A Robust Copyright Protection Scheme for Still Images

Wei-Bin Lee and Tung-Her Chen
Department of Information Engineering, Feng Chia University,
100 Wenhwa Road, Seatwen Taichung, Taiwan 407, Republic of China.
E-mail：lwb@iecs.fcu.edu.tw

ABSTRACT

A wavelet-based watermarking scheme that does not require the original image for watermark extraction is proposed. The scheme is strong enough to resist malicious manipulations including blurring, JPEG compression, noising, sharpening, scaling, rotation, and printing-photocopying-scanning attacks. It is worthwhile to mention that the scheme is resistant to StirMark and unZign attacks. This new scheme is not only a robust method but also a lossless one. A series of experiments are conducted to prove the robustness property of this method.

Index Terms: Digital watermarking, Copyright protection, Discrete wavelet transform

1. INTRODUCTION

It is no doubt that the progress of network technique introduces digital media, such as text, image, audio and video, being distributed much faster and easier. However, the copyright protection of digital media is rising. This is because the digital media duplicates easier than before. Hence, the enforcement of digital copyright protection is an important issue. Nowadays, the problem of copyright protection really obstructs the rapid evolution of computer and communication networks [14].

There are currently certain cryptographic tools, such as encryption, digital signature and digital timestamp to be well-defined security services for copyright protection [10]. Unfortunately, these techniques are not suitable to deal with digital media directly like images, audio and video. One reason is that the size is much greater than that of text, and need much time to encrypt/sign them. The other reason is that no distortion is allowed in the encrypted/signed data. This condition is, however, not always necessary for the digital media, such as images, audio and video. The digital media losing little fidelity is still acceptable, since human visual systems are not so sensitive. Consequently, a new solution should be provided for the digital media allowing distortion.

Recently, digital watermarking technique has received considerable attention. The essential reason is that it has a high commercial potential for copyright protection and authentication for digital media. A digital watermarking technique embeds a watermark, including a signature or a copyright message, such as a trade logo, a seal, or a sequence number, into an image. Subsequently, the watermark can be extracted/detected from the watermarked image and be adopted to verify the ownership. The reader may refer to [1-9, 14] for details.

There are two classes of digital watermarks for protecting the copyright ownership of digital images. One is the robust watermark designed to withstand various image attacks, such as image processing and geometric distortions. The other is the fragile watermark to verify whether an image has been maliciously altered or further to locate the exact locations where an image has been altered. The robust watermarking scheme is used to protect/verify copyright ownership while fragile watermarking scheme is used for authentication and integrity verification. Here, we focus on the robust watermark technology.

For the purpose of copyright enforcement of a digital image, a watermarking technology should meet the following properties:

1. *Transparency*: The embedded watermark must be perceptually invisible. In other words, the embedding process should not distort the image from the human visual aspect. Hence, the quality of the watermarked image must be little loss or even lossless.
2. *Robustness*: The embedded watermark must be retrieved after image processing and geometric distortions. Here, image processing includes blurring, JPEG compression, noising, and sharpening. The geometric distortions include scaling, rotation, and printing-photocopying-scanning. In other words, it must be robust against an attacker removing the watermark under the premise that a distorted image quality is acceptable. It is known that StirMark and unZign are two powerful benchmarks to evaluate the robustness of the watermarking schemes [9, 13]. In general, a watermarking scheme is easy to break if they cannot survive StirMark and unZign attacks. Unfortunately, StirMark is still a challenge for almost all proposed watermarking techniques.
3. *Unambiguity:* A watermarking technique must identify the owner of an image without ambiguity. That is, in a watermark retrieving process, the watermark retrieval rate must be as high as possible under possible attacks that do not destroy the commercial value of images.
4. *Security*: According to Kerckhoff's principle, the security of a cryptosystem should not depend on keeping the cryptography algorithm secret [10]. The security depends only on keeping the key secret. For the same reason, the security of the watermark should not depend upon the assumption that the pirate does not know the watermarking algorithm. The watermarking algorithm must be public while the embedded watermark is undeletable.
5. *Blindness*: In the watermark verification phase, it is not necessary that using the original image to identify the embedded watermark in the test image. That is, the copyright owners require no extra disk space to preserve the original image. For practice purpose, the blind watermarking scheme is prefer.
6. *Multiple watermarking*: This is an important issue for tracing the distribution of a digital image. For all legal distributors and users, their individual watermarks should be embedded into an image. There is a challenge that a later watermark must not cross against a former watermark in multiple watermarking schemes. Unfortunately, many proposed schemes can not solve this problem.
7. *Tamper-resistance*: For copyright protection purpose, robustness is necessary but not sufficient to guarantee security [4]. A watermarking scheme should resist collusion/averaging attacks [7], excluding image processing and geometric distortions. Assume that there are several identical images embedded with different watermarks for each. For the collusion attack, an attacker takes a small piece from each image. Unfortunately, there is no watermark detectable from the attacked image titled from these extracted small pieces. As compared with the collusion attack, the averaging attack averages the pixel values,

