# Wavelet-based Color Image Watermarking using Adaptive Entropy Casting

Ming-Shing Hsieh [1] and Din-Chang Tseng [2 *]

[1] Department of Information Management
Aletheia University, Tamsui, Taiwan 251

[2] Institute of Computer Science and Information Engineering
National Central University, Chung-li, Taiwan 320

* Email: tsengdc@ip.csie.ncu.edu.tw

## Abstract

An adaptive robust image watermarking technique for color image authentication is proposed. In the proposed approach, the *Y* channel of a *Yuv* color host image and a concatenated *RGB* color-image watermark are decomposed into wavelet coefficients. The contextual entropies of the host wavelet coefficients are computed by a log-sum entropy measurement. Then the watermark wavelet coefficients are embedded into the host wavelet coefficients with larger entropy in the corresponding wavelet subbands. An adaptive casting strategy is utilized to embed the watermark coefficients for fully controlling the imperceptibility of watermarked images and the robustness of watermarks. The experimental results show that the proposed approach provides extra robustness against *JPEG*-compression and image-processing attacks; moreover, the proposed approach has no need of the original host image to extract watermarks.

## 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. In general, a watermarking technique should exhibit the requirements: imperceptible watermarked images, robust extracted watermarks, unambiguous watermarks, and providing multimedia data security.

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] and frequency domain [2-10]. In general, the frequency-domain techniques can embed more bits of watermarks and resist more attacks than spatial-domain techniques do.

Several watermarking techniques based on the discrete cosine transform (*DCT*) have been proposed [3, 4, 9]. *DCT*-based methods are suitable to embed pseudo random numbers as watermarks; however, watermark embedded in *DCT* coefficients seems to be easily lost [11]. Recently, the discrete wavelet transform (*DWT*) has been used to hide data in the frequency domain [2, 7, 8]. 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.

In this paper, a wavelet-based watermarking approach for hiding color-image watermarks in color host images is proposed. In the approach, both host and watermark images are decomposed into wavelet coefficients with the same scale levels. The contextual entropies of the host coefficients are computed by a log-sum entropy measurement, and then the watermark coefficients are embedded into the host coefficients with larger entropy in the corresponding wavelet subbands by an adaptive casting technique. The proposed approach could maintain both imperceptibility of watermarked images and robustness of watermarks through high-ratio compression and image-processing attacks; moreover, the extraction of watermarks doesn't need the original host image. With practical experiments, the good properties of imperceptibility and robustness of the proposed approach will be verified.

## 2. The proposed approach

Contextual entropy is generally used for describing local characteristics of signals for analysis. In this study, we propose a context-based approach for watermark embedding. Unlike the methods of [1-6] that only used the larger coefficients to embed watermarks to obtain imperceptible watermarked images but no robust extracted watermarks after high-ratio compression and low-pass filters, we use the surrounding coefficients to calculate the entropy for the corresponding pixels, and embed watermarks in coefficients with larger entropy. A coefficient having larger entropy means that the corresponding pixels locate in a local area with violent spectrum variation in the host image; thus embedding watermarks in these coefficients will get higher imperceptible watermarked image and more robust extracted

watermarks.

Here, the local characteristic is defined by the weighted log sums of wavelet coefficients in a local area; such a characteristic is equivalent to a kind of entropy defined on the corresponding pixels in the original image. Let $\Gamma$ be the set of coefficients in a 5×5 area centered at the considered coefficient $c_i$. Let $\Gamma_2$ be the set of outer coefficients in $\Gamma$ and $\Gamma_1$ be the middle-layer coefficients in $\Gamma$. A coefficient in $\Gamma_2$ (or $\Gamma_1$) means that it has two (or one) units of *Eulerian* distance to $c_i$. The entropy $E_i$ of $c_i$ is defined as

$$E_i = \alpha \sum_{c_j \in \Gamma_2} \log|c_j| + \beta \sum_{c_k \in \Gamma_1} \log|c_k| + \gamma \log|c_i| - |c_i|, \quad (1)$$

where $\alpha$, $\beta$, and $\gamma$ are used for adjusting the weights of the different-layer coefficients; $\alpha + \beta + \gamma = 1$.

