A ROBUST IMAGE AUTHENTICATION METHOD BASED ON WAVELET TRANSFORM AND TEAGER ENERGY OPERATOR

Ming-Shing Hsieh

Department of Computer Science and Information Engineering,
Aletheia University, Damshui, Taiwan 251
sms.sms@msa.hinet.net

ABSTRACT

A novel digital watermarking for image authentication is proposed in this paper. Most previous proposed watermarking algorithms embed sequences of random numbers as watermarks. Here images are taken as watermarks for embedding. In the proposed approach, the host image is decomposed into wavelet coefficients. Local entropies of wavelet coefficients in the low-frequency subband are calculated by a Teager energy operator to select embedding locations. The selected coefficients are quantized and the watermark is encrypted; then the least significant bits or the second least significant bits of the quantized coefficients are replaced by the encrypted watermark. At last, the watermarked image is synthesized from the changed and unchanged wavelet coefficients. The experiments show that the proposed approach provides extra robustness against JPEG compression compared to the traditional embedding methods. Moreover, the proposed approach has no need of the original image to extract watermarks and need not sort the embedded coefficients and the watermark.

KEYWORDS

digital watermarking, discrete wavelet transform, Teager energy operator, JPEG compression, encryption.

1. INTRODUCTION

Digital watermarking techniques have been presented for the copyright protection of electronic multimedia data by hiding secret information, such as text and images, in images, videos, audios, or 3-D models. The main intended application of watermarking is to prove ownership of an image for copyright protection. This idea is to embed secret information into an image that can neither be removed nor be decoded without the required secret keys. The owner can add a watermark in an image that authenticates the legal copyright holder and that cannot be manipulated or removed without impairing the image. Indeed, there are a number of desirable characteristics that a watermarking technique should be exhibit; at least it should respect the following requirements:

a. Imperceptibility: The data embedding process should neither introduce any perceptible artifacts into the host image nor degrade the perceived quality of the host image.

b. Robustness: The digital watermark is still present in the image after distorted attack and can be detected by the watermark detector, especially to the attack from compression or other image processing.

c. Unambiguousness: A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, the extracted digital watermark can be used to identify the ownership and copyright unambiguously.

d. Security: A watermark should only be accessible by the authorized parties. This requirement

is regarded as a security of the watermark and is usually achieved by the use of cryptographic keys. As the information security techniques, the details of the digital watermarking algorithms must be published to everyone and the owner of the intellectual property is the only one who holds the private keys.

Watermarking techniques are generally designed for following special applications [22]:

a. Metadata or additional information: Embedding data to describe the information such as structure, indexing terms, *etc*.

b. Copyright protecting: Embedding the ownership of the information for preventing copyright from duplication or abuse.

c. Multiple data embedding: Embedding smaller images in a larger host image or multiple audio data in a video.

d. Copy/usage tracking: Verifying the copy and usage of the information by the embedded data.

Voloshynovskiy *et al*. categorized four classes of attacks [28]. Although not all requirements have to be satisfied for a specific watermarking application, robustness is still definitely important because many attacks already existed and new attacks will appear in the future [29].

Digital watermarking algorithms can be categorized according to their casting/processing domains, signal types of watermarks, and hiding locations. Based on the processing domain, the watermarking techniques can be broadly classified in two categories: spatial domain [1, 9, 16, 18, 21, 26] and frequency domain [3-8, 10, 11, 13, 17, 19, 23, 25, 27]. The earlier watermarking techniques were mostly spatial-domain approaches. The simplest approach was to modify the least significant bits (*LSBs*) of image pixels; however, such a technique still has relatively low-bit capacity and can't resist the lossy data compression and image processing. For example, a common-used image cropping operation can almost eliminate the watermark. Other than the spatial-domain watermarking techniques, the frequency-domain techniques can embed more bits of watermarks and resist more attacks.

Cox *et al*. [3] used the spread spectrum communication in multimedia watermarking. They embedded a set of independent and identical distributed values drawn from a Gaussian distribution into the perceptually most significant frequency components of the host image. Since the embedded value is only a small fraction of a significant coefficient in a typical image, there is not much perceptual degradation on the image. Hsu and Wu [6, 8] embedded the watermarks with visually recognizable patterns in images by selectively modifying the middle-frequency parts of the images. Their embedding and extracting methods are all based on the discrete cosine transform (*DCT*). Wu and Hsieh [27] proposed an efficient *DCT*-based watermarking technique by taking the advantage of zerotree in the rearranged *DCT* coefficients to embed watermarks in images.

Although *DCT*-based methods are easy to implement, have been wildly employed for multimedia compression, and are suitable to embed pseudo random numbers as watermarks, it is weak to claim the ownership of intellectual property; moreover, watermark embedded in *DCT* coefficients seems to be easily lost [2]. Recently, the discrete wavelet transform (*DWT*) [4, 5, 10, 11, 23, 25] has been used to hide data in the frequency domain. Wavelet transform has the excellent properties to minimize the data loss in the frequency transformation of images, to reduce noise and bias generation in images, and to provide extra robustness against irregular attacks.

The main issue of early watermarking techniques is how to embed watermarks in images without apparently degrading the image quality. Most techniques rarely consider the property of robustness, the embedded watermarks are easily removed by a high-ratio compression or smoothing filter. The current issue of watermarking techniques becomes how to maintain the imperceptibility and the robustness at the same time. In general, the imperceptibility and the

robustness are always conflict to each other. The key issue of the current watermarking techniques is to make a compromise between the imperceptibility and the robustness.

In this paper, we propose a wavelet-based watermarking approach to hide a bi-level image watermark into a host image by inserting bits of the watermark into the host-image *DWT* coefficients with larger Teager energy. The proposed approach has the following advantages: (*i*) the embedded watermark could maintain both imperceptibility and robustness through high-ratio compression and image-processing attacks, (*ii*) the extracted watermark is visually recognizable to claim one's ownership, (*iii*) the extraction of watermarks doesn't need the original host image, (*iv*) the embedded coefficients and watermark need not be sorted, (*v*) the approach is hierarchical and has multiresolution characteristics, and (*vi*) the approach matches the image/video compression standards. With practical experiments, the good properties of imperceptibility and robustness of the proposed approach will be verified.

