Blind Watermarking Technique Robust To Image Compression

Miin-Luen Day[13], Su-Yin Lee[1] and I-Chang Jou[2]

[1]Department of Computer Science and Information Engineering, National Chiao-Tung University, Hsin-Chu, Taiwan, R.O.C.
[2]Department of Computer and Communication Engineering, National Kaohsiung First University of Science and Technology, Kaohsiung, Taiwan, R.O.C.
[3]Telecommunication Laboratory, Chunghwa Telecom Co., Chung-Li, Taiwan, R.O.C.
e-mail: day@ms.chttl.com.tw , sylee@csie.nctu.edu.tw , icjou@ccms.nkfu.edu.tw

Abstract

The security and copyright issue is an emerging topic in multimedia communications. We present an invisible watermarking scheme to embed copyright or ownership information into digital image by altering the selected wavelet transformed coefficients. The watermark is embedded in the transform domain by confining each selected wavelet coefficient to a specified value to embed one bit of information. Watermark detection does not require the existence of the original image nor original watermark. Furthermore, to meet the security requirement, watermark casting and detection agree with a 3DES cipher key for embedding and extracting to prevent hackers from detecting or removing the watermark. Experimental results demonstrate that the watermark is robust to various lossy compression, e.g., those that result from vector quantization (VQ) based compression, DCT based compression (JPEG), and the state-of-the-art wavelet based compression (SPIHT). The scheme could also be applied to content annotation, covert communication channel, access control, content authentication and integrity verification.

***Keywords** – Blind Watermarking, Image Compression*

1. Introduction

Since Shapiro published his work on embedded zerotree wavelet (EZW) [1] image codec in 1993, which is based on simple uniform scalar quantization, wavelet transform codec [2-6] does outperform in rate-distortion performance over block transform method like DCT. Wavelet image coding methodology has become a state-of-the-art technique for image compression and motivates the ongoing JPEG2000/MPEG4 standardization effort. It is commonly believed that watermarks/labeling (protective image security) is one of the key features related to the JPEG 2000/MPEG4 IPR issues.

The design of watermarking algorithms implies the integration of many concepts coming from cryptography [7], digital communication and signal processing. The development for efficient watermarking algorithms is currently a very active topic [8-13] for researchers in these area. Watermarking is to hide data or information within image, audio or video. Although various applications may have different requirements and performance evaluation criteria, the key requirements for watermarking are as follows: (1) watermark should be perceptually and statistically invisible, (2) watermark should be resistant to various compression up to acceptable visual quality and to various digital image processing operations like filtering or noising, (3) watermark discovery and removal by opponent should be extremely hard, and (4) watermark detection should be blind, i.e, for resolving rightful ownership using invisible watermark, the original image is not necessary for watermark detection. The fulfillment of all these requirements is not so easy, and existing algorithms in the literature are fragile [14-16].

NEC Cox et al. [17] propose an image watermarking method based on spread spectrum theory, which shows pretty good performance among invisibility and robustness to signal processing operation and common geometric transformations. Yet, the main drawbacks are that it needs both the original image and watermark to detect, also its capacity is few, since it just tells whether the watermark exists or not. It is still not convincing for the third party to prove the rightful ownership. A similar but improved method by Piva et al. [18], does not require the original image while achieving strong robustness of the NEC system, however the watermark is still needed for detection.

Hsu and Wu [19] propose a DCT based image authentication technique by embedding a visually recognizable watermark. It can survive the cropping of an image, image enhancement, and the JPEG lossy compression, still it requires the original image to recover the watermark.

W. Zeng and B. Liu [20] propose a statistical scheme that exploits visual models to guarantee that the embedded watermark is imperceptible and robust, which is suitable for resolving the dispute of rightful ownership.

Koch and Zhao [21] propose a DCT based blind embedding scheme by enforcing a relationship between the selected 3 coefficients within 8 x 8 block to embed one bit of information, but it is less robust against geometric distortions.

Since image compression is commonly used for image database archives or transmission, it is essential for watermarking scheme to be resistant to image compression for JPEG (DCT-based) and JPEG2000 (competitive methods are almost wavelet-based, such as SPIHT, WTCQ, and EBCOT et al.). Techniques describing robustness for image compression are described in [22-25], our proposed method is quite competitive with theirs.

2. Proposed Method

To decrease bit error rate, error control coding (ECC) is applied to the binary watermark bit string prior to watermark casting. A (7,4) Hamming codes [26] is utilized, i.e., each nibble of the binary watermark bit string is encoded to a 7-bit code word with 3 extra parity bits, which has the ability to correct single bit error. The introduction of ECC increases retrieval accuracy at the sacrifice of capacity or visual quality.