### 2.1. Watermark embedding method

The watermark embedding algorithm is described as follows:

$S_1$: Convert *RGB* channels of a host image into *Yuv* channels. Decompose the *Y* channel into a three-level wavelet pyramid structure with ten *DWT* subbands. Let $H^k$ be the *k*th subband.

$S_2$: Concatenate a *n*×*n RGB* color watermark image into a 3*n*×*n* single-channel watermark and then decompose the watermark into ten *DWT* subbands. Let $W^k = \{w^k_i\}$ be the *k*th subband.

$S_3$: Take absolute values on coefficients of all $H^k$, and record their signs. Calculate the entropies of coefficients for all $H^k$ using the proposed method. In order to extract the embedded watermark without the host image, we need extra $r^k$ reference coefficients to hold the necessary information for $H^k$. Assume that the number of coefficients of $W^k$ is $n^k$. Then $p^k = n^k + r^k$ coefficients with larger entropy are selected from $H^k$ to embed watermark $W^k$. Let $\{c^k_i \mid 1 \le i \le p^k\}$ be the selected coefficient set called *the alternative coefficients*.

$S_4$: Sort $\{|c^k_i|\}$ to get $\{s^k_i\}$ called the *sorted alternative coefficients* and record the indexes of the sorted sequence.

$S_5$: Quantize $\{s^k_i\}$ to generate $\{q^k_i\}$ by meaning of dividing $\{s^k_i\}$ into segments with a pre-defined segment length $\tau$ and the coefficients in each segment are set to the same value.

$S_6$: Take absolute values on $\{w^k_i\}$, record their signs, and then sort $\{|w^k_i|\}$ to obtain $\{sw^k_i\}$ and record the indexes of the sorted sequence.

$S_7$: Embed $\{sw^k_i\}$ into $\{q^k_i\}$ sequence by the watermark embedding strategy,

$$q^k_j = q^k_j + \alpha^k_\mu sw^k_{index}, \quad (2)$$

where $\alpha^k_\mu$ is an adaptive scaling factor for robustness watermarking. In our experiments, $\alpha^k_\mu$ is set to $\rho(\sum_{l \in s_\mu} q^k_l \Big/ \sum_{l \in s_\mu} sw^k_l)$, where $\rho$ is an energy factor and $s_\mu$ is the $\mu$ th segment of the quantization sequence. A larger coefficient can embed more fraction of the watermark without obviously degrading the watermarked image.

$S_8$: Save segment length $\tau$, scaling factors $\{\alpha^k_\mu\}$ of quantization segments in all subbands, sign table of $\{w^k_i\}$, and indexes of sorted sequences $\{s^k_i\}$ and $\{sw^k_i\}$ for all subbands as the authenticated key. Recover the signs of all alternative coefficients; take *IDWT* of the changed and unchanged *DWT* coefficients to obtain the watermarked *Y* channel image. The watermarked *Y* channel and the original *U* and *V* channels are converted into *RGB* channels to form a watermarked color image.

### 2.2. Watermark extracting method

Based on the stored authenticated key, the extracting algorithm is described as follows:

$S_1$: The *RGB* channels of the watermarked image are converted into *YUV* channels. Decompose the *Y* channel into ten *DWT* subbands.

$S_2$: Re-fetch the stored authenticated key.

$S_3$: Extract the sorted watermark $\{sw^k_i\}$ for all *DWT* subbands by the equation

$$sw^k_{index} = (q^k_j - ((s^k_i + s^k_{i+\tau+1}) / 2)) / \alpha^k_\mu. \quad (3)$$

$S_4$: Reset the extracted watermark based on the sign table of $\{w^k_i\}$ and indexes of $\{sw^k_i\}$ sequence to get a three-level wavelet pyramid structure. Take *IDWT* of the *DWT* coefficients to obtain the concatenated watermark image and then the extracted color watermark image.

