International Journal of Fuzzy Logic and Intelligent Systems, vol. 1, no. 1, June 2001 pp. 24-28

A Study on the Performance of the Watermarking with Wavelet Transform

Hwan-Il Kang and Hwan-soo Choi

School of Electrical, Information and Control Engineering, Myongji University
Nam-Dong, Yongin, 449-728, Korea

Abstract

Wavelet transforms are used for implementing digital watermarking methods in the frequency domain. In this paper, we construct the digital watermarking using various wavelet transforms such as the Daubechies transform, Coiflets transform, Symlets transform and the biorthogonal transform, and we compare each digital watermarking method with the others. We investigate the preservation of the watermark after the data compression attack based on the discrete cosine transform. We show that the biorthogonal wavelet, denoted by bior3.5, has the best performance among the wavelet types we selected in an experiment.

Key Words : Wavelet transforms, Digital watermarking, Daubechics transform, Biorthogonal transform, Data Compression

I. Introduction

After the wide spread of the internet and the computer, information hiding techniques receive much attention. The reason is that the copies of the digital media such as mp3, vedio files, still images and electronic books have been copied very easily, rapidly and massively. Steganography is to concern about concealing the existence of the content of messages. For example, Wilkins used invisible ink to print the very small dots for document security [1]. Finger printing method is to identify the original digital media from the hiding information within the copied digital media. Secret information is hidden into the original digital media. When it is copied, we may know the original source of the copied one from the hidden information of the copied one. Watermarking is the technique of hiding information within a host digital media. The goal of the steganography is to conceal the very existence of the secret message while the goal of the watermarking is to provide additional functions through the information hiding [2]. For the public key watermarking, it provides the extraction of the hidden mark and the security of the extracted mark. Watermarking plays an important role as a passive method of digital copyright protection. Using the enscryption [3] or the biometrics, only authorized persons are allowed to access the digital media. Unlike the enscryption or the biometrics, watermarking does not restrict access of the host data.

There are several fields in the watermarking according to the host digital media such as still image watermarking, text image watermarking, audio watermarking [4,5] and video watermarking. The grey-level watermarking, color image watermarking, vector image watermarking and dither image watermarking belong to the category of the still image watermarking. Robust watermarking tries to keep the hidden mark against the attack such as compression, clipping and copy and re-sampling while fragile watermarking has the property that the hidden mark breaks easily by the small attack. Fragile watermarking may be used in the medical NMR imagery. If we can see the hidden mark, then we call it a visible watermarking. Otherwise we call it an invisible watermarking. If the original digital host media is needed when extracting the hidden watermark, we call this type of watermarking a private watermarking. When extracting the hidden watermark without the digital host media, we call this type of watermarking a blind watermarking. The hidden watermark may be a pseudo random number or a bit mapped image such as signatures or company logos. According to the domain of inserting watermarks, the spatial domain and frequency domain watermarking may be considered. For the case of frequency domain watermarking, discrete cosine transform or wavelet transform [6] are used separately, or both are simultaneously used [7].

Vector watermarking [8] methods are applied in files of Postcripts and Autocads. In this case, some watermarks are inserted in files so that the bit mapped image of the original file and that of the watermark inserted file may be indistinguishable. Recently, three dimensional watermarking methods are published [9]. In addition, two different types of watermarks are inserted into a single still image by the Gram-Schmidt orthogonalization method [10].

As a method of the information security, wavelet transform methods [11,12] are implemented for the digital watermark technique. In this paper, we construct the digital watermarking using various wavelet transforms

Maniscript received March 15, 2001; revised May 1, 2001.
This paper was supported by institute of information Technology Assessment (IITA) of Korea. (2000-0128)

such as the Daubechies transform, Coiflets transform, Symlets transform and the biorthogonal transform and we compare each digital watermarking method with the others. We investigate the preservation of the watermark after the data compression attack based on the discrete cosine transform.

This paper is organized as follows : Section 2 is a description of wavelet transform. Section 3 introduces proposed algorithms for the comparison of the various wavelet transform. Section 4 illustrates simulation results. Finally, conclusions are included in Section 5.

II. The Wavelet Transform

2.1 Preliminaries of Wavelet transform

Let $f(t)$ be any square integrable function. The continuous wavelet transform of $f(t)$ with respect to a wavelet $\Psi(t)$ is defind as [13]

$$W(a,b) = \int_{-\infty}^{\infty} f(t)\frac{1}{\sqrt{(|a|}}\Psi^*\left(\frac{t-a}{b}\right)dt. \qquad (1)$$

where a and b are real and * denotes complex conjugation. The inverse continuous wavelet transform is defined as

$$f(t) = \frac{1}{C}\int_{-\infty}^{\infty}\int_{b=-\infty}^{\infty}\frac{1}{|a|^2}W(a,b)\Psi_{a,b}(t)\,da\,db \qquad (2)$$

where C is derived from the Fourier transform for $\Psi(t)$. By sampling (2) at $a=2^k$, $b=2^k\ell$, we introduce a representation $f(t)$ of the form

$$f(t) = \sum_{k=-\infty}^{\infty}\sum_{\ell=-\infty}^{\infty} d(k,\ell)\,2^{k/2}\psi(2^{-k}t-\ell) \qquad (3)$$

The two-dimensional sequence $d(k,\ell)$ is called as the discrete wavelet transform of $f(t)$. [13]

2.2. Decomposition of Images with wavelet transform

The wavelet transform can be used as a perfect reconstruction filter. As a decomposition step, a lowpass and a highpass filters are used and then the filtered signal is subsampled by keeping every other pixel. Using this approach into the still image, a image can be decomposed into four images. The four images are the upper-left subimage that has been lowpass filtered in both the horizontal and vertical directions, the upper-right one that has been lowpass filtered in the horizontal direction and highpassed in the vertical direction, the bottom-left one that has been highpassed in the horizontal direction and lowpassed in the vertical directions, and the bottom-right one that has been highpass filtered in both the horizontal and vertical directions. We can continue to perform the wavelet transform on the upper-left subimage and perform it another time to get the ten subimages as in Figure 1. Many filters can be used to implement the wavelet transform, and the Daubechies, Coiflets, Symlets and the biorthogonal filters will be investigated.

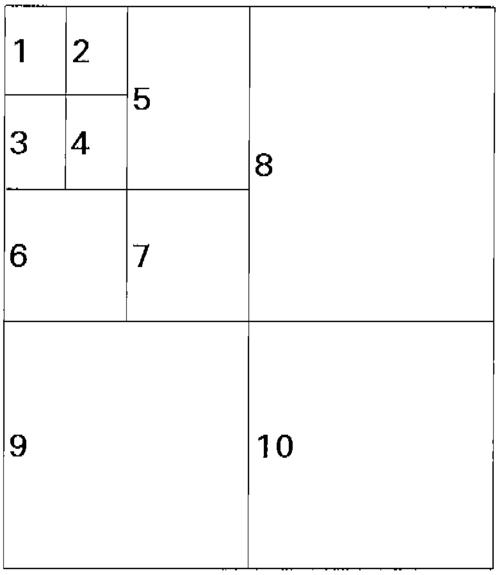

Fig. 1. Wavelet transform having ten subimages

2.3 Various wavelet filters

The low pass filter associated with the db4 wavelet proposed by Daubechies is of the finite impulse response type of length eight,

$$h = \begin{pmatrix} -0.0106, 0.0329, 0.0308, \\ -0.1870, -0.0280, 0.6309, \\ 0.7148,\ 0.2304 \end{pmatrix} \qquad (4)$$

