DCT-domain Copyright Protection Scheme Based on Secret Sharing Technique

MING-SHI WANG
National Cheng Kung University
Department of Engineering Science
No. 1, Ta-Hsueh Road, Tainan 701
TAIWAN

WEI-CHE CHEN
National Cheng Kung University
Department of Engineering Science
No. 1, Ta-Hsueh Road, Tainan 701
TAIWAN

Abstract: This paper presents a copyright protection scheme based on discrete cosine transform (DCT) and secret sharing techniques. The proposed scheme first utilizes the features of a host image, obtained by performing the DCT on the host image, to generate a master share. Then, the master share is used together with a binary watermark to create an ownership share by employing the secret sharing technique. To verify the rightful ownership of the host image, the hidden watermark can be revealed by using the master and ownership shares. Experimental results demonstrate that the proposed scheme accomplishes satisfactory robustness against several common image processing attacks.

Key–Words: Copyright protection, Digital watermarking, Discrete cosine transform, Secret sharing

1 Introduction

In the past years, digital watermarking has received significant attention as a potential technique for protecting the copyright of digital data. The basic concept of digital watermarking is to hide a known message (watermark) into digital data, where the hidden message can be detected or extracted later to make assertion of the copyright of the protected data.

Depending on the work domain in which the watermark is inserted, digital watermarking schemes can be divided into two categories, spatial domain and transform domain watermarking schemes. In a spatial domain watermarking scheme, the watermark is inserted into the host image by modifying its pixel values [1, 2]. In contrast, a frequency domain scheme first transforms an image into a specific frequency domain, such as discrete fourier transform (DFT), discrete cosine transform (DCT) or discrete wavelet transform (DWT). The watermark is then inserted by modifying the frequency coefficients [3, 4, 5, 6].

The embedding process of most conventional schemes inevitably introduces some permanent distortion. However, there are some applications, such as medical and military images, for which any distortion introduced to the images is not acceptable. This highlights the need to develop the lossless watermarking schemes, in which a watermark is embedded and extracted without any loss of information [7, 8]. In 1995, Naor and Shamir proposed a secret sharing technique for the protection of secret messages [9]. Due to its perfect security, this technique has been applied to copyright protection in recent years [10, 11].

In 2004, Hsieh and Huang proposed a copyright protection scheme based on DWT and secret sharing techniques that can resist common image processing attacks [10]. In 2005, another copyright protection scheme based on DWT and secret sharing techniques was developed by Lou et al. [11]. However, the size of the watermark to be hidden is restricted by the size of the host image in Hsieh and Huang's and Lou et al.'s schemes.

In this paper, we propose a robust copyright protection scheme based on DCT and secret sharing techniques, in which a binary image of any size can be used as the watermark regardless of the size of the host image. The proposed scheme first utilizes DCT technique to obtain the features of the host image, which are used to generate a master share. The master share is then used together with a watermark to create an ownership share according to the secret sharing technique. When the rightful ownership of the host image is needed to be verified, the master and ownership shares are used to reveal the hidden watermark. Experimental results demonstrate that the proposed scheme achieves strong robustness against several common image processing operations.

The remainder of this paper is organized as follows. Section 2 introduces the proposed copyright protection scheme. Section 3 shows the experimental results of the proposed scheme. Finally, conclusions

are drawn in Section 4.

2 Proposed Scheme

The proposed copyright protection scheme consists of two procedures: the ownership share generation procedure and the ownership verification procedure. The details of the proposed scheme are described as follows.

