A STUDY ON A WATERMARKING METHOD FOR BOTH COPYRIGHT PROTECTION AND TAMPER DETECTION

Jun Watanabe, Madoka Hasegawa, Shigeo Kato

Faculty of Engineering, Utsunomiya University
7-1-2 Yoto, Utsunomiya, Tochigi 321-8585 Japan
Email: wataj@mclaren.is.utsunomiya-u.ac.jp

ABSTRACT

Most of watermarking methods are either robust watermarking for copyright protection or fragile watermarking for tamper detection. We propose a watermarking method that has both robustness against image processing and ability of tamper detection. In the proposed method, three wavelet coefficients are treated as a vector and one bit of a watermark is embedded by using order relationships among the coefficients. The number of order relationships among three coefficients is six, while only two patterns of relationships are needed to represent one bit of a watermark. Order relationships that are not assigned to a watermark bit can be used for tamper detection.

1. INTRODUCTION

With the spread of digital imaging devices and improvement of personal computers, we can easily create, duplicate, and process digital image data. These useful properties of digital technologies, however, cause problems of copyright violations and malicious tampering. Digital watermarking technology is an active research area, and various watermarking methods have been proposed [1][2].

Most of watermarking methods are either robust watermarking for copyright protection or fragile watermarking for tamper detection. For example, watermarking methods using adjacent pairs of wavelet coefficients in the lowest frequency band are proposed by Kim et al. [3] and Yamada et al. [4]. These methods embed 1 bit of a watermark into a pair of wavelet coefficients. Though they are simple and effective for copyright protection, they are not suitable for tamper detection. On the other hand, the watermarking method proposed by Yeung et al. [5] is fragile watermarking method. This method can be used for image authentication, but in such method embedded information cannot be used when the image is tampered because the watermark has less robustness.

In this paper, we propose a new watermarking method. Our method is based on the work of Yamada et al. [4]. In our method, a watermark has robustness and our method can detect tampering without an original watermark. Relationships among three adjacent wavelet coefficients are used for embedding 1 bit of a watermark. By using 3 wavelet coefficients, there are 3! = 6 patterns in the order relationship among wavelet coefficients, and 2 patterns from them are assigned to express 1 bit of a watermark. Remaining patterns become an invalid set of patterns for watermark embedding, so that we utilize these patterns for detecting tampering. Attacks to a watermarked image can be detected by checking invalid patterns.

2. OUR PROPOSED METHOD

In this section, we describe the watermarking method to embed 1 bit of a watermark to a vector of 3 coefficients. Figure 1 shows the block diagram of our method. Assume that an original image I ($N_x \times N_y$ pixels, 8bpp) is sufficiently large compared to a watermark image W ($L_x \times L_y$ pixels, 1bpp) and a watermark image W is encrypted in advance.

At first, an original image is decomposed into some frequency bands by a wavelet filter. Secondly, coefficients in the lowest frequency band (LL band) are divided into k blocks composed of $3L_x \times L_y$ coefficients as shown in figure 2. Note that the size of block is dependent of the size of the watermark image. That is to say, one bit of the watermark is embedded in horizontally adjacent 3 wavelet coefficients. Thirdly, vectors composed of 3 adjacent coefficients of small differences are selected to embed 1 bit of the watermark image. For example, suppose that $C_i(3m,n)$, $C_i(3m+1,n)$, and $C_i(3m+2,n)$ are factors of a vector of 3×1 adjacent coefficients, where m ($0 \le m \le \lfloor L_x / 3 \rfloor - 1$) and n ($0 \le n \le L_y - 1$) mean the coordinate index in the horizontal and the vertical

0-7803-8554-3/04/$20.00 ©2004 IEEE.