The low pass filter denoted by db9 associated with the Daubechies wavelet is of length eighteen, one denoted by symlet8 associatied with the symlet filter is of length 16, one denoted by symlet3 associated with the symlet filter is of length 6, one denoted by coif3 associatied with the Coiflet filter is of length 18, one denoted by coif5 associatied with the Coiflet filter is of length 30, and the low pass filter and the high pass filter, denoted by bior3.5, of the biorthogonal wavelet are of length 12 and 4, respectively. Finally, the low pass filter and the high pass filter, denoted by bior6.8, of the biorthogonal wavelet are of length 17 and 11, respectively

The low pass filter coefficients [14, 15, 16] of the orthogonal wavelets are in Table 1 and the decomposition low pass and high pass filter coefficients [14, 15, 16] of the biorthogonal wavelets are in Table 2.

III. Algorithms

3.1 Proposed Algorithms

The proposed algorithm for the watermark (w) is as follows:

Step 1: Generate the watermark of length N in terms of the pseudo random number generation.

Step 2: We decompose the test image into 10 subimages by the wavelet transform method.

Step 3: For the N largest wavelet coefficients of the third subimage in the test image, embed the

Table 1: The low pass filter coeff. of various wavelets

Type of wavelets	The decomposition low pass filter coeff.			
db9	0.0000	-0.0003	0.0002	0.0018
	-0.0043	-0.0047	0.0224	0.0003
	-0.0676	0.0307	0.1485	-0.0968
	-0.2933	0.1332	0.6573	0.6048
	0.2438	0.0381		
db4	-0.0106	0.0329	0.0308	-0.1870
	-0.0280	0.6309	0.7148	0.2304
Symlet3	0.0352	-0.0854	-0.1350	0.4599
	0.8069	0.3327		
Symlet8	-0.0034	-0.0005	0.0317	0.0076
	-0.1433	-0.0613	0.4814	0.7772
	0.3644	-0.0519	-0.0272	0.0491
	0.0038	-0.0150	-0.0003	0.0019
Coif3	-0.0000	-0.0001	0.0005	0.0011
	-0.0026	-0.0090	0.0159	0.0346
	-0.0823	-0.0718	0.4285	0.7938
	0.4052	-0.0611	-0.0658	0.0235
	0.0078	-0.0038		
coif5	-0.0000	-0.0000	0.0000	0.0000
	-0.0000	-0.0000	0.0001	0.0003
	-0.0006	-0.0017	0.0024	0.0068
	-0.0092	-0.0198	0.0327	0.0413
	-0.1056	0.0620	0.4380	0.7743
	0.4216	-0.0520	-0.0919	0.0282
	0.0234	-0.0101	-0.0042	0.0022
	0.0004	-0.0002		

Table 2: Decomposition low & high filter coefficients of the biorthogonal wavelets

Type of wavelets	decomposition low & high filter coeff.		
bior3.5	-0.0138	0.0414	0.0525
	-0.2679	-0.0718	0.9667
LF filter	0.9667	-0.0718	-0.2679
	0.0525	0.0414	-0.0138
bior3.5	-0.1768	0.5303	-0.5303
HF filter	0.1768		
bior6.8	0.0019	-0.0019	-0.0170
	0.0119	0.0497	-0.0773
LF filter	-0.0941	0.4208	0.8259
	0.4208	-0.0941	-0.0773
	0.0497	0.0119	-0.0170
	-0.0019	0.0019	
bior6.8	0.0144	-0.0145	-0.0787
	0.0404	0.4178	-0.7589
HF filter	0.4178	0.0404	-0.0787
	-0.0145	0.0144	

watermark in Step 1 in the test image as follows:

$$v' = v^*(1+alpha^*w) \qquad (5)$$

Step 4: We decompose the original image into 10 subimages by the wavelet transform method.

Step 5: For the N largest wavelet coefficient of the third subimage of the original image (vo[1,N]) and the corresponding wavelet coefficient of test image (vt[1,N]), we extract the watermark (w*)

$$w^* = (vt - vo)/(alpha *vo). \qquad (6)$$

Step 6: Compare w* and w, we obtain the similarity

$$S = \langle w, w^* \rangle / \|w^*\|. \qquad (7)$$

Step 7: We modify the original image by performing from the Step 1 to Step 3 and then obtain the image by the inverse wavelet transform. This is the second test image.

