# WATERMARK SECURITY VIA WAVELET FILTER PARAMETRIZATION

*Peter Meerwald, Andreas Uhl*

Department of Scientific Computing,
Paris-Lodron-University of Salzburg,
Jakob-Haringer-Str. 2, A-5020 Salzburg, Austria

**ABSTRACT**

In this paper, we propose to use secret, key-dependent parametric wavelet filters to improve the security of digital watermarking schemes operating in the wavelet transform domain. We show that the parametrization of wavelet filters can be easily integrated into existing wavelet-based watermarking algorithms, resulting in improved security without additional computational complexity. Both, robustness and imperceptibility are adequate for many applications.

## 1. INTRODUCTION

Recently, numerous digital watermarking algorithms have been developed to help protect the copyright of digital images and to verify multimedia data integrity. Most watermarking algorithms transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way. Previous approaches often employed the discrete cosine transform (DCT) to mark perceptually significant coefficients in the low-frequency spectrum [1]. Also, the widely used JPEG compression standard is based on the DCT. However, new requirements such as progressive and low bit-rate transmission, quality scalability and region-of-interest (ROI) coding demand more efficient and versatile image coding. The upcoming compression standard JPEG2000 will be based on the discrete wavelet transform (DWT) to meet the new requirements [2]. Therefore, it is imperative to study watermarking schemes in the wavelet transform domain.

In this paper, we will focus on the possibility to construct secret wavelet filters to improve the security of watermarking applications. Fridrich [3] introduced the concept of key-dependent basis functions in order to protect a watermark from hostile attacks. Hostile attacks exploit the knowledge of the watermarking algorithm to destroy or remove the watermark . By embedding the watermark information in a secret transform domain, Fridrich's algorithm can better withstand attacks such as those described by Kalker [4] employing a public watermark detector device. However, Fridrich's approach suffers from the computational complexity and the storage requirements for generating numerous orthogonal patterns of the size of the host image. Nevertheless, watermarking schemes such as those presented by Wang [5] or Kundur [6] call for a mechanism to protect the location where watermark information has been embedded. Other security techniques, such as pseudo-random skipping of coefficients, seriously limit the robustness and capacity of the scheme. Therefore, we propose to construct secret wavelet filters via parametrization to decompose the host image. Due to the secret transform domain, the location of the watermark information is protected. Several parametrizations for orthogonal and bi-orthogonal wavelet filters are readily available [7], allowing to choose parameters from a vast key-space. We will show the applicability of this approach and demonstrate its robustness.

The next section gives an overview of current wavelet-based watermarking algorithms and their weaknesses. In section 3, we describe the concept of wavelet parametrization. Section 4 presents robustness results using parameterized filters. Concluding remarks are given in section 5.

## 2. WAVELET DOMAIN WATERMARKING

Based on the work of Cox [1] in the DCT domain, Kim [8] utilizes DWT coefficients of all subbands including the approximation image to equally embed a random Gaussian distributed watermark sequence in the whole image. Perceptually significant coefficients are selected by level-adaptive thresholding to achieve high robustness. However, the location of the watermark information is not protected and open for malicious attacks.

Following the design of his multi-threshold wavelet coding scheme, Wang [5] proposes a watermarking algorithm that refines Kim's thresholding scheme and selects significant coefficients on a per subband basis. Here, random skipping of significant coefficients is discussed as a mean to achieve non-invertibility [9] and improve watermark security although this will also limit the robustness and capacity of the scheme. Additionally, it is proposed to keep the wavelet transform structure and filters secret in order to protect the location of embedded watermark information.

Watermarking schemes of the above type have demonstrated excellent robustness to many forms of image processing distortions. On the other hand, their security is questionable without protecting the coefficients carrying the watermark information from a malicious attacker.

Kundur [6] is embedding a binary watermark by modifying the amplitude relationship of three transform-domain coefficients from distinct detail subbands of the same resolution level of the host image. The security of this schemes lies entirely in the pseudo-random selection of coefficient locations. To strengthen the blind watermark extraction process, Kundur resorts to repetition and a reference mark.

There is a tradeoff between robustness and capacity versus security. In the next section, we introduce filter parametrization to add a security framework to the watermarking schemes presented above without seriously harming robustness, capacity or imperceptibility.

