

A Multi-band Wavelet Watermarking Scheme

Xiangui Kang¹, Wenjun Zeng², and Jiwu Huang¹

(Corresponding author: Xiangui Kang)

Department of Electronics and Communication Engineering, Sun Yat-Sen (Zhongshan) University¹
Guangzhou 510275.China. (Email: {isskxg, isshjw}@mail.sysu.edu.cn)

Department of CS, University of Missouri-Columbia, MO 65211, USA (Email: zengw@missouri.edu)²

(Received Jan. 9, 2005; revised and accepted Apr. 29, 2006)

Abstract

This paper presents a new multi-band wavelet watermarking scheme. Compared with conventional watermarking schemes implemented in two-band wavelet domain, by incorporating the principal component analysis (PCA) technique the proposed blind watermarking in the multi-band wavelet domain can achieve higher perceptual transparency and stronger robustness. Specifically, the developed watermarking scheme can successfully resist common signal processing such as JPEG compression with quality factor as low as 15, and some geometric distortions such as cropping (cropped by 50%). In addition, the proposed multi-band wavelet based watermarking scheme can be parameterized, thus resulting in more security. That is, an attacker may not be able to detect the embedded watermark if the attacker does not know the parameter. Different from many other watermarking schemes, in which the watermark detection threshold is chosen empirically, the false positive rate of the proposed watermarking scheme can be calculated analytically so that watermark detection threshold can be chosen based solely on the targeted false positive.

Keywords: Multi-band wavelet, principal component analysis, watermarking

1 Introduction

Multimedia security and digital rights management (DRM) is becoming an increasingly important issue in multimedia applications and services [11]. One of the enabling technologies for DRM is digital watermarking. One significant advantage of the digital watermarking approach is that the protection is robustly integrated with the raw media data, independent of the specific representation format, which provides great flexibility that allows the protected content to be adapted or modified in the course of delivery without having to access the watermarking key for un-protection, adaptation, and re-protection. This network-friendly feature generally results in reduced processing overhead, lower cost, good er-

ror resiliency, and better end-to-end security.

Robustness and perceptual transparency are two fundamental issues in digital watermarking [7, 10]. Many existing watermarking techniques embed watermarks in the discrete dyadic wavelet transform (DWT) domain to take advantage of its unique characteristics. In terms of embedding strategy, most works propose that watermarks should be embedded in one or several selected detail frequency band coefficients because of the small impact on perceptual distortion [9]. Principle component analysis (PCA) has also been applied to non-overlapping spatial image blocks to achieve more robust watermark embedding [4], which nevertheless suffers from the common limitations of a rigid block based approach. This paper proposes a new approach that incorporates parameterized multi-band (M-band) wavelet transformation and PCA. By taking advantage of the strength of both multi-band wavelet transform (MWT) and PCA, the watermark energy is distributed to wavelet coefficients of every detail subband efficiently to achieve better robustness and perceptual transparency, and good localization.

2 Multi-band Wavelet Transformation

Different from conventional two-band wavelet ($M = 2$), there are a scaling function $\phi(x) \in L^2(R)$ and $M - 1$ wavelet functions $\{\psi_l(x) | 1 \leq l \leq M - 1, M > 2\}$ in the newly developed multi-band wavelets [1, 8]. These functions satisfy the following equation respectively:

$$\begin{aligned}\phi(x) &= \sum_{k \in Z} h_0(k) \phi(Mx - k) \\ \psi_l(x) &= \sum_{k \in Z} h_l(k) \phi(Mx - k), 1 \leq l \leq M - 1,\end{aligned}$$

where Z is the integer set and sequence $\{h_l(k), 0 \leq l \leq M - 1\}$ has finite length. The one dimensional Mallat decomposition and reconstruction formulae of orthogonal multi-band wavelet are expressed in Equations (1) and

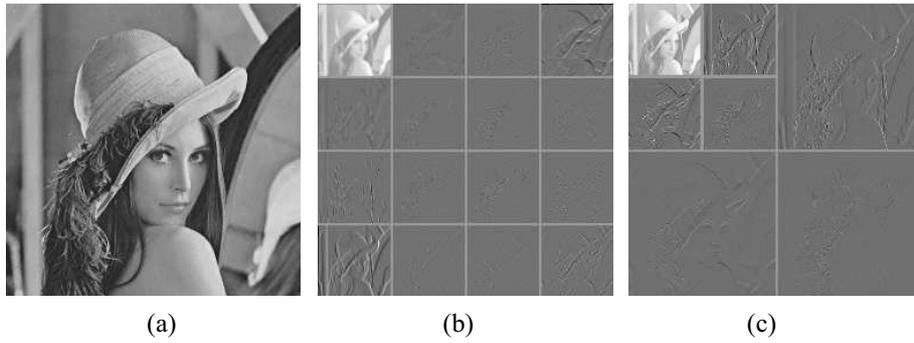


Figure 1: (a) Original image; (b) one-level decomposition with 4-band wavelet; (c) two-level decomposition with 2-band DWT

