Wavelet Tree Group Modulation (WTGM) for Digital Image Watermarking*

Min-Jen Tsai and Chang-Hsing Shen

Institute of Information Management, National Chiao Tung University, R.O.C.

ABSTRACT

Differential Energy Watermarking (DEW) based techniques have been applied in DEW, modified schemes of DEW or Wavelet Tree Quantization (WTQ) algorithms by differentiating the transformed coefficient energy to verify the watermark embedding for copyright protection and ownership verification. In this paper, we present a novel differential energy watermarking algorithm based on the wavelet tree group modulation (WTGM) structure. The wavelet coefficients of the image are divided into disjoint tree groups and each tree group contains two sub tree groups. The watermark is embedded in the tree components using the group strategy such that the energy of tree groups is close and each sub-group performs different modulation for watermark embedding. Therefore, the employment of wavelet tree structure, sum-of-subsets and positive/negative modulation effectively improve the watermark robustness. In addition, the contrast sensitive function (CSF) and noise visibility function (NVF) of human visual system are also considered for the better visual quality of the watermarked image. The experimental results demonstrate the effectiveness of WTGM algorithm in terms of robustness and imperceptibility of watermarking.

Index Terms—quantization, copyright protection, wavelet.

1. INTRODUCTION

As digital data are widely available online or elsewhere, and because they are easy to be modified, necessary works are required to protect the copyright and the verification of the embedded genuine information. Digital watermarking [1] has received significant attraction recently due to the popularity of the Internet and demand for the ownership protection. Among the techniques for watermarking [1-6], the robustness of the digital watermarking is very crucial to counteract the various attacks of unauthorized modification.

Cox et al. [1] had proposed a global DCT-based spread spectrum approach to hide watermarks. Langelaar and Lagendijk [2] introduced the DEW (Differential Energy Watermarking) algorithm for JPEG/MPEG streams in the DCT domain. The DEW algorithm embeds label bits (the watermark) by selectively discarding high frequency DCT coefficients in certain image regions. Das, Maitra and Mitra had presented a successful cryptanalysis against the DEW scheme in [3] and proposed a more robust scheme.

On the other hand, Wang and Lin [4] introduced the technique of WTQ (Wavelet Tree Quantization) in the DWT domain. The wavelet coefficients are grouped into so-called super trees. The wavelet tree based watermarking algorithm embeds watermark bits by selectively quantizing the super trees. Even if the attacker has no knowledge of which two trees are used for embedding, he can still quantize those super trees that are not quantized earlier with respect to the estimated quantization indices. Das and Maitra had presented how this can be accomplished in [5].

In this study, we proposed a WTGM algorithm which applies the concept of energy differentiation in the wavelet domain with the consideration of human visual system by using the contrast sensitive function (CSF) and noise visibility function (NVF). The purpose of the WTGM design is robust to the cryptanalysis of the watermarking attacks with high visual quality.

This paper will be organized as follows. The details of the algorithm will be explained in Section 2. Section 3 will show the experiments with discussion and conclusion is in Section 4.

2. THE APPROACH AND WTGM ALGORITHM

We employ the same wavelet tree structure as depicted in the WTQ scheme. However, each tree can be extended to involve high-frequency components as illustrated in Fig. 1. Suppose that a 512×512 image is transformed, each tree group will be a collection of 85 wavelet coefficients, one coefficient from level 4, 4 coefficients from level 3, 16 coefficients from level 2, and 64 coefficients from level 1.

Lu, et al. [6] had analyzed the behaviors of transformed coefficients under attacks. In principle, there are four possible types of modulations: Modu(+, +), Modu(+, –), Modu(–, +), and Modu(–, –), where Modu(+/–, –/+) denotes a positive/negative transformed coefficient modulated with a negative/positive watermark quantity. Since DEW and WTQ schemes only employed the philosophy of negative modulation, the scheme can be easily defeated by the attacker if it only employs unilateral modulation, regardless of the positive modulation (PM) or the negative modulation (NM). Thus, a good differential energy watermarking algorithm should take both modulated methods into account for higher detector response and better security.

Suppose that each watermark bit is embedded using one tree group, half of a tree group is used for PM and the other is used for NM. We use the term 'tree group" to refer the collection of n trees (i.e. 1 tree group = n trees). A particular tree group can be divided into two sub tree groups, each containing $n/2$ trees. The energy of a tree t is defined as the sum of absolute values of q-p+1 wavelet coefficients. The energies of sub tree group A and sub tree group B are given by: $E_A(p,q,n)=\sum_{t=0}^{\frac{n}{2}-1}\sum_{i=p}^{q}\left|\theta_{i,t}\right|$ and $E_B(p,q,n)=\sum_{t=\frac{n}{2}}^{n-1}\sum_{i=p}^{q}\left|\theta_{i,t}\right|$

* This work was partially supported by the National Science Council in Taiwan, Republic of China, under NSC94-2416-H009-018 and NSC95-2416-H009-027.

where $\theta_{i,t}$ denotes the ith wavelet coefficient in the tree group t, p and q denotes the coefficient number used to perform the modulation from p to q ($0 \le p \le 84$, $0 \le q \le 84$). The group selection is essential the sum-of-subset problem in [3]. Any two sub tree groups with $E_A \approx E_B$, i.e. $|E_A - E_B| \le \delta$, will be suitable for modulation.

The sensitivity of human vision is different from various spatial frequencies (frequency subbands). HVS (Human Visual System) is the key factor in providing a better visual effect and the imperceptibility of the watermarked image. We adopt the CSF of the HVS in [7] to determine the adequate modulation rate for a watermark encoder. The model of the CSF for luminance (or grayscale) images is defined as follows:

$H(f) = 2.6 * (0.0192 + 0.114 * f) * e^{-(0.114*f)^{1.1}}$ where $f = \sqrt{f_x^{\,2} + f_y^{\,2}}$ is the spatial frequency in cycles/degree of visual angle (f_x and f_y are the spatial frequencies in the horizontal and vertical directions, respectively). The HVS is most sensitive to normalized spatial frequencies between 0.025 and 0.125 and less sensitive to low and high frequencies.

To apply the CSF in the DWT domain, CSF masking is employed and refers to the method of weighting the wavelet coefficients relative to their perceptual importance. r^k represents the wavelet coefficient CSF of the perceptual importance weight as shown for each subband in Fig. 1, where k denotes the decomposed level. The HVS is most sensitive to the distortion in mid-frequency regions (level 3) and sensitivity falls off as the frequency value drifts on both sides (level 1, 2 and 4).

We use the square function in [7] to approximate the effect of CSF masking. The adequate modulation rate β^k for each subband is

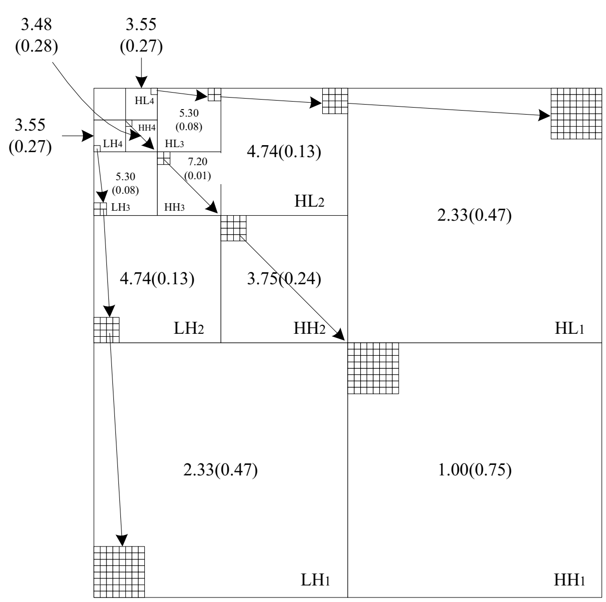

Fig. 1. A four-level wavelet tree structure. The coefficients correspond to the same spatial location are grouped together. Each tree consists of one coefficient from level 4, 4 coefficients from level 3, 16 coefficients from level 2, and 64 coefficients from level 1. $r^k(\beta^k)$ values for each level k are indicated at the center of each band.

determined by: $\beta^k = 0.01 + \dfrac{(7.20 - r^k)^2}{7.20^2}$ and the values are shown in Fig. 1.

S. Voloshynovskiy et al. [8] presented a stochastic approach based on the computation of a NVF (Noise Visibility Function) that characterizes the local image properties and identifies texture and edge regions. This allows us to determine the optimal watermark locations and strength for the watermark embedding stage in WTGM. The adaptive scheme based on NVF calculated from stationary GG model is applied in this study, which is defined as follows:

$NVF(x,y) = \dfrac{w(x,y)}{w(x,y) + \sigma_I^2}$ where $w(x,y) = \gamma[\eta(\gamma)]^{\gamma} \dfrac{1}{\|r(x,y)\|^{2-\gamma}}$

and σ_I^2 is the global variance of the cover image I,

$\eta(\gamma) = \sqrt{\Gamma(3/\gamma)/\Gamma(1/\gamma)}$, $\Gamma(s) = \int_0^{\infty} e^{-u} u^{s-1} du$ (gamma function)

and $r(x,y) = \dfrac{I(x,y) - \bar{I}(x,y)}{\sigma_I}$. γ is the shape parameter and $r(x,y)$ is determined by the local mean and the local variance. For most of real images, the shape parameter is in the range $0.3 \le \gamma \le 1$.

The complete design of the proposed algorithm is summarized as following:

WTGM Watermark Embedding:

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. Group the coefficients to form trees.
3) Randomly arrange the trees using some pseudorandom generator and group them in various tree groups. Each tree group should be divided into two sub tree groups such that $E_A \approx E_B$. Store this group information which we call the image key I_K.
4) FOR EACH watermark bit w_j (j = 0 to $N_w - 1$) DO
   a) Select the jth tree group consisting of n trees.
   b) Choose α.
   c) IF (w_j = -1) THEN
      i) $\theta_{i,t} = \theta_{i,t} * (1 + \alpha * \beta^k * \gamma^{k}_{x,y})$ for $t = 0, ..., (n/2) - 1$, and $i = p, ..., q$. (PM for sub tree group A)
      ii) $\theta_{i,t} = \theta_{i,t} * (1 - \alpha * \beta^k * \gamma^{k}_{x,y})$ for $t = (n/2), ..., n-1$, and $i = p, ..., q$. (NM for sub tree group B)
   d) ELSE
      i) $\theta_{i,t} = \theta_{i,t} * (1 - \alpha * \beta^k * \gamma^{k}_{x,y})$ for $t = 0, ..., (n/2) - 1$, and $i = p, ..., q$. (NM for sub tree group A)
      ii) $\theta_{i,t} = \theta_{i,t} * (1 + \alpha * \beta^k * \gamma^{k}_{x,y})$ for $t = (n/2), ..., n-1$, and $i = p, ..., q$. (PM for sub tree group B)
5) Arrange back the modulated trees to their original positions.
6) Pass the modified wavelet coefficients through the inverse DWT to obtain a watermarked image.

Note:

1) The watermark W is a binary PN sequence of ±1.
2) The length of the watermark = the number of tree groups.
3) α originally denotes the fractional change required to enforce the required energy difference, i.e., after the modification, we need $|(E_A' - E_B') / (E_A + E_B)| \ge \alpha$. E_A' and E_B' are E_A, E_B after the modification. If the HVS is employed, it stands for the strength of the watermark.

4) β^k is the CSF embedding parameter and $\gamma^{k}_{x,y} = 1 - \mathrm{NVF}(x, y)$ is the NVF embedding parameter where the (x, y) is the coordinates and k indicates the decomposed level.
5) If $\beta^k = 1$ and $\gamma^{k}_{x,y} = 1$, the HVS is not employed.

***WTGM Watermark Extraction*:**

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. Group the coefficients to form trees.
3) Reorganize the trees using the image key I_K.
4) FOR EACH watermark bit w_j ($j = 0$ to $N_w - 1$) DO
   a) Select the jth tree group consisting of n trees.
   b) Calculate E_A and E_B.
   c) IF ($E_A > E_B$) THEN $w_j = -1$ ELSE $w_j = 1$.
5) Compute the normalized correlation ρ.
6) If ρ is above the threshold ρ_T, the watermark W exists; otherwise, it does not exist.

3. EXPERIMENTS AND DISCUSSION

To evaluate the performance of the proposed method, the 512×512 Lena, Goldhill and Peppers images with 8 bits/pixel resolution are used for watermarking. We employ a four-level wavelet transform and a watermark sequence of length 512. Therefore, a tree group consists of 6 trees, half of the trees are used for PM and the others are used for NM.

The experiments of WTGM have two settings: WTGM(S_1) (Watermarking Parameter Set 1 (S_1)) uses coefficient number 1 ~ 21 (i.e. $p = 0$, $q = 20$) corresponds to relatively medium frequency components (level 2, 3 and 4 of DWT) for watermarking, which is the same as the WTQ scheme. WTGM(S_2) uses coefficient number 6 ~ 85 (i.e. $p = 5$, $q = 84$) corresponds to medium-high frequency components (level 1 and 2 of DWT). Each setting has its own characteristics and performance to counter different attacks.

To compare the performance with the WTQ scheme, we set the value of α (watermark strength) to meet the same PSNR values of 38.2, 38.7 and 39.8 dB for Lena, Goldhill and Peppers from [4] respectively. With watermark length $N_w = 512$, the threshold ρ_T is chosen to be 0.23 for a false positive probability of 1.03×10^{-7}. The visual quality under different parameter settings for watermarked Lena image is demonstrated in Fig. 2. The watermarked Lena images are all with PSNR values of 38.2 dB. Without the HVS setting in Fig. 2(b) and (c), there are obvious artifacts in the marked region. The employment of the HVS setting apparently improves the visual effect of the watermarked image in Fig. 2 (d).

For compression attack, we perform JPEG and SPIHT compression with different quality factors (QF) and bit rates on the watermarked image. The correlation values of the extracted watermarks are listed in Table I and WTQ data are from [4]. From those results, we can see that the proposed algorithm is robust to JPEG and SPIHT compression. The result of WTGM(S_1) is superior to that of WTGM(S_2). Even for the case that QF is equal to 30 or bit rate as low as 0.3bpp, we can still detect the embedded watermark.

Several spatial-domain signal processing techniques are performed as attacks on the watermarked image for Lena, Goldhill and Peppers. The normalized correlation values from the watermarked images are listed in Table I. For all cases, the watermark information therein can be successfully recognized. Especially for those cases of histogram equalization, Gaussian filtering and sharpening, the result of WTGM(S_2) is superior to that of WTGM(S_1). Except for the case of Gaussian filtering, the proposed algorithm can outperform the WTQ scheme with high normalized correlation values almost in all cases.

The geometric attacks including pixel shifting attacks (circular shift) and rotation attacks (rotation and scaling) along with multiple watermarking and bitplane removal attacks are also preformed for WTGM(S_1) and WTGM(S_2) by using the Lena, Goldhill and Peppers images. The outcomes are summarized in Table I as well. We can clearly see that WTGM outperforms WTQ in almost all categories. In general, the WTGM with medium-high frequency setting WTGM(S_2) is superior in resisting common signal processing, geometric distortions as well as cryptanalysis with better visual perception than WTGM(S_1). Due to the difference of watermark embedding location for setting S_1 and S_2, the results are expected compared with other wavelet based approaches. However, the weakness for the WTGM is that the tree combination information must be kept secret which addresses extra storage space. This study is currently working on the design to efficiently reduce this extra cost.

4. CONCLUSION

An efficient differential energy watermarking algorithm based on wavelet tree group modulation (WTGM) has been presented in this study. Compared with other watermarking schemes, the proposed algorithm can tolerate more common signal processing and geometric attacks. The length of the image key can be large, which renders a better confusion/diffusion for security. In addition, the

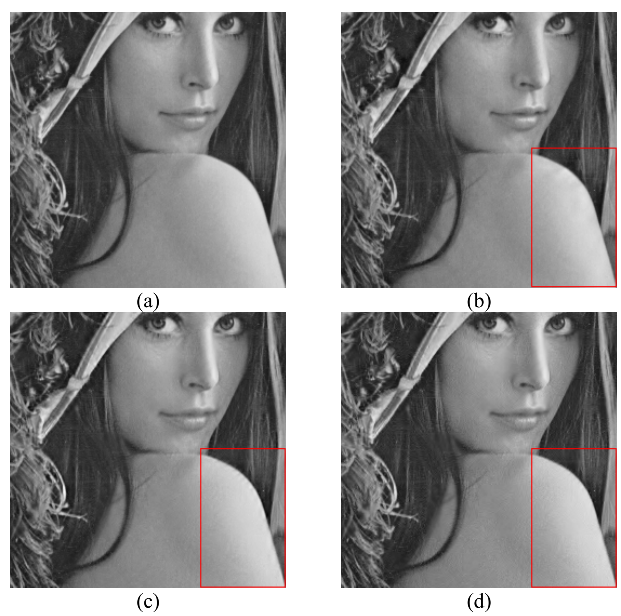

Fig. 2. Close-ups for comparison with visual effects (PSNR = 38.2 dB). (a)Original image. (b)WTGM(S_1) watermarked Lena without HVS setting (α = 0.177). (c)WTGM(S_2) watermarked Lena without HVS setting (α = 0.378). (d) WTGM(S_2) watermarked Lena with HVS setting(α = 2.131).

human visual characteristics are considered for better visual quality. Regarding the cryptanalysis of the algorithm, the algorithm can be public with the keys remained private.

REFERENCES

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon,, “Secure spread spectrum watermarking for multimedia”, IEEE Trans. on Image Proc., vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] G. C. Langelaar and R. L. Lagendijk, “Optimal differential energy watermarking of DCT encoded images and video”, IEEE Trans. on Image Proc., vol. 10, no. 1, pp. 148-158, Jan. 2001.

[3] T. K. Das, S. Maitra, and J. Mitra, “Cryptanalysis of optimal differential energy watermarking (DEW) and a modified robust scheme”, IEEE Trans. on Signal Proc., vol. 53, no. 2, pp. 768-775, Feb. 2005.

[4] S. H. Wang and Y. P. Lin, “Wavelet tree quantization for copyright protection watermarking”, IEEE Trans. on Image Proc., vol. 13, no. 2, pp. 154-165, Feb. 2004.

[5] T. K. Das and S. Maitra, “Cryptanalysis of wavelet tree quantization watermarking scheme”, IWDC 2004, pp. 219-230, 2004.

[6] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. Liao, “Cocktail watermarking for digital image protection”, IEEE Trans. on Multimedia, vol. 2, no. 4, pp. 209-224, Dec. 2000.

[7] B. B. Huang and S. X. Tang, “A contrast-sensitive visible watermarking scheme”, IEEE Multimedia, vol. 13, no. 2, pp. 60-66, April-June 2006.

[8] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, “A stochastic approach to content adaptive digital image watermarking”, in Proc. 3rd Int. Workshop Information Hiding, Dresden, Germany, pp. 211-236, Sep. 1999.

TABLE I
PERFORMANCE SUMMARY OF WTGM AND WTQ SCHEMES (a) LENA. (b) GOLDHILL. (c) PEPPERS.

