# Key-dependent pyramidal wavelet domains for secure watermark embedding

Werner M. Dietl, Peter Meerwald and Andreas Uhl
Department of Scientific Computing, University of Salzburg, Austria

## ABSTRACT

Wavelet filters can be parametrized to create an entire family of different wavelet filters. We discuss wavelet filter parametrization as a means to add security to wavelet based watermarking schemes. We analyze the influence of the number of filter parameters and use non-stationary multi-resolution decomposition where different wavelet filters are used at different levels of the decomposition. Using JPEG and JPEG2000 compression we assess the normalized correlation and Peak Signal to Noise Ratio (PSNR) behavior of the watermarks. The security against unauthorized detection is also investigated. We conclude that the proposed systems show good robustness against compression and depending on the resolution we choose for the parameters we get between $2^{99}$ and $2^{185}$ possible keys.

**Keywords:** parametrized wavelet filters, watermarking, security, robustness

## 1. INTRODUCTION

Fast and easy distribution of content over the Internet is a serious threat to the revenue stream of content owners. Watermarking has gained high popularity as a method to protect intellectual property rights on the Internet. For introductions to this topic see.[1–5]

Over the last several years wavelet analysis was developed as a new method to analyze signals.[6–8] Wavelet analysis is also used in image compression, where better energy compaction, the multi-resolution analysis and many other features make it superior to the existing discrete-cosine based systems like JPEG. The new JPEG2000 compression standard[9,10] uses the wavelet transformation and achieves higher compression rates with less perceptible artifacts and other advanced features.

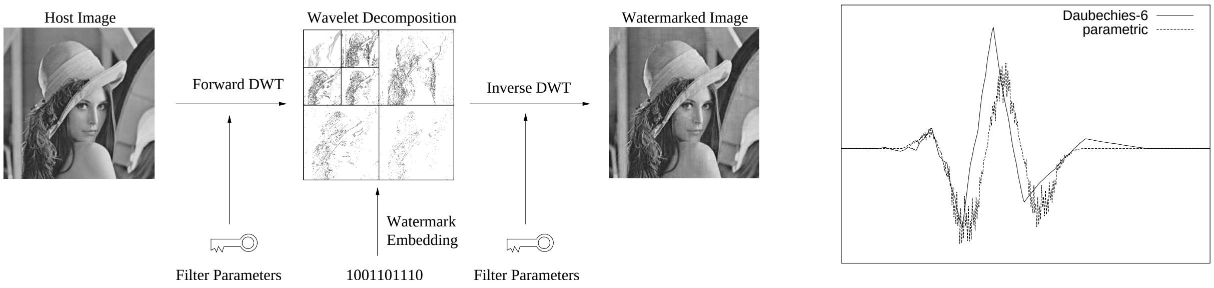
With the rising interest in wavelets also the watermarking community started to use them. Many watermarking algorithms have been developed that embed the watermark in the wavelet transform domain — Meerwald[11] compiled an overview.

The resilience of a watermarking system can be separated into robustness and security. In the following we will use the terminology suggested by Cox.[4] Robustness means the resistance against common signal distortions that are known beforehand. For example, a system that includes a transmission over a noisy communication channel needs to be robust against the noise. It is known in advance that the channel is noisy and without robustness against the noise the watermarking system is useless.

Security means the resistance against malicious, intentional modifications of the watermarked signal. Depending on the application scenario we can distinguish four types of attacks. Unauthorized detection allows the attacker to detect the existence of a watermark or extract the watermark information. Unauthorized removal tries to remove the embedded watermark information. Unauthorized embedding attempts to embed a watermark without the correct authorization. Finally a system attack tries to exploit weaknesses in the overall system.[4]

In previous work the following techniques to enhance the security of watermarks have been proposed. Pseudo-random skipping of coefficients has been proposed by Wang[12] or Kundur,[13] but skipping significant coefficients reduces the capacity of the systems. Fridrich[14] introduced the concept of key-dependent basis functions in order to protect a watermark from hostile attacks. By embedding the watermark information in a secret transform

Further author information:
E-mail: {wdietl,pmeerw,uhl}@cosy.sbg.ac.at
Address: Jakob-Haringerstrasse 2, 5020 Salzburg, Austria / Europe




(a) Proposed System (b) Wavelet Filters

**Figure 1.** Overview of watermark embedding procedure using parametrized wavelet filters (a) and a comparison of the standard Daubechies 6 and a parametrized wavelet filter using $\alpha_0 = -0.4815$ and $\alpha_1 = 2.6585$ (b)

domain, Fridrich's algorithm can better withstand attacks such as those described by Kalker[15] 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. In a later paper Fridrich reduced the computational complexity of the system.[16]

In this paper we propose the use of parametrized wavelet filters as a method to protect wavelet-based watermarks against unauthorized detection. We demonstrate this approach with the algorithms by Kim[17] and Wang.[12] Both use spread-spectrum techniques and need the original image to extract the watermark.

In section 2 we introduce wavelet filter parametrization and then use it in a six parameter system in section 3 and in a system with different numbers of parameters in section 4. We present a combined system that uses a total of 20 filter parameters in section 5 and close with the conlusions in section 6.