for example, from these identical images in human visual aspect to form an attacked image. Also, the watermark disappears from the attacked image.

However, almost all the proposed technologies cannot simultaneously meet all of these properties, especially StirMark and geometric distortions, such as rotation, and printing-photocopying-scanning [2,3,5,6]. In fact, a pirate is likely not to severely alter the image quality that would loss the image's commercial value. However, it is shown that even slight geometric distortions are strong enough to destroy the embedded watermark.

In [3,5,6], the authors propose the discrete cosine/wavelet transform schemes to embed the watermark by modifying the middle-frequency coefficients. The main drawback is requiring the original image to detect/extract the watermark. It is not suitable for multiple watermarking is another problem. Recently, Chang et al. [1,2] propose the novel schemes to protect the copyright of still images. The main advantages of these methods are (1) the watermarked image is the same as the original, i.e. lossless; (2) the original image is not required to extract the watermark (3) multiple watermarking technique is available and collusion/averaging can be avoided. Unfortunately, some geometric distortions, such as rotation and printing-photocopying-scanning, are still challenges.

In this paper, we propose a novel wavelet-based watermarking scheme, which meets all of the above watermarking property requirements, and there is no need to modify the original image. In contrast with the most current watermarking approaches, the proposed method overcomes the image processing and geometric distortion attacks simultaneously. To prove the feasibility of the scheme, certain watermarking attacks, including StirMark and unZign attacks, are conducted in our experiments.

This paper is organized as follows. In Section 2, we briefly introduce wavelet transform. In Section 3, we propose a new method to protect the copyright of digital images. Experimental results and discussions are given in Section 4 and 5, respectively. Conclusions are given in Section 6.

2. PRELIMINARIES

The Wavelet is a mathematical tool for decomposing functions; see [11,12] for details. In discrete wavelet transform (DWT) model, the image is first decomposed into four subbands, LL_1, LH_1, HL_1 and HH_1 (each 1/4 size of the original image), as shown in Figure 1. The subbands labeled LH_1, HL_1, and HH_1 contain the higher frequency detail information. The subband LL_1 is the low frequency component, which contains the most of the energy in the image. The wavelet transform can be applied again by further decomposing the subband LL_1 into the subbands LL_2, LH_2, HL_2 and HH_2. If the process is repeated t times, we can obtain the subband LL_t through t-scale level wavelet transformation.

3. PROPOSED SCHEME

According to the human visual system property, people are more sensitive to the low frequency components than the high frequency components. However, the lower frequency components can survive under considerable attacks. In addition, the subband LL_t of the original image is very similar to the new subband of the altered image. Based on these observations, we apply these low frequency component coefficients but do not modify them. Hence, this proposed scheme has the advantages of lossless distortions and robustness.