Operations	WTGM(S_1)	WTGM(S_2)	WTQ
[Signal Processing Attacks]			
JPEG (QF=90%)	1.000	1.000	1.00
JPEG (QF=50%)	0.977	0.941	0.26
JPEG (QF=30%)	0.945	0.770	0.15
SPIHT (bitrate = 0.7)	1.000	1.000	0.85
SPIHT (bitrate = 0.5)	0.996	0.988	0.85
SPIHT (bitrate = 0.3)	0.957	0.770	0.21
Median Filtering (4×4)	0.555	0.574	0.23
Gaussian Filtering	0.457	0.680	0.64
Sharpening	0.629	1.000	0.46
Histogram Equalization	0.824	1.000	N/A
Brightness Enhancement (10%)	1.000	1.000	N/A
Contrast Enhancement (10%)	1.000	1.000	N/A
[Geometric Attacks]			
Pixel Shifting (10 pixels)	0.129	0.531	0.19
Pixel Shifting (12 pixels)	0.086	0.367	N/A
Rotation (1.0°)	0.215	0.875	0.24
Rotation (2.5°)	0.102	0.414	N/A
[Security Measurement]			
Multiple Watermarking (4 watermarks)	0.617 (31.52 dB)	0.590 (26.81 dB)	0.11 (28.05 dB)
Bitplane Removal (5 bitplanes)	0.781 (32.74 dB)	0.879 (33.52 dB)	0.11 (18.47 dB)

(a)

Operations	WTGM(S_1)	WTGM(S_2)	WTQ
[Signal Processing Attacks]			
JPEG (QF=90%)	1.000	1.000	1.00
JPEG (QF=50%)	0.996	0.988	0.71
JPEG (QF=30%)	0.953	0.922	0.23
SPIHT (bitrate = 0.7)	1.000	1.000	0.35
SPIHT (bitrate = 0.5)	0.992	0.973	0.23
SPIHT (bitrate = 0.3)	0.945	0.875	-0.06
Median Filtering (4×4)	0.648	0.520	0.24
Gaussian Filtering	0.578	0.801	0.56
Sharpening	0.793	1.000	0.39
Histogram Equalization	0.707	0.996	N/A
Brightness Enhancement (10%)	1.000	1.000	N/A
Contrast Enhancement (10%)	1.000	1.000	N/A
[Geometric Attacks]			
Pixel Shifting (10 pixels)	0.160	0.617	0.21
Pixel Shifting (12 pixels)	0.129	0.406	N/A
Rotation (1.0°)	0.359	0.875	0.15
Rotation (2.5°)	0.145	0.359	N/A
[Security Measurement]			
Multiple Watermarking (4 watermarks)	0.738 (31.24 dB)	0.711 (29.87 dB)	0.18 (28.57 dB)
Bitplane Removal (5 bitplanes)	0.930 (31.70 dB)	0.875 (31.21 dB)	0.14 (16.18 dB)

(b)

Operations	WTGM(S_1)	WTGM(S_2)	WTQ
[Signal Processing Attacks]			
JPEG (QF=90%)	1.000	1.000	1.00
JPEG (QF=50%)	0.938	0.629	0.70
JPEG (QF=30%)	0.832	0.488	0.34
SPIHT (bitrate = 0.7)	0.984	1.000	0.85
SPIHT (bitrate = 0.5)	0.988	0.980	0.65
SPIHT (bitrate = 0.3)	0.926	0.641	0.36
Median Filtering (4×4)	0.559	0.398	0.25
Gaussian Filtering	0.355	0.418	0.74
Sharpening	0.551	0.996	0.62
Histogram Equalization	0.711	1.000	N/A
Brightness Enhancement (10%)	1.000	1.000	N/A
Contrast Enhancement (10%)	1.000	1.000	N/A
[Geometric Attacks]			
Pixel Shifting (10 pixels)	0.164	0.563	0.26
Pixel Shifting (12 pixels)	0.129	0.359	N/A
Rotation (1.0°)	0.184	0.785	0.17
Rotation (2.5°)	0.090	0.324	N/A
[Security Measurement]			
Multiple Watermarking (4 watermarks)	0.754 (32.45 dB)	0.637 (29.96 dB)	0.22 (28.81 dB)
Bitplane Removal (5 bitplanes)	0.734 (33.42 dB)	0.594 (33.39 dB)	0.14 (16.93 dB)

(c)