Watermark Security via High-Resolution Wavelet Filter Parametrization

Werner Dietl, Peter Meerwald, Andreas Uhl

Department of Scientific Computing – Salzburg University
Jakob-Haringerstr. 2
5020 Salzburg, Austria / Europe
{wdietl,pmeerw,uhl}@cosy.sbg.ac.at

Abstract. This paper explores the use of secret, key-dependent wavelet filters as a mean to increase the security of watermarking methods that use the wavelet transform domain. Algorithms by Kim, Wang, and Xia are examined under security and image quality aspects when subjected to both JPEG and JPEG2000 compression. We show more evidence that parametrized wavelet filters are a good method to increase the security of existing watermarking schemes without increased computational complexity.

1 Introduction

Digital image watermarking for copyright protection and integrity verification continues to be a very active field of study. For an overview of the topic, possible applications and attacks see [2].

Recently the Discrete Wavelet Transform (DWT) was popularized by its use in the new JPEG2000 [5] image compression standard. Many advanced features like progressive and low bit-rate transmission and region-of-interest coding are possible with JPEG2000.

It is therefore necessary to investigate the DWT both as an possible attack on existing watermarking schemes and as a new method to embed data. [7] gives an overview of different wavelet-based image watermarking schemes.

In this work we pick up on the ideas from [8] and extend them to higher filter parameter resolutions and investigate security and quality aspects.

2 Wavelet Domain Watermarking

Based on the work of Cox [1] in the DCT domain, Kim [6] 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 [10] 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 [3] and improve watermark security although this will also limit the robustness and capacity of the scheme.

Xia [11] proposes a 2-level decomposition using the Haar wavelet filter. The watermark is embedded in large coefficients of the high and middle frequency bands (detail subbbands). The LL subband does not carry any watermark information.

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 [4]. Schneid [9] describes a parametrization for suitable coefficients c_k based on the work of Zou [12] to facilitate construction of such wavelets. Given N parameter values $-\pi \leq \alpha_i < \pi$, $0 \leq i < N$, the recursion

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

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 α_i 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.

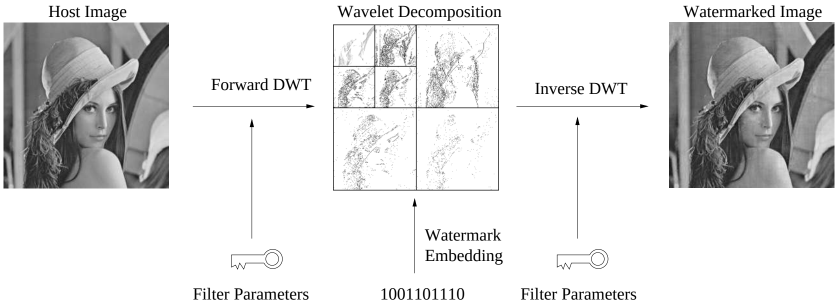


Fig. 1. Overview of watermark embedding procedure using parametrized wavelet filters.

4 Security Assessment

To test the security of the parametrized wavelet filters we embedded a watermark with the parameters $\alpha_0 = 0.150$ and $\alpha_1 = 0.650$ and an embedding strength that results in 40dB PSNR into the well known "Lena" image. We then tried to detect the watermark in the resulting image with different parameters α_i and measured the normalized correlation between the embedded watermark and the extracted one.

A perfect system would have a correlation of 1.00 only with the exact filter parameters and 0.00 everywhere else. In reality this optimum is not possible, but there is a significant difference in the correlation between right and wrong parameter values.

Figure 2 shows the results for the Kim algorithm with the parameters $\alpha_0, \alpha_1 \in \{-3.14, -3.13, \ldots, 3.13, 3.14\}$ with $\Delta = 0.01$. This results in 395641 samples, i.e. potentially different filter parameters. There is only one peak with a correlation of 0.903694 at the location of the embedding parameters. For the other samples the correlation is always smaller than 0.25, most of the time being below 0.10.