## 2. WAVELET 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 $c_k$.[6] Schneid[18] describes a parametrization for suitable coefficients $c_k$ based on the work of Zou[19] to facilitate construction of such wavelets. Given $N$ parameter values $-\pi \leq \alpha_i < \pi$, $0 \leq i < N$, the recursion

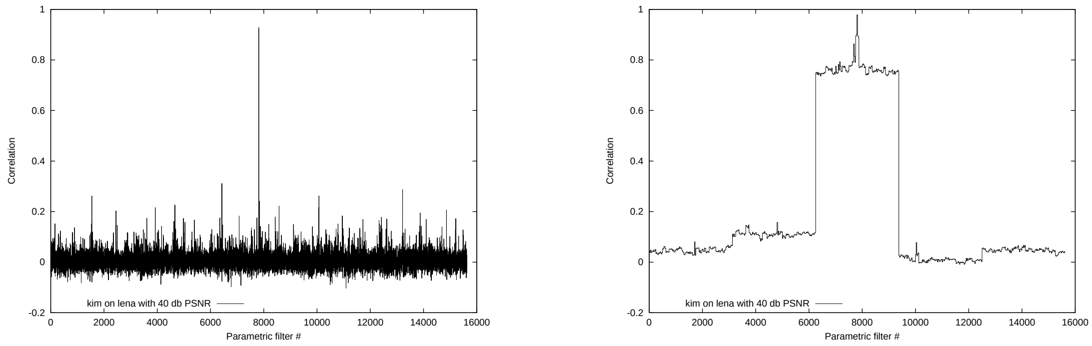
$$c_0^0 = \frac{1}{\sqrt{2}} \quad \text{and} \quad c_1^0 = \frac{1}{\sqrt{2}}$$

$$c_k^n = \frac{1}{2}\Big( (c_{k-2}^{n-1} + c_k^{n-1}) \cdot (1 + \cos \alpha_{n-1}) + (c_{2(n+1)-k-1}^{n-1} - c_{2(n+1)-k-3}^{n-1})(-1)^k \sin \alpha_{n-1} \Big)$$

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 $\alpha_i$ 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(a) and in figure 1(b) a standard Daubechies 6 filter is compared with a parametrized filter with $N = 2$ that was generated using $\alpha_0 = -0.4815$ and $\alpha_1 = 2.6585$, resulting in a 6-tap filter.

Our approach to generating key-dependent wavelet filters is, in principle, applicable to all wavelet-based watermarking systems and can also be integrated with the JPEG2000, Part 2, standard for image compression.




(a) One filter with six parameters

(b) Six filters each with one parameter

**Figure 2**. Security assessment of the Kim algorithm — Overview

# 3. NON-STATIONARY DECOMPOSITION WITH SIX PARAMETERS

In previous work[20, 21] we analyzed the security and quality aspects of using two filter parameters as watermarking key. We have seen that with two parameters we have a keyspace from a few hundred-thousands to a few millions, depending on the selected resolution.

We have two options if we are interested in a larger possible keyspace. We could use more than two parameters to create a filter or use different filters for the different wavelet decomposition levels, which is also called Non-Stationary Multi-Resolution Analysis (NSMRA).[22] Of course we can also combine those two possibilities.

Non-stationary MRA can be used for improving image compression.[23] Here we use non-stationary MRA as a method to increase security. To get a larger parameter space we use different parametrized filters for the decomposition levels. We hope that the number of parameters for the different levels add up and produce a system with a large number of parameters.

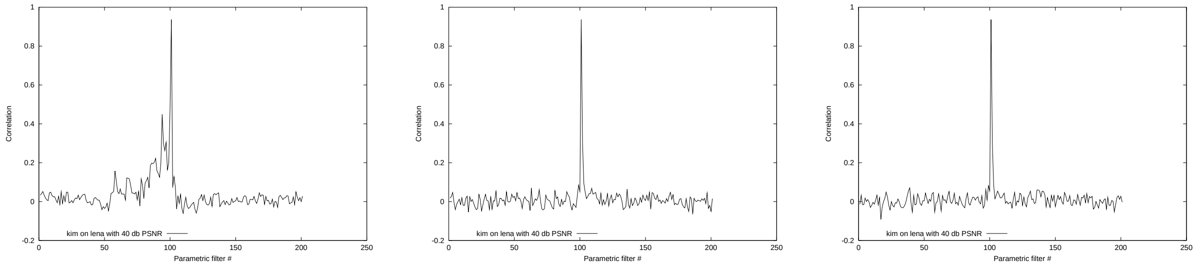
In this section we are going to look at different possibilities to distribute six parameters over the decomposition levels. We analyze different parameter numbers in detail in section 4 and look at a combined system in section 5.

We experimented with different distributions of the six parameters over the decomposition levels. Because of space restrictions we can only present a subset of the available results. For the security assessment we only present the two extreme cases. We either use all six parameters to generate one filter and use that filter for all decomposition levels or we use every single parameter to create a filter that is used for one of the six decomposition levels. For the robustness assessment against JPEG2000 and JPEG compression we present the results for the four systems that use an equal number of parameters for every level. This includes the two extreme cases, plus using two or three parameters per filter. We do not present the results for the systems that use a different number of parameters for the different decomposition levels.

## 3.1. Protection Against Unauthorized Detection

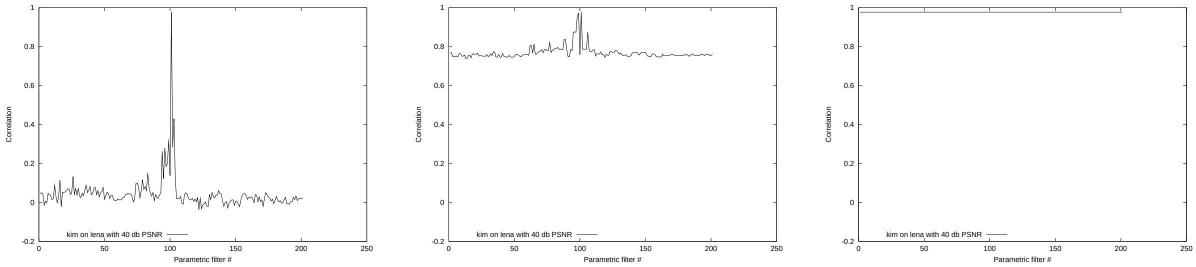
To test the security of the system we embed a fixed watermark with one key parametrization and then try to detect the watermark with other parametrizations. The optimal system would have a normalized correlation between the embedded and the extracted mark of 1.0 only with the correct parameters and would be zero everywhere else. We embed the watermark into the well-known “Lena” image with an embedding strength that results in 40dB PSNR. We use the parameters ”-1.5 2.5 -1.0 1.5 0.5 -2.5” to embed the watermark.

