Key-Dependency for a Wavelet-Based Blind Watermarking Algorithm

Michael Brachtl and Andreas Uhl
Department of Scientific Computing
University of Salzburg
5020 Salzburg, Jakob Haringer Str. 2
Austria
{mbrachtl,uhl}@cosy.sbg.ac.at

Werner Dietl
Software Component Technology Group,
Department of Computer Science
ETH Zürich
ETH Zentrum, RZ J8, 8092 Zürich
Switzerland
dietlw@inf.ethz.ch

ABSTRACT

When a host image is watermarked multiple times by the same algorithm collisions can occur. This makes it difficult for an image to host multiple watermarks. But this hosting is necessary for an image distribution chain, where several persons all watermark the same image. Wavelet domain transformations provide several possibilities to customize the transformation process. We discuss the applicability of the methods of wavelet filter parametrization and wavelet packet decomposition for secret watermark embedding on the algorithm of Dugad et al. We conclude that filter parametrization is not suited while wavelet packet decomposition shows good results.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Intellectual property rights—*Digital Watermarking*; I.4.0 [**Image Processing and Computer Vision**]: General—*Image Processing Software*

General Terms

Security

Keywords

Blind watermarking, wavelet packets, parameterized wavelet filters, multiple watermarking

1. INTRODUCTION

Watermarking of digital media content has gained high popularity as a method to protect intellectual property rights of content owners. Blind watermarking techniques can perform detection of the watermark without use of the original image.

MM&Sec'04, September 20-21, 2004, Magdeburg, Germany.

To provide a copy of the unwatermarked image for every detector would be contrary to the idea of a lot of applications - e.g. proof of ownership.
In the following we will be concerned with a method potentially enabling multiple watermarks - several watermarks embedded by the same algorithm into the same host image - and the suitability of the investigated algorithm for this purpose.
We propose the use of wavelet filter parametrization and wavelet packet decomposition as a method to provide key-dependency to a blind watermarking algorithm as a means to enable multiple watermarking without collisions. In section 2 we discuss the idea and the requirements of a system for multiple watermarks and show the application of the methods described in section 3 and 4. In these sections we analyse the suitability of the algorithm by Dugad et al.[6] for the proposed methods, followed by conclusions in section 5.

2. MULTIPLE WATERMARKING

Blind watermarking is best suited to implement the idea of multiple watermarks for distribution chains. In contrast to [9] where the embedding of different classes of watermarks is discussed, we want a host image to carry several watermarks of the same algorithm.
Such a system would enable all copyright holders of an image to add their custom watermark in the sense of fingerprinting, i.e. with different content - e.g. the producer, the music creator, the distributer and the retailer of a movie. Each embedding process is controlled by a secret personal key, resulting in a multiple watermarked image where each mark is detectable with the corresponding key only. Figure 1 shows the concept, using the later described method of wavelet packet decomposition.

We want a distribution chain watermarking application to have the following characteristics:

1. A arbitrary watermark can be added to the host image at any time.
2. If the host image contains a watermark M_i, it is detectable at any time without knowledge of other contained watermarks.
3. For embedding and detection of a certain watermark M_i, the corresponding key K_i has to be known.

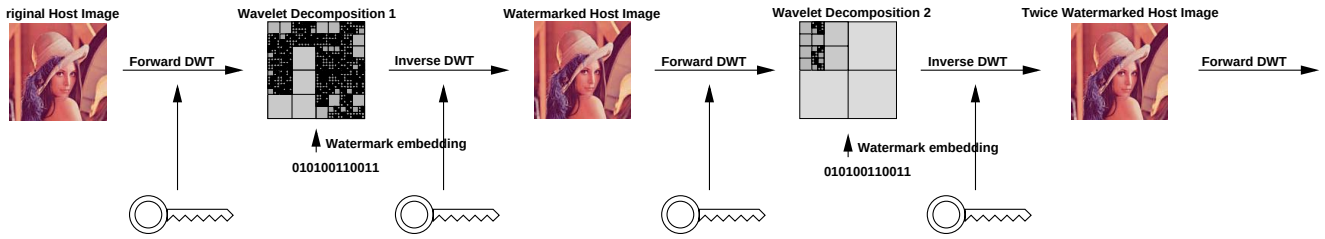


Figure 1: Basic System Design for wavelet packets, similar for filter parametrization

