A Robust Watermarking Technique for Still Image Using Compression Concept and Coefficient Difference

Der-Chyuan Lou, Jiang-Lung Liu, and Hao-Kuan Tso
Department of Electrical Engineering
Chung Cheng Institute of Technology
National Defense University
Tahsi, Taoyuan, Taiwan
dclou@ccit.edu.tw, jlliu@ccit.edu.tw, g950305@ccit.edu.tw

Abstract*-In this paper, a robust watermarking technique for embedding a watermark into gray level image is proposed. The watermark is designed to be extracted without the original image so that the application is more feasible in practice. It is well-known that lossy compression will remove high frequency components of an image. By using the concept of compression to embed a watermark into the coefficients difference between the middle frequency of the original image and the compression one, the proposed scheme provides a robust characteristic and maintains good visual quality of an image. Experimental results show that the scheme not only meets the requirements of the imperceptibility and security, but also features the robustness against various image processing attacks.*

Keyword: Digital watermarking, compression, copyright protection, wavelet transform, robustness.

1. Introduction

In the past few years, there has been enormous growth in computer network and multimedia technologies. Thus, distribution and duplication of digital multimedia such as image, audio and video have become fairly fast and easy. Digital multimedia is easy to duplicate but difficult to distinguish between the original and the duplicated one. Hence, the copyright protection of digital multimedia has become a severe problem. Digital watermarking is an effective solution and plays an important role in copyright protection. By embedding directly some digitized information i.e. digital watermark into digital media, the watermark information can be detected or extracted after suffering from attacks. Thus, the digital watermarking can be used to identify the rightful owner.

An effective watermarking scheme should conform to the following basic requirements: imperceptibility, robustness, and security. However, a watermarking scheme that meets all these requirements is not an easy work [16-17]. For example, digital watermarking embeds a short message into digital image. Such a scheme may not cause noticeable artifact, but might be too weak to stand signal processing attacks. Hence, it is an important issue to develop a robust watermarking scheme with a better tradeoff between robustness and imperceptibility [14].

Current techniques for digital watermarking can be classified into two groups: (1) Spatial domain watermarking methods [1-3] which embed message by directly modifying the pixel values of images. Its advantage is its lower computational complexity because it doesn't need to perform signal transformation. But the disadvantage is its lower security and weak to common attacks. (2) Frequency domain watermarking methods [5-10] which embed message by modulating the coefficients of frequency domain, such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) are mainly researching field. In general, embedding the watermark into frequency domain can increase the imperceptibility, security, and robustness than spatial domain [15].

There are existing different schemes for the watermark extraction depending on whether the original image is necessary or not. In general, the schemes which require the original image for the watermarking extraction process are robust to resist signal processing attacks. However, it will cause two problems: (1) The severe problem of counterfeit attack will increase greatly for ownership verification [11-12]. (2) Searching the original image corresponding to a given watermarking image will be very time-consuming [16]. Furthermore, the schemes we mentioned above are not feasible in practice such as DVD copy protection where the original information may not be available for watermark detection. On the other hand, the schemes which do not require the original image for the watermarking extraction process are more feasible in that situation.

However, the schemes have lower robustness than the former ones [9].

In this paper, we utilize the concept of compression based on the aspects we mentioned above and embed a watermark into the coefficients difference between the middle frequency of the original image and the compression one. The proposed scheme provides a robust characteristic and maintains good visual quality of an image. Moreover, the watermark is designed to be extracted without the original image so that the application is more feasible in practice. The rest of this paper is organized as follows. In Section 2, the related background is introduced. In Section 3, the details of the proposed algorithm are described. The experimental results are shown in Section 4. Finally, the conclusions are drawn in Section 5.

2. Wavelet transformation

It is well-known that the significant portions of an image are concentrated in low frequency. Hence, watermarking information should not be embedded into low frequency to avoid causing noticeable artifacts. Furthermore, in order to survive lossy compression, the important information of a watermark should not be embedded into high frequency of an image [8]. Thus the best way is to embed a watermark into middle frequency component of an image. The hierarchical structure of wavelet transform provides us a straightforward analysis way to embed watermark into an image. Moreover, it also provides excellent spatial-frequency localization for analyzing image features such as edges or textured areas [13].

