Filter Bank Selection for the Ownership Verification of Wavelet Based Digital Image Watermarking*

Min-Jen Tsai
Institute of Information Management, National Chiao Tung University, R.O.C.
E-mail: mjtsai@cc.nctu.edu.tw

ABSTRACT

Wavelet transform has been widely used in many signal processing applications. Advanced researches have intensively investigated the characteristics of wavelet filters, adaptive wavelet decomposition structure for coding optimization and different combination of mathematical operations for digital image watermarking implementations. Among these studies, there are researches shown that the combination of wavelet filters or filter bank decomposition structure can be implemented as the function of the keys for the watermarking. Even this property provides the flexibility for practical usage, the false alarm of the rightful ownership verification is essentially existed since the resolution requirement for the transformed coefficients can be less demanded than other applications like compression or encryption. Therefore, this study has investigated and discussed the issues and proposed a solution which utilizes the distinguishing index as the selection criterion for wavelet based digital image watermarking in order to increase the difficulty of guessing the right filter banks, in the mean time, to reduce the probability of the misjudgment.

1. INTRODUCTION

Due to the wide acceptance of the Internet and broadband communication, digital watermarking [1-5] recently has become an important technique to guard against unauthorized reproduction. Since the digital information can be easily copied, distributed and modified, the ownership right verification is a critical issue in protecting the author's copyright or legal users' possession. Generally, the verification scheme is based on the statistical calculation where the mathematical values can be identified based on the existence of the watermark. For example, Cox el. in [1] has used the random noise as the watermark and the similarity function to identify the watermark existence. Correlation in [6] is also adopted as the judging criteria for the wavelet transform based techniques. However, we have found that the correlation method can not uniquely identify watermark ownership among different wavelet based approaches and lead to the false copyright claim (high false alarm). Following approaches explain our findings and a distinguishing procedure for the wavelet filter selection is proposed to increase the robustness to the choice of the filter banks and reduce the possibility of judging confusion.

*This work was partially supported by the National Science Council in Taiwan, Republic of China, under Grant NSC 91-2416-H009-012, NSC92-2416-H009-012 and NSC93-2416-H-009-009.

2. THE APPROACH

Before we get into the discussion of the wavelet based implementation, a hypothesis is proposed that the embedded information in the wavelet domain can be almost or exactly extracted if the embedded procedure is well guessed and performed even the filters are not the original ones.

To identify this claim, we have found both orthogonal and biorthogonal filter cases that the transformed coefficients can be pretty close even the transform themselves are different. In real implementation, further operation like the truncation, rounding or quantization procedure may even result in the same mathematical values for some digital signal processing applications.

To verify this hypothesis, the watermarking approach in [6] has been implemented for the Lena image and other frequently quoted images. Interested readers can refer the details in [6] and here only gives briefly explanation. The watermark embedding procedures can be summarized as the following steps:

1. watermark rotation, scrambling and normalization
2. based on the watermark and image information, the decision of wavelet tree structure for wavelet decomposition
3. random orthonormal filter bank generation
4. replacement of the selected band for the watermark and then reconstruction of the watermarked image
5. key information preservation

The watermark extraction procedures are also summarized as the following:

1. key information restoration and decomposition of the watermarked image
2. watermark extraction from the selected band, descramble and renormalization.
3. correlation calculation.

0-7803-8554-3/04/$20.00 ©2004 IEEE.

There is high freedom to select the decomposition structure of the wavelet tree and the filter banks where the information must be preserved as the keys for watermark extraction. One decomposition structure is shown in Figure 1 where image is horizontally and vertically filtered and decomposed into high and low frequency subbands. In this study, one set of filter bank is performed horizontally and vertically for each wavelet decomposition level to simplify the comparison with the algorithm in [6] even we understand the filters used in the horizontal and vertical direction can be different. The original Lena image is used as the decomposition example in Figure 1 as the subband 9 is selected as the embedding band. A watermark constructed from the 16×16 binary "PSU" pattern "  "(similar pattern as used in [6]) is rotated, scrambled, normalized and inserted in the desired band as circled in the Figure 1. To have the large sidelobes of the filter banks, the relationship of $a_1+a_3+a_5 = 0.5$ and $a_1 \le 0.2$ requirement is satisfied for the autocorrelation sequence $P(z) = 1 + a_1(z+z^{-1}) + a_3(z^3+z^{-3}) + a_5(z^5+z^{-5})$. To achieve the ownership verification capability, a correlation identification procedure is adopted and 0.4 is suggested as the correlation threshold (with false alarm probability as low as 1.365×10^{-11}) to identify the watermark existence [6].