2.1 Ownership Share Generation

Assume that a copyright owner wants to embed a binary watermark $\mathbf{W}$ of size $m \times n$ pixels into a gray-scale host image $\mathbf{H}$ of size $M \times N$ pixels for protecting his or her copyright. The ownership share is generated by performing the following steps:

1. Divide the host image $\mathbf{H}$ into non-overlapping 16×16 blocks b_ℓ $(1 \leq \ell \leq \frac{M}{16} \times \frac{N}{16})$.
2. Perform the DCT on all the blocks of $\mathbf{H}$ to obtain the coefficient sets c_ℓ $(1 \leq \ell \leq \frac{M}{16} \times \frac{N}{16})$.
3. Extract the DC coefficient from each coefficient set to form a DC map of size $M/16 \times N/16$.
4. Generate a feature matrix $\mathbf{X}$ consists of $2m \times 2n$ feature values selected from the DC map by using a pseudorandom number generator seeded with a secret key K.
5. Divide $\mathbf{X}$ into non-overlapping 2×2 blocks x_ℓ $(1 \leq \ell \leq m \times n)$ and calculate the threshold T_ℓ for each block x_ℓ by

$$T_\ell = \frac{1}{4}\sum_{i=1}^{4} x_{\ell i}, \tag{1}$$

where $x_{\ell i}$, $1 \leq i \leq 4$, is the element of x_ℓ.

6. Create a master share $\mathbf{M}$ consists of 2×2 blocks m_ℓ $(1 \leq \ell \leq m \times n)$ by

$$m_{\ell i} = \begin{cases} 1, \text{ if } x_{\ell i} \geq T_\ell, \\ 0, \text{ if } x_{\ell i} < T_\ell. \end{cases} \tag{2}$$

where 1 denotes a white pixel and 0 denotes a black pixel.

7. Construct an ownership share $\mathbf{O} = \{o_\ell \mid 1 \leq \ell \leq m \times n\}$, according to the master share $\mathbf{M}$ and the binary watermark $\mathbf{W}$, by using the following rule:

$$\text{if } \ w_\ell = 0 \ \text{ then } \ o_\ell = m_\ell$$

$$\text{else } \ o_\ell = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} - m_\ell$$

where w_ℓ $(1 \leq \ell \leq m \times n)$ denotes a pixel of the binary watermark $\mathbf{W}$.

8. Register the constructed ownership share $\mathbf{O}$ to the certified authority (CA) for further authentication.

2.2 Ownership Verification

When a dispute over the copyright of the host image arises, the ownership verification procedure must be performed to reveal the hidden watermark. Therefore, the rightful ownership of the suspected image can be verified. The ownership verification procedure can be describes by the following steps:

1. Divide the host image $\mathbf{H}'$ into non-overlapping 16×16 blocks b'_ℓ $(1 \leq \ell \leq \frac{M}{16} \times \frac{N}{16})$.
2. Perform the DCT on all the blocks of $\mathbf{H}'$ to obtain the coefficient sets c'_ℓ $(1 \leq \ell \leq \frac{M}{16} \times \frac{N}{16})$.
3. Extract the DC coefficient from each coefficient set to form a DC map of size $M/16 \times N/16$.
4. Generate a feature matrix $\mathbf{X}'$ consists of $2m \times 2n$ feature values selected from the DC map by using the PRNG seeded with the secret key K.
5. Divide $\mathbf{X}'$ into non-overlapping 2×2 blocks x'_ℓ $(1 \leq \ell \leq m \times n)$ and calculate the threshold T'_ℓ for each block x'_ℓ by using (1).
6. Create a master share $\mathbf{M}'$ consists of 2×2 blocks m'_ℓ $(1 \leq \ell \leq m \times n)$ by using (2).
7. Retrieve the hidden watermark $\mathbf{W}'$ with a size of $2m \times 2n$ pixels, according to the generated master share $\mathbf{M}'$ and the ownership share $\mathbf{O}$ kept by the CA, by the following operation

$$\mathbf{W}' = \mathbf{M}' \oplus \mathbf{O}, \tag{3}$$

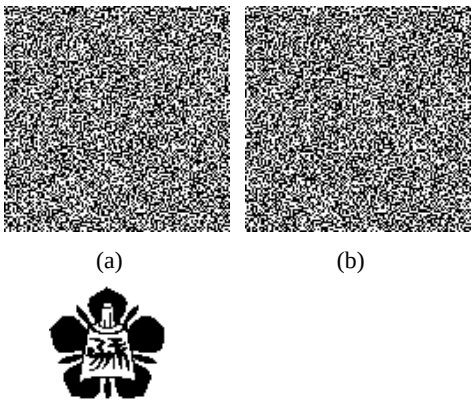
where the symbol $\oplus$ represents the exclusive-or (XOR) operation.