3.1 Watermark Embedding Algorithm

Assume that the original image is a gray-level image with 8 bits per pixel, and the digital watermark is a binary image. The original image X and the watermark image W are defined as follows.

$$X = \{x_{i,j} \mid 0 \le x_{i,j} \le 255, 0 \le i < W_X, 0 \le j < H_X\}, \quad (1)$$

where W_X and H_X is the width and height of X, respectively.

$$W = \{w_{i,j} \mid w_{i,j} \in \{0,1\}, 0 \le i < W_W, 0 \le j < H_W\}, \quad (2)$$

where W_W and H_W is the width and height of W, respectively.

Step 1 Wavelet transforming of the Original Image

The original image is decomposed by repeating wavelet transform t times and to obtain the subband LL_t. The size of subband LL_t (L for short) is W_L by H_L. In our algorithm, L is the same size as the watermark. Without losing the generality, let W_L and H_L be power of 2. Thus, we have

$$W_L = \frac{W_X}{2^t}, \text{ and} \quad (3)$$

$$H_L = \frac{H_X}{2^t}. \quad (4)$$

Here, L is defined as

$$L = \{l_{i,j} \mid 0 \le l_{i,j} \le 255, 0 \le i < W_L, 0 \le j < H_L\}. \quad (5)$$

Step 2 Permuting the Watermark

To against the geometric distortions, especially rotation, the watermark W should be permutated by using a 2-dimension pseudo-random permutation [5,6], for example. The permutated watermark W' is defined as follows:

$$W' = \{w'_{i',j'} \mid w'_{i',j'} = w_{i,j}, 0 \le i', i < W_W, 0 \le j', j < H_W\}. \quad (6)$$

Step 3 Constructing the Polarity Table

The average value P_{av} of all pixels in L is calculated. Each pixel in L is compared with P_{av} and then to construct the polarity table P as follows.

$$P = \{p_{m,n} \mid p_{m,n} \in \{0,1\}, 0 \le m < W_W, 0 \le n < H_W\}, \quad (7)$$

where $p_{m,n} = \begin{cases} 0, & if\ l_{m,n} < P_{av} \\ 1, & if\ l_{m,n} \ge P_{av} \end{cases}$.

Step 4 Generating the Secret Key

After obtaining the binary polarity table P, the secret key K, used to retrieve the watermark, can be computed as

$$K = P \ XOR \ W'. \quad (8)$$

Note that the watermarked image is identical to the original image in our scheme; that is, our scheme is a lossless watermarking technique.

3.2 Watermark Extracting Algorithm

The watermark extraction does not require the original image. The extraction steps are similar to the embedding steps and shortly described as follows.

Step 1 Wavelet Transforming of the Test Image: to obtain the subbnad LL'_t (*L'* for short).

Step 2 Constructing the New Polarity Table: to obtain *P'*.

Step 3 Extracting the Watermark with the Secret Key: to obtain *W"*.

The extracted watermark *W"* is obtained by

$$W'' = P' \ XOR \ K. \quad (9)$$

Step 4 Reverse-permuting the Watermark: to obtain the embedded watermark $\tilde{W}$.

4. EXPERIMENTAL RESULTS

To prove the feasibility of our robust watermarking scheme, we conduct some experiments in this subsection. Figure 2 shows a "classical" image *Lena* as the original image X and a binary image as the watermark W. The original image is a 256 gray-level image with the size of 512x512 pixel and the watermark is a visual recognizable binary image with the size of 64x64. The *Lena* image is 3-scale level wavelet transformed and the subband LL_3 is obtained with size 64x64.

We use the peak signal-to-noise ratio (PSNR) to evaluate the quality between the watermarked image and the original image. The PSNR formula is defined as follows:

$$PSNR = 10\log_{10} \frac{E_{\max}^2 \times X_H \times X_W}{\sum [X(x,y) - X^{'}(x,y)]^2},$$

where X_H and X_W are the image's height and width, respectively. $X(x,y)$ is the original value of the coordinate (x,y) and $X^{'}(x,y)$ is the altered value of the coordinate (x,y). E_{max} is the largest energy of the image pixels (e.g. E_{max} =255 for 8 bits /pixel). The watermark retrieval rate is computed as the ratio of the number of accurate pixels recovered from the retrieved watermark.