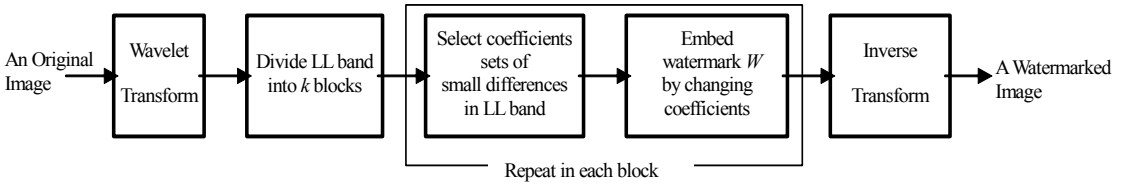

Fig.1: Outline of the watermark embedding method.

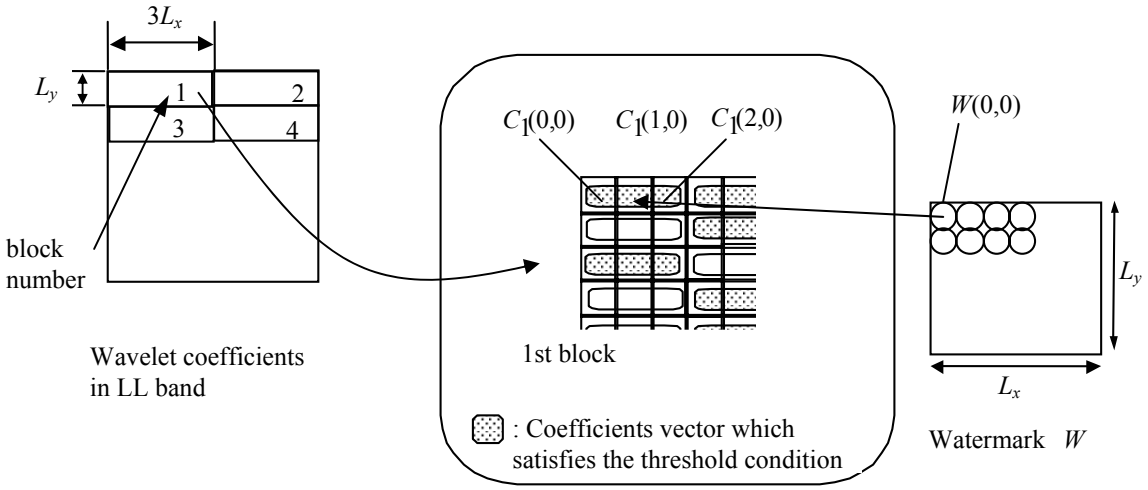

Fig.2: Blocks and vectors of 3×1 coefficients

Table 1: Embedding rules

	$W(m,n)$	Conditions	Ca	Cb	Cc
rule 1	0	$Ca>Cb>Cc$	$M+\alpha$	M	$M-\alpha$
	1	$Cc>Cb>Ca$	$M-\alpha$	M	$M+\alpha$
rule 2	0	$Ca>Cc>Cb$	$M+\alpha$	$M-\alpha$	M
	1	$Cb>Cc>Ca$	$M-\alpha$	$M+\alpha$	M
rule 3	0	$Cb>Ca>Cc$	M	$M+\alpha$	$M-\alpha$
	1	$Cc>Ca>Cb$	M	$M-\alpha$	$M+\alpha$
rule 4	0	$Cb>Cc>Ca$	$M-\alpha$	$M+\alpha$	M
	1	$Ca>Cc>Cb$	$M+\alpha$	$M-\alpha$	M
rule 5	0	$Cc>Ca>Cb$	M	$M-\alpha$	$M+\alpha$
	1	$Cb>Ca>Cc$	M	$M+\alpha$	$M-\alpha$
rule 6	0	$Cc>Cb>Ca$	$M-\alpha$	M	$M+\alpha$
	1	$Ca>Cb>Cc$	$M+\alpha$	M	$M-\alpha$