8. Divide the watermark $\mathbf{W}'$ into non-overlapping 2×2 blocks w'_ℓ $(1 \leq \ell \leq m \times n)$ and obtain the reduced watermark $\mathbf{W}''$ of size $m \times n$ by

$$w''_\ell = \begin{cases} 1, \text{ if } \sum_{i=1}^{4} w'_{\ell i} \geq 2, \\ 0, \text{ if } \sum_{i=1}^{4} w'_{\ell i} < 2. \end{cases} \tag{4}$$

(a) (b)

Fig. 1. The host image and the binary watermark.



(a) (b)

(c)

Fig. 2. Sample results of the proposed scheme. (a) Master share, (b) ownership share, (c) revealed watermark.

3 Experimental Results

In this section, the effectiveness of the proposed copyright protection scheme was demonstrated. A gray-scale image "Lena" of size 512×512 pixels, as shown in Fig. 1(a), is used as the test image and a visually meaningful binary image with a size of 64×64 pixels, as shown in Fig. 1(b), is adopted as the watermark in the experiments. Fig. 2 illustrates sample results of the proposed scheme. Figs. 2(a) and 2(b) are the master and ownership shares generated by the proposed scheme. Fig. 2(c) shows the revealed watermark obtained by Figs. 2(a) and 2(b).

To quantitatively evaluate the performance of the proposed copyright protection scheme, two similarity measurements, the peak signal-to-noise ratio (PSNR) and the normalized correlation (NC), were employed in this study. The PSNR is used to measure the image

(a) (b)

Fig. 3. Experimental results under sharpening. (a) Sharpened image, (b) revealed watermark.

quality and is defined as

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}} \,(\text{dB}), \tag{5}$$

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left\| \mathbf{H}_{i,j} - \mathbf{H'}_{i,j} \right\|^2, \tag{6}$$

where $\mathbf{H}_{i,j}$ represents a pixel color of the original host image, $\mathbf{H'}_{i,j}$ represents a pixel color of the attacked image, and $M \times N$ is the image size. The NC, used to measure the similarity between the original binary watermark and the revealed watermark, is defined as

$$\text{NC} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \overline{\mathbf{W}_{i,j} \oplus \mathbf{W''}_{i,j}}}{m \times n}, \tag{7}$$

where $\mathbf{W}_{i,j}$ denotes a pixel color of the original watermark, $\mathbf{W''}_{i,j}$ denotes a pixel color of the revealed watermark, $\oplus$ represents the XOR operation, and $m \times n$ is the watermark size.

The attacks, used to evaluate the performance of the proposed scheme, are sharpening, Gaussian blurring (with a radius of 7 pixels), median filtering (with a width of 11 pixels), color quantization (reduction from 256 colors to 16 colors), noise addition (Gaussian noise with a variance of 60), JPEG lossy compression (with a quality factor of 20), histogram equalization and cropping. Figs. 3-10 demonstrate the revealed watermarks under diverse attacks. In addition, the evaluation results are summarized in Table 1.

Figs. 3-10 show that all the revealed watermarks can be clearly and easily identified by human eyes, even if the test image has undergone severe attacks. Furthermore, the NC values listed in Table 1 are all greater than 0.9. This indicates that the proposed scheme achieved satisfactory resistance to common image processing attacks.

(a) (b)

Fig. 4. Experimental results under Gaussian blurring. (a) Blurred image, (b) revealed watermark.