The embedding locations and criteria for altering wavelet transformed coefficients are determined by a 3DES cipher key (a pseudo random bit sequence) to deter tampering and extraction of embedded information by hostile parties.

2.1. Watermark casting

The watermark is a m x m bitmap logo, indicated as W(k), k = 1, ..,m^2, 3DES key is denoted as D(j), j=1,.., 168. For a n x n image (I), the embedding procedure consists of four steps:

Step 1: Compute the forward DWT of I using a six-stage octave band decomposition with the 9/7 tap biorthogonal filters [27], and image is decomposed into 19 subbands.

Step 2: Reorganize the DWT coefficients using a zigzag scan to obtain a 1 x n^2 vector. The 0^{th} coefficient is skipped.

Step 3: For each coefficient C(i) (i= 1,..n^2-1)

Set Idx = i mod 168.

If D(Idx) is 0, then we don't embed any information for this coefficient, and determine how many following coefficients should be skipped by checking D((Idx+1) mod 168) and D((Idx+2) mod 168).

There are four cases for these two bits:

00: skip one coefficient

01: skip two coefficients

10: skip three coefficients

11: skip four coefficients

If D(Idx) is 1, an embedding is done by a bisection method depending on the modulus residue value to determine whether the implicit bit is 0 or 1. 3DES cipher key (D) is again referenced for embedding in the following:

Let direction = D((Idx+1) mod 168).

Calculate residue = (C(i) mod R).

If ((direction = 1 and W(k) = 1) or (direction = 0 and W(k) = 0)) then set

C(i) = C(i) + 3/4 R – residue,

Otherwise set

C(i) = C(i) + 1/4 R – residue.

In this work, R is set to be 60 to achieve good performance both for robustness and better visual quality.

Step 4: Compute the inverse DWT to reconstruct a watermarked image.

2.2. Watermark detection

For an attacked n x n image (I'), the detection procedure consists of four steps:

Step 1: Compute the forward DWT of I' using a six-stage octave band decomposition with the 9/7 tap biorthogonal filters, and image is decomposed into 19 subbands.

Step 2: Reorganize the DWT coefficients using a zigzag scan to obtain a 1 x n^2 vector. The 0^{th} coefficient is skipped.

Step 3: For each coefficient C(i) (i= 1,..n^2-1)

Set Idx = i mod 168.

If D(Idx) is 0, then there is no bit embedded here, and determine how many following coefficients should be skipped by checking D((Idx+1) mod 168) and D((Idx+2) mod 168).

There are four cases for these two bits:

00: skip one coefficient

01: skip two coefficients

10: skip three coefficients

11: skip four coefficients

If D(Idx) is 1, an extraction is done by a bisection method depending on the modulus residue value to determine whether the implicit bit is 0 or 1, 3DES cipher key (D) is again referenced for extraction in the following:

Let direction = D((Idx+1) mod 168).

Calculate residue = (C(i) mod R).

If ((direction = 1 and residue > 1/2 R) or (direction = 0 and residue <= 1/2 R)) then

W' (k) = 1

else

W' (k) = 0

As in casting phase, R is set to be 60.

Step 4: W' is the extracted watermark.

3. Experimental Results

To evaluate the effectiveness of the proposed method, a 32 x 32 CHT bitmap logo[1] (Fig. 1.) is embedded into two standard images[2] of Lena (Fig. 2) and Barbara (Fig. 3). The wavelet transform used in this work is a six-stage octave band decomposition with the 9/7 tap biorthogonal filters. The watermarked images are shown as Fig. 4 and Fig. 5. The extracted watermark after VQ[3] (1.25bpp), JPEG[4] (quality factor 20%) and SPIHT[5] (0.25bpp) for Lena are shown as Fig. 6, Fig. 7 and Fig. 8, respectively. The retrieval rate and PSNR value of bitmap embedded "Lena" and "Barbara" under VQ compression, JPEG compression, and SPIHT compression are summarized in Table1, Table 2 and Table 3, respectively.

The comparison with other methods in the literature is quite difficult due to that the different methods use different test image, watermark capacity, and the degree of robustness they achieve. Our proposed method is quite competitive with those methods [22-25] that reach the same requirements for invisibility, resistant to compression up to

---

[1] A coarser and smaller version from http://www.hinet.net

[2] obtained from ftp://ipl.rpi.edu/pub/image/still/usc

[3] obtained from ftp://isdl.ee.washington.edu/pub/VQ/code

[4] generated using stirmark 3.1 http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

[5] SPIHT executable obtained from ftp://ipl.rpi.edu/pub/EW_Code

acceptable visual quality, and the original image is not necessary for watermark detection.