*) $C_a = C_i(3m,n)$, $C_b = C_i(3m+1,n)$, $C_c = C_i(3m+2,n)$, $M = (C_a+C_b+C_c) / 3$

directions in the i-th block ($0 \le i \le k$-1), respectively. The value $d_i(m,n)$ expressed by the equation (1) is calculated to examine whether a bit of the watermark image can be embedded or not in the coefficients:

$$d_i(m,n) = C_{max} - C_{min} \qquad (1)$$

where C_{max} and C_{min} are the maximum and the minimum coefficients of $C_i(3m,n)$, $C_i(3m+1,n)$, and $C_i(3m+2,n)$, respectively. If $d_i(m,n) \le T$, a watermark pixel $W(m,n)$ is embedded according to a embedding rule. Before the watermark pixel is embedded, one of the embedding rules shown in Table 1 is chosen according to a PN sequence. The seed of the sequence is a secret key.

For example, the embedding is executed as follows. If $W(m,n) = 0$, coefficients $C_i(3m,n)$, $C_i(3m+1,n)$, and $C_i(3m+2,n)$ are changed as the inequality $C_i(3m,n) > C_i(3m+1,n) > C_i(3m+2,n)$ is satisfied when the "rule 1" is selected. Specifically, coefficients are changed according to the rules shown in the first row of table 1, where M is a mean value of 3 coefficients, and α is a parameter

Table 2: CER against various types of attacks and number of valid and invalid vectors

Attacks	CER [%]	Valid vectors	Invalid vectors
Not attacked	100.00	12749	0
JPEG compression(Q=70)	99.71	4924	8079
Gaussian filtering	99.90	5012	8271
Sharpening	97.85	2819	1570
Histogram equalization	100.00	10304	787

Fig.3: auto (384×512 pixels)

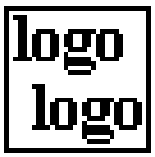

Fig.4: a watermark
(32×32pixels)

concerning image quality and strength of watermark embedding. If coefficients already satisfy this condition, coefficients are not changed. The appropriate inequality is selected and values of coefficients are changed as shown in table 1 according to the bit information of watermarks.

This process is performed in each block repeatedly and the watermarked image ***I'*** is generated by the inverse wavelet transform.

In extracting the watermark, the watermarked image is transformed by the wavelet transform and divided into blocks. Then, vectors of coefficients are examined whether they satisfy the threshold condition by equation (1) or not. If $d_i(m,n) \leq T$, the order of the coefficients is examined, and one bit of the watermark image is extracted. This process is performed in each block repeatedly and the watermark image is decided by a majority decision for each bit of the extracted watermarks.

Fig.5: A watermarked image

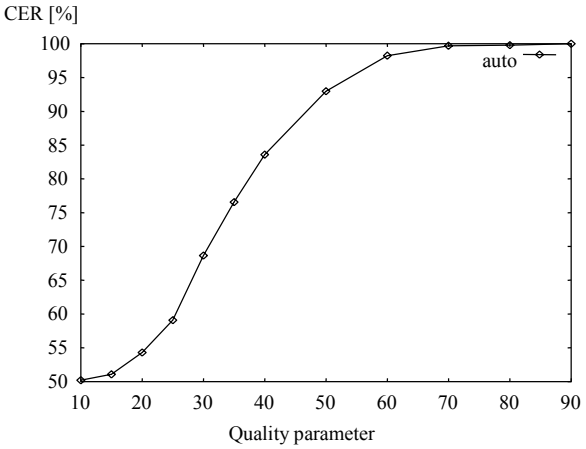

Fig.6: CER against JPEG compression

3. TAMPER DETECTION

Our method can also detect tampering while our method is a robust watermarking method. In our method, there are order relationships of coefficients that are not representing watermark bit. If the watermarked image is tampered, the order relationship will change and invalid vectors such as $C_i(3m,n) > C_i(3m+2,n) > C_i(3m+1,n)$ will appear. Invalid

vectors would not appear if the watermarked image is not tampered, so that we can know whether the image is tampered or not by checking the existence of invalid vectors satisfied the threshold condition.