## 3. FILTER PARAMETRIZATION

In order to construct compactly supported orthonormal wavelets, solutions for the dilation equation

$$\phi(t) = \sum_{k \in \mathbb{Z}} c_k \phi(2t - k),$$

with $c_k \in \mathbb{R}$, have to be derived, satisfying two conditions on the coefficients $c_k$ [10]. Schneid [11] describes a parametrization for suitable coefficients $c_k$ based on the work of Zou [7] to facilitate construction of such wavelets. Given $N$ parameter values $-\pi \leq \alpha_i < \pi$, $0 \leq i < N$, the recursion

$$\begin{aligned} c_0^0 &= \tfrac{1}{\sqrt{2}} \text{ and } c_1^0 = \tfrac{1}{\sqrt{2}} \\ c_k^n &= \tfrac{1}{2}((c_{k-2}^{n-1} + c_k^{n-1}) \cdot (1 + \cos \alpha_{n-1}) + \\ &\quad (c_{2(n+1)-k-1}^{n-1} - c_{2(n+1)-k-3}^{n-1})(-1)^k \sin \alpha_{n-1}) \end{aligned}$$

can be used to determine the filter coefficients $c_k^N$, $0 \leq k < 2N + 2$. We set $c_k = 0$ for $k < 0$ and $k \geq 2N + 2$.

We propose to decompose the host image using wavelet filters constructed with the above parametrization. The parameter values used for construction and the resulting wavelet filter coefficients are kept secret. Hence, the watermark information can be embedded in a secret multi-resolution transform domain, making it difficult to mount a hostile attack that seeks to destroy or remove watermark information at specific locations. Our concept is illustrated in figure 1.

A problem with randomly-constructed parametric wavelet filters is that the high-pass/low-pass decomposition property is partially lost. Some degree of wavelet smoothness is desirable for most applications. Therefore, we calculate the second-order local variation (difference) of a wavelet sequence

$$V_\phi^{(2)} = \sum_n \left| g_n^{(J)} - g_{n-1}^{(J)} + g_{n-2}^{(J)} \right|$$

as a simple measure to ensure wavelet smoothness [12]. We can restrict our key-space to parameters such that only wavelets of certain smoothness are produced, e.g. $V_{\phi_\alpha}^{(2)} < V_H^{(2)}$, where $V_H^{(2)}$ is the smoothness measure of the Haar wavelet. Clearly, this is a tradeoff between security (key-space) and decomposition properties of the transform.

Hsu [13] states that the choice of the wavelet filter is a critical issue for the quality of the watermarked image and the robustness to compression attacks. However, the filter criteria for watermarking purposes are different compared to image compression applications. Filters that pack most energy of the original image in the lowest resolution approximation image give best compression performance because information in the detail subbands can be easily discarded without severe perceptible image distortion. However, watermarking applications using such filters to embed watermark information in the detail subbands will seriously suffer from compression attacks.

Employing secret filter parametrization in wavelet-based watermarking algorithms has the following advantages. First, security is improved because hostile attacks have to operate in the transform domain used for watermark embedding. Our experiments indicate that the size of the key-space is at least 63000 parameter combinations. Second, filter coefficients for watermark embedding can be constructed in an image-adaptive way to maximize robustness against specific compression attacks. Third, there is no need to modify proven watermarking schemes (only absolute thresholds have to be adjusted). A wavelet transform based on secret filters can act as a security framework independent of the embedding algorithm.

## 4. RESULTS

We conduct all our experiments with the $512 \times 512$ grayscale image 'Lena'. One blind and two non-blind wavelet-based watermarking algorithms (described in section 2) are used to embed and extract watermark information without perceptible image degradation. The performance of the watermarking schemes is evaluated by calculating the normalized correlation measure.

First, we demonstrate the robustness against compression attacks that can be achieved when using randomly chosen wavelet filter parameters. We construct 169 different wavelet filters, uniformly separated in the parameter space ($N = 2; \alpha_0, \alpha_1 \in \{-3.1, -2.6, \ldots, 2.4, 2.9\}; \Delta = 0.5$). Next, we embed a watermark in the host images using one of the available parametric filters for wavelet decomposition; for reference we also test the Daubechies-6 and 9/7-bi-orthogonal filter. The embedding algorithms are briefly discussed in section 2. The watermarked images are sub-

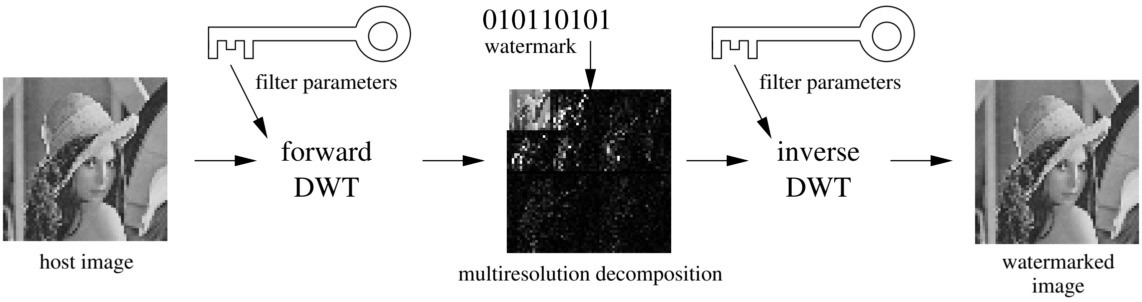


**Fig. 1**. The watermark embedding process using filter parametrization. The forward and inverse wavelet transform is based on secret wavelet filters.