The overview diagrams vary all the parameters with $\pm 0.1$ around the correct value and use a step size $\Delta = 0.05$. This results in 5 possibilities for every parameter and a total of $5^6 = 15625$ analyzed filter parametrizations. Using $\Delta = 0.05$ over the complete parameter space results in more than $2^{40}$ possible filter parametrizations.




(a) Detail A (b) Detail B (c) Detail F

**Figure 3**. Security assessment of the Kim algorithm — One filter with six parameters




(a) Detail A (b) Detail B (c) Detail F

**Figure 4**. Security assessment of the Kim algorithm — Six filters each with one parameter

The detail diagrams vary only one parameter with $\pm 0.2$ and $\Delta = 0.002$; all the other parameters are set to the correct key position. This results in $0.4/0.002 + 1 = 201$ analyzed filters. "Detail A" means that only the first of the six parameters is varied, "Detail B" that only the second parameter is varied and so on. We only present the detailed results for parameters 1, 2 and 6.

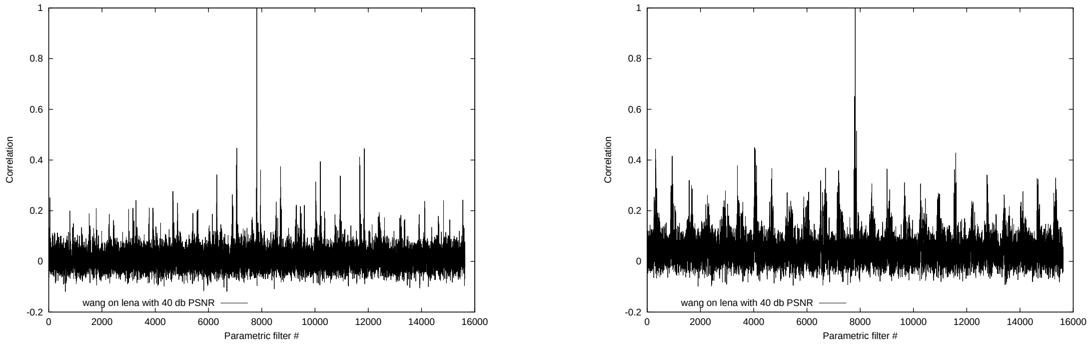
Figure 2(a) shows the behavior when the Kim algorithm is used and all six parameters are used to generate one filter. The response when just one parameter is modified is shown in figure 3. There is one clear peak at the embedding position and all other correlation values are below 0.4. All detail diagrams show just a very small area of high correlation and an impact from all parameters.

The other extreme case is that every parameter is used for a different filter, generating six filters for six decomposition levels. Figure 2(b) gives the overview and figure 4 the single parameter behavior. We can already see from the overview that there is a security problem. There is a range from roughly parametrization 6000 to 9000 that has a correlation of more than 0.70. This means that even if you are only close to the correct embedding parameters you already get a very high correlation value.

By looking at figure 4 we see what the problem is. Figure (a) shows good behavior and we only have one peak in the correlation. But as soon as the first parameter has the correct value we have an increase in correlation to more than 0.70. Figure (b) has a correlation of nearly 0.80 over the complete parameter range. The other parameters look even worse. In figure (c) there is no significant difference in correlation if you vary the parameter for the sixth decomposition level.

Clearly the security of this system is not what we expect. From all six parameters only the first one has real significance. The other five parameters do not influence the correlation in the expected way.

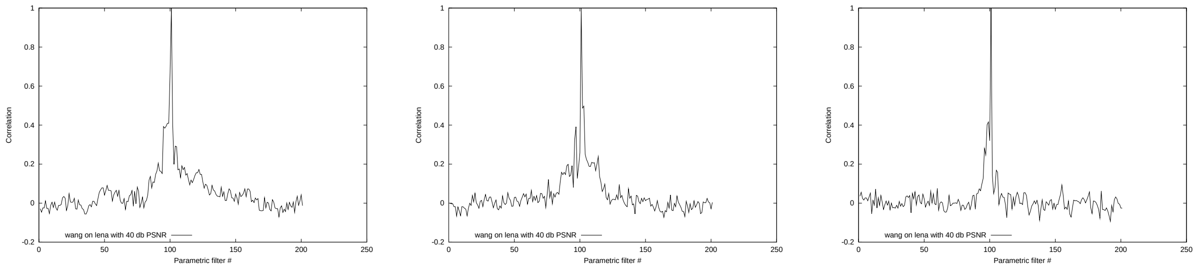
When the Wang algorithm is used and we let all six parameters produce one filter, then we get the results shown in figures 5(a) and 6. As expected there is one clear peak and generally very low correlation everywhere