(a) (b)

Fig. 7. Experimental results under Gaussian noise addition. (a) Noisy image, (b) revealed watermark.

(a) (b)

Fig. 5. Experimental results under median filtering. (a) Filtered image, (b) revealed watermark.

(a) (b)

Fig. 8. Experimental results under JPEG compression. (a) Compressed image, (b) revealed watermark.

(a) (b)

Fig. 6. Experimental results under color quantization. (a) Image with 16 colors, (b) revealed watermark.

(a) (b)

Fig. 9. Experimental results under histogram equalization. (a) Equalized image, (b) revealed watermark.

(a) (b)

Fig. 10. Experimental results under cropping. (a) Cropped image, (b) revealed watermark.

Table 1. Evaluation results of the proposed scheme under diverse attacks

	Lena	
Attack	PSNR	NC
Sharpening	30.15	0.999
Blurring	22.46	0.994
Median filtering	26.88	0.998
Color quantization	15.82	1.000
Noise addition	13.39	0.998
JPEG	32.99	0.999
Histogram equalization	19.47	0.998
Cropping	17.09	0.937

4 Conclusion

In this paper, a robust copyright protection scheme based on DCT and secret sharing techniques was proposed. Experimental results show that the hidden watermarks can be effectively extracted under diverse attacks. And all the extracted watermarks can be clearly and easily identified by human eyes. In summary, the proposed scheme has the following four advantages. First, a binary image of any size can be used as the watermark regardless of the size of the host image. Second, the protection of rightful ownership of digital images is accomplished without modifying original images, which is helpful for some applications in which any modifications of images is unacceptable. Third, the hidden watermark can be revealed without resorting to original images. Fourth, the proposed scheme can effectively resist common image processing operations.

Acknowledgements: This work was supported in part by the National Science Council of the Republic of China under Grant No. NSC-95-2221-E-006-159-MY3.

References:

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, Techniques for data hiding, *IBM system Journal*, Vol. 35, 1996, pp. 313–336.

[2] I. Pitas, A method for signature casting on digital images, in: *Proceeding of IEEE International Conference on Image Processing*, 1996, pp. 215–318.

[3] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, Rotation, scale and translation resilient watermarking for images, *IEEE Transactions on Image Processing*, Vol. 10, 2001, pp. 767–782.

[4] W. C. Chu, DCT-based image watermarking using subsampling, *IEEE Transactions on Multimedia*, Vol. 5, 2003, pp. 34–38.

[5] M. Barni, F. Bartolini, and A. Piva, Improved wavelet-based watermarking through pixel-wise masking, *IEEE Transactions on Image Processing*, Vol. 8, 2001, pp. 783–791.

[6] S. H. Wang and Y. P. Lin, Wavelet tree quantization for copyright protection watermarking, *IEEE Transactions on Image Processing*, Vol. 13, 2004, pp. 154–165.

[7] C. De Vleeschouwer, J. F. Delaigle and B. Macq, Circular interpretation of bijective transformations in lossless watermarking for media asset management, *IEEE Transactions on Multimedia*, Vol. 5, 2003, pp. 97–105.

[8] M. U. Celik, G. Sharma, A. M. Tekalp, E. Saber, Lossless generalized-LSB data embedding, *IEEE Transactions on Image Processing*, Vol. 14, 2005, pp. 253–266.

[9] M. Naor and A. Shamir, Visual cryptography, in: *Proceeding of Advances in Cryptology- EUROCRYPT*94, *LNCS* 950, 1995, pp. 1–12.

[10] S. L. Hsieh and B. Y. Huang, A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation, in: *Proceeding of International Computer Symposium*, 2004, pp. 661–666.

[11] D. C. Lou, J. M. Shieh, and H. K. Tso, Copyright protection scheme based on chaos and secret sharing techniques, *Optical Engineering*, Vol. 44, 2005, 117004.