Watermark Security via Secret Wavelet Packet Subband Structures

Werner Dietl and Andreas Uhl

Dept. of Scientific Computing, University of Salzburg,
Jakob-Haringer-Str. 2, A-5020 Salzburg, Austria
{wdietl,uhl}@cosy.sbg.ac.at

Abstract. Wavelet packet decompositions generalize the classical pyramidal wavelet structure. We use the vast amount of possible wavelet packet decomposition structures to create a secret wavelet domain and discuss how this idea can be used to improve the security of watermarking schemes. Two methods to create random wavelet packet trees are discussed and analyzed. The security against unauthorized detection is investigated. Using JPEG and JPEG2000 compression we assess the normalized correlation and Peak Signal to Noise Ratio (PSNR) behavior of the watermarks. We conclude that the proposed systems show improved robustness against compression and provide around 2^{1046} possible keys. The security against unauthorized detection is greatly improved.

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 [1,2,3,4,5].

Over the last several years wavelet analysis was developed as a new method to analyze signals [6,7,8]. 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 pyramidal wavelet decomposition recursively decomposes only the approximation subband. The wavelet packet decomposition does not have this limitation and allows further decomposition of all subbands. There are special algorithms to select the best decomposition for a specific input. For an introduction to wavelet packets and the best basis algorithm see [7].

A. Lioy and D. Mazzocchi (Eds.): CMS 2003, LNCS 2828, pp. 214–225, 2003.

Wavelet packets have not found too much attention in the watermarking community yet. Wang [12] uses one non-standard decomposition to embed a watermark sequence in the middle frequencies of an image. The algorithm by Tsai [13] uses wavelet packets, but the selection is not specified and no experimental results are provided. One interesting approach is used by Vehel in [14]. The wavelet decomposition structure itself is used as the watermark sequence.

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 [15] or Kundur [16], but skipping significant coefficients reduces the capacity of the systems. Fridrich [17] 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 domain, Fridrich's algorithm can better withstand attacks such as those described by Kalker [18] 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 [19]. Parametrized wavelet filters were proposed in [20,21] to improve the security of wavelet based watermarking systems.

In this paper we propose to embed the watermark sequence using a secret wavelet decomposition and to use the decomposition structure as embedding key. This protects wavelet-based watermarks against unauthorized detection — the watermark should only be detectable using the specific wavelet decomposition that was used for embedding. Section 2 describes the details of our proposed system. Then in sections 3 and 4 we assess the security against unauthorized detection and the behavior under JPEG and JPEG2000 compression. We finish the paper with the conclusions in section 5.

2 Proposed Method

Our system is based on the Wang algorithm proposed in [15]. In the paper the authors already suggest to keep the wavelet decomposition structure secret, but no further details or experimental results are provided.

The basic system design is shown in Fig. 1. For the forward wavelet transformation we use a secret wavelet packet tree and then embed the watermark in the generated wavelet coefficients. After embedding the watermark we apply the inverse transformation using the same wavelet packet tree to generate the watermarked image.

The Wang algorithm embeds the watermark sequence based on Successive Subband Quantization (SSQ), which has been developed by the same authors [22,23], and is used in the Multi-Threshold Wavelet Codec (MTWC). Within a selected subband all unselected coefficients $C_s(x,y)$ that are larger than a threshold T_s are used to embed a watermark element W_k according to

$$C'_{s,k}(x,y) = C_s(x,y) + \alpha_s \beta_s T_s W_k \quad . \tag{1}$$

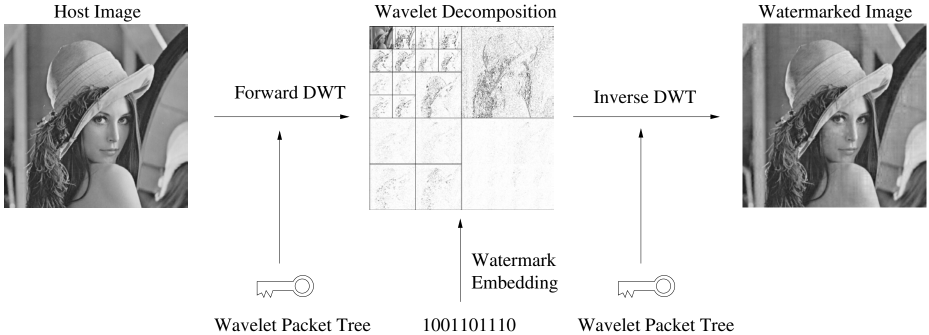


Fig. 1. Basic system design

The two factors α_s and β_s are used to determine the embedding strength of the algorithm.