In our scheme, the extracted watermark *W*' is a visually recognizable color image. A subjective measurement based on the standard *correlation* defined as

$$\frac{\sum (w - \overline{w})(w' - \overline{w}')}{\sqrt{\sum (w - \overline{w})^2} \sqrt{\sum (w' - \overline{w}')^2}} \quad (4)$$

is used to evaluate the quality of the extracted watermark by measuring the similarity of the original watermark *W* and the extracted watermark *W*'.

In our watermarking embedding approach, there are a few distortions between a host image and its watermarked image. We use the peak signal-to-noise ratio (*PSNR*) to evaluate the quality of the watermarked images. The larger *PSNR* is, the better the image quality will be. In general, a watermarked image is acceptable by human perception if its *PSNR* is greater than 30 *dBs*.

## 3. Experiments

The proposed perceptual watermarking framework was implemented for evaluating its imperceptibility and robustness. We also examined the detectability of watermarks. In all experiments, the 8-point filters were used

for wavelet decomposition and synthesis.

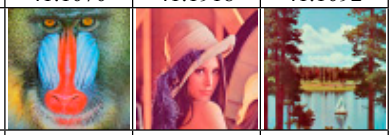
### 3.1. Imperceptibility of watermarked images

Four famous 512×512 color images: *Baboon*, *Lena*, *Pepper*, and *Scene*, were taken as the host images and the re-sampled 64×64 *Pepper* image was taken as the watermark. The *PSNRs* of the watermarked images, the extracted watermarks, and the correlations are given in Table 1, where energy factors were set to 0.2. The *PSNRs* are all greater than 38 *dBs*; that is, the difference between a watermarked image and its original image is imperceptible. The correlations are all greater than 0.98 without attacks; thus the proposed watermarking technique actually yields satisfactory results in imperceptibility and detectability. The high imperceptibility and detectability were not resulted from a specific watermark. The four host images had been shrunken and taken as the watermarks with *Lena* image as the host image to evaluate the generalization of the proposed approach's imperceptibility and detectability. The *PSNRs* of the watermarked images, the extracted watermarks, and the correlations are given in Table 2. All *PSNRs* are greater than 41 *dBs* and all correlations are greater than 0.999 without attacks. Besides, the proposed approach doesn't extract watermark from a no-embed-watermarked host image. An experiment has been conducted to extract a watermark from a no-watermark image; the correlation of the extracted result is 0.0232; it means that we can't extract watermarks from no-watermark images.

Table 1. The *PSNRs* of The Watermarked Images, The Extracted Watermarks (*W*), and Their Correlations (*Corr.*) by The Proposed Approach, Where Energy Factor Are 0.2

| | *Baboon* | *Lena* | *Pepper* | *Scene* |
|---|---|---|---|---|
| *PSNR* | 38.6663 | 41.2006 | 44.9570 | 42.2608 |
| *W* |  | | | |
| *Corr.* | 0.9997 | 0.9995 | 0.9852 | 0.9982 |

Table 2. The *PSNRs* of Watermarked *Lena* Images with three Watermarks, The Extracted Watermarks (*W*), and Their Correlations (*Corr.*) by The Proposed Approach, Where Energy Factor Are All 0.2

| | *Baboon* | *Lena* | *Scene* |
|---|---|---|---|
| *PSNR* | 41.1070 | 41.1918 | 41.1092 |
| *W* |  | | |
| *Corr.* | 0.9996 | 0.9997 | 0.9997 |

### 3.2. Robustness to *JPEG*-compression attack

We here examined watermark robustness with *JPEG* compression. Table 3 shows the correlations of watermarks and the extracted watermarks after *JPEG* compression with compression ratios (*CRs*): 12, 20.6, 32.3, and 65.2, where *Lena* image was taken as the host image, the energy factor is 0.2, and *PSNR* of the watermarked image is 41.2006. The correlations of the extracted watermarks are 0.9838, 0.9616, 0.9239, and 0.8519, respectively. The extracted watermark is visually recognizable even if the compression rate is highly 65.2.

Table 3. The Extracted Watermarks after *JPEG* Attacks with Different Compression Ratios, where The Host Image is *Lena* Image and The Energy Factor is 0.2

| *CR* | 12 | 20.6 | 32.3 | 65.2 |
|---|---|---|---|---|
| *W* |  | | | |
| *Corr.* | 0.9838 | 0.9616 | 0.9239 | 0.8519 |

### 3.3. Robustness to image-processing attacks

We here examined watermark robustness with attacks of smoothing, sharpening, and composite image processing. The correlations of the extracted watermarks from smoothing, sharpening, and composite attacks which are composed of smoothing, sharpening, and *JPEG* compression with *CR* = 65.2 are 0.9044, 0.9288, 0.9307, and 0.8768, respectively, where *Lena* image was also taken as the host image.

### 3.4. Robustness to cropping attacks

Experiments were also conducted to measure how much a color watermark is remained after the watermarked image was cropped. The watermarked *Lena* image was cropped into 410×410 and 384×384 pixels; that is, only 64% and 56% of the watermarked image were remained. The correlations are 0.7414 and 0.6840, respectively. The extracted watermarks are still recognizable after image cropping from the proposed watermarking approach; the extracted results are much better than that of the method proposed by *Cho et al.* [11].

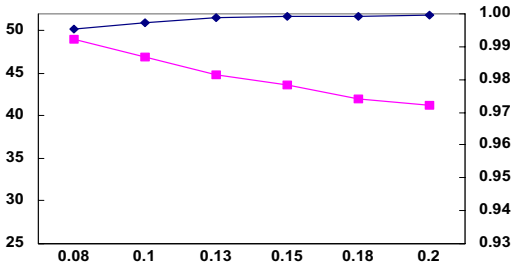
### 3.5. Imperceptibility to different energy factors

We here examined imperceptibility of watermarked images with different energy factors, where *Lena* image was also taken as the host image. Fig. 1 illustrates the *PSNRs* of watermarked images and the correlations of extracted watermarks without attacks. From the experimental results, we see that the imperceptibility is decreasing and the correlation is increasing while the energy factor is enlarged. In other words, the more fraction of a watermark is embedded in the host image, the more robust the watermark is but the less imperceptible the watermarked image is.

### 3.6. Comparisons of imperceptibility and robustness to traditional methods

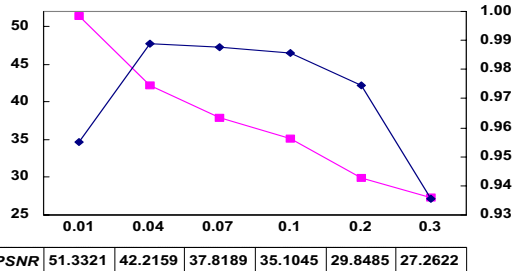
Direct sorting *DWT* coefficients in high-frequency subbands to select larger coefficients to embed watermarks is commonly used by traditional methods. We here examined the method's imperceptibility without attacks and robustness with *JPEG* attack. Fig. 2 illustrates the *PSNRs* of watermarked images and the correlations of extracted watermarks on different energy factors without attacks, where *Lena* image was also taken as the host image. Comparing with the results shown in Fig. 1, the proposed approach is far superior to the traditional methods. As shown in Fig. 2, the correlation seems unstable.