(2), respectively [8]:

$$\begin{aligned}
 C_{j+1}(k) &= M^{1/2} \sum_{k' \in Z} c_j(k') h_0(k' - Mk) \\
 d_{j+1,l}(k) &= M^{1/2} \sum_{k' \in Z} d_j(k') h_l(k' - Mk), \\
 & \quad 1 \leq l \leq M - 1 \\
 C_j(k) &= M^{-1/2} \sum_{k' \in Z} c_{j+1}(k') h_0(k' - Mk) + \\
 & \quad M^{-1/2} \sum_{l=1}^{M-1} \sum_{k' \in Z} d_{j+1}(k') h_l(k' - Mk), \\
 & \quad 1 \leq l \leq M - 1,
 \end{aligned} \tag{1}$$

where $\{c_{j+1}(k), j = 0, 1, 2, \dots\}$ is the approximation coefficients of the $j + 1$ level M -band wavelet decomposition of one dimensional signal $\{c_0(k)\}$, and $\{d_{j+1}(k), j = 0, 1, 2, \dots\}$ is the detail coefficients of the $j + 1$ level M -band wavelet decomposition. For image signal, the above one-dimensional multi-band discrete wavelet transformation is easy to extend to two-dimensional multi-band discrete wavelet transformation (MWT) by applying one-dimensional multi-band wavelet transformation along the image rows then columns separately [8].

Figure 1 shows an example of two-dimensional multi-band discrete wavelet transformation (MWT) [1] and two-band discrete wavelet transform (DWT). In multi-band discrete wavelet transformation, we only use the one-level image decomposition, every wavelet coefficient is a band-pass filtering result of a local region of the original image at the same scale. Every wavelet subband of MWT has the same number of coefficients (Figure 1b). This is different from the two-level DWT (Figure 1c), where the coefficients might belong to different scales.

The multi-band wavelet $\psi_l(x)$ used in this paper is symmetric, parameterized by a parameter $\lambda \in R$. Modulo value $t = \text{mod}(\lambda, 2\pi)$ assumes a real value between 0 and 2π [1]. Here mod denotes the signed remainder after division. Different values of t lead to different multi-band wavelets.

3 Watermark Embedding

An encrypted *logo* (Figure 2) (watermark) is embedded in the principle component of the multi-band wavelet domain of the host image. The motivation of encryption is to enhance the security of the watermark, and make the watermark pseudo-random so that a reasonable watermark detection threshold is deducible. The motivations of incorporating multi-band wavelet and PCA are as follows: parameterized M -band wavelet provides a secure embedding domain and excellent space-frequency localization; while PCA further concentrates the energy of the wavelet coefficient vectors and distributes the watermark energy over all detail subbands, resulting in enhanced watermark invisibility and/or robustness. It is well known that even after the orthogonal wavelet decomposition, typically there still exists some correlation between the wavelet coefficients, especially those corresponding to the same spatially local region at the same scale. This correlation between the coefficients corresponding to different frequencies but the same spatial location could be removed based on the PCA technique and the energy of the image could be further concentrated, leading to an embedding domain that permits the embedding of larger watermark energy, which in turn lead to better perceptual transparency, or translates into improved robustness. This approach makes the watermark less visible or more robust to lossy compression than embedding watermarks in only one or several selected wavelet subbands.



Figure 2: The embedding logo

The watermark embedding process (Figure 3) is divided into the following steps.

- 1) Encrypt the embedding *logo* (Figure 2) using a 2D

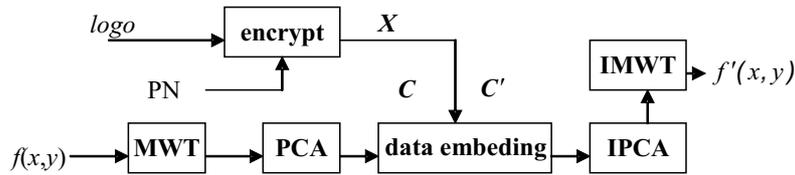


Figure 3: The watermark embedding process

pseudo-random sequence with the same size of the *logo*. The 2D pseudo-random binary (0 and 1) sequence is generated by a key. The binary image *logo* (Figure 2) is XOR operated with the 2D pseudo-random sequence, then is 2DPSK modulated and is raster scanned to obtain a 1-D watermark sequence $X = \{x_i\} (1 < i < N)$, which is composed of -1 and 1. The occurrence probability of -1 or 1 in X is close to 0.5 because the above encrypting binary sequence is a pseudo-random sequence (PN).