The remaining sections of this paper are organized as follows. The discrete wavelet transform and Teager energy operator for our watermarking approach are described in Section 2. Section 3 presents the proposed watermark embedding and extracting methods. Experiments and the results are demonstrated in Section 4. The conclusions are given in Section 5.

2. THE PRINCIPLE OF THE PROPOSED WATERMARKING TECHNIQUE

In this section, we first give a brief review on the wavelet representation of an image and then describe the Teager energy operator for embedding and extracting watermarks.

2.1. Wavelet transform of images

The *discrete wavelet transform* (*DWT*) is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. For a 1-D signal, a 1-D wavelet Ψ function and a 1-D scaling function Φ are chosen to iteratively decompose the signal into different-scaled high-frequency subbands. The 1-D *DWT* can be implemented by the Mallat's *Direct Pyramid Algorithm* [14].

For a 2-D image, the same wavelet function Ψ and scaling function Φ are used in both vertical and horizontal to decompose the image. For example, scaling function $\Phi_{LL}(x, y)$ of the low-low subband in a 2-D wavelet transform is completed by $\Phi(x)\ \Phi(y)$. Three other 2-D wavelet functions are obtained by the wavelet function $\Psi(x)$ as

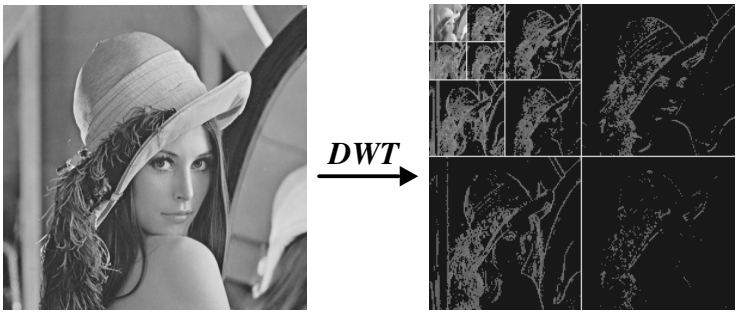
$$\Psi_{LH}(x, y) = \Phi(x)\ \Psi(y) \quad ; \text{horizontal}$$

$$\Psi_{HL}(x, y) = \Psi(x)\ \Phi(y) \quad ; \text{vertical}$$

$$\Psi_{HH}(x, y) = \Psi(x)\ \Psi(y) \quad ; \text{diagonal}$$

where *H* means a high-pass filter and *L* is a low-pass filter.

The basic idea of 2-D *DWT* of images is described as follows. An image is firstly decomposed into four parts of low and high frequencies (*i.e.*, LL_1, LH_1, HL_1, HH_1) subbands, by cascading horizontal and vertical subsampled filter banks. The subbands labeled LH_1, HL_1, and HH_1 represent the finest scale wavelet subbands. To obtain a coarser-scaled wavelet coefficients, the subband LL_1 is further decomposed and critically subsampled. This process is repeated an arbitrary number of times, which is determined by the application at hand. A layout of *DWT* subbands with three-level dyadic decomposition of *Lena* image is shown in Fig. 1. In the figure, *Lena* image is decomposed into ten subbands with three scale levels. Each level has several band information such as low-low, low-high, high-low, and high-high frequency bands. Furthermore, the original image can be reconstructed from these *DWT* coefficients. The reconstruction process is called the inverse *DWT* (*IDWT*).



(a) (b)

Fig. 1. An example of *DWT* decomposition. (a) The original *Lena* image. (b) The hierarchical *DWT* subbands.

2.2. The Teager energy operator

In this study, local characteristics are taken into consideration to select casting *DWT* coefficients. The local characteristics are defined by the entropies of *DWT* coefficients and the entropy is defined by the considered coefficient and its neighboring coefficients. A coefficient has higher entropy if the variance of coefficients around it is large enough. In other words, a coefficient having higher entropy means that it locates in an area where is random and busy enough. If we embed a watermark in those locations, the watermark is imperceptible.

The proposed approach is based on the Teager energy operator (or simply called Teager's operator) to choose the *DWT* coefficients with larger entropy to embed watermarks. Teager's operator was originally proposed by Kaiser [12] to estimate the energy of an oscillating signal. The main property of Teager's operator is responding to a mean-weighted highpass response [12]. Teager's operator is also called Teager's filter and has been shown to be useful for image analysis. For 1-D input and output signals, $\{x_i\}$ and $\{y_i\}$, Teager's operator [20] is given by

$$y_n = x_n^2 - x_{n-1}x_{n+1}. \tag{1}$$

For 2-D signals, cross-shape Teager's operator defined as

$$y_{m,n} = 2x_{m,n}^2 - x_{m,n-1}x_{m,n+1} - x_{m-1,n}x_{m+1,n} \tag{2}$$

and x-shape Teager's operator defined as

$$y_{m,n} = 2x_{m,n}^2 - x_{m-1,n-1}x_{m+1,n+1} - x_{m-1,n+1}x_{m+1,n-1} \tag{3}$$

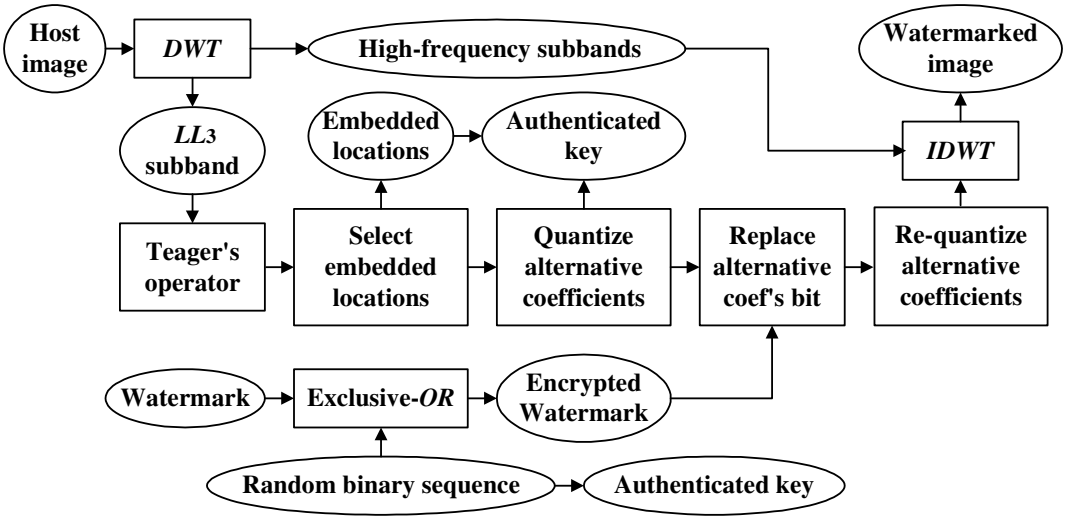
can be used. The output of a Teager's operator is called the Teager energy which represents a local entropy in the processed domain. LL_3 *DWT* subband is taken as the processed domain; LL_3 coefficients with larger Teager energy are selected to embed watermarks. LL_3 subband provides the function of dispersing embedded watermarks to increase robustness.

3. THE PROPOSED WATERMARKING APPROACH

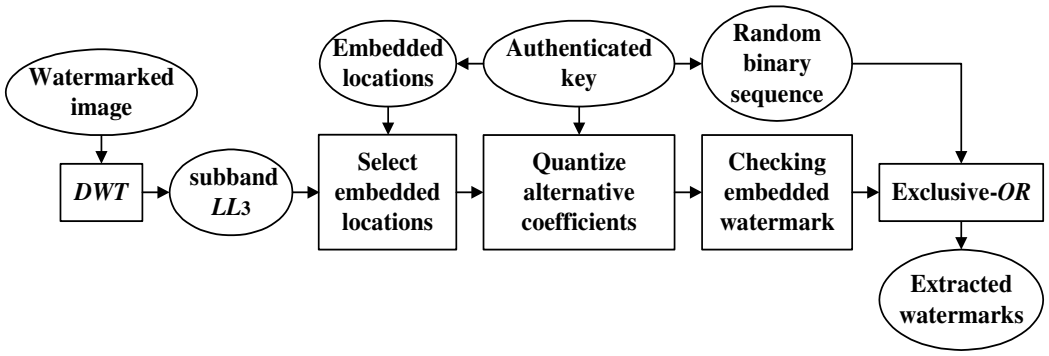
The current study task of digital watermarking is to make watermarks invisible to human eyes as well as robust to various attacks. The proposed watermarking approach can hide visually recognizable patterns in images. The proposed approach is based on the discrete wavelet transform (*DWT*). The *DWT* has the properties: precise localization ability, excellent multi-scale analysis, and the publicly available masking thresholds [24]; thus it is suitable for the watermarking applications.

In the proposed approach, we embed encrypted watermarks in the coarsest *DWT* subband of the

host image by modifying the least significant bit (*LSB*) or the second *LSB* of coefficients with larger Teager energy. The block diagram of the proposed watermarking approach is shown in Fig. 2.



(a)



(b)

Fig. 2. Block diagrams of the proposed watermarking approach. (a) Embedding procedure. (b) Extracting procedure.

3.1. Watermark embedding method

The algorithm for embedding watermarks in LL_3 coefficients of the host image is described as follows:

Step 1: Decompose a host image H into three levels with ten *DWT* subbands, $F(H)$. The coarsest subband LL_3 is taken as the target subband for embedding watermarks.

Step 2: For more security of watermarks, the watermark W is converted to a sequence and then a random binary sequence R of size n is adopted to encrypt the watermark, where n is the size of the watermark image. The encrypted watermark sequence W_1 is generated by executing exclusive-*OR* operation on W and R,

$$W_1 = W \oplus R. \tag{4}$$

Step 3: Calculate the Teager energy of coefficients in LL_3 subband of $F(H)$. In order to extract

the embedded watermark without host image, two extra reference coefficients are used to hold the necessary information. Thus p, $p = n + 2$, coefficients with larger Teager energy (absolute value) are selected from LL_3 subband to embed watermark. The coefficients are denoted as $\{c_i \mid 1 \le i \le p\}$ and called the alternative coefficients.

Step 4: Quantize the alternative coefficients into k levels. The quantized coefficients $\{q_i\}$ is generated by the equation,

$$q_i = round\ ((c_i - c_{min}) / ((c_{max} - c_{min})/(k\text{-}1))), \tag{5}$$

where *round* is the round-off operation, c_{max} is the largest alternative coefficient, and c_{min} is the smallest alternative coefficient. c_{max} and c_{min} are just taken as the reference coefficients and not quantized.

Step 5: Embed watermark W_1. For robustness, imperceptibility, and security, the encrypted watermark W_1 is embedded in the *LSBs* or the second *LSBs* of coefficients according to the quantized coefficient compared to the average of quantized coefficients. Denoting a quantized coefficient $q_i = \sum_{j=1}^{8} b_j 2^{j-1}$ into the binary form $b_8 b_7 \ldots b_2 b_1$. The binary-form watermarked coefficient q'_i is obtained by

$$q'_i = \begin{cases} b_8 b_7 b_6 b_5 b_4 b_3 b_2 w & \text{if} \quad q_i \le average\{q_k\} \\ b_8 b_7 b_6 b_5 b_4 b_3 w b_1 & \text{if} \quad q_i > average\{q_k\} \end{cases}, \tag{6}$$

where w is a bit of W_1 for embedding. The embedding process is done by the proposed *Casting watermark algorithm*.

Begin {*Casting watermark algorithm*}
  j=1
  For i = 1 to p
    If $i \neq max$ and $i \neq min$ then
      If q_i <= *average* ($\{q_k\}$) then
        Replace bit b_1 of q_i with w_j
      Else
        Replace bit b_2 of q_i with w_j
      End-if
      j=j+1
    End-if
  End-for

Step 6: Re-quantize watermarked coefficients q'_i. The re-quantized coefficient sequence $\{r_i\}$ is generated by the equation,

$$r_i = q'_i\ (c_{max} - c_{min})/(k\text{-}1) + c_{min}\ . \tag{7}$$

A watermarked image is then generated by inverse *DWT* with all changed and unchanged *DWT* coefficients.

Step 7: Save alternative coefficients' indexes, random binary sequence R, quantization level, and index of the embedded subband as authenticated key.

3.2. Watermark extracting method

The embedded watermark can be detected using the stored public key after wavelet decomposition of the watermarked image. The extracting process is described as follows:

Step 1: Decompose a watermarked image into three levels with ten *DWT* subbands.

Step 2: Re-fetch the authenticated key. The alternative coefficient sequence $\{r_i\}$ is derived from LL_3 subband.

Step 3: Quantize the alternative coefficients $\{r_i\}$ into k levels to get the quantized coefficient sequence $\{t_i\}$ by the equation,

$$t_i = round\ ((r_i - c_{min}) / ((c_{max} - c_{min})/(k\text{-}1))). \quad (8)$$

Step 4: Find watermark sequence W'_1 by fetching the replaced bits in $\{t_i\}$. The fetching process is done by the proposed *extracting watermark algorithm*.

Begin {*Extracting watermark algorithm*}

$W'_1 = null$; j=1

For i = 1 to p

If $i \neq max$ and $i \neq min$

If t_i <= *average* ($\{t_i\}$)

Let w_j' be bit b_1 of t_i

Else

Let w_j' be bit b_2 of t_i

End-if

j=j+1

End-if

End-for

Step 5: Induce the watermark sequence W' by executing exclusive-*OR* operation on the sequence W'_1 and random binary sequence R,

$$W' = W'_1 \oplus R. \quad (9)$$

In the proposed scheme, the extracted watermark W' is a visually recognizable image. A subjective measurement based on the normalized correlation defined as

$$NC = \frac{\sum_i w_i \cdot w'_i}{\sum_i w_i^{\,2}} \quad (10)$$

is used to evaluate the quality of the extracted watermark by measuring the similarity of the original watermark W and the extracted watermark W' [6]. Moreover, the peak signal-to-noise ratio (*PSNR*) is used to evaluate the quality of the watermarked image. The *PSNR* is defined as

$$PSNR = 20\log_{10}\frac{255}{MSE}(dB), \quad (11)$$

where mean-square error (*MSE*) of two $m \times n$ images is defined as

$$MSE = \frac{1}{m\,n}\sum_{i=1}^{m}\sum_{j=1}^{n}(h_{i,j} - h'_{i,j})^2 , \tag{12}$$

where $\{h_{i,j}\}$ and $\{h'_{i,j}\}$ are the gray levels of pixels in the host and watermarked images, respectively. The larger *PSNR* is, the better the image quality is. In general, a watermarked image is acceptable by human perception if its *PSNR* is greater than 30 *dBs*. In other words, the *NC* is used for evaluating the robustness of watermarking technique and the *PSNR* is used for evaluating the imperceptibility of watermarking technique. For a bi-level extracted watermark, the change from "1" pixel to "0" pixel will influence the *NC*, but the change from "0" pixel to "1" pixel doesn't influence the *NC*; thus the "error bit" of an extracted watermark is supplemented for more detailedly describing robustness of watermarking techniques.

4. EXPERIMENTS AND DISCUSSION

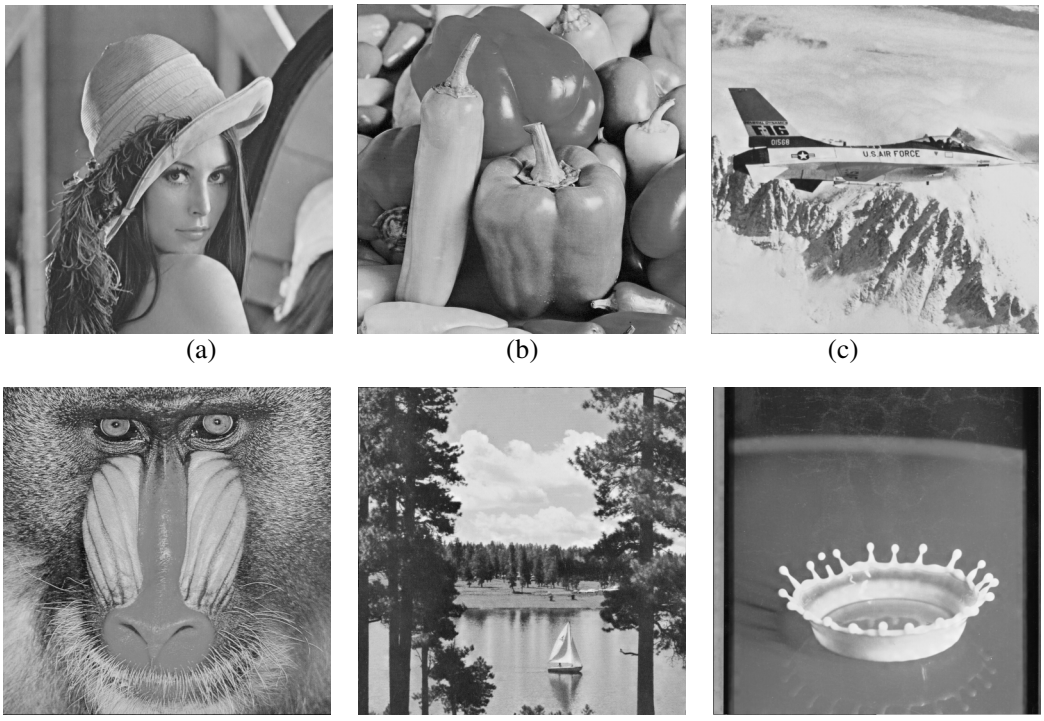
The proposed perceptual watermarking framework was implemented for evaluating both properties of imperceptibility and robustness. Six 512×512 images: *Lena*, *Pepper*, *Jet*, *Baboon*, *Scene*, and *Milk*, shown in Fig. 3 were taken as the host images to embed a 32×32 binary watermark image with "NCU CSIE" characters. In the experiments, 8-point filters: {-0.0106, 0.0329, 0.0308, -0.1870, -0.0280, 0.6309, 0.7148, 0.2304} and {-0.2304, 0.7148, -0.6309, -0.0280, 0.1870, 0.0308, -0.0329, -0.0106} were used for wavelet decomposition and filters: {0.2304, 0.7148, 0.6309, -0.0280, -0.1870, 0.0308, 0.0329, -0.0106} and {-0.0106, -0.0329, 0.0308, 0.1870, -0.0280, -0.6309, 0.7148, -0.2304} were used for image reconstruction.