(a) One filter with six parameters

(b) Six filters each with one parameter

**Figure 5**. Security assessment of the Wang algorithm — Overview




(a) Detail A

(b) Detail B

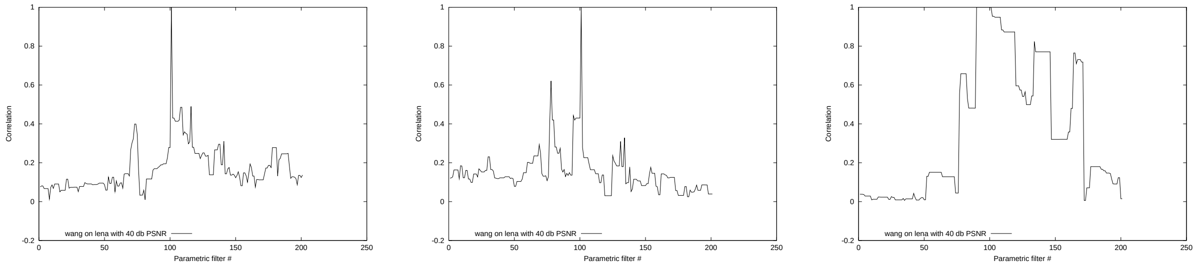
(c) Detail F

**Figure 6**. Security assessment of the Wang algorithm — One filter with six parameters

else. Also the influence from each of the six parameters looks similar and each one has a very small area of high correlation.

Figures 5(b) and 7 show the six parameters distributed over six filters. With the Wang embedding scheme we see very good results. Figures 7(a) and (b) look very good and only have one clear peak. Figure 7(c) has a larger area of high correlation, but still shows that even the last parameter has an effect on the correlation.

We see that using the Wang watermarking method with non-stationary MRA shows higher security than

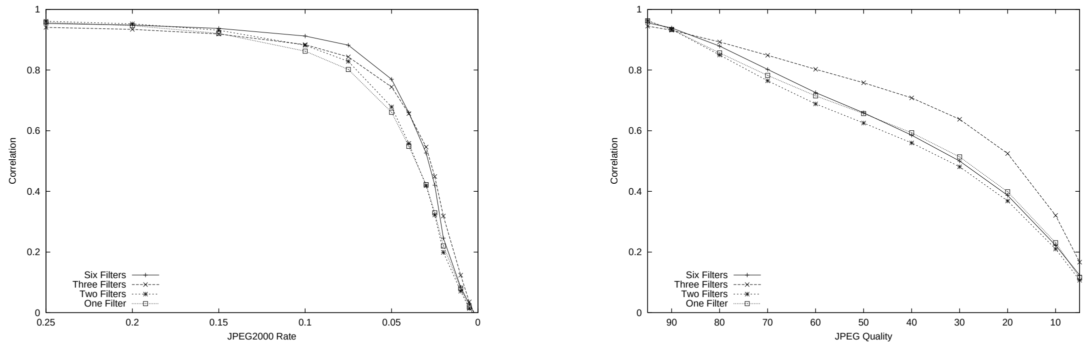



(a) Detail A

(b) Detail B

(c) Detail F

**Figure 7**. Security assessment of the Wang algorithm — Six filters each with one parameter




(a) JPEG2000

(b) JPEG

**Figure 8**. Quality assessment of the Kim algorithm — Correlation under JPEG2000 and JPEG compression

using the Kim method. All parameters from all decomposition levels have an influence on the correlation result. NSMRA can be used to increase the parameter-space and enhance the security of the system only if the Wang method is used. The different sequence of levels selected by the Wang algorithm is a clear advantage over the top-down approach used by Kim.

### 3.2. Quality Assessment and Robustness

To analyze the influence of the parametrized filters on the image quality and correlation under compression we embed a watermark with different filters. Each filter parameter $\alpha_i$ is chosen from $\{-1.5, 0.50, 2.5\}$, therefore we assess $3^6 = 729$ different parametrizations. Again we choose an embedding strength that results in 40dB PSNR with the "Lena" image. Then we compress the watermarked images using JPEG and JPEG2000 with different quality levels.

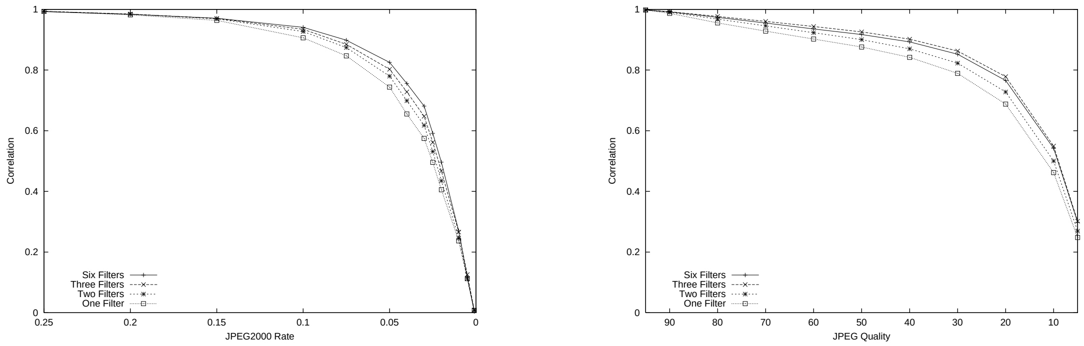
We measure the PSNR of the compressed image to see the effect of the parameterized filters on the image quality. We also try to detect the watermark in the compressed image with the known parameters and measure the resulting correlation between the embedded and the extracted watermarks. Then the minimum, maximum and average of all parametrized filters are calculated and used for comparing the different parameter distributions.

The average results for the Kim algorithm are presented in figure 8. In both figures you can see that the correlation after strong compression is better when the filter was generated from fewer parameters. For a JPEG2000 compression rate of 0.05 the system that uses all six parameters to create the filters has a correlation of around 0.1 below the correlation for the system that uses each parameter to create six different filters.

The behavior of the Wang systems is shown in figure 9. It is again clear to see that for compression rates between 0.15 and 0.025 the shorter filters show better resistance to the compression. For a JPEG2000 rate of 0.05 the correlation for the single-parameter filters is around 0.1 higher than the correlation for the six-parameter filter. For JPEG compression the filters that were generated by one or two parameters are clearly above the filters generated by six parameters. The difference at a quality factor of 10 is 0.08 in advantage of the shorter filters.

## 4. DIFFERENT NUMBERS OF PARAMETERS

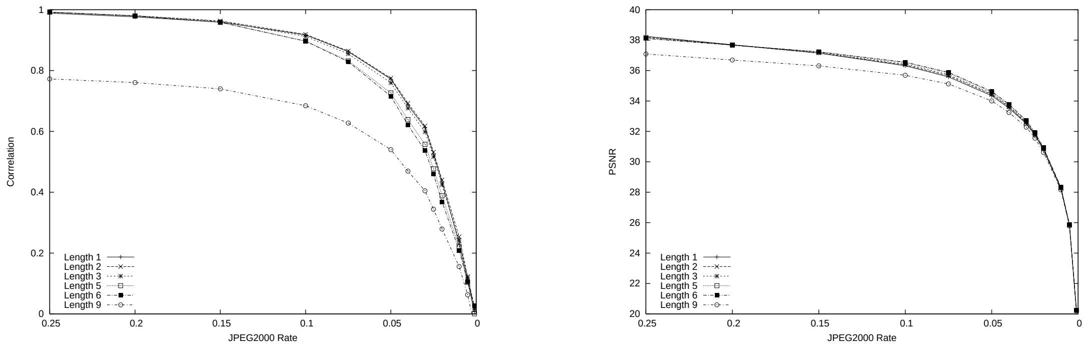
In the last section we looked at the distribution of six parameters over the different decomposition levels. For the quality assessment we varied the $\alpha_i \in \{-1.5, 0.50, 2.5\}$, which results in 729 different parametrizations. Now if the six parameters are used for one long filter we have $3^6 = 729$ different filters that are used for the decompositions. But if we use each single parameter to create a filter, then we only have 3 distinct filters that are distributed in different combinations over the six decomposition levels.




(a) JPEG2000

(b) JPEG

**Figure 9.** Quality assessment of the Wang algorithm — Correlation and PSNR under JPEG2000 and JPEG compression




(a) JPEG2000 Correlation

(b) JPEG2000 PSNR

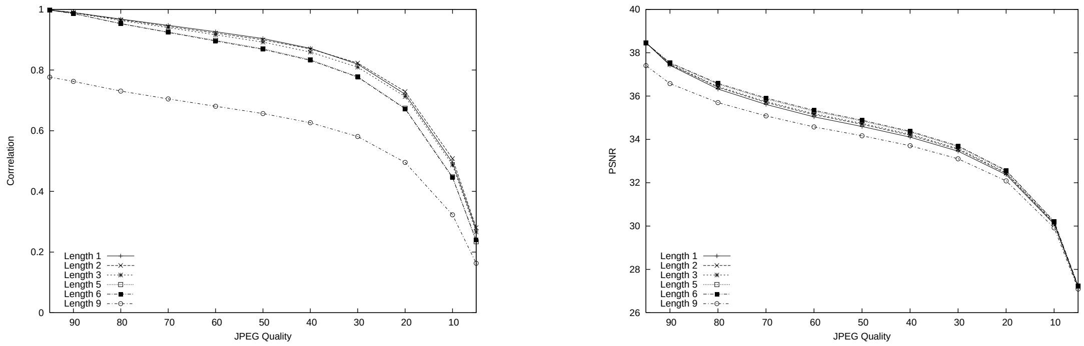
**Figure 10**. Systems with a different number of parameters under JPEG2000 compression

The different number of parametrizations used for the different filter lengths could produce skewed results. To make sure the different filter lengths produce comparable results we now look at filters with 1, 2, 3, 5, 6 and 9 parameters. For each length we choose parameters to get between 512 and 1024 different filter parametrizations. The same filter is used for all decomposition levels. We present the average results for the Wang algorithm alone, because we have already seen that using the Kim algorithm results in inferior security.

Figure 10(a) shows the average correlation under JPEG2000 compression. As expected the longer filters show worse behavior under compression. What needs to be noted is the behavior of the nine parameter filters. They show an average correlation of around 0.20 below the other filters. A look at the minimum correlation revealed that there are filters with which no correlation could be detected. Close inspection showed that for more than 10% of the 9 parameter filters the wavelet decomposition and composition could not be performed with 40dB PSNR. Even without modification from the watermarking algorithms these filters created distorted images with a quality below 40dB PSNR.

The influence of the different number of filter parameters on the image quality (as measured by the PSNR) is minimal. Figure 10(b) shows the average PSNR under JPEG2000 compression. The longer filters show only a slight advantage for compression rates between 0.15 and 0.025.

The same behavior can be seen under JPEG compression, shown in figure 11. Figure 11(a) shows the average correlation under JPEG compression. Filters with 1, 2 and 3 parameters are very close together, but are clearly




(a) JPEG Correlation (b) JPEG PSNR

**Figure 11**. Systems with a different number of parameters under JPEG compression

separated from the 5 and 6 parameter filters. We again see that the average value for the 9 parameter case is around 0.20 below the other values.

The average PSNR under JPEG compression is shown in figure 11(b). From a compression quality of 90 down to 10 the longer filters have a higher PSNR than the shorter filters. But again the difference is rather small.

From these results we see that the shorter filters do show better correlation behavior under compression. A comparable number of different filters was used for the different filter lengths to make sure that the results are not skewed. We also repeated the experiments with 512 random parameter selections for every filter length and got the same results.

## 5. MULTI-LEVEL SYSTEM

Now we present a combined system that only uses the Wang algorithm. We use filters that are generated by five parameters and use four different filters for the first four decomposition levels. This results in a combined system with 20 parameters as embedding key.

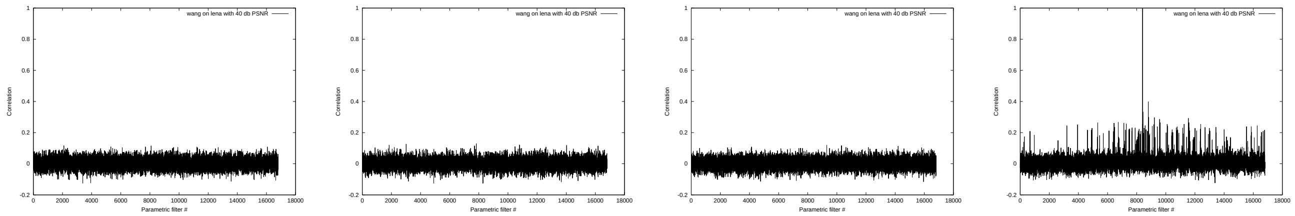
### 5.1. Protection Against Unauthorized Detection

For 20 parameters examining every parameter variation is not easily possible. Therefore we decided to look at the system and try to "attack" it. The attacker knows the basic design of the system, but does not know the key that was used for embedding. He in turn looks at the different decomposition levels and tries to independently guess the value of the 5 parameters used for that level. The parameters for the lower levels are set to zero.

The watermark was embedded using the parameter values:

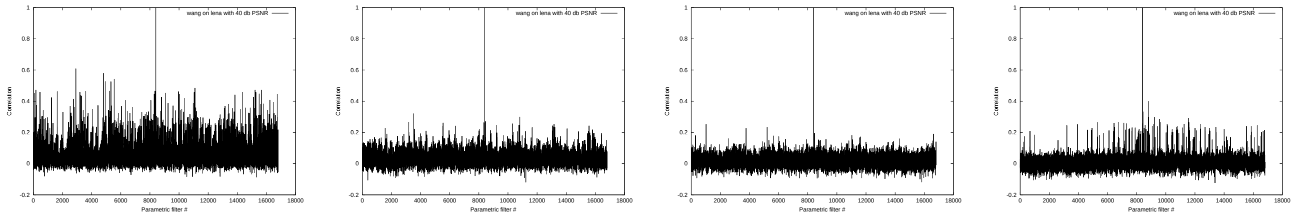
| Parameter | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Level 1 | -0.5 | 2.5 | -1.0 | 1.5 | 0.5 |
| Level 2 | -2.5 | 2.0 | -2.0 | 0.5 | 1.0 |
| Level 3 | 2.0 | -1.5 | 0.5 | 2.5 | -2.0 |
| Level 4 + higher | -1.0 | -2.0 | 1.0 | -0.5 | 2.5 |

In the following tests we vary all five parameters for each level at the same time. We take the starting value 0.6 below the correct value for each of the five parameters. Then we increment the parameters by 0.2 until all parameters are 0.6 above the correct value. We therefore have $7^5 = 16807$ measurements for every level.




(a) First Level (b) Second Level (c) Third Level (d) Fourth Level

**Figure 12**. Guessing all four levels of the multi-level system




(a) First Level (b) Second Level (c) Third Level (d) Fourth Level

**Figure 13**. Variations of all levels of the multi-level system

In figure 12(a) we try to attack the first level. We vary the five parameters for the first decomposition level and keep the other parameters set to zero. From the correlation response to the different parametrizations there is no way for the attacker to guess the correct values.

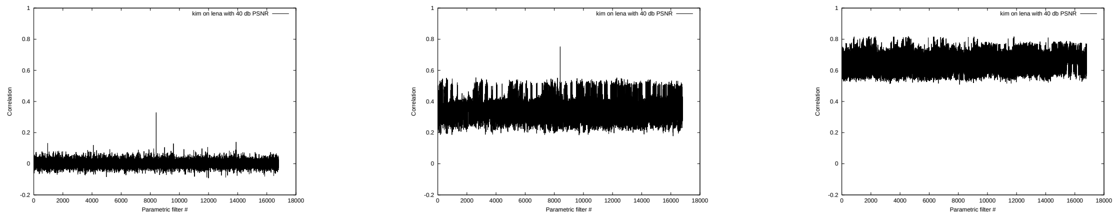
If for some reason the attacker knows the correct parameter values for the first decomposition level, then he only needs to search for the remaining 15 parameters. Again we focus on the next set of five parameters used for the second decomposition level. The first decomposition is performed with the correct filter and the third and higher filter parametrizations are unknown to the attacker. In figure 12(b) we see that the attacker did not get any additional knowledge from knowing the first decomposition filter. The correlation is low over the complete range of guessed parametrizations, although the correct parametrization for the second decomposition level was tested.

The same is true for the third level. If we already have the first and second decomposition level parameters and only need to find the third and fourth level, then we will again first try to find the five parameters for the third decomposition. Figure 12(c) shows the correlation when the first two levels are set to the correct keys, the fourth level is set to zero and the five parameters for the third level are varied over a set of parametrizations that contain the correct parameter values. Again there is no sign which of the tested parametrizations is the correct one and the attacker has no way of knowing that he has tested the correct parameters for the third level.

Only in case the attacker already knows the decomposition parameters for the first three levels is he able to determine the correct parameters for the fourth level. In figure 12(d) the attacker already knows the first 15 keys and only varies the last five parameters for the fourth decomposition level. There is a clear peak at the location of the correct embedding parametrization and low correlation everywhere else.

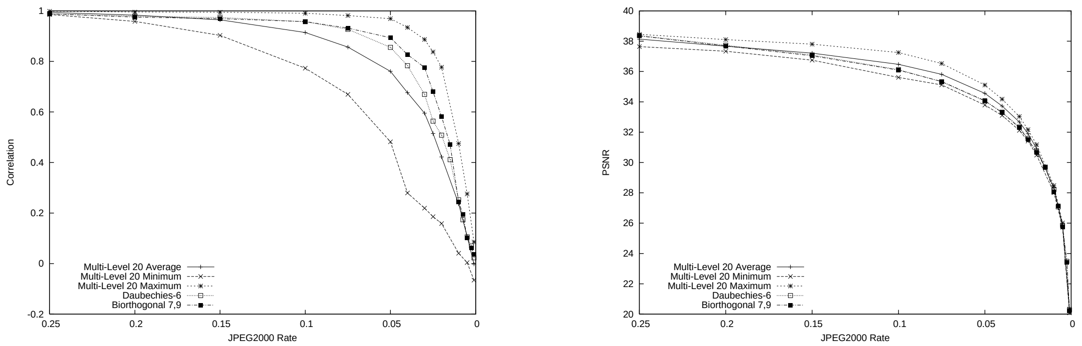
So only after having all 20 parameters right does the attacker get a high correlation.

Next we look at the sensitivity of the different levels to parameter changes. We set all levels to the correct embedding parameters and only vary the five parameters for one level and measure the correlation. In figure 13(a) we vary the parameters for the first level and have the correct values for the other three levels. There is one peak at the embedding position and low correlation everywhere else. For levels two and three we see the




(a) First Level (b) Second Level (c) Third Level

**Figure 14**. Multi-level system with Kim embedding – Guessing the first three levels




(a) JPEG2000 Correlation (b) JPEG2000 PSNR

**Figure 15**. Correlation and PSNR of multi-level system under JPEG2000 compression

respective results in figures 13(b) and 13(c). For the fourth level this attack is the same as the previous attack on the fourth level. The results are shown again in figure 13(d). We see that the first level has higher correlation for wrong parameter values. Overall the behavior of the system is very good and there is always one clear peak.

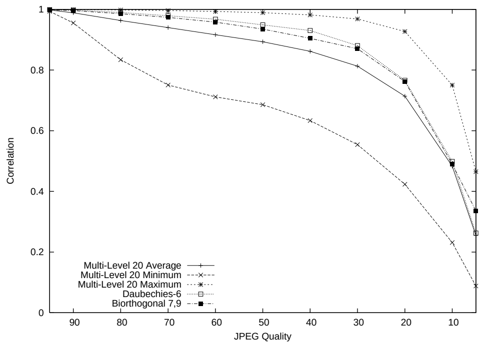
To give a clear view of the security advantage of using the Wang embedding scheme we show the attacks on the first three levels for the Kim method in figure 14. For figure 14(a) we varied the five parameters for the first levels and set all remaining 15 parameters to zero. There is one clear peak with a correlation of around 0.30. So although we do not get a 1.00 correlation by only guessing the first level we still see a significantly higher correlation for the correct parameters for this level.

Now by using the correct filters for the first level, setting the third and higher levels to zero and only varying the second level parameters we get figure 14(b). The first thing to notice is that the correlation is above 0.20 for all tested parametrizations. But again there is a significantly higher correlation for the correct filter parametrization. We see the same behavior for the third and fourth levels, only that the overall correlation gets higher and higher. From this last experiment we conclude that only by using the Wang embedding algorithm we get the real security of all 20 parameters.

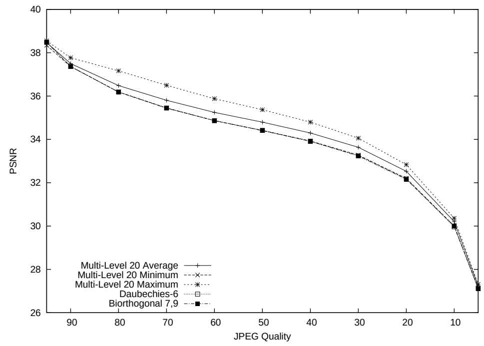
Using 20 filter parameters we get a vast key space. If we use a resolution of 0.20 we have around $(2*\pi/0.20)^{20} \approx 2^{99}$ possible filter parametrizations. For a finer resolution of 0.01 we get $(2*\pi/0.01)^{20} \approx 2^{185}$ filters. If we choose a parameter resolution between 0.20 and 0.01 we have a very large key space and have very good separation between the correct key and incorrect embedding parametrizations.

## 5.2. Quality Assessment and Robustness

In this investigation we look at the correlation and PSNR behavior of the combined system under JPEG and JPEG2000 compression. We create 768 different filter parametrizations by randomly choosing values for the 20




(a) JPEG Correlation




(b) JPEG PSNR

**Figure 16**. Correlation and PSNR of multi-level system under JPEG compression

parameters between -3.14 and 3.14. For each parametrization we embed a given watermark with an embedding strength that results in 40dB PSNR into the Lena image. Then we compress the watermarked image with JPEG and JPEG2000 at different compression rates. We try to detect the watermark in the compressed images and measure the correlation between the extracted watermark and the embedded one. Also the PSNR is measured to determine how strongly distorted the compressed image is.

We calculate the average, minimum and maximum values from all 768 different parametrizations and compare the results for the combined system to the results for the two standard systems using the Daubechies 6 and the Biorthogonal 7/9 filters.

Figure 15(a) shows the correlation behavior under JPEG2000 compression, figure (b) shows the PSNR. The corresponding values for JPEG compression are shown in figure 16(a) and (b). The average behavior of the combined system is very close to the two standard systems. The range of possible behavior includes filters that are above the standard systems and even the worst behaving filters produce acceptable results for medium compression rates.

## 6. CONCLUSIONS

In this work we analyzed the effect of non-stationary decomposition where different filters are used for different decomposition levels. We concluded that the Wang method of selecting significant coefficients is best suited. For the Kim algorithm non-stationary decomposition is not improving the security as much as expected.

We also investigated the influence of the number of parameters on the robustness against JPEG and JPEG2000 compression. We have seen that more parameters lead to less resistance against compression. The use of 5 parameters to generate a filter seems to be a good compromise between possible key-space and robustness against compression.

Finally we presented a combined system that uses a total of 20 parameters. We use 5 parameters per filter and use four different filters for the non-stationary decomposition. This combination of filter parametrization and non-stationary wavelet decomposition achieves a keyspace of cryptographically reasonable size, with between $2^{99}$ and $2^{185}$ possible filters. Also, robustness against JPEG and JPEG2000 compression is on an equal level as compared to the use of standard wavelet filters.

## ACKNOWLEDGMENTS

Part of this work was funded by the Austrian Science Fund FWF project P15170 “Sicherheit für Bilddaten in Waveletdarstellung”.

## REFERENCES


1. S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, Dec. 1999.
2. J. Dittmann, ed., *Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete*, Springer Verlag, 2000.
3. N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures*, Kluwer Academic Publishers, 2000.
4. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.
5. J. J. Eggers and B. Girod, *Informed Watermarking*, Kluwer Academic Publishers, 2002.
6. I. Daubechies, *Ten Lectures on Wavelets*, no. 61 in CBMS-NSF Series in Applied Mathematics, SIAM Press, Philadelphia, PA, USA, 1992.
7. M. Wickerhauser, *Adapted wavelet analysis from theory to software*, A.K. Peters, Wellesley, Mass., 1994.
8. S. Mallat, *A wavelet tour of signal processing*, Academic Press, 1997.
9. ISO/IEC JPEG committee, "JPEG 2000 image coding system — ISO/IEC 15444-1:2000," Dec. 2000.
10. D. Taubman and M. Marcellin, *JPEG2000 — Image Compression Fundamentals, Standards and Practice*, Kluwer Academic Publishers, 2002.
11. P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," in *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, P. W. Wong and E. J. Delp, eds., **4314**, SPIE, (San Jose, CA, USA), Jan. 2001.
12. H.-J. Wang and C.-C. J. Kuo, "Watermark design for embedded wavelet image codec," in *Proceedings of the SPIE's 43rd Annual Meeting, Applications of Digital Image Processing*, **3460**, pp. 388–398, (San Diego, CA, USA), July 1998.
13. D. Kundur, "Improved digital watermarking through diversity and attack characterization," in *Proceedings of the ACM Workshop on Multimedia Security '99*, pp. 53–58, (Orlando, FL, USA), Oct. 1999.
14. J. Fridrich, A. C. Baldoza, and R. J. Simard, "Robust digital watermarking based on key-dependent basis functions," in *Information hiding: second international workshop*, D. Aucsmith, ed., *Lecture notes in computer science* **1525**, pp. 143–157, Springer Verlag, Berlin, Germany, (Portland, OR, USA), Apr. 1998.
15. T. Kalker, J.-P. Linnartz, G. Depovere, and M. Maes, "On the reliability of detecting electronic watermarks in digital images," in *Proceedings of the 9th European Signal Processing Conference, EUSIPCO '98*, pp. 13–16, (Island of Rhodes, Greece), Sept. 1998.
16. J. Fridrich, "Key-dependent random image transforms and their applications in image watermarking," in *Proceedings of the 1999 International Conference on Imaging Science, Systems, and Technology, CISST '99*, pp. 237–243, (Las Vegas, NV, USA), June 1999.
17. J. R. Kim and Y. S. Moon, "A robust wavelet-based digital watermark using level-adaptive thresholding," in *Proceedings of the 6th IEEE International Conference on Image Processing, ICIP '99*, p. 202, (Kobe, Japan), Oct. 1999.
18. J. Schneid and S. Pittner, "On the parametrization of the coefficients of dilation equations for compactly supported wavelets," *Computing* **51**, pp. 165–173, May 1993.
19. H. Zou and A. H. Tewfik, "Parametrization of compactly supported orthonormal wavelets," *IEEE Transactions on Signal Processing* **41**, pp. 1423–1431, Mar. 1993.
20. P. Meerwald and A. Uhl, "Watermark security via wavelet filter parametrization," in *Proceedings of the IEEE International Conference on Image Processing (ICIP'01)*, **3**, pp. 1027–1030, IEEE Signal Processing Society, (Thessaloniki, Greece), Oct. 2001.
21. W. Dietl, P. Meerwald, and A. Uhl, "Watermark security via high-resolution wavelet filter parametrization," in *Proceedings of 7th International Scientific Conference, Section 1: Applied Mathematics*, K. Stanislav and P. Miron, eds., pp. 21–28, (Košice, Slovakia), May 2002.
22. A. Cohen, "Non-stationary multiscale analysis," in[24], pp. 3–12, Academic Press, 1994.
23. A. Uhl, "Image compression using non-stationary and inhomogeneous multiresolution analyses," *Image and Vision Computing* **14**(5), pp. 365–371, 1996.
24. C. Chui, L. Montefusco, and L. Puccio, *Wavelets: Theory, Algorithms and Applications*, Academic Press, San Diego, 1994.