To verify our hypothesis, we randomly generated more than 76000 orthogonal wavelet filters with length of six and selected one set of filter to perform the watermark embedding. Accordingly, we used all the generated filters to perform the watermark extraction and found there are 21313 filters with correlation values higher than 0.9 (Figure 2(a)) with no any attack to the watermarked image. Even the high correlation value of 0.999914 for the exact wavelet filters, there are still many other filters with correlation close to one which confuse the ownership right verification. In addition, if the watermarked image is under JPEG 2000 [7] attack at the bit rate of 0.5, we can get much lower correlation values in Figure 2(b). However, there are 25592 set of filters with correlation value higher than 0.4 which contributes more than 33.6% of the total filters. The figure 2(b) also shows quite a large number of filter with correlation value higher than the exact filter combination with correlation value at 0.596301. Therefore, the misjudgment situation is pretty significant in the no attack and under attack conditions if the counterfeiter can perform the wavelet filter banks with good approximation to the actual filters and well guess the embedding procedures. Since it is a quite well known fact that the embedding band should be in the medium frequency bands to avoid the perceptual detection and then removal by attackers, our experiment results contradict to the claim in [6] as the paper suggests that the scheme is hard for counterfeiters to find the embedded band and different filter banks can be unique as the private keys for the watermark.

Since the scheme in [6] allows multiple filter banks to be applied in the wavelet transform, we deliberately substitute the filters in Figure 1 for multiple sets of filter bank application. However, the false alarm condition with high correlation values still exists while only a single set of filter bank is used during the watermark extraction procedure. Since all the filters are generated from the same autocorrelation sequence, the similarity between the filters may cause the confusion. We are aware that there are some discussions about the characteristics of the wavelet filters like the property of regularity, impulse response or others [8]. However, we have tested them but can not find close approximation in this application. Therefore, we propose a filter bank distinguish index as the selection criteria for the algorithm in [6] to reduce the possibility of false alarm. The distinguishing index of the filter banks can be summarized in the following steps and the flow chart of the algorithm is shown in Figure 3:

Step (*i*) both filter banks perform *n* stages of one dimensional uniform wavelet decomposition where *n* can be a sufficiently large number as long as the wavelet transformation is still meaningful.

Step (*ii*) impulse sequence as the input for both filter banks where a length of 256 is used in this study.

Step (*iii*) The correlation values of each decomposed band

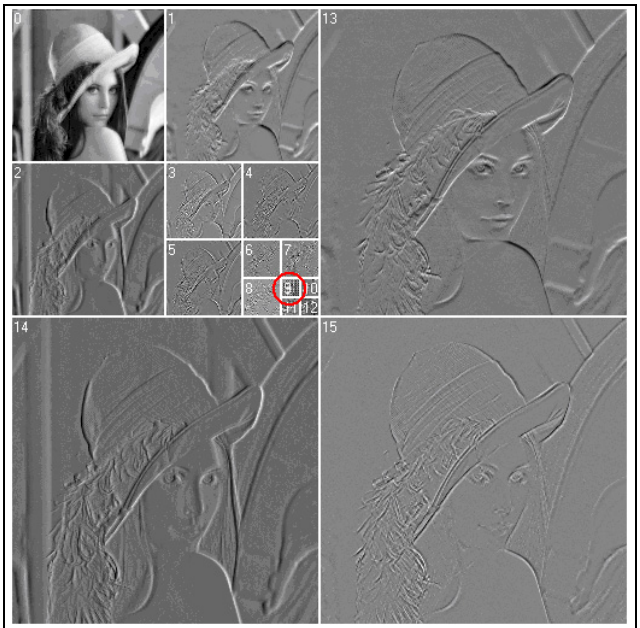

Figure 1. Illustration of the wavelet packet decomposition of Lena image where the subband numbering is labeled on the upper left corner of each subband and the watermark embedded subband is circled. In this example, the embedded subband is the band 9.