Nowadays, many researchers have explored and developed the utility of the wavelet transform. Moreover, wavelet transform has replaced DCT and become a main technique in JPEG2000 compression standard. Fig. 1 shows a two-level wavelet decomposition of an image. First, an image is decomposed into four sub-bands (LL1, HL1, LH1, HH1), where L (H) represents the low (high) sub-band and the subscript denotes the pyramid level index. Furthermore, LL, LH, HL and HH represent the approximation, the horizontal detail, the vertical detail and the diagonal detail of an image respectively. The sub-band LL1 can be further decomposed into four sub-bands (LL2, HL2, LH2, HH2). The process is iterated several times that depends on user's applications.

Furthermore, the energy of each sub-band can be computed by the following formula:

$$E = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} y^2(i,j), \qquad (1)$$

where M and N represent the size of the sub-band and y signifies the wavelet coefficients of the image. The energy of the three sub-bands (HL1, LH1, HH1) is relatively small and less than 1% of the total energy [11]. Moreover, human visual system is less sensitive to noise in high resolution bands and in those bands having orientation of 45 degrees [4].

Hence, these sub-bands of high frequency can be modified or removed suitably based on the concept of compression we mentioned above and the modified image will not cause noticeable artifacts.

3. The proposed algorithm

This section will illustrate the proposed scheme in detail. The embedding and extraction process of the proposed scheme are described in Section 3.1 and Section 3.2 respectively.

3.1. Watermark embedding process

The original image X is a gray-level image with M by N pixels. The watermark W is a binary image with S by T pixels. They are defined as follows:

$$X=\{x(i,j) \mid 0\le i\le M-1,\ 0\le j\le N-1,\ 0\le x(i,j)\le 255\}, \qquad (2)$$

and

$$W=\{w(k,l) \mid 0\le k\le S-1,\ 0\le l\le T-1,\ 0\le w(k,l)\le 1\}, \qquad (3)$$

First, the proposed embedding technique decomposes an image into seven sub-bands by wavelet transform. Then a filter is used to filter off high frequency components base on the concept of compression. Finally, the watermark is embedded into the coefficients difference between the middle frequency of the original image and the filtered one. The watermark embedding process is depicted as follows.

Step 1: Generate a pseudo random bit-sequence by using a seed and form the same size matrix as the watermark, i.e.,

$$S=\{s(k,l) \mid 0\le k\le S-1,\ 0\le l\le T-1,\ 0\le s(k,l)\le 1\}, \qquad (4)$$

Step 2: Encrypt the watermark by a bit-wise logical exclusive-OR (XOR) operation with S, i.e.,

$$sw(k,l) = w(k,l)\oplus s(k,l). \qquad (5)$$

Step 3: Decompose the original image into seven sub-bands by using the DWT.

Step 4: Filter off one of three high sub-bands (HL1, LH1, and HH1).

Step 5: Perform the inverse wavelet transform and obtain the filtered image.

Step 6: Decompose the filtered image into seven sub-bands by using the DWT.

Step 7: Extract and compare the coefficient difference between the middle frequency of

the original image and the filtered one by computing $a \le \left| I_{o\_mid} - I_{f\_mid} \right| \le b$.

Step 8: According to the result of Step 7 and randomly select the candidate locations to embed watermark. The watermark is embedded as follows:

$$I_{o\_mid}(i,j) = I_{f\_mid}(i,j) + (2 \times sw(k,l) - 1) \times b, \quad (6)$$

where ß is the visual weight to balance the tradeoff of the robustness of the watermark and the visual quality of the watermarked image.

Step 9: Perform the inverse wavelet transform and obtain the watermarked image.

Note that the sequence of embedded locations of the watermark should keep as the secret key for subsequent watermark extraction. The watermark embedding diagram is shown as Fig. 2.

3.2. Watermark extraction process

The watermark extraction procedure doesn't need the original image. We utilize the sequence of embedded locations and seed to retrieve the watermark. The watermark extraction process is depicted as follows.

Step 1: Decompose the watermarked image into seven sub-bands by using the DWT.

Step 2: Filter off one of three high sub-bands (HL1, LH1, and HH1).

Step 3: Perform the inverse wavelet transform and obtain the filtered watermarked image.

Step 4: Decompose the filtered watermarked image into seven sub-bands by using the DWT.