Step 8: We transform the image in Step 7 by the block 8-by-8 discrete cosine transform.

Step 9: For each 8-by-8 pixels, the left-upper 12 pixels are unchanged and other block pixels are asssigned to zero.

Step 10: We transform the image in Step 9 by the inverse block 8-by-8 discrete cosine transform.

Step 11: Assign a test image as the image made in Step 10. Applying Steps 5 and 6, we obtain the similarity measure T.

Step 12: We define the compression performance index as

$$(S-T)*100/S(\%). \qquad (8)$$

If the compression performance index gets larger, the degradation effect of the watermark is worse due to the image compression.

IV. Simulation Results

4.1 Experiments

By the black and white Lena image, we test the compression performance index by averaging data 10 times. See the figures 2, 3 and 4. The compression ratio is assigned to 81.25%. In Table 3, we obtain the similarity measures before the compression and after the compression, respectively. In Table 4, the mean value of the compression performance index for the various wavelet types. We show that the biorthogonal wavelet, denoted by bior3.5, has the best performance among the wavelet types we select in the experiment.

V. Conclusions

In this paper, we constructed the digital watermarking using various wavelet transform such as the Daubechies transform, Coiflets transform, Symlets transform and the biorthogonal transform and we compare each digital watermarking method with the others. We investigated the preservation of the watermark after the data compression attack based on the discrete cosine transform. We showed that the biorthogonal wavelet, denotee by bior3.5, has the best performance among the wavelet types we select in the experiment.

Table 3. A wavelet transform and the compresson performance index

wavelet types	Similarity measure with the compressi-on	Similarity measure without the compression	Compression Performance index(%)
symlet3	3.6483	14.2097	74.32
	4.0030	12.7573	68.62
	3.9686	12.8963	69.22
symlet8	1.8595	9.9412	81.29
	2.0432	9.3840	78.23
	1.9603	6.6391	70.47
db4	0.7352	0.9446	22.17
	0.8425	4.1483	79.69
	0.8411	1.6201	48.07
db9	2.4765	8.8522	72.02
	3.0910	9.1724	66.30
	2.2386	5.1449	56.48
bior3.5	0.2218	0.7342	69.79
	3.0910	1.0240	14.41
	2.2386	1.4532	43.80
bior6.8	3.9422	10.1205	61.05
	4.3807	9.6662	54.68
	4.2981	8.7987	51.15
coif3	0.7269	11.2643	93.54
	0.6668	3.5385	81.15
	0.2043	10.6512	98.08
coif5	0.6071	11.6804	94.80
	0.9029	9.2662	90.25
	0.8597	12.9086	93.34

Fig. 2. An original image

Fig. 3. A Compressed image with the watermark

Fig. 4. A watermarked image without the compression

Table 4. Average values of compression performance index

Type of wavelets	Average values of compression performance index(%)
bior3.5	37.59
db9	55.37
bior6.8	59.83
db4	62.43
Symlet3	70.52
Symlet8	73.43
Coif3	85.08
coif5	94.99

References

[1] Fabien A. P. Petitcolas, "Intorduction to information hiding", pp. 11-14, in *Text of Information Hiding Techniques for steganography and digital watermarking edited by Stefan Katzenbeisser and Fabien A. P.* Petitcolas, Artech House, Boston, 2000.

[2] Hyung Woo Choi, "Steganography for digital copyright", pp. 703-726, *Workshop of the internet security and application of the nexr generaion*, Seoul, 2001.

[3] C. Ko, M. Ruschitzka & K. Levitt, "Execution Monitoring of security-critical programs in distributed systems: a specification-cased approach", pp. 134-144, *Proceedings of the IEEE Synposium on Security and Privacy*, 1997.