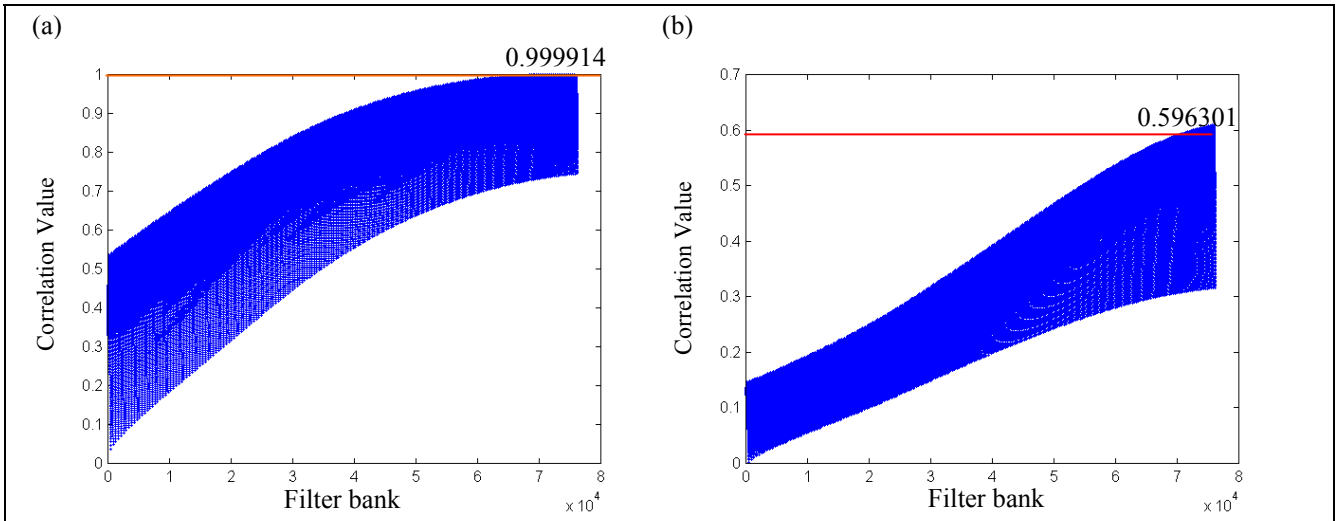

Figure 2. Illustration of the correlation values vs. filter bank where single set of filters are performed across the wavelet Transform domain. (a) watermarked Lena image with no attack (b) image under 0.5bpp JPEG2000 compression.

from both filter banks are averaged and a n stage decomposition should have 2^n inputs at the average stage and the averaged value named as the distinguishing index for filter selection reference.

3. DISCUSSION

Since the threshold is 0.4 formulated in [6] and the study generally performs five level of wavelet decomposition as shown in Figure 2, the distinguish index threshold is gained at $(0.4)^{1/5} \approx 0.83$ as the criteria. Therefore, we randomly