Step 5: Extract and compare the coefficient difference between the middle frequency of the watermarked image and the filtered watermarked one according to the embedded location and obtain the embedded information, i.e.,

$$sw'(k,l) = \begin{cases} 1 & if \quad I_{w\_mid}(i,j) \ge I_{fw\_mid}(i,j) \\ 0 & if \quad I_{w\_mid}(i,j) < I_{fw\_mid}(i,j). \end{cases} \quad (7)$$

Step 6: Generate a pseudo random bit-sequence by the seed and form the same size matrix as the watermark, i.e.,

$$S = \{ s(k,l) \mid 0 \le k \le S-1, \quad 0 \le l \le T-1, \quad 0 \le s(k,l) \le 1 \}, \quad (8)$$

Step 7: Decrypt the watermark by a bit-wise logical exclusive-OR (XOR) operation with S, i.e.,

$$w'(k,l) = sw'(k,l) \oplus s(k,l). \quad (9)$$

Step 8: Compare the extracted watermark with the original watermark.

4. The experimental results

In the following experiments, two gray-level images with size of 256 by 256 are used as the original image, called Lena and Pepper. An institute's name with size of 32 by 32 is used as the watermark (as shown in Fig 3). The embedded sub-band is HH2. Furthermore, Photoimpact 7.0 is used to perform image processing attacks. First, the watermark is encrypted using a pseudo random bit-sequence generated by a seed. Then the watermark is embedded into the experimental images through the proposed scheme.

After embedding the watermark into the images, we can evaluate the quality of the images by PSNR (Peak Signal to Noise Ratio) value. PSNR of the watermarked image is defined as:

$$PSNR = 10.\log_{10} \frac{255^2}{MSE} (\text{dB}), \quad (10)$$

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (X_{ij} - X'_{ij})^2, \quad (11)$$

where X_{ij} represents the original image and X'_{ij} represents the watermarked image. A large value for PSNR means less difference between the original image and the watermarked one. In general, it is very difficult to recognize the difference between the original image and the watermarked one in vision if the PSNR value is greater than 30 dB.

Furthermore, after extracting the watermark, we can evaluate the visually recognizable patterns subjectively. However, the subjective measurement is determined by the factors such as expertise of the viewers, experimental environments, and so on. To evaluate the performance of the proposed method, some objective measures are adopted in this paper and described as follows.

A. Both normalized cross-correlation (NC) coefficient and standard correlation (also referred to as correlation) coefficient are used to judge the similarity between the original watermark and the extracted one exploited in [7]. The NC coefficient is defined as:

$$\text{NC} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} w(i,j) w'(i,j)}{\sum_{i=1}^{m} \sum_{j=1}^{n} [w(i,j)]^2}. \quad (12)$$

On the other hand, the correlation coefficient (CC) is defined as:

$$\text{CC} = \frac{\sum_{i}^{i=m} \sum_{j}^{j=n} \left(w(i,j) - \overline{w} \right) \left(w'(i,j) - \overline{w'} \right)}{\sqrt{\sum_{i}^{i=m} \sum_{j}^{j=n} \left(w(i,j) - \overline{w} \right)^2} \sqrt{\sum_{i}^{i=m} \sum_{j}^{j=n} \left(w'(i,j) - \overline{w'} \right)^2}}, \quad (13)$$

where W is the original watermark and W' is the extracted watermark. Their corresponding mean values are $\overline{W}$ and $\overline{W}'$ respectively.

B. The bit error rate (BER) is computed as:

$$BER = \frac{N_e}{W_x \cdot W_y}, \quad (14)$$

where N_e denotes the number of bits that has different values in the extracted watermark compared to the original one, W_x and W_y denote the length and width of image respectively [7]. No error bit means the extracted watermark is identical with the original one.

Table 1 shows the PSNR values of the watermarked images and the results of watermark extraction respectively. It is obvious that the watermarked images maintain very good visual quality and the embedded watermark has perfectly extracted from the watermarked image.

On the other hand, we use several image processing tools, including lossy JPEG and JPEG2000 compression methods, scaling, cropping, mixed filtering and, noise adding, to evaluate the robustness of the proposed scheme.