- 2) The multi-band discrete wavelet transformation (MWT) [8] is applied to the cover image $f(x, y)$ first. We obtain one approximate subband and fifteen detail subbands. (Figure 1b).
- 3) Then the coefficients corresponding to the same spatial location in all detail subbands form a one-dimensional data array $g_i = (g_{i,1}, g_{i,2}, g_{i,3}, \dots, g_{i,16})$, $1 < i < N$, e.g., a vector of a total of fifteen coefficients, one per subband, for the case of Figure 1b. The principle component analysis (PCA) [4] is then applied to the obtained one-dimensional arrays respectively. First, calculate the covariance matrix $V = E(g_i \times g_i^T)$, where vector g_i is the i -th one-dimensional data array, T denotes the matrix transpose operation, E denotes expectation operation. Finding the eigenvectors Φ (basis function) corresponding to eigenvalues ζ of the covariance matrix V . $V\Phi = \zeta\Phi$, where eigenvectors ζ are sorted in descending order, $\Phi = (\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_{16})$. Then calculate the PCA components: $p_i = \Phi^T g_i = (p_{i,1}, p_{i,2}, p_{i,3}, \dots, p_{i,16})$, $1 < i < N$ for each g_i respectively.
- 4) All the obtained first principle components $p_{i,1} (1 < i < N)$ form a 1-D array $C \{C(i) | C(i) = p_{i,l}, 1 < i < N\}$ in the same raster scanning fashion as in step 1. Finally, watermark X is embedded in the principle components C using quantization-based method (Equation (3) to obtain C' [2, 6, 10], where $C(i)$ and $C'(i)$ denote the i th element in C and C' , respectively. The quantizer $q(\cdot)$ is a uniform, scalar quantization function of step size S , and $q(x) = kS + 0.5S$, $k = \lfloor \frac{x}{S} \rfloor (k \in Z)$, where $\lfloor \cdot \rfloor$ denotes the floor operation. The embedding strength S can be chosen so as to achieve a good compromise between the contending requirements of imperceptibility and robustness. Note that the difference between $C(i)$ and $C'(i)$ is be-

tween $-0.5S$ and $+0.5S$. If $x_i = -1$, $C'(i) \bmod S = 0.25S$. If $x_i = +1$, $C'(i) \bmod S = 0.75S$. Here mod denotes the signed remainder after division.

- 5) Apply inverse PCA (IPCA in Figure 3) [4] on the modified PCA components $p'_i = (C'(i), p_{i,2}, p_{i,3}, \dots, p_{i,16})$ to obtain the modified one-dimensional wavelet coefficients array $g'_i = \Phi p'_i$, respectively.
- 6) Performing inverse MWT (IMWT in Figure 3) [8] on the modified image coefficients, we obtain a watermarked image $f'(x, y)$.

$$\begin{cases} C'(i) = q(C(i) - \frac{1}{4}S) + \frac{1}{4}S, & \text{if } x_i = 1 \\ C'(i) = q(C(i) + \frac{1}{4}S) - \frac{1}{4}S, & \text{if } x_i = -1 \end{cases} \quad (3)$$

$$x_i^* = \begin{cases} +1, & r = C^*(i) \bmod S > \frac{S}{2} \\ -1, & \text{otherwise} \end{cases} \quad (4)$$

4 Watermark Detection

The watermark extraction is the inverse process of watermark embedding. The test image is MWT decomposed, then PCA is applied, and the first principle components are obtained to form a 1-D array $C^* \{C^*(i), (1 < i < N)\}$. $C^*(i)$ is the extracted principle component. According to Equation (4), we could extract the hidden binary data $X^* \{x^*(i), (1 < i < N)\}$. Equation (4) indicates that if $r (r = C^*(i) \bmod S)$ is in the interval $(0, 0.5S)$, then the decision is made in favor of “ $x^*_i = -1$ ”. Otherwise, “ $x^*_i = 1$ ”. Then the following correlation coefficient is used to decide if the watermark exists in the test image.

$$\rho_{x,x^*} = \frac{X \cdot X^*}{\|X\|},$$

where $\|X\|$ is the size of the watermark X (that is, N , in this paper), and $X \cdot X^*$ is the inner product of X and the extracted sequence X^* .