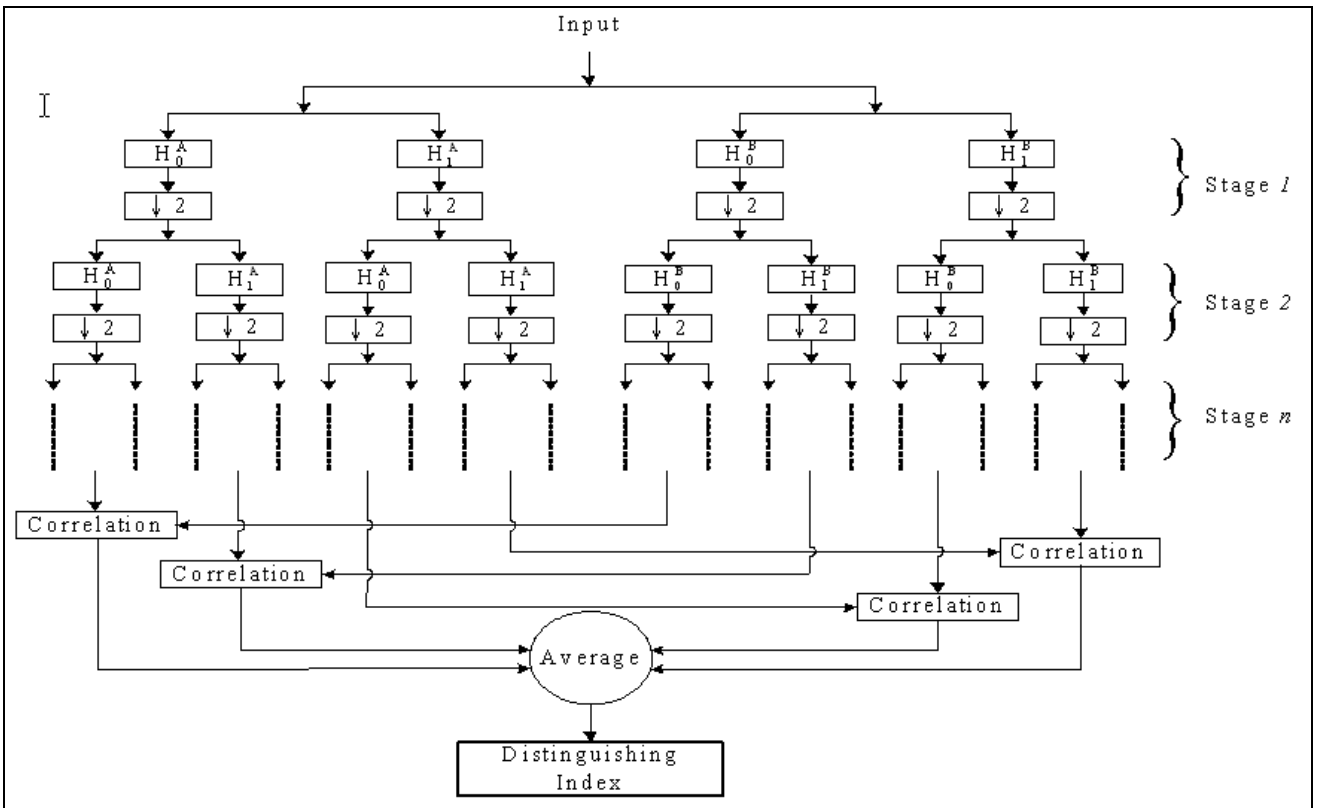

Figure 3. Flowchart of distinguishing index generation for wavelet filter bank A and B.