4. SIMULATION RESULTS

Simulation experiments are performed to investigate capability for detecting tampered image and robustness against attacks. In the simulation, a 384×512 image (auto) shown in Fig. 3 with the eight-bit grayscale resolution is used as an original test image. Our binary watermark is a 32×32 "sample logo" pattern as shown in Fig. 4. The original test image is decomposed to 4 sub-bands by S-transform that is an integer wavelet transform used in [6]. The LL band is composed of 192×256 coefficients; therefore, LL band is divided into 2×8 blocks. We used parameters α=2 and T=12 to embed the watermark. The parameters α and T are decided by preliminary investigations. Watermarked image is shown in Fig. 5. We could recognize little perceptual degradation in the watermarked image. PSNR of the watermarked image to the original image is 40.17[dB].

We examined the robustness and capability of detection of tampering. We evaluate the performance to JPEG compression, Gaussian filtering, sharpening, and histogram equalization. Table 2 shows the correctly extracted ratio (CER) of watermark information against various types of attacks and numbers of valid and invalid vectors. CER is defined in equation (2):

$$CER = \frac{B_c}{L_x \times L_y} \times 100 \quad [\%] \qquad (2)$$

where $L_x \times L_y$ means size of the watermark image, and B_c is the number of correctly extracted watermark bits. The numbers of valid and invalid vectors mean the sum of each vector in all blocks. We used StirMark.3.1.79 for JPEG compression and filtering. In JPEG compression, we examined various quality parameters. Table 2 indicates that our method is effective for the attacks. Figure 6 shows CER against JPEG compression for various quality parameters. CERs are more than 90% if the quality parameter is more than 50. In normal use of JPEG compression, the quality parameter is set to about 70, so that our method has enough robustness against JPEG compression. Invalid vectors appear when the watermarked image is attacked, so that we can detect that the image has been tampered.

The sum of the valid and invalid vectors is different each other because the attacks vary coefficients' values and some watermarked vectors do not satisfy the threshold condition of $d_t(m,n) \leq T$.

5. CONCLUSION

In this paper, we proposed a watermarking method for both copyright protection and tamper detection using wavelet coefficients. The proposed scheme does not require an original image to extract embedded data, and can detect unlawful attacks without original watermark by detecting invalid vectors caused by attacks. The simulation results show that our proposed scheme indicates capability of detection of tampering and good picture quality in the watermarked image. In our future work, we will test more kind of image processing like geometric transform to investigate our method.

6. REFERENCES

[1] X. Xia, C. Boncelet, G. Arce, "A Multiresolution Watermark for Digital Images," *Proc. ICIP'97*, vol. 1, pp. 450-454, 1997.

[2] D. Kundur, D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-based Fusion," *Proc. ICIP'97*, vol. 1, pp. 544-547, 1997.

[3] H. S. Kim, S. H. Bae, O. K. Yoon, K. H. Park, "Watermarking for Digital Images Using Differences and Means of the Neighboring Wavelet Coefficients," *Proc. ITC-CSCC 2000*, vol. 1, pp.466-469, 2000.

[4] T. Yamada, T. Onuki, M. Hasegawa, S. Kato, "Study on a Digital Watermarking Method for Still Images Using Wavelet Transform," *Proc. PCS 2001*, pp.109-112, 2001.

[5] M. Yeung, F. Mintzer, "An Invisible Watermarking Technique for Image Verification," *Proc. ICIP'97*, Santa Barbara, California, 1997. vol. 2, pp. 680-683, 1997

[6] A. Zandi, E. L. Schwartz, and M. Boliek, "CREW: Compression with Reversible Embedded Wavelets," *Proc. Data Compression Conference*, pp.212-221, 1995.