4. Conclusion

We present an invisible watermarking scheme to embed copyright or ownership information into digital image by modifying the selected wavelet transformed coefficients. Several tests have shown the robustness of the watermarking scheme to various lossy compression, including VQ compressipn, JPEG compression, and the wavelet based SPIHT compression. It is a very challenging problem for robust digital watermark to survive numerous kinds of malicious or incidental attacks which still calls for further research.

Table 1. Retrieval rate and PSNR value of bitmap embedded "Lena" and "Barbara" under VQ compression.

VQ (bpp)	Lena		Barbara	
	Retrieval rate(%)	PSNR (dB)	Retrieval rate(%)	PSNR (dB)
2.25	100.00	35.52	99.51	30.54
2	100.00	34.42	98.44	29.44
1.75	99.22	33.26	96.09	28.44
1.5	97.36	32.11	90.62	27.39
1.25	91.50	30.97	83.20	26.36

Table 2. Retrieval rate and PSNR value of bitmap embedded "Lena" and "Barbara" under JPEG compression.

JPEG Quality factor Q(%)	Lena		Barbara	
	Retrieval rate(%)	PSNR (dB)	Retrieval Rate(%)	PSNR (dB)
70	100.00	35.92	100.00	34.12
60	100.00	35.28	100.00	32.96
50	100.00	34.77	100.00	32.04
40	99.51	34.23	100.00	31.10
35	99.90	33.93	99.71	30.54
30	99.90	33.53	98.14	29.87
25	97.46	33.03	97.17	29.06
20	90.43	32.38	91.11	28.07
15	77.05	31.49	76.27	26.92
10	62.11	30.13	58.11	25.61

Table 3. Retrieval rate and PSNR value of bitmap embedded "Lena" and "Barbara" under SPIHT compression.

SPIHT Compression ratio(bpp)	Lena		Barbara	
	Retrieval rate(%)	PSNR (dB)	Retrieval rate(%)	PSNR (dB)
2	100.00	39.86	100.00	38.99
1.0	100.00	37.93	100.00	35.34
0.75	100.00	37.11	100.00	33.55
0.5	100.00	35.95	98.54	30.96
0.25	99.02	33.29	73.73	27.43
0.125	73.63	30.77	50.68	24.83

Fig. 1. Watermark (32 x 32 CHT bitmap logo)

Fig. 2. Original Lena (512 x 512 with a grey scaled level)

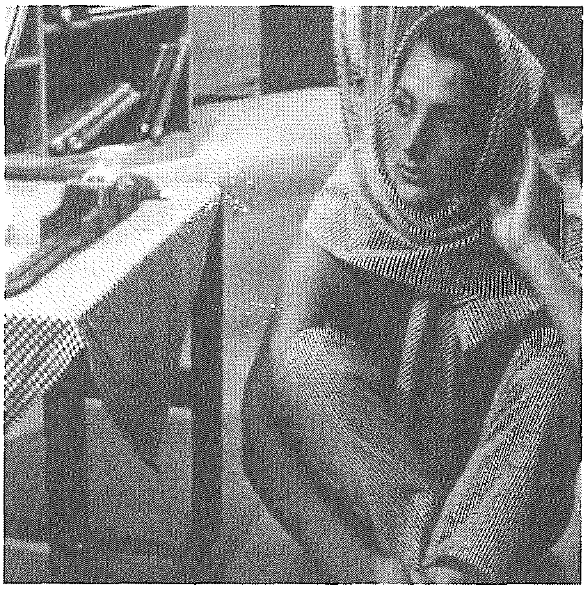

Fig. 3. Original Barbara (512 x 512 with a grey scaled level)

Fig. 4. Watermarked Lena (PSNR 41.42)

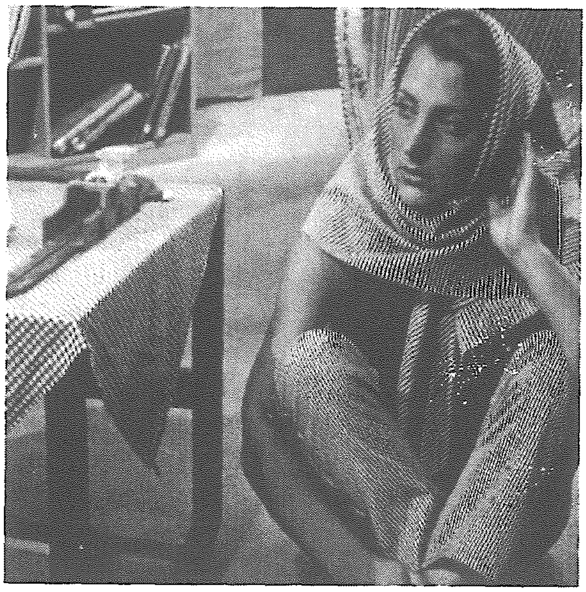

Fig. 5. Watermarked Barbara (PSNR 41.56)

Fig. 6. Extracted watermark after VQ at 1.25bpp (Retrieval rate 91.50%)

Fig. 7. Extracted watermark after JPEG at quality factor 20% (Retrieval rate 90.43%)

Fig. 8. Extracted watermark after SPIHT at 0.25bpp (Retrieval rate 99.02%)

Acknowledgement

This work was supported in part by the National Science Council under grant NSC 88-2612-E-327-001

References

[1] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," IEEE Trans. on Signal Processing, Vol. 41, pp. 3445-3463, December 1993.