If the correlation coefficient between the embedded sequence X and the extracted sequence X^* from a test image is larger than a threshold, i.e., $\rho_{x,x^*} \geq \text{thresh}$, we determine that watermark exists. Here we can calculate the corresponding probability of false positive as $H_{fp} = (0.5)^N \cdot \sum_{k=N-e}^N \binom{N}{k}$, where $e = \text{round}(\frac{N}{2}(1 - \text{thresh}))$, and $\text{round}(\cdot)$ means taking the nearest integer. In our work, we choose $N = 63 \times 63 = 3969$. When the threshold is set to 0.10, we have $H_{fp} = 1.27 \times 10^{-10}$, which may



Figure 4: (a) The marked image with DWT (PSNR=40.2dB); (b) The marked image with MWT (PSNR=40.1dB)

Table 1: Comparison of watermarking in MWT and DWT domain

StirMark functions	MWT	DWT
JPEG 20~100	1	1
JPEG 15	1	0
Gauss filtering	1	1
3x3median_filter	1	1

be sufficiently low for many applications. It should be noted that this is different from many other watermarking schemes, where the watermark detection threshold is chosen empirically [3]. In the above, we assume the embedded sequence X is a PN sequence.

5 Simulation Results

We have tested the proposed MWT algorithm on many images with StirMark 3.1 functions. The results on $256 \times 256 \times 8$ image Lena, Baboon, Peppers are reported here. In our work, we choose $S = 36, N = 63 \times 63, thresh = 0.10$. The watermark is robust to JPEG compression with quality factor as low as 15% (JPEG_15) and is also robust to common image processing such as median filtering, Gaussian filtering etc. The watermark could be detected when the marked image has been cropped by 50%. We compare the proposed MWT watermarking with DWT watermarking on Lena image. For fair comparison, in DWT watermarking with Daubechies 9/7 filter, HL_2 subband is chosen to embed same watermark X with the same embedding Equation (3) and same embedding strength $S = 36$, as is done with the above watermarking in MWT domain. The obtained marked images are shown in Figure 5. The obtained PSNR value with DWT and MWT is similar, 40.2dB and 40.1dB respectively. But the marked image in DWT domain has obvious horizontal artifacts, while the marked image in MWT domain has excellent perceptual quality without any artifacts.

The test results are shown in Table 1. In Table 1, “1” represents the presence of watermark, that is, the correlation coefficient ρ_{x,x^*} between the embedded sequence X

and the extracted sequence X^* obtained from a test image is larger than thresh, while “0” means the absence of watermark. It is noted that the scheme in MWT domain performs better in resisting JPEG compression. The watermark in MWT is robust to JPEG_15, while the watermark in DWT domain fails this test. Taking account of the improvement in the watermark invisibility, we can embed larger intensity watermark in MWT domain than in DWT domain to achieve more robustness, so the proposed MWT watermarking is more robust than the watermarking in DWT domain.

The parameterized M-band wavelet, which is parameterized by a parameter $\lambda \in R$, leads a secure watermark embedding domain. The parameter λ used in embedding needs to be known in watermark extraction, otherwise the watermark cannot be detected. For example, if $\lambda = 0.5$ is chosen in watermark embedding and $\lambda = 1.6$ is used in watermark extraction, the correlation coefficient ρ_{x,x^*} is less than threshold *thresh* even if the embedding strength S and original watermark X are known in extraction. If without usage of parameterized wavelet transform, only is the very same wavelet filter bank used. If the watermarking scheme is known to the public, the scheme is easy to be attacked [5]. So the parameterized M-band wavelet makes attacks more difficult.

6 Conclusions

The proposed watermarking M-band wavelet scheme has the following advantages.

- 1) We embed watermark in the principle components of the multi-band discrete wavelet coefficients. Specifically, watermark signal is embedded into the principle components of the multi-band wavelet coefficients corresponding to the same spatial location at the same scale. With such a well-chosen embedding domain, the watermark is robustly and efficiently distributed to every detail frequency subband. Our experimental results have shown that the watermark thus embedded has better invisibility and is more robust against JPEG compression than watermarks embedded in the DWT domain.
- 2) Parameterized multi-band wavelet leads to a more secure watermark embedding domain, which makes the attack more difficult.
- 3) Different from many other watermarking schemes, in which watermark detection threshold is chosen empirically, the detection threshold of the proposed watermarking scheme can be calculated according to the targeted false positive.