Because only the region around the embedding parameters shows higher correlation we will confine our further examinations to this area.

In figure 3 we see the results for the Kim algorithm. The top-left diagram (a) shows the correlation when $\alpha_0 \in \{0.000, \ldots, 0.300\}$ and $\alpha_1 \in \{0.500, \ldots, 0.800\}$ with $\Delta = 0.002$ resulting in 22801 measurements. Applied to the whole parameter space using $\Delta = 0.002$ would result in 9865881 possible filter keys. There are two peaks in the correlation – at the embedding position and in very close proximity.

To better visualize this result we used the parameter values α_0 and α_1 as X- and Y-axis and mapped the correlation to a shade of gray. A correlation

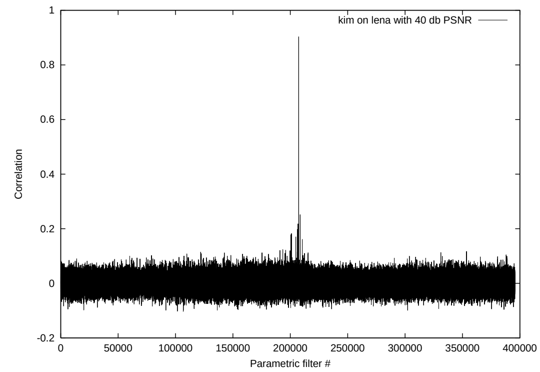


Fig. 2. Security evaluation of Kim algorithm. There is only one peak at the exact parameter values used for embedding. $\alpha_0, \alpha_1 \in \{-3.14, -3.13, \ldots, 3.13, 3.14\}$ with $\Delta = 0.01$.

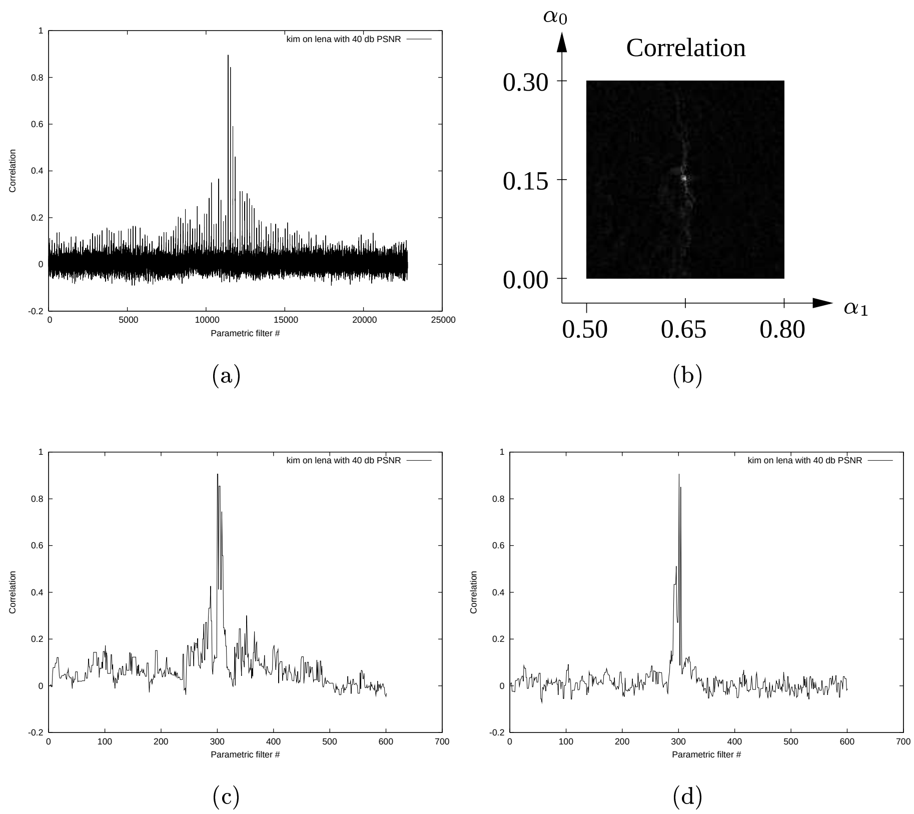


Fig. 3. Parameter security evaluation for Kim algorithm. The watermark was embedded with a PSNR of 40db at $\alpha_0 = 0.150$ and $\alpha_1 = 0.650$.

of zero corresponds to black and a correlation of one to white. In figure 3(b) you can see one white dot at the center of the image.

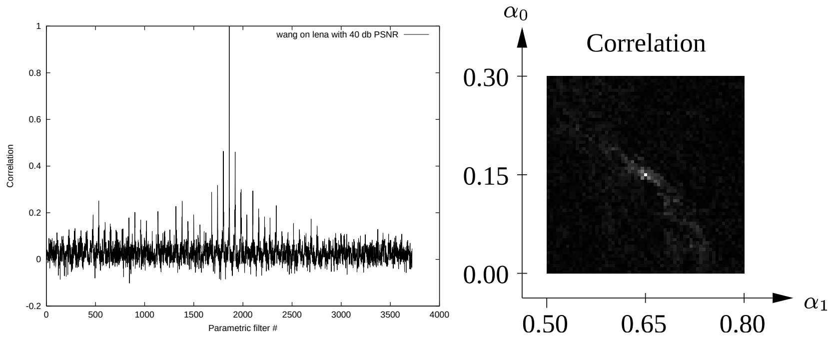


Fig. 4. Parameter security evaluation for Wang algorithm. The watermark was embedded with a PSNR of 40db at $\alpha_0 = 0.150$ and $\alpha_1 = 0.650$.

This picture helped us see that there is a higher correlation around the Y-axis for $\alpha_1 = 0.650$. To further analyse this we looked at the sensitivity of one parameter if the other parameter is already set to the right value.

Diagram (c) shows the correlation when $\alpha_1 = 0.650$ and $\alpha_0 \in \{0.000, \ldots, 0.300\}$; Diagram (d) sets α_0 to 0.150 and varies $\alpha_1 \in \{0.500, \ldots, 0.800\}$; both diagrams use $\Delta = 0.0005$ which results in 601 measurements each, which would be equivalent to 157778721 different filter keys.

At this fine resolution we see that there are several peaks close to the embedding values. Diagram (c) also has a broader region with high correlation than diagram (d). This results in the vertical "stripe" in diagram (b). With Δ at around 0.0005 we are approaching the finest meaningful resolution, further refinement would lead to multiple peaks around the true embedding key.

Figures 4 and 5 show the corresponding results for the Wang and Xia algorithms. The diagrams show the correlation when $\alpha_0 \in \{0.000, \ldots, 0.300\}$ and $\alpha_1 \in \{0.500, \ldots, 0.800\}$ with $\Delta = 0.005$ resulting in 3721 measurements. At this resolution we have 1580049 possible filter keys.

For both algorithms the correlation has only one clear maximum at the embedding values. A good choice for Δ therefore is in the range of 0.005 and 0.001 which results in a large number of possible keys and either one clear peak or a small area of high correlation.

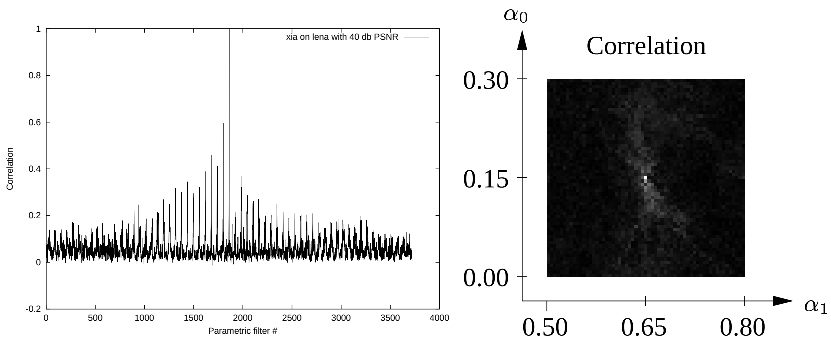


Fig. 5. Parameter security evaluation of Xia algorithm. The watermark was embedded with a PSNR of 40db at $\alpha_0 = 0.150$ and $\alpha_1 = 0.650$.

5 Quality Assessment

We explored the difference between the parametric filters and the Daubechies-6 and the 9/7-Biorthogonal filters with regard to correlation and PSNR under JPEG and JPEG2000 compression.

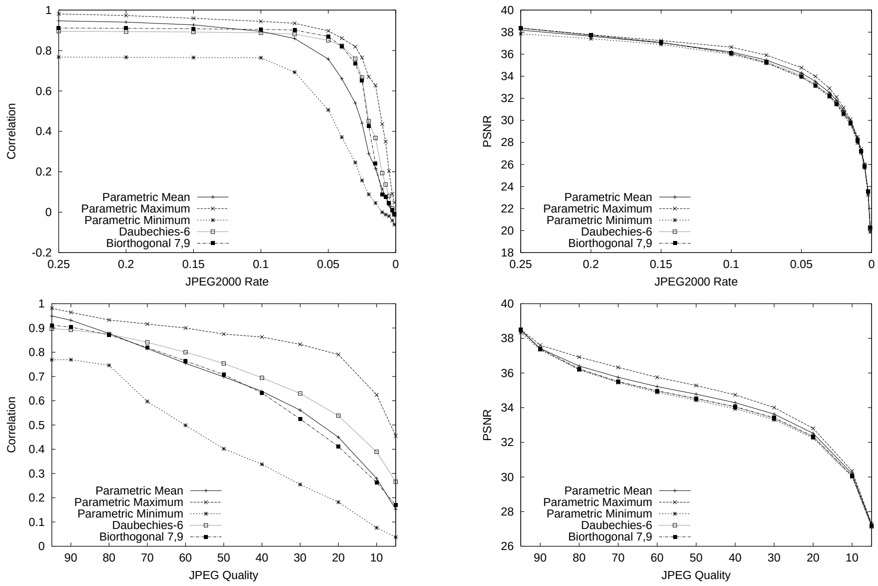
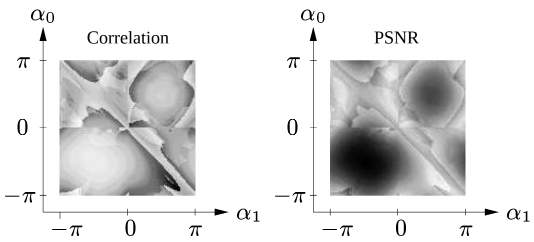


Fig. 6. Correlation and PSNR of Kim watermarks under JPEG and JPEG2000 compression.

We watermarked the "Lena" image with each parametrized filter $\alpha_0, \alpha_1 \in \{-3.00, \ldots, 3.00\}$ with $\Delta = 0.20$. The watermark was embedded with an embedding strength that resulted in a 40dB PSNR. Each picture was JPEG and JPEG2000 compressed with different quality levels and then the correlation and PSNR was measured.

Figure 6 shows the results for the Kim algorithm. The diagrams contain the average of all measured parametrized filters and the minimum and maximum for each compression rate. The average parametrized filters PSNR values are slightly above the standard filters and behave very similarly to them. The influence of parametrization on image quality is therefore minimal. The correlation values vary in a wider range. The average parametric correlation is close to the standard filters. For the Wang and Xia algorithms the results look comparable.



Max. Correlation: 0.988097
Max. PSNR: 42.309034
Avg. Correlation: 0.950132
Avg. PSNR: 38.741370
Min. Correlation: 0.854893
Min. PSNR: 34.180642

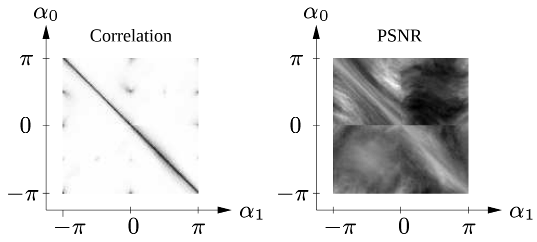
Fig. 7. Kim watermark embedded with strength 0.37501

For the next test we embedded a watermark with 40dB PSNR with the wavelet filters that are generated by α_0 and α_1 both equal to zero. We saved the embedding strength that was used to achieve this PSNR and then used it for the other parametrized filters with $\alpha_0, \alpha_1 \in \{-3.10, \dots, 3.10\}$ with $\Delta = 0.05$. For each filter we measured the correlation and PSNR that results from using this fixed embedding strength.

Figures 7 and 8 show the correlation and PSNR over the parameter values as two-dimensional plots. For these plots we scaled the shades of gray in such a way that black means the minimum and white means the maximum of all measured values. We also show the maximum, average and minimum values measured.

The correlation values are very good for all possible values and the PSNR is in a reasonable range.

What should be noted is that the minima and maxima of correlation and PSNR are complementary. This means that the correlation is lower in regions with a high PSNR and the other way around. Therefore a desired PSNR should always be possible by adjusting the embedding strength to the selected filter values.



Max. Correlation: 0.999966
Max. PSNR: 41.050860
Avg. Correlation: 0.999554
Avg. PSNR: 39.356588
Min. Correlation: 0.989557
Min. PSNR: 38.252465

Fig. 8. Wang watermark embedded with strength 0.16568

6 Conclusion

We showed further evidence that the use of parametrized filters is a viable way to increase the security of wavelet-based watermarking schemes.

References

1. Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon. Secure spread spectrum watermarking for multimedia. In *Proceedings of the IEEE International Conference on Image Processing, ICIP '97*, volume 6, pages 1673–1687, Santa Barbara, California, USA, October 1997.
2. Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom. *Digital Watermarking.* Morgan Kaufmann, 2002.
3. Scott A. Craver, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung. On the invertibility of invisible watermarking techniques. In *Proceedings of the IEEE International Conference on Image Processing, ICIP '97*, volume 1, page 540, Santa Barbara, California, USA, October 1997.
4. Ingrid Daubechies. *Ten Lectures on Wavelets.* Number 61 in CBMS-NSF Series in Applied Mathematics. SIAM Press, Philadelphia, PA, USA, 1992.
5. ISO/IEC JPEG committee. JPEG 2000 image coding system — ISO/IEC 15444-1:2000, December 2000.
6. 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*, page 202, Kobe, Japan, October 1999.
7. P. Meerwald and A. Uhl. A survey of wavelet-domain watermarking algorithms. In Ping Wah Wong and Edward J. Delp, editors, *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, volume 4314, San Jose, CA, USA, January 2001. SPIE.
8. P. Meerwald and A. Uhl. Watermark security via wavelet filter parametrization. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'01)*, volume 3, pages 1027–1030, Thessaloniki, Greece, October 2001. IEEE Signal Processing Society.
9. J. Schneid and S. Pittner. On the parametrization of the coefficients of dilation equations for compactly supported wavelets. *Computing*, 51:165–173, May 1993.
10. 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*, volume 3460, pages 388–398, San Diego, CA, USA, July 1998.
11. Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce. Wavelet transform based watermark for digital images. *Optics Express*, 3(12):497, December 1998.
12. H. Zou and Ahmed H. Tewfik. Parametrization of compactly supported orthonormal wavelets. *IEEE Transactions on Signal Processing*, 41(3):1423–1431, March 1993.