The wavelet packet tree is generated by a random process that depends on a secret seed number. In the following we will also call this seed number either simply key or tree number. Two tree numbers that are close together do not necessarily generate similar trees.

We select a tree number and create a random wavelet packet tree using that number. This tree number is kept secret and is later needed to extract the watermark. When it is time to detect the watermark we use the secret tree number to generate the same wavelet packet tree again and extract the watermark sequence. Then we apply a normalized correlation calculation to the embedded and the extracted sequences and determine the likeliness that a watermark was embedded.

There is a vast number of possible wavelet packet trees. According to [24], for a decomposition with n+1 levels there are

$$f(n) = \sum_{i=0}^{4} \binom{4}{i} \cdot (f(n-1))^i \tag{2}$$

possible trees ($f(0) = 1$). For 4 decomposition levels this results in around 2^{65} trees and for 7 levels around 2^{4185} trees are possible.

For all decompositions we use the standard Biorthogonal 7/9 filter.

2.1 Generation of Tree Decompositions

We have three parameters that influence the tree decomposition: the tree number, the number of decomposition levels and the decomposition method. We implemented two methods to randomly construct a tree. The first method randomly decomposes the subbands and the second one puts more focus on decomposing middle frequencies.

Random Tree Decomposition 1. For this method we initialise a random number generator with the tree number as seed and then use a 50% probability for each subband to decide whether it should be further decomposed or not.

This decomposition strategy gives us the full range of possible decomposition trees, but could also result in trees that are generally not good for watermark embedding. For example, if the generated tree only applies decompositions to the detail subbands on all levels, then we are likely to embed the watermark in a high frequency domain which is more sensitive to image compression.

Random Tree Decomposition 2. We developed this decomposition specifically for our watermarking system. The focus is on building a wavelet tree that has a good resolution of the middle and low frequencies, which are best suited for watermark embedding. No decomposition of the three detail subbands on the first level (HL_1, LH_1 and HH_1) is performed, only the first approximation subband is further decomposed. Therefore, more emphasis is put on decomposing in the middle frequencies.

Using this decomposition strategy we basically loose all the trees that are below the three top-level detail subbands. Therefore we have only around 83521 trees for 4 levels, but still around 2^{1046} trees for 7 levels.

2.2 Embedding Variations

From the security analysis we learn that common subtrees can happen and can result in high correlation even for wrong tree numbers (see section 3, Figs. 2 and 3). To protect against this problem we implemented two embedding variations that add another dependency on the tree number. Then two trees can have a common subtree, but through the embedding variation there are still enough differences between the two watermarks to make the system secure.

Both embedding variations can also be used with the standard watermarking system. Instead of using the tree number again as seed for the embedding variation we could use another number and use it as additional key element. But to limit the complexity of our analysis we simply reuse the tree number for the embedding variations.

