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
{pmeerw,uhl}@cosy.sbg.ac.at

Abstract

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

1.1 Secret transform domain watermarking

We focus on the construction of secret wavelet filters to improve the security of watermarking applications. Fridrich [1] 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 [2] employing a public watermark detector device. However, Fridrich's approach suffers from computational and space complexity due to generating numerous orthogonal patterns of the size of the host image.

1.2 Security measures

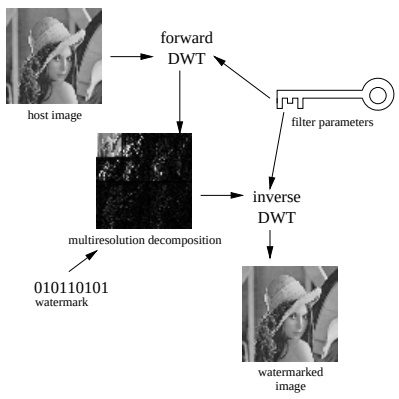
Nevertheless, watermarking schemes such as those presented by Wang [3] or Kundur [4] call for a mechanism to protect the location where watermark information has been embedded. Other security techniques, such as pseudo-random skipping of coefficients, seriously limit the robustness and capacity of the scheme. The security of these schemes lies entirely in the pseudo-random selection of coefficient locations. The authors suggested to keep the wavelet transform structure secret in order to protect the location of embedded watermark information. Clearly, there is a tradeoff between robustness and capacity versus security.

1.3 Key-dependent wavelet transform domain

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 [5], allowing to choose parameters from a vast key-space. We introduce wavelet filter parametrization to add a security framework to the watermarking schemes presented above without seriously harming robustness, capacity or imperceptibility.

1.4 Watermarking with parametric wavelet filters

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.



2 Filter parametrization

2.1 Computation

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

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

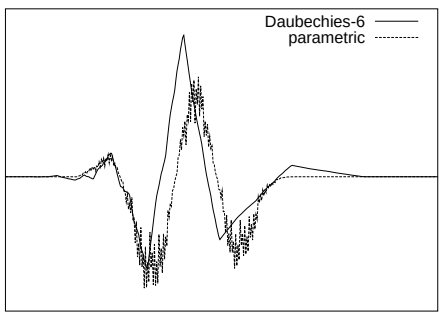
with $c_k \in \mathbb{R}$, have to be derived, satisfying two conditions on the coefficients c_k [6]. Schneid [7] describes a parametrization for suitable coefficients c_k based on the work of Zou [5] to facilitate construction of such wavelets. Given N parameter values $-\pi \le \alpha_i < \pi$, $0 \le i < N$, 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, $0 \le k < 2N+2$. We set $c_k = 0$ for $k < 0$ and $k \ge 2N+2$.

2.2 Example

Below see the Daubechies-6 wavelet and a parametric wavelet constructed with the parameter values ($\alpha_0 = -0.4815, a_1 = 2.6585$).

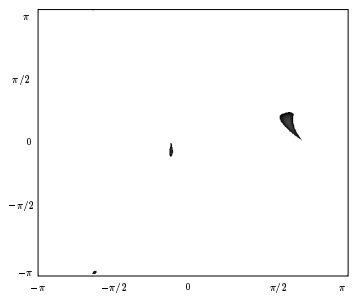


2.3 Smoothness

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 [8]. 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.
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.



2.4 Watermarking versus compression: transform domain issues

Hsu [9] 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.

2.5 Advantages

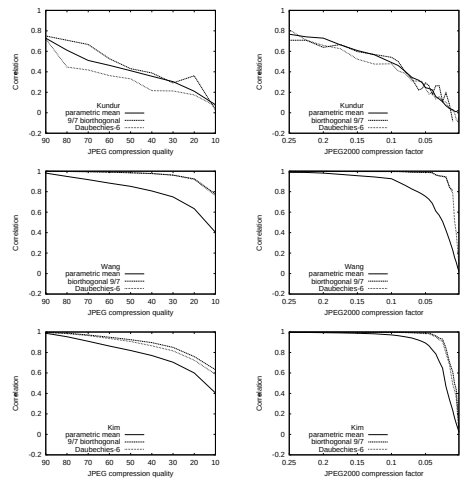
Employing secret filter parametrization in wavelet-based watermarking algorithms has the following advantages. First, security is improved because hostile attacks have to operate in the transform domain used for watermark embedding. Our experiments indicate that the size of the key-space is at least 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.