The experimental results show that the retrieved watermarks are still recognizable while the original image is seriously distorted. Table 1 shows the experimental results under possible attacks.

All attacks used for the experiments are described here:

1. Image blurring: We blur *Lena* such that the PSNR value is reduced to 29dB.
2. Image JPEG compression: The JPEG compression version of *Lena* is obtained with parameters of 10% quality and 0% smoothing.
3. Image noising: Gaussian noise is added to *Lena* such that the PSNR is reduced to 30dB.
4. Image sharpening: We have sharpened *Lena* until the PSNR is reduced to 28dB.
5. Image scaling: We scale *Lena* from 512x512 to 128x128 pixels and then rescale back to 512x512 pixels.
6. Image rotation: *Lena* is rotated 2 degrees and then resized to 512x512 pixels.
7. Image printing-photocopying-scanning: We print *Lena* using a 1200dpi laser printer. The image was then photocopied and further scanned at a 300dpi and 256 gray-level scanner. Finally, the image is resized to 512x512 pixels.
8. StirMark attack: We apply the StirMark attack to *Lena* one time with the default parameters. The PSNR value is thus reduced to 18dB; however, *Lena* is not severely distorted in human visual aspect.
9. unZign attack: We apply the unZign attack to *Lena* one time with the default parameters. The PSNR value is thus reduced to 25dB; however, *Lena* is not severely distorted in human visual aspect.
10. StirMark and unZign attacks: We apply the StirMark and unZign attacks one time, respectively. The PSNR value is thus reduced to 20dB; however, *Lena* is not severely distorted in human visual aspect.

5. DISCUSSIONS

Here, we will verify that our scheme can satisfy all the robust watermarking properties.

1. *Transparency:* The watermarked image is transparent and lossless against distortion. For medical images, for example, this is a very important property.
2. *Robustness:* According to the experimental results, the watermarking scheme is robust for various image processing and geometric translations. The worst case still has high retrieved ratio up to 82.2%. Especially, the rotation and printing-photocopying-scanning are still challenging for many current watermarking schemes.
3. *Security:* The security of this watermarking technique is based on the secret keys and the seed of permutation function.

4. *Unambiguity:* Because the original image is modified, we can embed several watermarks without distorting the image. Furthermore, according to the experimental results, the retrieval ratios are very high. Obviously, all watermarks are recognizable and thus does convince a verifier that the existence of watermarks without ambiguity.
5. *Blindness:* The watermarking extraction phase does not require the original image. In practice, this is an essential property of the watermarking scheme.
6. *Multiple watermarking:* Because the original image is not modified, this scheme allows the existences of multiple watermarks. The owner can just cast another watermark by generating the corresponding secret key, and save all of the secret keys to verify the ownership of his digital image in the future.
7. *Tamper-resistance:* Because our scheme does not really modify the original image, our scheme is resistant to collusion/averaging attacks.
8. *StirMark and unZign attacks:* Experiments 8, 9 and 10 show that our scheme still survives under StirMark and unZign attacks while these attacks are sensitive to almost all proposed watermarking techniques.

6. CONCLUSIONS

In the proposed scheme, we embed the watermark into the lowest frequency components without modifying them. This property implies that our scheme meets both of the lossless distortion and robustness requirements. Hence, the scheme is adaptive to embed more than one watermark by preserving more than one secret key and collusion/averaging attacks can be avoided. Experimental results show that this scheme is robust simultaneously for blurring, JPEG compression, noising, sharpening, scaling, rotation, printing-photocopying-scanning, StirMark and unZign attacks. It is worthwhile to mention that StirMark attack, rotation, and printing-photocopying-scanning are still challenges for almost all the proposed watermarking schemes.