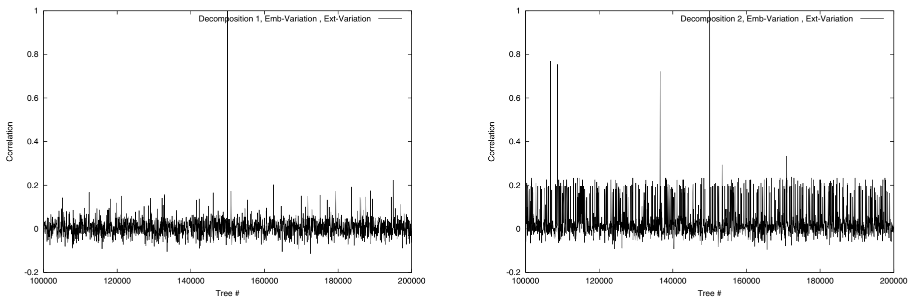
Variation 1 — Tree-Dependent Coefficient Skipping. This first variation skips a part of the selected significant coefficients, as proposed by Wang [15]. We use 95% of the coefficients that are selected. The disadvantage of coefficient skipping could be reduced robustness to compression and reduced capacity. We expect that using 95 percent of the coefficient results in very good robustness results and does not limit the capacity too severely.

Variation 2 — Tree-Dependent Watermark Shuffling. The second variation creates a permutation of the watermark sequence before we embed it into the wavelet coefficients. Depending on the tree number we shuffle the elements of the watermark and then embed them into the selected wavelet coefficients. This variation should not have an influence on the robustness or capacity of the watermark, because we select the same coefficients for embedding.

3 Security Assessment

For the security assessment we embed a 1000 element watermark with 40dB PSNR into the Lena image. We use the tree that is generated by the tree number 150000 for embedding and then use a set of keys with which we try to detect the watermark. The set starts at 100000 and goes up to 200000 in increments of 50 — giving 2001 measurements. We also compare the behavior for 4 and 7 decomposition levels.

Besides showing the effect of using the wrong key to extract the watermark we also look at the effect of using the wrong variation. When we embed the watermark with one of the variations we only want to be able to successfully extract the watermark with that variation.

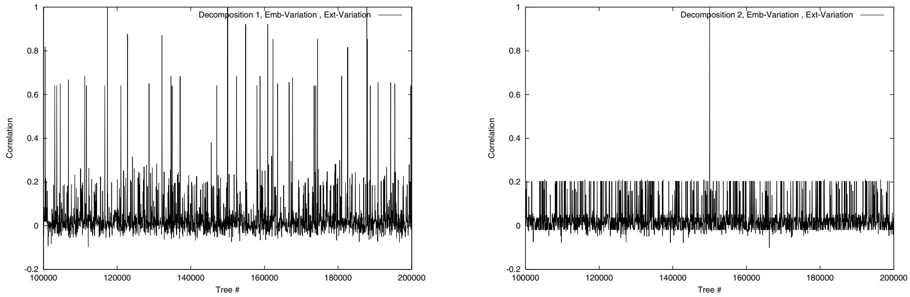


(a) Decomposition 1 (b) Decomposition 2

Fig. 2. Security assessment with 7 levels and without embedding variation

Fig. 2 compares the response for decomposition 1 and 2 with 7 decomposition levels without an embedding variation. For decomposition 1 there is one clear peak at 150000 and low correlation for all other tree numbers. But for decomposition 2 there is one peak at 150000 and also three other tree numbers with more than 60 percent correlation. There are also many other tree numbers with a correlation of around 0.20.

Because for decomposition 2 we do not allow decompositions at the top level and also have a different probability distribution at the lower levels we have more common subtrees than in decomposition 1. This leads to more common sequences in different trees and therefore to higher correlation for the wrong

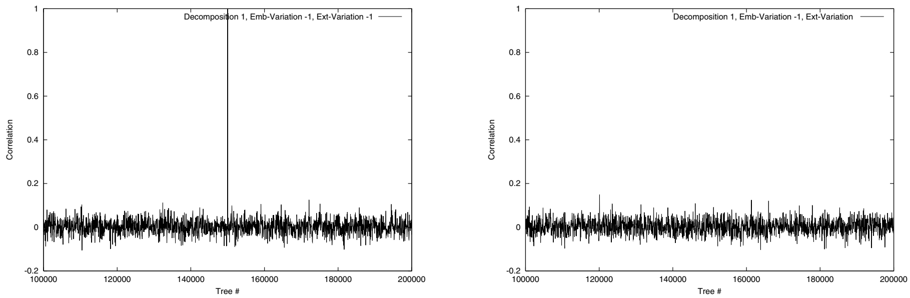


(a) Decomposition 1 (b) Decomposition 2

Fig. 3. Security assessment with 4 levels and without embedding variation

extraction parameters. If two trees are very similar this will lead to the high correlation we see at the three additional peaks in Fig. (b).

