ \frac{y}{2^k})}{16^k} \right)^2 + \sigma^2 (I^{|L^L}_{r,s} (\{1,2\} + x, \{1,2\} + y))
\]

JND-based watermarking assumes that most wavelet coefficients will be close to zero in the frequency bands HL2 and LH2. We calculate the JND values for the HL2 and LH2 bands and use the smallest JND as the embedding threshold value. If the absolute value of the wavelet coefficient is greater than the threshold, then that coefficient is considered an important one; otherwise it is defined as an unimportant coefficient. To embed a watermark, we separate HL2 and LH2 into 8 × 8 blocks, each with 64 wavelet coefficients. The wavelet coefficients are modified according to the value of each watermark bit. If a watermark bit is equal to 1, then the first 32 unimportant coefficients are replaced by the corresponding JND values and the polarity is left unchanged. Otherwise, the last 32 unimportant coefficients are modified.

**Watermarking by Singular Value Decomposition Quantization Index Modulation**

Equation (12) describes an N × N image \( A \) based on three N × N singular value decomposition (SVD) matrices, where \( U \) and \( V \) are two orthogonal matrices. If \( A \) is symmetric, \( U \) will be equal to \( V \). The diagonal component of matrix \( S \) is the eigenvalue of \( A \). This eigenvalue is a singular value composed of N nonzero singular values, organized in decreasing numerical order from the top left to the bottom right of the matrix. SVD has an intriguing mathematical virtue, whereby a singular value represents the luminance of a target image and \( U \) and \( V \) represent the geometry of the image: a bigger singular value will not only maintain image intensity better but will also be most robust against attacks. Also, a slight change to a singular value will not be noticed by the human eye [13].

\[
A = USV^T
\]

To embed watermark bits using a SVD Quantization Index Modulation (QIM), we separate the HH1 subband into 16 × 16 blocks, decompose each block with SVD, and then calculate the Euclidean distance of the diagonal singular matrix. To extract watermark bits using SVD and QIM, the Euclidean distance of each singular value is dividing by the quantized step to determine the integer. If the integer is an odd number, the embedded watermark bit is 1; otherwise it is 0.

Arnold’s cap map [14] is an important encryption technique used to improve the security of digital watermarks. It exhibits periodicity depending on the size of a watermark logo, whereby after several transform processes, the logo will revert back to the original one. So it can be viewed as a key for retrieving the watermark.

**Watermark Verification**
To verify an extracted watermark, we use normalized correlation (NC) as shown in equation (13), where \( W \) and \( W' \) are the original and extracted watermarks, and \( N_w \) is the number of watermark bits, respectively.

\[
NC(W, W') = \sum_{m=1}^{N_w} w_m w'_m / N_w \tag{13}
\]

The closer the resulting NC value is to 1, the higher the similarity will be between the extracted and original watermark.

**Watermark Extraction Procedure**

1. Apply two-level DWT decomposition to the watermarked image, divide each LL2, LH2, and LH2 subband into \( 8 \times 8 \) blocks and each HH1 subband into \( 16 \times 16 \) blocks, where \( Ci \) \( \{i=1,2,3..., N \} \) and \( N \) is the number of blocks.

2. For \( i = 0 \) to \( N - 1 \)
   - if \( s = LL2 \) then
     \[
     W1i = \text{Lattice\_decode}(Ci , \beta);
     \]
   - else if \( s = LH2 \) or \( s = HL2 \) then
     \[
     W2i = \text{Coefficients\_Compare}(Ci , T);
     \]
   - else if \( s = HH1 \) then
     \[
     W3i = \text{SVD\_QIM\_decode}(Ci , qs );
     \]
   end if
end for

3. Apply Arnold’s cap map transform using the embedding key to obtain the original watermark.

**4 Experimental results**

The watermark used in this experiment was a 256-bit binary image as shown in Fig. 2. After the Arnold’s cap map process, we presented it with a \( \{1,-1\} \) series and then embedded it into a \( 512 \times 512 \) Lena grayscale image as shown in Fig. 3. To demonstrate the robustness of the proposed watermarking scheme, we performed seven different attacks on the watermarked image and then compared the results to previous watermarking schemes [3][4]. The experimental results are presented in Figures 4–6. The watermark produced by our proposed scheme performed much better than those produced by previous methods.
5 Conclusion

A robust, blind watermarking method was presented in this paper. It embeds a watermark using a gray-level image to perform two-level wavelet transform and modify wavelet coefficients using four different methods according to the differences in wavelet coefficients on different wavelet subbands. According to the results of an experiment, our method improves the robustness of watermarks. Our method has the following features: it only slightly modifies wavelet parameters, minimizing image degradation and provides better protection against various attacks.

6 Acknowledgment

The authors would like to thank the National Science Council of the Republic of China for financially supporting this research under Contract NSC 98-2218-E-002-010- and 98-2221-E-166-008-.

References: