Digital Watermarking by Rearranging and Modifying DCT Coefficients

Hee Sup Lee, Sang Heun Oh, Keun Young Lee
School of Electrical and Computer Engineering, Sungkyunkwan University
300, Chunchundong, Jangangu, Suwon, Kyunggido, 440-746, South Korea
Tel: +82-331-290-7193, Fax: +82-331-290-7180
E-mail: sky@mickey.skku.ac.kr

Abstract: Because of the rapid growth of Internet and multimedia applications, how to protect IPR (intellectual property rights) has become a critical issue. Digital watermarking is one of the ways to overcome the problem of the protection of IPR. Digital watermarking can be applied to multimedia data, such as digital images, digital video, and digital audio. In this paper, we propose a digital watermarking technique for digital images to authenticate an owner or an image by embedding visually recognizable patterns, such as logos, signatures, or stamps into images in BDCT (block discrete cosine transform) frequency domain. The proposed method sorts the components of an original image twice. At the same time, the method, also, rearranges the components of a watermark twice in order to be more robust, and finally embeds the watermark into the image. From the experimental results, the conjunction of three similarity measurements shows that our proposed method is robust to image cropping, image filtering, and JPEG (the Joint Photographic Experts Group) both subjectively and objectively.

1. Introduction

Since the early 90's, a number of papers on digital watermarking methods have been introduced to protect IPR. Digital watermarking has mainly three application fields: data monitoring, copyright protection, and data authentication. In the case of image watermarking, there are two broad categories: in spatial domain and in frequency domain, to embed digital watermarks. The early stages of digital watermarking techniques [1]-[3] use the spatial domain. However, because the spatial domain based watermarking is not robust to the most common attacks, the frequency domain based watermarking methods [4]-[7] are preferred these days.

In the most of the previous works [4]-[5], the watermark is a sequence of random numbers or a symbol, which is invisible and can only be detected by employing "the detection theory [4]." In this paper, we introduce a digital watermarking technique, which embeds a visually recognizable pattern, such as a logo, a signature, or a stamp so that not only the similarity measurement can be provided for verification, but also an extracted visual pattern.

Because human eyes are more sensitive to lower frequency noise, intuitively the watermark should be embedded into the higher frequency coefficients to satisfy one of the critical watermark features "Perceptually invisibility" [4]. However, the information hidden in the higher frequency components can be easily discarded after quantization of lossy compression. Therefore, to achieve another important characteristics of the watermarks "Robustness," a reasonable trade-off should be required. As a result of that, some previous works [6], [7] alter the midrange frequency coefficients.

In this paper, first of all, an original image is BDCT transformed and the coefficients of each block are sorted from the maximum value to the minimum value. After that, the proposed method employs the significant frequency components in order to be more robust, but with acceptably less alterations, which introduce visible artifacts.

This paper was supported by SamSung Research Fund. Sungkyunkwan University, 1999.

2. Embedding Watermarks

2.1 Choice of the Frequency Coefficients of the Perceptually Significant regions

The overall of the proposed watermark embedding sequence is illustrated in figure 1.

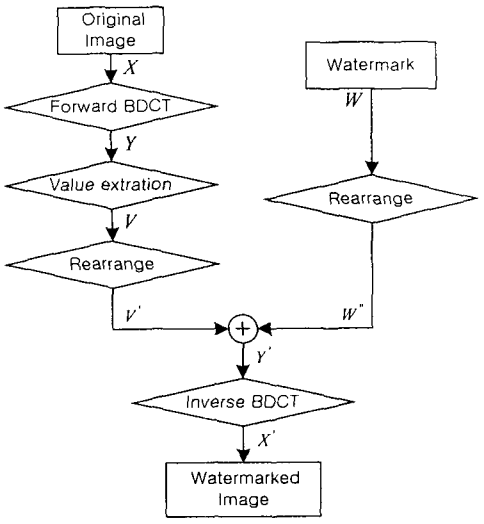


Figure 1. The block diagram of the proposed watermark-embedding scheme.

The original image X and the digital watermark W are represented as

$$X = \{x(i,j), 0 \le i < N, 0 \le j < N\} \qquad (1)$$

where $x(i,j) \in \{0,1,...,2^L - 1\}$ is the magnitude of pixel $x(i,j)$ and L is the number of bits used in each pixel.

$$W = \{w(i,j), 0 \le i < M, 0 \le j < M\} \qquad (2)$$

where $w(i,j) \in \{0,1\}$.

Firstly, the original image is divided into blocks of size 8x8, and the each block is DCT transformed. That is

$$Y = FDCT(X)$$

This is the same basic decomposition currently used in

the still image compression standard, JPEG. Secondly, the method extracts ns highest magnitude coefficients from each sub-block, except the DC component. Because the proposed method embeds a binary image of size $M \times M$, into a gray-level image of size $N \times N$, the method needs $(M/(N/8)) \times (M/(N/8))$ AC coefficients from each sub-block. The selected coefficients are formed as sequences of values V_s.

$$V_s = v_{s1}, v_{s2}, \ldots, v_{sn}$$

where $s = 1,2,3,\ldots,(M/(N/8)) \times (M/(N/8))$, and n is $(N/8) \times (N/8)$.

Next, the each of the sequences V_s is separately rearranged from maximum value to minimum value.

$$V_s' = arrange(V_s)$$

2.2 Structure of the Watermark and Modification of the Selected AC Coefficients

In our approach, the watermark is a binary image of size $M \times M$ (i.e., '1' represents black, and '0' represents white): a logo, a signature, or a stamp, and is embedded into a gray-level images of size $N \times N$.

First, the proposed method divides the watermark into blocks W_s. That is

$$W_s = \left\{ w_s(i,j), 0 \le i < \left(\frac{N}{8}\right), 0 \le j < \left(\frac{N}{8}\right) \right\} \quad (3)$$

where $w_s(i,j) \in \{0,1\}$. After that, the method arranges W_s in order of the number of '1' in each block.

$$W_s' = arrange(W_s)$$

Figure 2 depicts the process of arranging the watermark W_s.

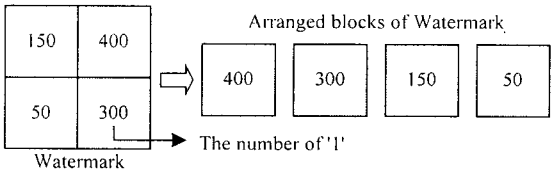


Fig 2. The example of rearranging the watermark.

Second, each of the blocks W_s' is divided into sub-blocks of size $(M/(N/8)) \times (M/(N/8))$, and the sub-blocks are sorted in order of the number of '1' again. After that, each of the sorted blocks W_s' is arranged according to the conventional scanning order to make 1-D sequences. As a result of that, we obtain sorted digital watermarks sequences W_s''. That is

$$W_s'' = w_{s1}'', w_{s2}'', \ldots, w_{sn}''$$

Next, the watermark W_s'' is embedded into the corresponding components of the sequences V_s' by using equation (4).

$$Y' = \begin{cases} NINT(V_S' + (QF - V_S' \bmod QF)), & if\ W_S' = 1 \\ V_S' - V_S' \bmod QF, & if\ W_S' = 0 \end{cases} \quad (4)$$

QF is the quality factor, which controls the trade-off between the robustness of watermarks and the quality of images. The larger the value of QF gets, the more robust the watermarks are. On the contrary, the smaller it gets, the better quality the watermarked images are.

3. Extracting the Watermarks

The extraction of embedded watermarks requires the original image, the watermarked image, and the watermark.

First of all, the locations of the embedded watermarks must be obtained from the original image. This sequence is exactly the same as the watermark-embedding scheme.