In Fig. 3 we compare the behavior if only 4 decomposition levels are used. Here we see that also decomposition 1 can create many common subtrees that lead to high correlation for wrong tree numbers. For decomposition 2 there are many trees with a correlation of around 0.20. The reason for this exact behavior is unknown at the moment.



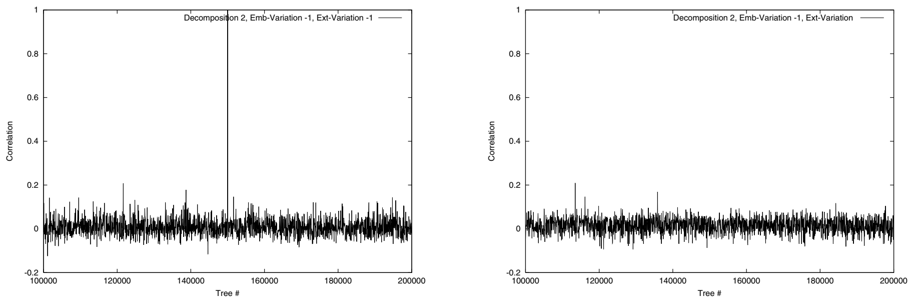
(a) Correct Extraction (b) Incorrect Extraction

Fig. 4. Effect of skipping some coefficients with decomposition 1 and 7 levels

These result were the reason why we introduced the two embedding variations. Different coefficients should be modified or the same coefficients should be modified in a different way, even if common subtrees happen. We implemented the two tree-number-dependent embedding variations described earlier to add this feature. Decomposition 1 with a 7 level decomposition has a lower likeliness of common subtrees and can be used without a variation. But decomposition 2 with 7 levels and both decompositions with only 4 decompositions need one or both of the variations to protect against common subtrees.

In Fig. 4 we see the effect of embedding variation one — skipping some coefficients — in combination with decomposition 1 with 7 levels. There is again one clear peak and the correlation of wrong tree numbers was further decreased.

In Fig. (b) we see what happens when we do not use variation 1 for watermark extraction. There is low correlation for all tree numbers and the watermark is not found.



(a) Correct Extraction

(b) Incorrect Extraction

Fig. 5. Effect of variation 1 on decomposition 2 with 7 levels

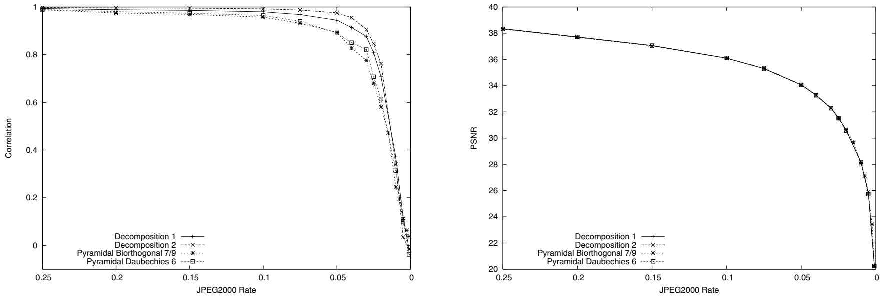
In Fig. 5 we see the effect of variation 1 on decomposition strategy 2 with 7 levels. There is only one peak for the correct tree number and the correlation for the wrong trees is reduced. The introduction of the embedding variations makes decomposition 2 a useable system.

Fig. (b) shows the result when the wrong extraction variation is used. Again there is very low correlation for all tree numbers and the correct tree number can not be found. This shows that the embedding variations can also be used to further increase the security of the watermark.