The proposed watermarking approach yields satisfactory results in watermark imperceptibility and robustness. With quantization level k = 52, the *PSNRs* of the watermarked images produced by the proposed approach are all greater than 41 *dBs*, which are perceptually imperceptible as shown in Fig. 4. We have found that the quantization level has influence on the *PSNRs* of watermarked images and the error bit of extracted watermarks after attacks. The influence of quantization level on the *PSNRs* of watermarked *Lena* image and error bits of extracted watermarks is shown in Fig. 5, where quantization level is from 32 to 63, and the error bit is under a *JPEG* compression attack with compression ratio = 16.7. The error bits increase when the *PSNR* is increases; thus we should describe the error bits when we describe *PSNR* for a watermarked image. The *PSNRs* of the six watermarked images are respectively: (a) 43.76 *dB*, (b) 43.43 *dB*, (c) 41.85 *dB*, (d) 44.98 *dB*, (e) 42.24 *dB*, and (f) 43.20 *dB*; their corresponding error bits after *JPEG* compression with compression ratio = 16.7 are (a) 3, (b) 0, (c) 0, (d) 21, (e) 0, and (f) 6. The watermarked results are excellent.

(a) (b) (c)

(d) (e) (f)

Fig. 3. The host images for watermarking. (a)-(f) *Lena*, *Pepper*, *Jet*, *Baboon*, *Scene*, and *Milk*.



(a) (b) (c)

(d) (e) (f)

Fig. 4. Watermarked images produced by the proposed approach and their *PSNRs*. (a) 43.76 *dB*, (b) 43.43 *dB*, (c) 41.85 *dB*, (d) 44.98 *dB*, (e) 42.24 *dB*, and (f) 43.20 *dB*. Their error bits after *JPEG* compression with compression ratio = 16.7 are (a) 3, (b) 0, (c) 0, (d) 21, (e) 0, and (f) 6.

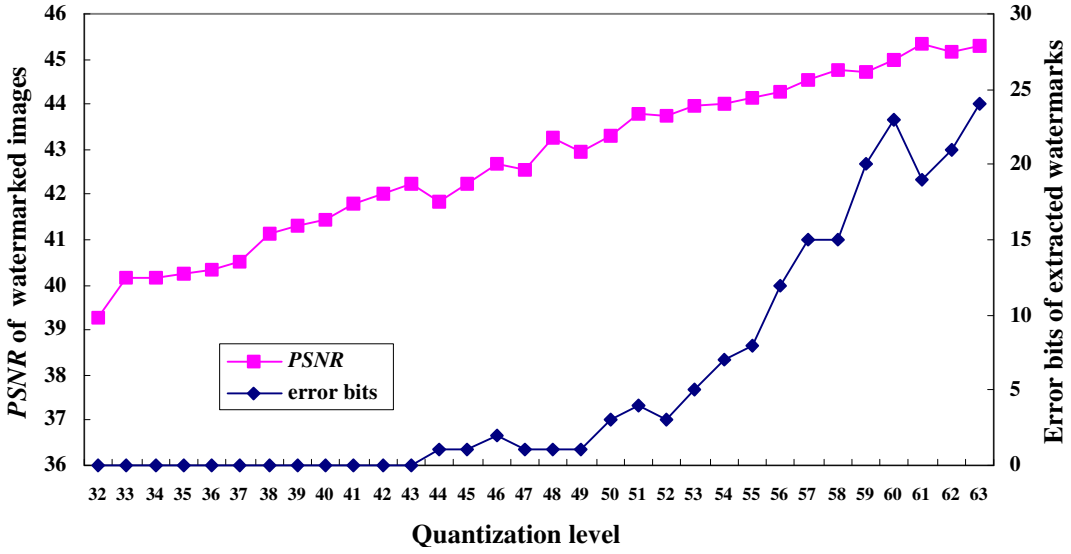


Fig. 5. The influence of quantization level on the *PSNRs* of watermarked *Lena* image and error bits of extracted watermarks, where quantization level is shown from 32 to 63 and the error bits are counted after *JPEG* compression with compression ratio = 16.7.

4.1. Robustness from *JPEG*-compression attacks

The proposed approach emphasizes the local energy characteristics. Here we evaluated the quality of the watermarked images and the detectability of watermarks after *JPEG* compression attack. Table 1 shows the correlations of watermarks and their extracted watermarks after *JPEG* compression attack, where quantization level is 31. In the experiments, we found that the extracted watermarks are excellent if the *JPEG* compression quality of watermarked images are greater than 50. Normalized correlations between the watermarked images and their original host images are still greater than 0.998 even if the *JPEG* compression qualities are less than 30. The extracted watermarks still show satisfactory quality under a high-ratio compression.

Table 1. Extracted watermarks after *JPEG* attacks, where LL_3 coefficients with larger Teager energy are selected to embed encrypted watermarks by replacing the *LSBs* of the coefficients.