[2] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," IEEE Trans. Circuits and Systems for Video Technology, Vol.6, pp. 243-250, June 1996.

[3] D. Taubman, "High Performance Scalable Image Compression with EBCOT", submited to IEEE Trans. Image Proc., March 1999.

[4] A. Bilgin, P. Sementilli, and M. W. Marcellin, "Progressive image coding using trellis coded quantization,"submitted to IEEE Trans. on Image Processing, 1997.

[5] Z. Xiong, K. Ramchandran and T. Orchard, "Space-Frequency Quantization for Wavelet Image Coding," IEEE Trans. on Image Proc. Vol. 6, pp. 677-693, May 1997.

[6] M. J. Tsai, J. D. Villasenor, and F. Chen, "Stack-Run Image Coding," IEEE Trans. Circuits and Systems for Video Technology, Vol.6, pp. 519-521, Oct. 1996.

[7] Bruce Schneier, Applied Cryptography: Protocols 、 Algorithms and Source Code in C. John Wiley & Sons, Inc, 1996.

[8] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," Proceedings of the IEEE, Vol. 86, No. 6, June 1998.

[9] Special Issue on Copyright and Privacy Protection, IEEE Journal on Selected Areas of Communications, Vol. 16, No. 4, May 1998.

[10] Special Issue on Digital Watermarking, Communications of the ACM, Vol. 41, No. 7, July 1998.

[11] Special Issue on Watermarking, Signal Processing Vol 66, No. 3, May 1998.

[12] Information Hiding, Proceedings of the First International Workshop , Springer, Cambridge, U.K., May/June 1996.

[13] Information Hiding, Proceedings of the Second International Workshop, IH'98, Portland, Oregon, USA, April 1998.

[14] Scott Craver, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Tevhniques: Limitations, Attacks, and Implicaton," IEEE Journal on Selected Areas of Communications, Vol. 16, No. 4, May 1998.

[15] Fabien A.P. Petitcolas, Ross J. Anderson, "Weakness of copyright marking systems," Multimedia and Security Workshop at ACM Multimedia '98. Bristol, U.K., September 1998.

[16] Martin Kutter and Fabien A. P. Petitcolas, "A fair benchmark for image watermarking systems," proceedings of Electronic Imaging '99, vol. 3657, pp. 226--239, San Jose, CA, USA, 25--27 January 1999.

[17] Cox J. I, J. Kilian, T. Leighton, and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6, No. 12, December 1997.

[18] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," Proceedings of 4th IEEE International Conference on Image Processing ICIP'97, Santa Barbara, CA, USA, October 26-29, 1997, Vol I, pp. 520-523.

[19] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden Digital Watermarks in Images," IEEE Transactions on Image Processing, Vol. 8, No. 1, December 1997.

[20] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownership of digital images," to appear in IEEE Trans. Image Processing, 1999.

[21] Koch, E. and Zhao, J., "Towards Robust and Hidden Image Copyright Labelling," Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing.

[22] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "The Effect of Matching Watermark and Compression Transforms in Compressed Color Images," Proceedings of the IEEE International Conference on Image Processing, October 4-7,1998, Chicago, Illinois.

[23] Houng-Jyh Wang, Po-Chyi Su and C. C. Jay Kuo, "Wavelet Based Blind Watermark Retrieval Technique," SPIE Phonics East - Symposium on Voice, Video, and Data Communications, Boston, MA, 2-5 November 1998.

[24] Po-Chyi Su, C. C. Jay Kuo and Houng-Jyh Wang, "Blind Digital Watermarking for Cartoon and Map Images, " SPIE Phonics West - Electrical Imaging (EI 99), San Jose, CA January 25-29 1999.

[25] Hisashi INOUE et al., "A Digital Watermark Techniques Based on the Wavelet Transform and Its Robustness on Image Compression and Transformation," IEICE TRANS. FUNDAMENTALS, Vol. E82-A, No. 1, Jan. 1999.

[26] Stefan Katzenbeisser, "Towards Robust Steganography, " http://stud3.tuwien.ac.at/~e9625414/robust-st.html.

[27] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform," IEEE Trans. on Image Proc. Vol. 1, pp. 205-220, Apr. 1992.