4 Quality Assessment

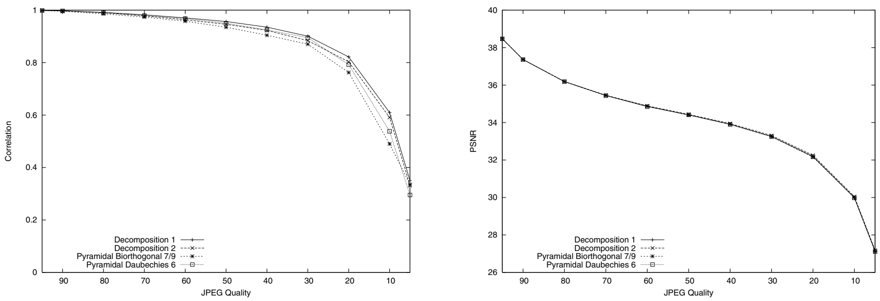
For the quality assessment we embed a watermark with 40dB PSNR and compress the watermarked image with JPEG and JPEG2000. We then try to detect the watermark in the compressed image and measure the correlation. As a measure of the distortion we use the PSNR of the compressed image.

To get a good variation of different trees we use tree numbers from 100000 to 200000 with increments of 400. From all those 251 measurements we calculate the average, maximum and minimum correlation and PSNR.



(a) Correlation (b) PSNR

Fig. 6. Comparison of the proposed systems with the standard systems under JPEG2000 compression



(a) Correlation (b) PSNR

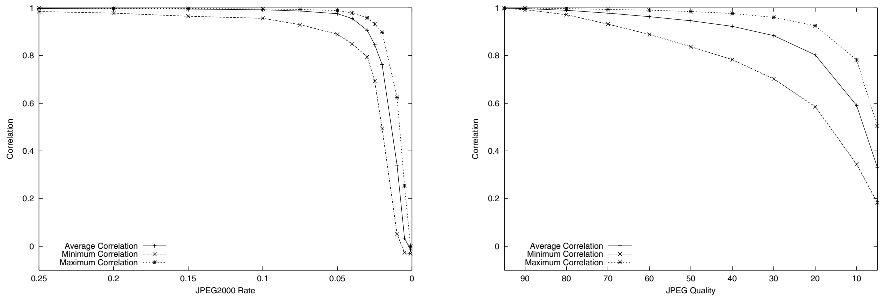
Fig. 7. Comparison of the proposed systems with the standard systems under JPEG compression

We compare tree decomposition 1 and 2 and expect that tree decomposition 2 will have better results for higher compression rates. The results of the wavelet packet methods are compared with the standard Wang watermarking system using the Daubechies 6 and the Biorthogonal 7/9 filters.

With more subband decompositions we expect that it will be possible to embed longer watermark sequences compared to the pyramidal decomposition. To see whether this is true we analyze the image quality with watermark lengths 1000, 5000 and 20000.

Figs. 6 and 7 show the compression behavior of the two different wavelet packet decompositions in comparison with the standard system with the Biorthogonal 7/9 and the Daubechies 6 filters.

In Fig. 6(a) we see the correlation behavior under JPEG2000 compression. The performance of decomposition 2 is superior to all other systems and the wavelet packet system with decomposition 1 is also better than the two standard systems.



(a) JPEG2000 Correlation

(b) JPEG Correlation

Fig. 8. Details for tree decomposition 2

Fig. 7(a) shows the JPEG compression results. In this case the difference is smaller than under JPEG2000 compression. The decomposition 1 system performs slightly better than decomposition 2 and both wavelet packet systems are above the standard decompositions.

The results for the PSNR performance are shown in Figs. 6(b) and 7(b). All systems behave very similarly without a significant difference. Therefore we will not show further PSNR results.

Fig. 8 gives a close look at the results for decomposition 2. This diagram shows the average, minimum and maximum correlation behavior under compression. The minimum correlation behavior is still very good and the average is closer to the maximum.