4.1. JPEG and JPEG2000 compression techniques

Compression is a common application which appears often for saving the bandwidth of transmission and the capacity of storage. JPEG compression technique is popular among image compression for still image. Recently, JPEG2000 compression technique has been used widely as a result of its excellent performance in compression.

Table 2 and Table 3 show the results after JPEG and JPEG2000 compression with a quality factor of 10% respectively. Obviously, the extracted watermarks are nearly the same with the original watermark.

4.2. Scaling

In the experiments, the watermarked images are first reduced to 1/4 of its original size. In order to detect the watermark, the reduced image is recovered to its original dimension. From Table 4, the proposed method is also robust against the scaling attack.

4.3. Cropping

This is a very common attack because in many cases the attacker is interested in a small portion of the watermarked images. Table 5 shows the extracted results with 50% of the image has been removed. Although the image quality is degraded greatly, the extracted watermarks are still very good.

4.4. Mixed filtering

We test the robustness of the proposed method by mixing smoothing with sharpening. Table 6 shows the extracted results of applying mixed filtering attack. The test results show the proposed method can also survive the filter attack.

4.5. Noise adding

In the experiment, we evaluate the robustness by adding Gaussian noise on the watermarked image. Table 7 shows the results of adding Gaussian noise with variance 100. The experimental result is still good. It indicates that the proposed scheme is remarkable robust to noise attack.

5. Conclusions

In the paper, we propose a robust watermarking technique by using the concept of compression to embed a watermark into the coefficients difference between the middle frequency of the original image and the compression one. On the other hand, by a pseudo random bit-sequence generated by a seed to encrypt the watermark, the security has strongly enhanced. Furthermore, the watermark is designed to be extracted without the original image so that the application is more feasible in practice. Experimental results show that the scheme not only meets the requirements of the imperceptibility and security, but also features the robustness against various signal processing attacks such as JPEG and JPEG2000 lossy compression techniques, scaling, cropping, mixed filtering and, noise adding.

6. References

[1] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing*, vol. 66, no. 3, pp. 385-403, 1998.

[2] D.-C. Lou and J.-L. Liu, "Steganographic method for secure communications," *Computers & Security*, vol. 21, no. 5, pp. 449-460, 2002.

[3] S.-C. Chu, J. F. Roddick, Z.-M. Lu and J.-S. Pan, "A digital image watermarking method based on labeled bisecting clustering algorithm," *IEICE Transactions on Fundamentals*, vol. E87-A, no. 1, pp. 282-285, Jan. 2004.

[4] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783-791, May 2001.

[5] D.-C. Lou and T.-L. Yin, "Adaptive digital watermarking using fuzzy clustering technique," *IEICE Transactions on Fundamentals*, vol. E84-A, no. 8, pp. 2052-2060, Aug. 2001.

[6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[7] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, Oct. 2001.

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

[9] Peter H. W. Wong, Oscar C. Au, and Y. M. Yeung, "A novel blind multiple watermarking technique for images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 813-830, Aug. 2003.

[10] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77-88, Feb. 2002.

[11] Y.-S. Kim, O. H. Kwon, and R. H. Park, "Wavelet based watermarking method for digital images using the human visual system", *Proceedings of the IEEE International Symposium on Circuits and System*, 1999, vol. 4, pp. 80-83.

[12] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Transactions on Image Processing*, vol. 8, no. 11, pp. 1534-1548, Nov. 1999.

[13] P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, vol. 4314, San Jose, CA, USA, Jan. 2001.

[14] D.-C. Lou and J.-L. Liu, "A robust watermarking scheme based on the just-noticeable-distortion," *Journal of Chung Cheng Institute of Technology*, vol. 31, no. 2, pp. 11-22, May 2003.

[15] D. Zhao, G. Chen, and W. Liu, "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos, Solitons and Fractals*, vol. 22, pp. 47-54, Oct. 2004.

[16] L.-H. Chen and J.-J. Lin, "Mean quantization based image watermarking," *Image and Vision Computing*, vol. 21, pp. 717-727, 2003.

[17] D.-C. Lou and C.-H. Sung, "A steganographic scheme for secure communications based on the chaos and euler theorem," *IEEE Transactions on Multimedia*, vol. 6, no. 3, June 2004.