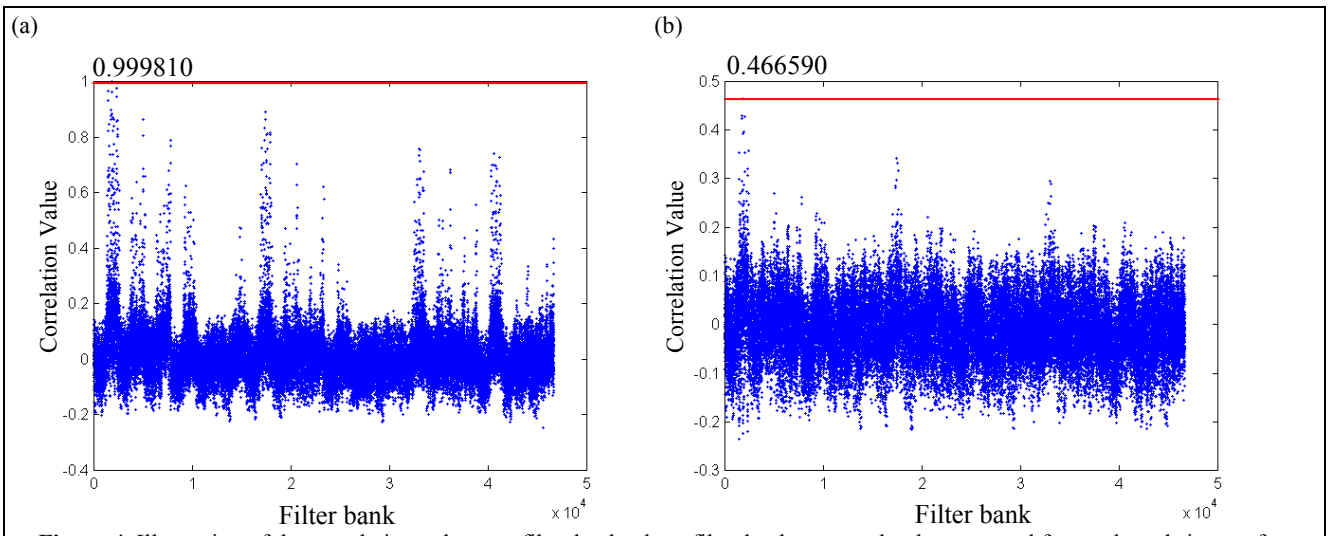

Figure 4. Illustration of the correlation values vs. filter bank where filter banks are randomly generated from selected six set of filter banks. (a) watermarked Lena image with no attack (b) image under 0.5 bpp JPEG 2000 compression.

select six filters from the orthogonal [6] and biorthogonal wavelet bases [8] where each filter must have the distinguishing index value less than 0.8 with other filters in order to achieve the combined correlation less than 0.4 theoretically. We choose 6 set of filters because there is one more wavelet filter set needed for the watermark reconstruction in [6] as shown in subband 9 of Figure 1. After this procedure, we test all combination of the selected filters (there are $6^6 = 46656$ different wavelet trees) and the results are shown in Figure 4 (a) and (b). From the statistics, we can tell that the exact filter combination truly has high correlation for the the unattacked situation in (a) and the uniqueness property is more significantly for the JPEG 2000 attack in (b). Even there is still some confusion among close combination of the filter banks, the probability of misjudgment has been significantly reduced. Similar results from other images have shown convincing performance and this approach is believed to be pretty general in applications.

4. CONCLUSION

In this paper, we have shown that the keys of watermarking in algorithm [6] can not uniquely identify the copyright information if there is no wise selection mechanism during the stage of the wavelet filter implementation. Therefore, we propose a distinguishing index determination procedure of the wavelet filter bank for the digital image watermarking to reduce the false alarm probability of ownership verification. The performance of this study has shown dramatic improvement for watermarking applications and even small percentage of misjudgment is still inevitable.

5. ACKNOWLEDGMENT

The author would like to thank Prof. Benjamin Belzer from Washington State University, Pullman who contributes valuable suggestion and biorthogonal filter bank coefficients for the simulation comparison and Li-Hsing Tseng at National Chiao Tung University who helps to write the programs and Matlab scripts for software experiments.

6. REFERENCES

[1] I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. on Image Processing,* vol.6, No.12, pp.1673-1678, Dec. 1997.

[2] M. Swanson, M. Kobayashi and A. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies", *Proceeding of the IEEE*, vol. 86, no.6, June 1998.

[3] N. Memon and P. W. Wong, "Protecting Digital Media Content", *Comm. of the ACM*, pp. 35-43, vol. 41, no. 7, July, 1998.

[4] M.J. Tsai, K.Y. Yu, and Y.Z. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking" *IEEE Transactions on Consumer Electronics,* pp. 241-245, vol. 46, no. 1, Feb. 2000.

[5] M.J. Tsai, K.Y. Yu, and Y.Z. Chen, "Wavelet packet and adaptive spatial transformation of watermark for digital image authentication", *IEEE ICIP2000*, pp. 450 -453,volume: 1, Sep, Vancouver, Canada.

[6] Yiwei Wang, John F. Doherty and Robert E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", *IEEE Transactions on Image Processing*, pp. 77-87, vol. 11, no. 2, Feb. 2002.

[7] http://www.jpeg.org/JPEG2000.html.

[8] J. D. Villasenor, B. Belzer, and J. Liao, "Wavelet Filter Evaluation for Image Compression", *IEEE Trans. on Image Processing,* pp. 1053-1060, vol. 4, no.8, Aug. 1995.