After *JPEG* attack with *CR* = 12, 20, 32, 64 on the watermarked image, the correlations of the extracted watermarks by the traditional method are 0.9077, 0.8294, 0.7642, and 0.6742, respectively, where energy factor is 0.08. Comparing with the results of the proposed approach, the proposed approach still generated better results than the traditional methods generated.




| | | | | | | |
|---|---|---|---|---|---|---|
| PSNR | 48.9701 | 46.9669 | 44.8571 | 43.6669 | 42.0657 | 41.2006 |
| Corr. | 0.9952 | 0.9974 | 0.9988 | 0.9991 | 0.9994 | 0.9995 |

Fig. 1. *PSNRs* and correlations on different energy factors by the proposed approach, where the host image is *Lena* image.




| | | | | | | |
|---|---|---|---|---|---|---|
| PSNR | 51.3321 | 42.2159 | 37.8189 | 35.1045 | 29.8485 | 27.2622 |
| Corr. | 0.955 | 0.989 | 0.9876 | 0.9857 | 0.9747 | 0.9355 |

Fig. 2. *PSNRs* and correlations on different energy factors by a traditional sorting method, where the host image is *Lena* image.

## 4. Conclusions

We have introduced a watermarking framework for embedding visually recognizable color watermarks in color images, which can resist image-processing attacks, such as *JPEG* compression and compound image operations. The proposed watermarking approach is based on the context-based wavelet transform, which considers the local characteristics to choose the larger-entropy *DWT* coefficients to embed watermarks. An adaptive casting strategy was proposed to embed watermark coefficients for completely controlling the imperceptibility of watermarked images and the robustness of watermarks. The experimental results show that the proposed method provides extra imperceptibility and robustness of watermarking. Moreover, the proposed approach has no need of the original host image to extract watermarks.

## References


[1] M.-S. Hwang and C.-C. Chang, "A watermarking technique based on one-way hash functions," in *Proc. Int. Conf. on Image Processing*, vol. 3, 1996, pp. 391-395.

[2] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hidden digital watermarks using multiresolution wavelet transform," *IEEE Trans. Industrial Electronics*, vol. 48, no. 5, pp.875-882, Oct. 2001.

[3] C.-T. Hsu and J.-L. Wu, "DCT-based watermarking for video," *IEEE Trans. Consumer Electronics*, vol. 44, no. 1, pp. 206-216, Feb. 1998.

[4] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Processing*, vol. 8, no. 1, pp. 58-68, Jan. 1999.

[5] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Selected Areas in Communications,* vol. 16, no. 4, pp. 525-539, May 1998.

[6] X.-M. Niu, Z.-M. Lu and S.-H. Sun, "Digital watermark of still image with gray-level digital watermarks," *IEEE Trans. Consumer Electronics*, vol. 46, no. 1, pp. 137-144, Feb. 2000.

[7] N. Kaewkameerd and K. R. Rao, "Wavelet based image adaptive watermarking scheme," *Electronic Letters*, vol. 36, no. 4, pp. 312-313, Feb. 2000.

[8] Z. H. Wei, P. Qin and Y. Q. Fu, "Perceptual digital watermark of images using wavelet transform," *IEEE Trans. Consumer Electronics*, vol. 44, no. 4, pp. 1267-1272, Nov. 1998.

[9] C.-F. Wu and W.-S. Hsieh, "Digital watermarks using zerotree of DCT," *IEEE Trans. Consumer Electronics*, vol. 46, no. 1, pp. 87-94, 2000.

[10] C.-T. Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," *IEEE Trans. Circuits and Systems II*: *Analog and Digital Signal Processing*, vol. 45, no. 8, pp. 1097-1101, Aug. 1998.

[11] J. S. Cho, S. W., Shin, W.H., Lee, J. W., Kim, and J. U. Choi, "Enhancement of robustness of image watermarks embedding into colored image, based on WT and DCT, " in *Proc. Information Technology: Coding and Computing*, 27-29 Mar. 2000, pp. 483-488.