3 Experiments

We conduct all our experiments with the 512×512 gray-scale image 'Lena'. One blind [4] and two non-blind [3, 10] wavelet-based watermarking algorithms 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.

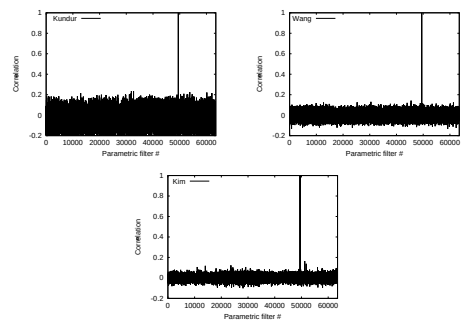
3.1 Robustness to compression

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 watermarked images are subjected to JPEG and JPEG2000 compression with different quality or bit-rate settings, respectively, resulting in compression ratios from approximately 1:4 up to 1:80. 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.



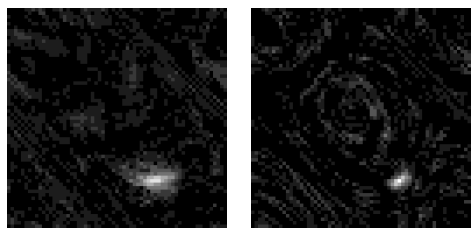
3.2 Security evaluation

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. The watermark can only be retrieved correctly with matching wavelet filters. We tested 63504 uniformly distributed parameters ($N = 2$; $\alpha_0, \alpha_1 \in \{-3.14, -3.11, \ldots, 3.11, 3.13\}; \Delta = 0.025$).

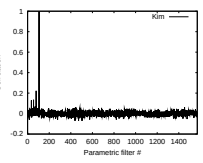


3.3 Correlation map and smoothness

We search for a known watermark in the restricted key-space of parameters that produce wavelet filters subject to our smoothness contraint. The watermark correlation obtained by varying two parametrization values ($N = 2$) is shown for two blind watermarking algorithms [11, 4] (light color means higher correlation).



Correlation measure for Kim's watermarking scheme, the key-space is restricted to smooth wavelets – the embedded mark can only be retrieved with the correct filter parameter.



4 Conclusions

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.

References

[1] Jiri Fridrich, Arnold C. Baldoza, and Richard J. Simard, "Robust digital watermarking based on key-dependent basis functions," in *Information hiding: second international workshop*, David Aucsmith, Ed., Portland, OR, USA, April 1998, vol. 1525 of *Lecture notes in computer science*, pp. 143 – 157, Springer Verlag, Berlin, Germany.

[2] Ton Kalker, Jean-Paul Linnartz, Geert Depovere, and Maurice Maes, "On the reliability of detecting electronic watermarks in digital images," in *Proceedings of the 9th European Signal Processing Conference, EUSIPCO '98*, Island of Rhodes, Greece, September 1998, pp. 13 – 16.

[3] Houng-Jyh Wang and C.-C. Jay Kuo, "Watermark design for embedded wavelet image codec," in *Proceedings of the SPIE's 43rd Annual Meeting, Applications of Digital Image Processing*, San Diego, CA, USA, July 1998, vol. 3460, pp. 388 – 398.

[4] Deepa Kundur, "Improved digital watermarking through diversity and attack characterization," in *Proceedings of the ACM Workshop on Multimedia Security '99*, Orlando, FL, USA, October 1999, pp. 53 – 58.

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

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

[7] 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.

[8] S. Maslakovic, I. R. Linscott, M. Oslick, and J. D. Twicken, "Smooth orthonormal wavelet libraries: design and application," in *Proceedings of IEEE ICASSP '98*, Seattle, WA, USA, May 1998, pp. 1793 – 1796.

[9] Chiou-Ting Hsu and Ja-Ling Wu, "Multiresolution watermarking for digital images," *IEEE Transactions on Circuits and Systems II*, vol. 45, no. 8, pp. 1097 – 1101, August 1998.

[10] Jong Ryul Kim and Young Shik Moon, "A robust wavelet-based digital watermark using level-adaptive thresholding," in *Proceedings of the 6th IEEE International Conference on Image Processing, ICIP '99*, Kobe, Japan, October 1999, p. 202.

[11] Liehua Xie and Gonzalo R. Arce, "Joint wavelet compression and authentication watermarking," in *Proceedings of the IEEE International Conference on Image Processing, ICIP '98*, Chicago, IL, USA, 1998.