Secondly, according to the obtained locations, the AC coefficients are extracted from the watermarked image. That is

$$V_s^{*'} = v_{s1}^{*'}, v_{s2}^{*'}, \ldots, v_{sn}^{*'}$$

After that, the watermarks are detected by comparing the values $V^{*'}$ from the watermarked image, with the values V' from the original image. Equation (5) decides the extracted watermark whether it is '1' or '0'.

$$W^* = \left\{ \begin{array}{l} 1, \ if \ \ NINT\left(\frac{V_S^{*'}}{QF}\right) > INT\left(\frac{V_S'}{QF}\right) \\ 0, \ otherwise \end{array} \right\} \quad (5)$$

The overall block diagram of the watermark extraction scheme is illustrated in figure3.

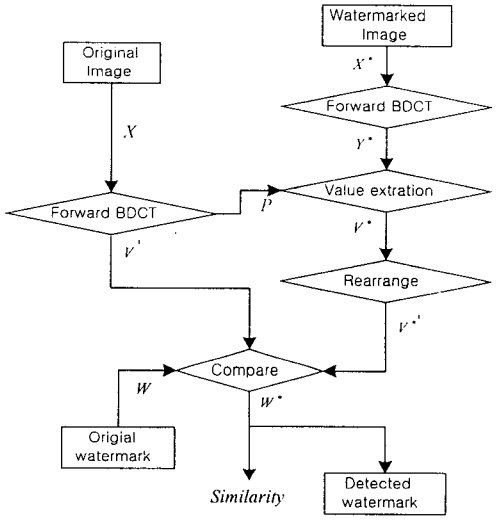


Fig 3. The block diagram of embedded watermarks extraction sequence.

4. Evaluation of the Similarity

There are a number of ways to evaluate the similarity between two watermarks. In this paper, the proposed method defines three different similarity measurements: a visually recognizable pattern, normalized crosscorrelation, and bit-error rate. Because the watermarks are visually recognizable patterns, we can compare the results with the original watermarks subjectively. However, for a number of reasons, quantitative measure-

ments are also required to provide objective judgment. Therefore, our scheme also employs the normalized cross-correlation and the bit-error rate as objective measures. As a result of the conjunction of three measurements above, we can get more secure verification, not only subjectively but also objectively. Equation (3) represents the normalized cross correlation.

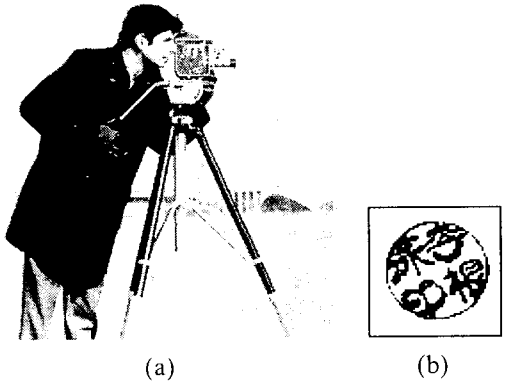
$$Normalized\ Correlation = \frac{\sum_{i,j} W(i,j)W^*(i,j)}{\sum_{i,j} W(i,j)^2} \quad (6)$$

5. Experimental Results

In this section, some experimental results are presented to show the robustness of the watermarks embedded by the proposed method. Figure 3 and Figure 4 illustrate two test images and two watermarks used in the experiments. Because the size of the test images is 256×256 and that of the watermark is 64×64, the method embeds four bits into each sub-block of size 8×8, in other words, it embeds 4096 bits into the original image.

(a) (b)

Fig 4. Test image and watermark. (a) Lenna (256×256), (b) Watermark 1 (64×64).



(a) (b)

Fig 5.Test image and watermark.
(a) Cameraman (256×256), (b) Watermark 2 (64×64).

5.1 JPEG Lossy Compression

Figure 6 shows the watermarked image, "Lenna," with watermark 1, QF 25 and PSNR 38.75 dB. Figure 7 also illustrates the other watermarked image "Cameraman," with the watermark 2, QF 25, and PSNR 38.74 dB.

Figure 8 is a JPEG encoded version of Figure 6 with Compression ratio 17.76 and PSNR 29.55 dB. Figure 9 and 10 show the extracted results from JPEG encoded version of watermarked images, Figure 6, and 7, respectively. Figure 8, 9, and 10, and Table 1 support that most of the embedded watermarks survive JPEG lossy compression even at the very high compression ratio.