Lena								
Quality/*CR*	90/4.6	80/7.0	70/8.9	60/10.9	50/12.4	40/14.1	30/16.6	20/20.5
NC	1	1	1	1	1	1	1	1
Error bits	0	0	0	0	0	0	0	0
Watermark	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE
Pepper								
Quality/*CR*	90/3.9	80/6.4	70/8.2	60/9.9	50/11.4	40/13.2	30/16.2	20/20.1
NC	1	1	1	1	1	1	1	0.9987
Error bits	0	0	0	0	0	0	0	1
Watermark	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE	NCU CSIE

Jet								
Quality/*CR*	90/4.3	80/6.5	70/8.1	60/9.6	50/10.8	40/12.3	30/14.3	20/17.8
NC	0.9987	0.9987	0.9987	0.9987	0.9987	0.9987	0.9987	0.9987
Error bits	1	1	1	1	1	1	1	1
Watermark								
Baboon								
Quality/*CR*	90/2.3	80/3.3	70/4.2	60/4.9	50/5.7	40/6.5	30/7.8	20/10.1
NC	1	1	1	1	1	1	1	0.9987
Error bits	0	0	0	0	0	0	0	5
Watermark								
Scene								
Quality/*CR*	90/3.1	80/4.9	70/6.4	60/7.6	50/8.7	40/9.9	30/11.7	20/14.8
NC	1	1	1	1	1	1	1	1
Error bits	0	0	0	0	0	0	0	0
Watermark								
Milk								
Quality/*CR*	90/6.2	80/9.6	70/12.2	60/14.7	50/16.7	40/19.3	30/22.49	20/26.7
NC	1	1	1	1	1	1	1	1
Error bits	0	0	0	0	0	0	0	1
Watermark								

4.2. Robustness comparison with direct sorting on HL_3

Direct sorting the wavelet coefficients in high-frequency subbands to select casting locations for embedding watermarks is commonly used by the previous methods. We here embed encrypted watermarks in the larger coefficients (absolute values) of subband HL_3 and then examine the watermark fragility after a *JPEG* compression attack, where watermarks were embedded in the *LSBs* or the second *LSBs* of HL_3 coefficients. Table 2 illustrates the extracted watermarks after *JPEG* compression, where quantization level is 31. Comparing the results of Table 1 and Table 2, we found that the proposed framework is obviously robust than the previous frameworks. Fig. 6 shows the embedding locations in *Lena* image, where Fig. 6 (a) and (b) indicate that LL_3 coefficients with larger Teager energy calculated by the cross-shape and x-shape Teager's operator, respectively; Fig. 6 (c) indicates that the larger HL_3 coefficients are the alternatives to be embedded. All embedding locations are at the boundary of regions; however, the embedded watermarks were scattered in a larger area by the proposed approach to provide more robustness.

Table 2. Extracted watermarks after *JPEG* attacks, where larger HL_3 coefficients are selected to embed encrypted watermarks by replacing the *LSBs* or the second *LSBs* of the coefficients.

Lena								
Quality/*CR*	90/4.6	80/7.0	70/8.9	60/10.9	50/12.4	40/14.1	30/16.6	20/20.2
NC	0	1	0.9987	0.9975	0.9772	0.9544	0.8897	0.7592
Error bits	0	0	1	2	21	49	122	244
Watermark								
Pepper								
Quality/*CR*	90/3.9	80/6.4	70/8.2	60/9.9	50/11.4	40/13.2	30/16.2	20/19.7
NC	1	1	0.9962	0.9696	0.9480	0.8847	0.7731	0.6426
Error bits	0	0	4	30	56	115	225	372
Watermark								
Jet								
Quality/*CR*	90/4.3	80/6.5	70/8.1	60/9.6	50/10.8	40/12.3	30/14.3	20/17.6
NC	1	1	1	0.9975	0.9886	0.9708	0.8923	0.7427
Error bits	0	0	0	2	13	35	111	257
Watermark								
Baboon								
Quality/*CR*	90/2.3	80/3.3	70/4.2	60/4.9	50/5.7	40/6.5	30/7.8	20/10.1
NC	1	1	0.9823	0.9113	0.8720	0.7807	0.6857	0.5767
Error bits	0	0	20	91	130	226	331	428
Watermark								
Scene								
Quality/*CR*	90/3.1	80/4.9	70/6.4	60/7.6	50/8.7	40/9.9	30/11.7	20/14.6
NC	1	1	0.9975	0.9556	0.8923	0.8289	0.7224	0.6413
Error bits	0	0	2	47	107	171	282	388
Watermark								
Milk								
Quality/*CR*	90/6.2	80/9.6	70/12.2	60/14.7	50/16.7	40/19.3	30/22.49	20/26.4
NC	1	1	1	0.9848	0.9506	0.8809	0.7719	0.6565
Error bits	0	0	0	16	55	112	234	366
Watermark								

(a) (b) (c)

Fig. 6. Locations of embedded watermarks. (a) The LL_3 coefficients with larger Teager energy calculated by the cross-shape Teager's operator. (b) The LL_3 coefficients with larger Teager energy calculated by the x-shape Teager's operator. (c) The larger HL_3 coefficients.

4.3 Roubstness comparison with embedding in a high-frequency subband

Teager's operator was used to estimate the energy of an oscillating signal and responding to a mean-weighted highpass response [12]. We here want to know how much robust is the strategy by embedding watermarks in HL_3 coefficients, where coefficients with larger Teager energy were selected for embedding. The watermarks were embedded in the *LSB* or the second *LSB* of coefficients. The experimental results are shown in Table 3, where quantization level is 31. Comparing the results, we found that Teager's operator on LL_3 subband is most robust, and then is the Teager's operator on HL_3 subband. Direct sorting on HL_3 subband is least robust.

Table 3. Extracted watermarks after *JPEG* attacks, where HL_3 coefficients with larger Teager energy are selected to embed encrypted watermarks by replacing the *LSBs* or the second *LSBs* of the coefficients.