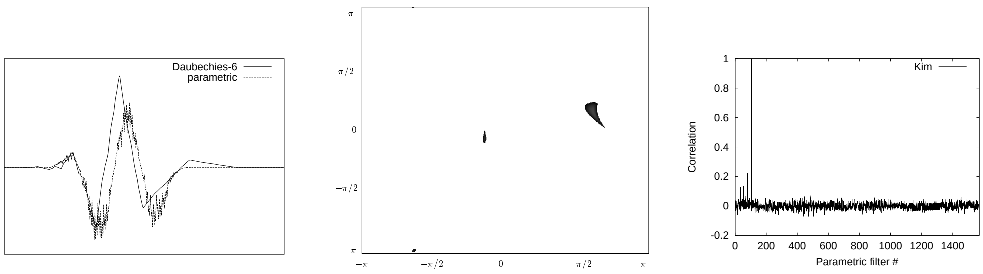


**Fig. 2**. Daubechies-6 and a parametric wavelet ($\alpha_0 = -0.4815$, $a_1 = 2.6585$) (left). Regions of smoothness (black) with $V^{(2)}_{\phi_\alpha} < V^{(2)}_H$ for $N = 2$ (middle). Correlation measure for Kim's scheme, key-space restricted to smooth wavelets – the embedded mark can only be retrieved with the correct filter parameter (right).

jected to JPEG and JPEG2000[1] compression with different quality or bit-rate settings, respectively, resulting in compression ratios from approximately 1:4 up to 1:80. Figure 3 shows that all wavelet filters provide adequate robustness, however, the 9/7-bi-orthogonal filter gives best results. We conducted the experiment with all 169 parametric filters but only show the average correlation. The performance of our parametric filters can be improved by restricting the parameter space such that only reasonable smooth wavelets are used. In that case, one can expect results close to the Daubechies-6 filter.

The next experiment examines the security of our filter parametrization approach. For each algorithm, we generate a watermark and embed it using a secret parametric wavelet filter (e.g. $\alpha_0 = 1.7585, \alpha_1 = 1.0585$). Then we try to extract that watermark but randomly 'guess' the transform parameters within the key-space. Figure 4 suggests that the watermark can only be retrieved correctly with matching wavelet filters. We tested 63504 uniformly distributed parameters ($N = 2$; $\alpha_0, \alpha_1 \in \{-3.14, -3.11, \ldots, 3.11, 3.13\}$; $\Delta = 0.025$).

We repeat the experiment but restrict the key-space to parameters that produce smooth wavelets according to our measure, $V^2_{\phi_\alpha} < V^2_H$. The embedded watermark can only be retrieved with matching parametric filters (see figure 2).

## 5. CONCLUSION

We have introduced the concept of wavelet filter parametrization to improve the security of watermarking applications. Our approach is easy to integrate in existing watermarking schemes. The experiments indicate that the level of security provided is adequate for many applications. Because our proposed security framework does not require any computational overhead, it is especially suited for video watermarking or other real-time applications. Further work will investigate the parametrization of bi-orthogonal wavelet filters.

## 6. REFERENCES

[1] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon, "Secure spread spectrum watermarking for multimedia," in *Proc. ICIP*, Santa Barbara, CA, USA, Oct. 1997, vol. 6, pp. 1673 – 1687.