[4] Hwan Il Kang & Chul-Kyun Chung, "Audio watremarking based on the wavelet transform", pp. 421--424, *Conference of information processing*, Seoul, 2001.

[5] Jong Won Kim, "The technique of the extraction-based and detection-based watermarking", pp. 120-124, *Information security 21c*, Security information Inc, Seoul, 2001.

[6] D. Kundur, D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," *IEEE ICIP*, Santa Barbara, California, Vol. 1, pp. 544- 547, Oct. 1997.

[7] J. S. Cho, S. W. Shin, W. H. Lee, J. W. Kim, J. U. Choi, "Enhancement of robustness of image watermarks embedding into colored image, based on WT and DCT", pp. 438-448, *Information Technology : Coding*

and Computing, 2000.
[8] Hwan I Kang, Kab Il Kim & Jong-Uk Choe, "A vector watermarking using the generalized square mask", pp. 234-236, *Intenational Conference on Information Technology: Coding & Computing,* Las Vegas, 2001.
[9] R. Ohbuchi, H. Masuda and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modifications", pp. 551 -560 Selected Areas in Communications, *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, 1998.
[10] Yun-Hee Oh & Ji-Hwan Park, "Multiple watermarking technique for copyright protection", pp. 161-166, *Conference of broadcasting engineering*, Seoul, 2000
[11] X. Xia, C. G. Boncelet, G. R. Arce, "A Multiresolution Watermark for Digital Images," *Proc. IEEE ICIP*, Vol. 3, pp. 548-551, 1997.
[12] M. Kutter, "Watermarking resisting to translation, rotation, and scaling," *Proc. of SPIE.*, Boston, USA, Nov., 1998.
[13] I. Daubechies, Ten lectures on wavewlets, CBMS series. Philadelphia : SIAM, 1992.
[14] G. Strang, T. Nguyen, Wavelets & Filter Banks, Wellesley_Cambridge Press, Wellesley, MA., 1996.
[15] C. S. Burrus, R. A. Gopinath, H. Guo, Introduction to wavelets and wavelet Transforms: A primer, Prentice-Hall, Upper Sadle River, NJ., 1998.
[16] M. Misiti, Y. Misiti, G. Oppenheim & J. M. Poggi, Wavelet Toolbox, User's Guide. The MathWorlks, Inc., Natick, MA, 1996.

Hwan Il Kang

Hwan Il Kang was born November 27 1956. He received the B.S. and M.S. degrees in Department of Electronics Engineering from Seoul National University and in Department of Electrical Engineering, KAIST, Seoul Korea, in 1980 and 1982 respectively, and Ph. D. degree in Department of Electrical Engineering from the University of Wisconsin-Madison, USA, in 1992. Since 1993, he has been a faculty member of the Dept. of Control and Instrumentation Engineering at the Gyeong-Sang National University. In 1998, he has become an associate professor in Myongji University at the School of Electrical, Information & Control Eng. His research interests are in the areas of multimedia technology softwares such as vector, audio and video watermarking & biometrics. He is a member of IEEE, KIEE, ICASE, and KFIS.

Phone : +82-31-330-6476
Fax : +82-31-321-0271
E-mail : hwan@mju.ac.kr

Hwansoo Choi

Hwansoo Choi was born Dec. 25, 1961. He received the B.S. degree in Control and Instrumentation Egineering from Seoul National University, Korea, in 1984 and M.S. and Ph.D. degrees in Electrical Engineering from University of Washington at Seattle, USA, in 1986 and 1990, respectively. From 1990 to 1992, he performed research at the Laboratory of Computer of LG, Korea. Since 1992, he had joined as a faculty member at the Department Electrical Engineering of Myongji University. He is now an Associate Professor. His research interests are Biometrics, Evolutionary Computation, & Artificial Intelligence. He is a member of IEEE, KITE, KIEE, ICASE, and KFIS.

Phone : +82-31-330-6363
Fax : +82-31-321-0271
E-mail : hschoi@mju.ac.kr