Lena								
Quality/*CR*	90/4.6	80/7.0	70/8.9	60/10.9	50/12.4	40/14.1	30/16.6	20/20.2
NC	1	1	1	0.9987	0.9924	0.9721	0.9303	0.8074
Error bits	0	0	0	1	8	27	74	210
Watermark								
Pepper								
Quality/*CR*	90/3.9	80/6.4	70/8.2	60/9.9	50/11.4	40/13.2	30/16.2	20/19.7
NC	1	1	0.9975	0.9937	0.9582	0.9011	0.8264	0.6755
Error bits	0	0	2	6	45	105	179	335
Watermark								
Jet								
Quality/*CR*	90/1.65	80/6.45	70/8.04	60/9.57	50/10.82	40/12.30	30/14.34	20/17.64
NC	1	1	1	0.9987	0.9962	0.9658	0.9100	0.7934
Error bits	0	0	0	1	5	41	101	204
Watermark								

Baboon								
Quality/*CR*	90/2.3	80/3.3	70/4.2	60/4.9	50/5.7	40/6.5	30/7.8	20/10.1
NC	1	0.9987	0.9924	0.9696	0.9176	0.8492	0.7896	0.6502
Error bits	0	1	6	35	82	156	207	376
Watermark								
Scene								
Quality/*CR*	90/3.1	80/4.9	70/6.4	60/7.6	50/8.7	40/9.9	30/11.7	20/14.6
NC	1	1	0.9987	0.9886	0.9442	0.9100	0.8175	0.6743
Error bits	0	0	1	13	50	96	181	337
Watermark								
Milk								
Quality/*CR*	90/6.2	80/9.6	70/12.2	60/14.7	50/16.7	40/19.3	30/22.49	20/26.4
NC	1	1	0.9987	0.9886	0.9658	0.8973	0.8276	0.6806
Error bits	0	0	1	15	37	104	189	334
Watermark								

4.4. Imperceptibility and robustness comparisons among various embedding strategies

The proposed approach shows satisfactory imperceptibility and excellent robustness from six tested benchmark images. *PSNRs* of these tested images are all above 39 *dBs*, while normalized correlations of extracted watermarks to the original watermarks are near 100% even attacked by high *JPEG* compression (Quality = 20). Table 4 illustrates the comparison among several embedding strategies: (*i*) embedding watermarks in the 1st/2nd, 2nd/3rd, or 3rd/4th *LSBs* of the larger HL_3 coefficients, (*ii*) embedding watermarks in the *LSBs* of the LL_3 coefficients with larger Teager energy, and (*iii*) embedding watermarks in the 1st/2nd, 2nd/3rd, or 3rd/4th *LSBs* of the HL_3 coefficients with larger Teager energy; where *Lena* image was used as the host image, *JPEG* compression quality is 30, *JPEG* compression ratio is 16.7, and the quantization level is 52. Embedding watermarks in the *LSB* or the second *LSB* of the alternative coefficients by (*i*) directing sorting the coefficients in HL_3 subband or (*ii*) selecting the coefficients based on Teager's operator in HL_3 subband could get more imperceptible watermarked images, but obtain worse extracted watermarks. In the comparison, we found that the proposed approach still provides imperceptible watermarked images and the most robust extracted watermarks.

Table 4. Comparisons among several embedding strategies: (*i*) embedding watermarks in the 1st/2nd, 2nd/3rd, or 3rd/4th *LSBs* of the larger HL_3 coefficients, (*ii*) embedding watermarks in the *LSBs* of the LL_3 coefficients with larger Teager energy, and (*iii*) embedding watermarks in the 1st/2nd, 2nd/3rd, or 3rd/4th *LSBs* of the HL_3 coefficients with larger Teager energy.

Subband/ Replaced bits	HL_3/1,2 (larger)	HL_3/2,3 (larger)	HL_3/3,4 (larger)	LL_3/1 (Teager)	HL_3/1,2 (Teager)	HL_3/2,3 (Teager)	HL_3/3,4 (Teager)
PSNR	51.76	45.84	39.76	43.76	50.35	44.14	39.43
Correlation *	0.2904	0.6062	0.8031	0.9918	0.3843	0.6972	0.8319
NC	0.6933	0.8099	0.9049	0.9962	0.7136	0.8745	0.943
Error bits	326	179	83	3	289	126	64
Watermark							

* C*orrelation* is defined as $\frac{\sum (w-\overline{w})(w'-\overline{w}')}{\sqrt{\sum (w-\overline{w})^2}\sqrt{\sum (w'-\overline{w}')^2}}$.

4.5. Security

The proposed embedding approach used a random sequence R to encrypt watermarks. In our experiments, the length of the watermark image is 1024; thus, one who doesn't have the sequence need to test 2^{1023} cases to decode the watermark in average. If he uses a 100 *MIPS* computer to test, the computational load is greater than $4*10^{138}$ years. It is clear that an illegal user cannot extract the watermark image without the random sequence. One can use other cryptic scheme as the pre-processing of the watermark image for security in our proposed approach; for example, one-way hash function [9, 15].

4.6. The length of the authenticated key

The proposed approach used authenticated key instead of the original host image to extract watermark images. For a bi-level watermark image with n pixels and k quantization levels, the authenticated key of the proposed approach need about $(16(n+2) + 2\ ceil(\log_2(n+2)) + n + k + 4)/8$ bytes $\approx 2.13K$ bytes with $n = 1024$ and $k = 64$, where *ceil* function returns a minimum integer which is greater than the parameter.

5. CONCLUSIONS

We have introduced a watermarking framework for embedding visually recognizable digital watermark images. The proposed approach can resist image-processing attacks, especially the *JPEG* compression. The proposed approach is based on the discrete wavelet transform and Teager energy operator, which considers the local characteristics to choose the larger-entropy *DWT* coefficients in the low-frequency subband to embed watermarks. The proposed approach has the following characteristics:

a. A host image is decomposed into wavelet coefficients; then the coefficients with larger Teager energy in the low-frequency subband are selected to embed the watermark. At least, the watermarked image is synthesized from all subband coefficients.

b. The embedded watermarks are visually recognizable. Before embedding, the watermark is pre-encrypted by a random binary sequence for security. The embedded coefficients and the watermark need not be sorted.

c. The proposed embedding approach replaces an encrypted watermark with the *LSBs* or the second *LSBs* of the wavelet coefficients to raise the security.

d. The proposed approach has no need of the original host image to extract watermarks.

e. The quantization in embedding and extracting watermarks always includes quantization error, but the error is small in the proposed approach.

f. The experimental results show that the proposed approach provides extra robustness against *JPEG*-compression compared to the traditional methods.

ACKNOWLEDGEMENTS

The authors would like to thank Prof Tseng D-C, and the anonymous reviewers of this paper.

REFERENCES

[1] Bender WR, Gruhl D, Morimoto N (1995), "Techniques for data hiding," in *Proc. of SPIE: Storage and Retrieval of Image and Video Database*, Vol. 2420, pp164-173.