7. REFERECNES

[1] Chin-Chen Chang and Hsien-Chu Wu, “Computing Watermarks from Images Using Quadtrees,” in Proceedings of the Seventh International Conference on Parallel and Distributed Systems: Workshops, July 2000, Iwate, Japan, pp. 123-128.

[2] Chin-Chen Chang, Kuo-Feng Hwang and Min-Shiang Hwang, “A block based digital watermarks for copy protection of images,” in Fifth Asia-Pacific Conference On Communications/Fourth Optoelectronics And Communications Conference, Beijing, China, October 1999.

[3] 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, 1997.

[4] Scott Craver, Boon-Lock Yeo, and Minerva Yeung, “Technical Trials and Legal Tribulations,” COMMUNICATIONS OF THE ACM, Vol. 41, No. 7, July 1998.

[5] Chiou-Ting Hsu and Ja-Ling Wu, “Multiresolution Watermarking for Digital Images,” IEEE Transactions on Circuits and System—II: Analog and Digital Signal Processing, Vol. 45, No. 8, August 1998.

[6] Chiou-Ting Hsu and Ja-Ling Wu, “Hidden Digital Watermarks in Images,” IEEE Transactions on Image Processing, vol. 8, no. 1, January 1999.

[7] Martin Kutter, Sviatoslav Voloshynovskiy,

Alexander Herrigel, "The Watermark Copy Attack," Proceedings of SPIE: Security and Watermarking of Multimedia Contents II, Volume 3971, San Jose, California, 2000, 1999.

[8] N. Nikolaidis, and I. Pitas, "Digital image watermarking: an overview," IEEE International Conference on Multimedia Computing and Systems, Volume: 1, 1999, Page(s): 1 -6 vol.1

[9] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding—A Survey," Proceedings of the IEEE, special issue on protection of multimedia contents, July 1999.

[10] B. Schneier, Applied Cryptography. WILEY, 2nd edition, 1996.

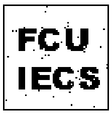
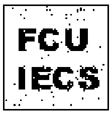
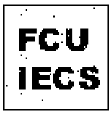
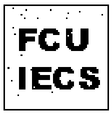
[11] J.M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," IEEE Transactions on Signal Processing, Volume: 41, no. 12, Dec. 1993, Page(s): 3445 -3462

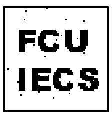
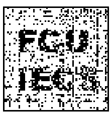
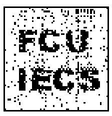
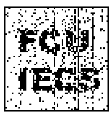
[12] Eric J. Stollnitz, Tony D. DeRose, and David H. Salesin, "Wavelets for computer graphics: A primer," IEEE Computer Graphics and Applications, May 1995.

[13] "unZign Watermark Removal Software", http://altern.org/watermark, 1997.

[14] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: A framework," IEEE Computer Graphics and Applications, vol. 19, no. 1, pp. 18-24, 1999.

Table 1: The attacked images, the corresponding PSNR values, the retrieved watermarks and the corresponding ratio values (%)

	Blurring	JPEG	Noising	Sharpening
Attacked image				
PSNR	29	31	30	28
Extracted watermark				
Ratio	99.0	98.1	99.5	99.5

	Scaling	Rotation	Print-Photocopy-Scan	StirMark
Attacked image				
PSNR	29	14	19	18
Extracted watermark				
Ratio	99.5	82.2	90.4	85.7

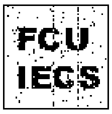
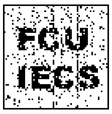
	UnZign	StirMark + unZign
Attacked image		
PSNR	25	20
Extracted watermark		
Ratio	93.1	80.4

Figure 1: The original image is divided into 7 subbands through 2-scale level wavelet transformation

Figure 2: (a) The original image: *Lena,* (b) the watermark