Fig 6. Watermarked image, Lenna. (with watermark 1, QF = 25, PSNR = 38.75 dB).

Fig 7. Watermarked image, Cameraman. (with watermark 2, QF = 25, PSNR = 38.74 dB).

Fig 8. JPEG encoded image, Lenna, after watermarking (PSNR = 29.55 dB, compression ratio = 17.76).

(a) (b) (c)

Fig 9. Extracted watermarks from JPEG encoded version of Fig 6. (a) The result from Figure 8, (b) Compression ratio = 13.08, PSNR = 31.01 dB, (c) Compression ratio =

9.65, PSNR= 32.94 dB.

(a) (b) (c)

Fig 10. Extracted watermarks from JPEG encoded version of Figure 7. (a) Compression ratio = 15.64, PSNR = 28.48 dB, (b) Compression ratio = 11.89, PSNR = 29.74 dB, (c) Compression = 8.61, PSNR= 31.79 dB.

Table 1. NC values and Bit-error rate under JPEG lossy compression (Lenna, watermark 1, QF=25).

	Digital Watermarking under JPEG						
CR	17.8	16.2	13.1	8.23	6.7	6.36	5.53
PSNR (dB)	29.5	29.9	31.0	32.9	33.8	34.7	36.4
NC	1.29	1.28	1.19	1.04	1.02	1.03	1.01
Bit-error rate	0.05	0.04	0.027	0	0	0	0

5.2 Image Cropping

Figure 11 illustrates a cropped version of the Figure 7 and the detected watermark. As depicted in here the watermark is robust to the cropping since the proposed method rearranges the watermark twice as well as the selected significant frequency components of the original image.

(a) (b)

Fig 11. (a) Quarter of Fig 7 is discarded. (b) The extracted watermark (NC = 0.77, bit-error rate = 0.034).

5.1 Filtering

(a) (b)

Fig 12. (a) His-pass filtered version of figure 6. (b) The extracted watermark (NC = 0.95, bit-error rate = 0.025).

Fig 12 shows High-pass filtered version of Figure 6 and the extracted watermark. Since the watermark is embedded into the significant frequency components, it is robust to one of the most popular image processing operations, high-pass filtering.

6. Conclusions

The paper has presented a digital watermarking technique based on DCT. Because the scheme embeds watermarks into the significant DCT coefficients by rearranging the watermarks as well as the selected components, it is robust to some common attacks as shown in the experimental results. The method can control the trade-off between the robustness of the watermarks and the quality of the images with QF. In the verification stage of the work, the extracted visually recognizable pattern in conjunction with the normalized crosscorrelation and the bit-error rate is used to enhance the secure verification.

As the last remark, some other kinks of attacks are still challenging to our current work, especially regarding geometrical transformations. Overcoming these problems is one of the main goals of our future work.

References

[1] Maxwell T. Stanford II, Jonathan N. Bradley, and Theodore G Handel, "The data embedding method," in Proceedings of the SPIE Photonics East Conference Philadelphia, September 1995.

[2]R. Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in IEEE Proc. Int. Conf. Image Processing. 1994, VOL. 2.

[3] I. Pitas, "A method for signature casting on digital images," in IEEE Proc. Int. Conf. Image Processing, 1996, VOL. 3

[4] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shanoon, "A Secure, Robust Watermark for Multimedia," Workshop on Information Hiding, Newton Institute, Univ. of Cambridge, May 1996.

[5] Christine I Phdilchuk, and Wenjun Zeng, "Image-Adaptive Watermarking Using Visual Models," IEEE Journal on Selected Areas in Communications, VOL. 16, NO. 4, May 1998.

[6] Chiou-Ting Hsu, and Ja-Ling Wu, "Hidden digital Watermarks in Images," IEEE Trans. on Image Processing, VOL. 8, NO. 1, January 1999.

[7] Juan R. Hernandez, Martin Amado, and Fernando Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure," IEEE Trans. On Image Processing, VOL. 9, NO. 1, January 2000.