Figs. 9 and 10 compare the performance of decompositions 1 and 2 with 7 decomposition levels for watermarks of length 1000, 5000 and 20000. We see that under JPEG2000 compression decomposition 2 is the better system for all watermark lengths. The advantage of decomposition 2 gets bigger for longer watermarks. Fig. 10 shows the results under JPEG compression. For a watermark of length 1000 decomposition 1 has a slight advantage, but for lengths 5000 and 20000 decomposition 2 is clearly the better system. In comparison to the pyramidal decomposition the wavelet packet systems clearly have a higher robustness to compression.

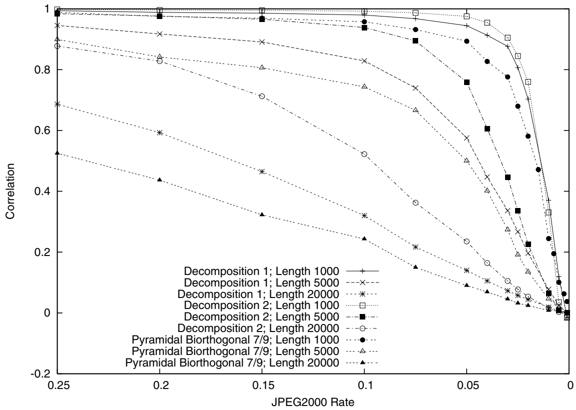


Fig. 9. Correlation comparison under JPEG2000 compression

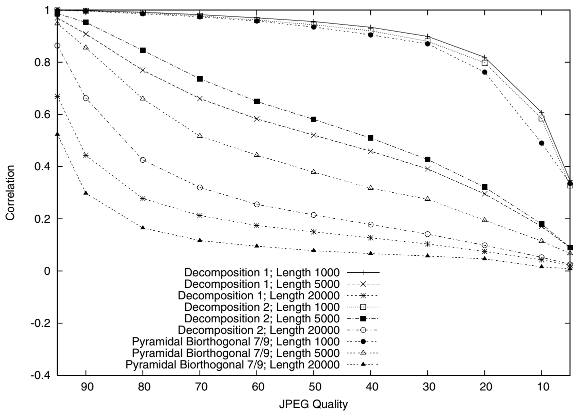


Fig. 10. Correlation comparison under JPEG compression

Decomposition 1 with 7 levels shows good security properties even without embedding variation and good robustness for a 1000 element watermark. For longer watermark lengths decomposition 2 has significantly better robustness results, but one of the embedding variations should be used to guard against common subtrees.

5 Conclusions

In this paper we described how the wavelet packet decomposition can be used to enhance the security of wavelet-based watermarking systems. We use the Wang coefficient selection method and propose two methods for generating random trees. The first method uses a 50% probability of decomposition for all subbands. The second method does not decompose the detail subbands on the first level and puts more emphasis on decomposing in the low and middle frequency range. The seed for the random number generator is used as key and is kept secret. For 7 decomposition levels we have 2^{4185} or 2^{1046} possible tree decompositions for the first and the second decomposition method, respectively. We also introduced two methods to protect against common subtrees that can result in higher correlation even for the wrong tree number.

Both the security and the quality assessment show that the wavelet packet systems show better performance than the standard pyramidal system. Decomposition 1 can be used without embedding variation for 1000 element watermarks. Decomposition 2 has higher robustness for long watermarks and clearly outperforms the pyramidal decomposition.

Overall we conclude that a random tree decomposition that focuses on the low and middle frequency range and uses either coefficient skipping or watermark shuffling results in a robust and secure watermarking system.

Acknowledgments. Parts of this work were funded by the Austrian Science Fund FWF projects P15170 "Sicherheit für Bilddaten in Waveletdarstellung" and P13732 "Objekt-basierte Bild- und Videokompression mit Wavelets".