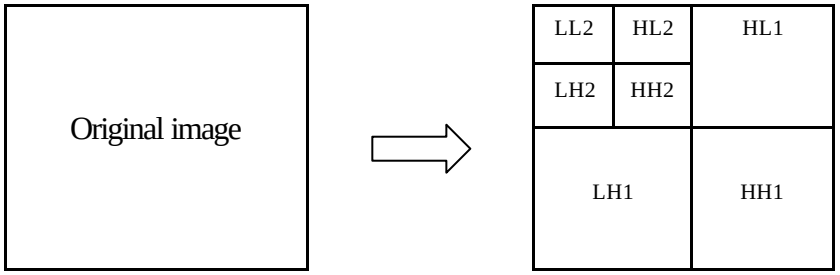

Fig. 1 Two-level wavelet decomposition of an image

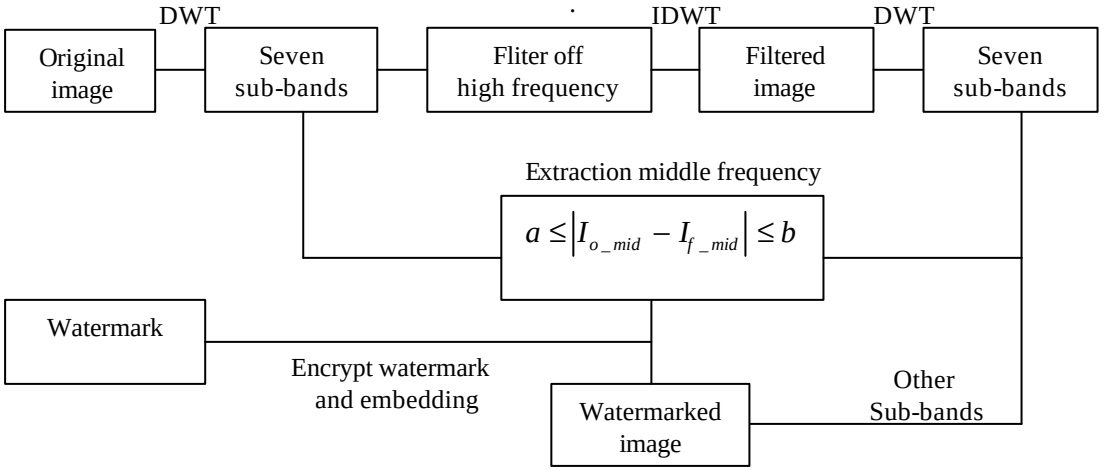

Fig. 2 The diagram of watermark embedding process.



Fig. 3 The experimental images and the watermark, (a) Lena, (b) Pepper, (c) an institute name.

Table 1. The watermarked image under no attack and the results of extraction.

	No attack	Extraction results		
	PSNR	NC	CC	BER
Lena	46.74	1	1	0
Pepper	46.71	1	1	0

Table 2. The watermarked image with a JPEG compression quality factor of 10% and the results of extraction.

	JPEG attack	Extraction results		
	PSNR	NC	CC	BER
Lena	29.14	1	1	0
Pepper	28.56	1	1	0

Table 3 The watermarked image with a JPEG2000 compression quality factor of 10% and the results of extraction.

	JPEG2000 attack	Extraction results		
	PSNR	NC	CC	BER
Lena	23.67	1	1	0
Pepper	21.26	1	1	0

Table 4. The watermarked image by scaling attack and the results of extraction.

	Scaling attack	Extraction results		
	PSNR	NC	CC	BER
Lena	31.19	1	1	0
Pepper	29.29	1	1	0

Table 5. The watermarked image by cropping 50% and the results of extraction.

	Cropping attack	Extraction results		
	PSNR	NC	CC	BER
Lena	8.45	1	1	0
Pepper	7.22	1	1	0

Table 6. The watermarked image by mixed filtering attack (sharpening + blurring) and the results of extraction.

	Mixed attack	Extraction results		
	PSNR	NC	CC	BER
Lena	28.13	1	1	0
Pepper	25.61	1	1	0

Table 7. The watermarked image by adding Gaussian noise with variance 100 and the results of extraction.

	Noise attack	Extraction results		
	PSNR	NC	CC	BER
Lena	10.26	1	1	0
Pepper	10.5	1	1	0