[2] Cho J-S, Shin S-W, Lee W-H, Kim J-W, Choi J-U (2000), "Enhancement of robustness of image watermarks embedding into colored image, based on WT and DCT," in *Proc. of 2000 International Conference on Information Technology: Coding and Computing*, pp483-488.

[3] Cox IJ, Kilian J, Leighton FT, Shamoon T (1997), "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, Vol. 6, No. 12, pp1673-1687.

[4] Nizar Sakr, Nicolas Georganas, and Jiying Zhao, (2006) "Copyright Protection of Image Learning Objects using Wavelet-based Watermarking and Fuzzy Logic," in *Proc. I2LOR 2006 - 3rd annual e-learning conference on Intelligent Interactive Learning Object Repositories Montreal*, Quebec, Canada, 9–11 November.

[5] Hsieh M-S, Tseng D-C, Huang Y-H (2001), "Hidden digital watermarks using multiresolution wavelet transform," *IEEE Trans. Industrial Electronics*, Vol. 48, No. 5, pp. 875-882.

[6] Hsu C-T, Wu J-L (1998), "DCT-based watermarking for video," *IEEE Trans. Consumer Electronics*, Vol. 44, No. 1, pp. 206-216.

[7] Hsu C-T, Wu J-L (1998), "Multiresolution watermarking for digital images," *IEEE Trans. Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 45, No. 8, pp1097-1101.

[8] Hsu C-T, Wu J-L (1999), "Hidden digital watermarks in images," *IEEE Trans. Image Processing*," Vol. 8, No. 1, pp58-68.

[9] Hwang M-S, Chang C-C (1996), "A watermarking technique based on one-way hash functions," *Proc. of 1996 International Conference on Image Processing*, Vol. 3, pp391-395.

[10] Manabu Shinohara and Fumiaki Motoyoshi, (2007), "Wavelet-Based Robust Digital Watermarking Considering Human Visual System", in *Proc. 2007 WSEAS International Conference on Computer Engineering and Applications, Gold Coast, Australia*, pp. 177-180.

[11] Kaewkameerd N, Rao KR (2000), "Wavelet based image adaptive watermarking scheme," *Electronic Letters*, Vol. 36, No. 4, pp312-313.

[12] Kaiser JF (1993), "Some useful properties of Teager's energy operators," in *Proc. of IEEE International Conference on Acoustics Speech and Signal Processing*, Vol. 3. pp149-152.

[13] Kim S-M, Suthaharan S, Lee H-K, Rao K-R (1999), "Image watermarking scheme using visual model and BN distribution," *Electronic Letters*, Vol. 35, No. 3, pp212-213.

[14] Mallat S (1989), "Multifrequency channel decomposition of images and wavelets models," *IEEE Trans. Acoustics Speech and Signal Processing*, Vol. 37, No. 12, pp2091-2110.

[15] Merkle RC (1989), "One-way hash functions and DES," in *Proc. of 1989 Advances in Cryptology, CRYPTO'89, Lecture Notes in Computer Science*, Vol. 435, pp 428-446.

[16] Nikolaidis N, Putas I (1996), "Copyright protection of images using robust digital signatures," in *Proc. of 1996 IEEE Symposium on Acoustics, Speech and Signal Processing*, Vol. 4. IEEE Computer Society Press, pp2168-2171.

[17] Niu X-M, Lu Z-M, Sun S-H (2000), "Digital watermark of still image with gray-level digital watermarks," *IEEE Trans. Consumer Electronics*, Vol. 46, No. 1, pp. 137-144.

[18] Pitas I (1996), "A Method for signature casting on digital image", in *Proc. of 1996 International Conference on Image Processing*, Vol. 3, pp. 391-395.

[19] Podilchuk CI, Zeng W (1998), "Image-adaptive watermarking using visual models," *IEEE J. Selected Areas in Communications*, Vol. 16, No. 4, pp525-539.

[20] Restrepo A, Zuluata LF, Ortiz H, Ojeda V (1997), "Analytical properties of Teager's filter," in *Proc. of 1997 IEEE International Conference on Image Processing*, Vol. 1. IEEE Computer Society Press, pp397-400.

[21] Schyndel RG, Tirkel AZ, Osborne CF (1994), "A digital watermark," in *Proc. of 1994 IEEE Symposium on Image Processing*, Vol. 2. IEEE Computer Society Press, pp 86-90.

[22] Swanson MD, Kobayashi M, Tewfik AH (1998), "Multimedia data-embedding and watermarking technologies," IEEE Proceedings, Vol. 86, No. 6, pp1064-1087.

[23] Ming-Shing Hsieh and Din-Chang Tseng (2006), "Wavelet-based Color Image Watermarking Using Adaptive Entropy Casting," in *Proc. of IEEE Int. Conf. on Multimedia & Expo* (ICME), Toronto, Canada, July 9-12, 2006

[24] Watson AB, Yang GY, Solomon JA, Villasenor J (1997), "Visibility of wavelet quantization noise," *IEEE Trans. Image Processing*, Vol. 6, No. 8, pp1164-1175.

[25] Wei Z-H, Qin P, Fu Y-Q (1998), "Perceptual digital watermark of images using wavelet transform," *IEEE Trans. Consumer Electronics*, Vol. 44, No. 4, pp1267-1272.

[26] Wolfgang R, Delp E (1996), "A watermark for digital image," in *Proc. of 1996 International Conference on Image Processing*, Vol. 3. pp211-214.

[27] Wu, C-F, Hsieh, W-S (2000), "Digital watermarks using zerotree of DCT," *IEEE Trans. Consumer Electronics*, Vol. 46, No. 1, pp87-94.

[28] S. Voloshynovskiy, S. Pereira, V. Iquise, and T, Pun, (2001), "Attack Modelling: Towards a Second Generation Watermarking Benchmark," *Signal Processing*, Vol. 81, pp1177-1214.

[29] C. S. Lu, (2005), "Towards robust image watermarking: combining content-dependent key, moment normalization, and side-informed embedding," *Signal Processing: Image Communication*, Vol. 20, pp129-150.