References

1. Katzenbeisser, S., Petitcolas, F.A.P.: Information Hiding Techniques for Steganography and Digital Watermarking. Artech House (1999)
2. Dittmann, J., ed.: Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete. Springer Verlag (2000)
3. Johnson, N.F., Duric, Z., Jajodia, S.: Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Kluwer Academic Publishers (2000)
4. Cox, I.J., Miller, M.L., Bloom, J.A.: Digital Watermarking. Morgan Kaufmann (2002)
5. Eggers, J.J., Girod, B.: Informed Watermarking. Kluwer Academic Publishers (2002)
6. Daubechies, I.: Ten Lectures on Wavelets. Number 61 in CBMS-NSF Series in Applied Mathematics. SIAM Press, Philadelphia, PA, USA (1992)
7. Wickerhauser, M.: Adapted wavelet analysis from theory to software. A.K. Peters, Wellesley, Mass. (1994)
8. Mallat, S.: A wavelet tour of signal processing. Academic Press (1997)
9. ISO/IEC JPEG committee: JPEG 2000 image coding system — ISO/IEC 15444-1:2000 (2000)
10. Taubman, D., Marcellin, M.: JPEG2000 — Image Compression Fundamentals, Standards and Practice. Kluwer Academic Publishers (2002)

11. Meerwald, P., Uhl, A.: A survey of wavelet-domain watermarking algorithms. In Wong, P.W., Delp, E.J., eds.: Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III. Volume 4314., San Jose, CA, USA, SPIE (2001)
12. Wang, Y., Doherty, J.F., Dyck, R.E.V.: A wavelet-based watermarking algorithm for copyright protection of digital images. IEEE Transactions on Image Processing **11** (2002) 77–88
13. Tsai, M.J., Yu, K.Y., Chen, Y.Z.: Wavelet packet and adaptive spatial transformation of watemark for digital image authentication. In: Proceedings of the IEEE International Conference on Image Processing, ICIP '00, Vancouver, Canada (2000)
14. Levy-Vehel, J., Manoury, A.: Wavelet packet based digital watermarking. In: Proceedings of the 15th International Conference on Pattern Recognition, Barcelona, Spain (2000)
15. Wang, H.J., Kuo, C.C.J.: Watermark design for embedded wavelet image codec. In: Proceedings of the SPIE's 43rd Annual Meeting, Applications of Digital Image Processing. Volume 3460., San Diego, CA, USA (1998) 388–398
16. Kundur, D.: Improved digital watermarking through diversity and attack characterization. In: Proceedings of the ACM Workshop on Multimedia Security '99, Orlando, FL, USA (1999) 53–58
17. Fridrich, J., Baldoza, A.C., Simard, R.J.: Robust digital watermarking based on key-dependent basis functions. In Aucsmith, D., ed.: Information hiding: second international workshop. Volume 1525 of Lecture notes in computer science., Portland, OR, USA, Springer Verlag, Berlin, Germany (1998) 143–157
18. Kalker, T., Linnartz, J.P., Depovere, G., Maes, M.: 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 (1998) 13–16
19. Fridrich, J.: 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, Las Vegas, NV, USA (1999) 237–243
20. Meerwald, P., Uhl, A.: Watermark security via wavelet filter parametrization. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'01). Volume 3., Thessaloniki, Greece, IEEE Signal Processing Society (2001) 1027–1030
21. Dietl, W., Meerwald, P., Uhl, A.: Key-dependent pyramidal wavelet domains for secure watermark embedding. In Delp, E.J., Wong, P.W., eds.: Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents V. Volume 5020., Santa Clara, CA, USA, SPIE (2003)
22. Wang, H.J., Bao, Y.L., Kuo, C.C.J., Chen, H.: Multi-threshold wavelet codec (MTWC). Technical report, Derpartment of Electrical Engineering, University of Southern California, Los Angeles, CA, USA, Geneva, Switzerland (1998)
23. Wang, H.J., Kuo, C.C.J.: High fidelity image compression with multithreshold wavelet coding (MTWC). In: SPIE's Annual meeting - Application of Digital Image Processing XX, San Diego, CA, USA (1997)
24. Pommer, A., Uhl, A.: Selective encryption of wavelet packet subband structures for secure transmission of visual data. In Dittmann, J., Fridrich, J., Wohlmacher, P., eds.: Multimedia and Security Workshop, ACM Multimedia, Juan-les-Pins, France (2002) 67–70