Acknowledgements

This work is supported by NSFC (60403045, 60325208, 60572140), NSF of Guangdong (04205407, 04009742,

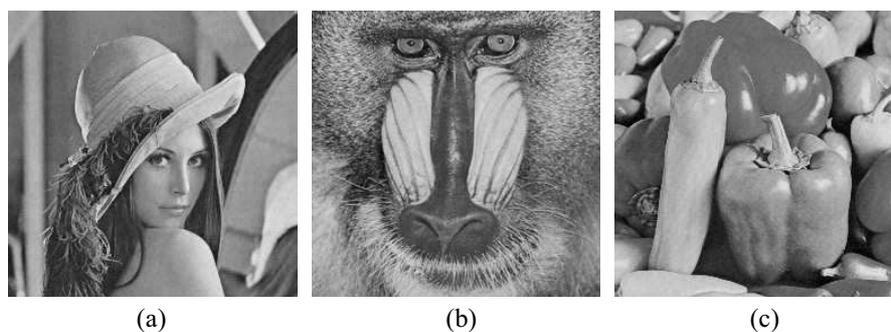


Figure 5: The marked image with 4-band wavelet. (a) Lena (PSNR=40.1dB); (b) Baboon (PSNR=40.1dB); (c) Peppers. (PSNR=40.0dB)

04009739), NSF of Guangzhou (2006Z3-D3041). The first author thanks Dr. Ning Bi for helpful discussions in multi-band wavelets with him.

References

- [1] N. Bi, D. Huang, Q. Dai, and F. Li, "A class of orthogonal and symmetric 4-band wavelets with one-parameter," *Mathematica Numerica Sinica*, vol. 27, no. 2, pp. 1-10, May 2005.
- [2] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423- 1443, May 2001.
- [3] I. Cox, J. Kilian, T. Leighton, and T. Shamon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.
- [4] T. D. Hien, Y. W. Chen, and Z. Nakao, "Robust digital watermarking based on principle component analysis," *International Journal of Computational Intelligence and Applications*, vol. 4, no. 2, pp. 183-192, 2004.
- [5] J. Huang, J. Hu, D. Huang, and Y. Q. Shi, "Improve security of fragile watermarking via parameterized wavelet," in *2004 international Conference on Image Processing*, pp. 721-724, Singapore, Oct. 2004.
- [6] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.13, no. 8, pp. 776-786, Aug. 2003.
- [7] F. A. P. Petitcolas, "Watermarking schemes evaluation," *IEEE Signal Processing*, vol. 17, no. 5, pp. 58-64, Sep. 2000.
- [8] Q. Sun, N. Bi, and D. Huang, *An Introduction to Multi-band Wavelets*, Zhejiang University Press, 2001.
- [9] M. J. Tsai, K. Y. Yu, and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 241-245, 2000.
- [10] M. Wu, and B. Liu, "Data hiding in images and video: Part I: fundamental issues and solutions," *IEEE Transactions on Image Processing*, vol. 12, no. 6, pp. 685-695, Jun. 2003.
- [11] W. Zeng, J. Lan, and X. Zhuang, "Network friendly media security: rationales, solutions, and open issues," in *2004 International Conference on Image Processing (ICIP)*, pp. 565- 568, Singapore, Oct. 2004.



Xiangui Kang received his B.S degree, M.S degree Ph. D. from Peking University, Nanjing University, Sun Yat-Sen University, China respectively. He is currently an associate professor with the Department of Electronics and Communication Engineering, Sun Yat-Sen University. He serves

as a member of Multimedia Communications Technical Committee of IEEE Communications Society. His research interests include multimedia security and watermarking.



Wenjun Zeng is an Associate Professor in the Computer Science Department of University of Missouri, Columbia, MO. He received his B.E., M.S., and Ph.D. degrees from Tsinghua University, China, the University of Notre Dame, and Princeton University, respectively, all in electrical engineering.

His current research interests include multimedia communications and networking, content and network security, wireless multimedia, and distributed source and channel coding. Dr. Zeng has served as an Organizing Committee Member and Technical Program Committee Chair/Member for a number of IEEE international conferences. He is an Associate Editor of the

IEEE Transactions on Multimedia, and is on the Editorial Board of IEEE Multimedia Magazine. He is a member of the IEEE Signal Processing Society's Multimedia Signal Processing Technical Committee and a member of the IEEE Communication Society's Multimedia Communications Technical Committee.



Jiwu Huang received his B.S. degree from Xidian University, China, in 1982, M.S. degree from Tsinghua University, China, in 1987, and Ph.D. degree from Institute of Automation, Chinese Academy of Science in 1998. He is currently a professor with the School of Information Science and

Technology, Sun Yat-Sen University, P.R. China. He serves as a member of IEEE CASS Technical Committee of Multimedia Systems and Applications. His current research interests include multimedia security and data hiding.