[2] Maryline Charrier, Diego Santa Cruz, and Mathias Larsson, "JPEG2000, the next millennium compres-

[1]using JasPer (based on the JPEG2000 working draft), see `http://spmg.ece.ubc.ca/people/mdadams/jasper/index.html`

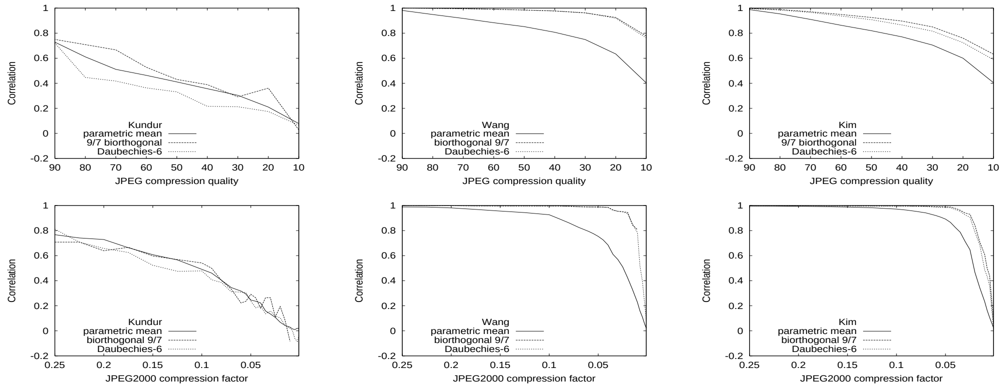


**Fig. 3**. Robustness of the watermark. The host images were subjected to JPEG (first row) and JPEG2000 (second row) compression. Testing the correlation of the extracted watermark with algorithms by Kundur, Wang and Kim (first to third column) with Daubechies-6, 9/7-bi-orthogonal and parametric filters.

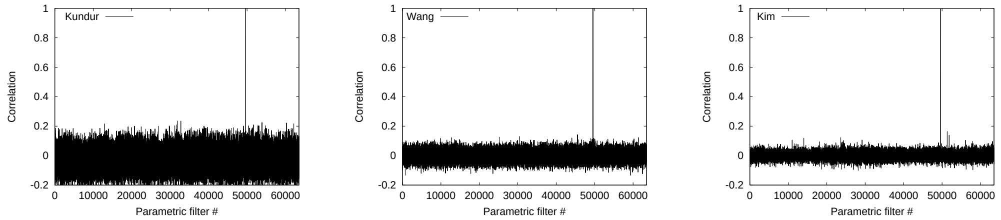


**Fig. 4**. The watermark can only be detected with matching filter parameters from a key-space of 63504 parametric wavelet filters. Testing with algorithms by Kundur, Wang and Kim (left to right).

sion standard for still images," in *Proc. ICMCS*, Florence, Italy, June 1999, vol. 1, pp. 131 – 132.

[3] Jiri Fridrich, Arnold C. Baldoza, and Richard J. Simard, "Robust digital watermarking based on key-dependent basis functions," in *LNCS: IH*, Portland, OR, USA, April 1998, vol. 1525, pp. 143 – 157.

[4] Ton Kalker, Jean-Paul Linnartz, Geert Depovere, and Maurice Maes, "On the reliability of detecting electronic watermarks in digital images," in *Proc. EUSIPCO*, Rhodes, Greece, Sept. 1998, pp. 13 – 16.

[5] Houng-Jyh Wang and C.-C. Jay Kuo, "Watermark design for embedded wavelet image codec," in *Proc. SPIE*, San Diego, CA, USA, July 1998, vol. 3460, pp. 288 – 398.

[6] Deepa Kundur, "Improved digital watermarking through diversity and attack characterization," in *Proc. ACM Workshop on Multimedia Security*, Orlando, FL, USA, Oct. 1999, pp. 53 – 58.

[7] H. Zou and Ahmed H. Tewfik, "Parametrization of compactly supported orthonormal wavelets," *IEEE Trans. on Signal Proc.*, vol. 41, no. 3, pp. 1423 – 1431, March 1993.

[8] Jong Ryul Kim and Young Shik Moon, "A robust wavelet-based digital watermark using level-adaptive thresholding," in *Proc. ICIP*, Kobe, Japan, Oct. 1999, p. 202.

[9] Scott Craver, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung, "On the invertibility of invisible watermarking techniques," in *Proc. ICIP*, Santa Barbara, California, USA, Oct. 1997, p. 540.

[10] Ingrid Daubechies, *Ten lectures on wavelets*, SIAM Press, Philadelphia, PA, USA, 1992.

[11] J. Schneid and S. Pittner, "On the parametrization of the coefficients of dilation equations for compactly supported wavelets," *Computing*, vol. 51, pp. 165 – 173, May 1993.

[12] S. Maslakovic, I. R. Linscott, M. Oslick, and J. D. Twicken, "Smooth orthonormal wavelet libraries: design and application," in *Proc. ICASSP*, Seattle, WA, USA, May 1998, pp. 1793 – 1796.

[13] Chiou-Ting Hsu and Ja-Ling Wu, "Multiresolution watermarking for digital images," *IEEE Trans. on Circ. and Sys.*, vol. 45, no. 8, pp. 1097 – 1101, August 1998.