To meet the second requirement, a system with a non-blind algorithm would have to provide the collection of the i different unwatermarked host images to detect i different watermarks. Beside the mentioned problem of providing an unwatermarked copy, this would result in an increased file size of the watermarked image by factor $1+i$, since a detection process requires access to all i unwatermarked images, i.e. these i images have to be stored additionally.
The following classification of multiple watermarking algorithms into three groups has been given [11]: re-watermarking, segmented watermarking and composite watermarking. Re-watermarking is the most obvious method of multiple watermarking where the watermarks are just added one after the other. In segmented watermarking the space available for watermarking is divided between the watermarks, e.g. square blocks for spatial domain watermarking. Composite watermarking builds a single composite watermark from a collection of watermarks.
The last group of watermarking algorithms does not meet the requirement (1), since all watermarks have to be known in advance. Our proposed method is of the type of re-watermarking, but due to the different wavelet transformations where the watermark is embedded, it implicitly is a kind of segmented watermarking also.

In order to establish key-dependency, we apply two methods which have been successfully used for secret embedding with non-blind algorithms [7, 12, 14] - filter parametrization [2, 3, 8] and wavelet packet decomposition [4, 5].

2.1 The Algorithm by Dugad et al.

The blind watermarking algorithm used throughout this work is due to Dugad et al.[6]. The algorithm operates in the wavelet domain, adding the watermark to the significant coefficients only.
Embedding:

- Watermark is embedded into all subbands except the low pass subband.
- Choose a threshold T_1.
- Mark all coefficients $K_i \geq T_1$ with $K_i' = K_i + \alpha |K_i| x_i$, where x_i is the watermark at position i.

Detection:

- Select $T_2 \geq T_1$. (Implementation: $T_2 = 1.2 * T_1$)
- Select all coefficients $\geq T_2$. Number: M. $z = \frac{1}{M} \sum_i K_i' x_i$ where K' is the coefficient and x_i is the watermark at position i.
- Calculate threshold S: $S = \frac{\alpha}{2M} \sum_i |K'|$.
- If $z \geq S$ the watermark is detected, otherwise not.

Since the algorithm does not return a correlation-coefficient between 0 and 1 like other watermarking algorithms, we do our evaluation based on the value z/S. So if $z/S \geq 1$ the watermark exists, otherwise not. This not only allows us to compare the results of different watermarks but also enhances the algorithm, since it provides a measurement for the strength of the detected watermark.

3. FILTER PARAMETRIZATION

Wavelet filters can be parametrized to create an entire family of different wavelet filters. We propose to decompose the host image with a DWT using this parametrized filters, embed the watermark and apply the inverse transformation. The parameter values used for construction are kept secret, so the watermark is embedded in a secret multi-resolution transform domain.

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

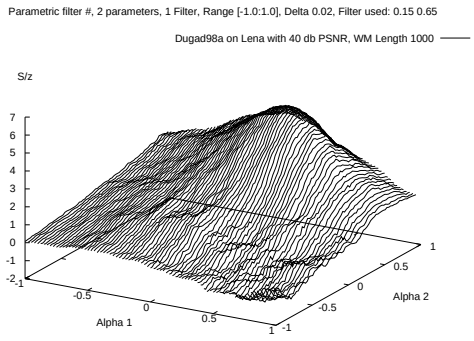
$$\phi(t) = \sum_{k \in Z} c_k \phi(2t - k),$$

with $c_k \in R$, have to be derived, satisfying two conditions on the coefficients c_k [1]. Schneid [10] describes a parametrization for suitable coefficients c_k based on the work of Zou [15] to facilitate construction of such wavelets. Given N parameter values $-\pi \leq \alpha_i < \pi$, $0 \leq i < N$, the recursion

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

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 $k \geq 2N+2$.

Since we hope to use the parameter values α_i as a secret key there should be no correlation in a detection process that uses the wrong parameters. We embed a watermark in the well known picture 'Lena' with an embedding strength that results in 40 dB PSNR. Then we try to detect the mark while we vary the parameters of the filter.
In previous work [2, 8] one clear peak for the correct parameters can be realized although there are also some other higher correlations in close proximity. Dietl et al are able to realise a meaningful resolution of $5 * 10^{-4}$ for the values of the parameters in their work on non-blind additive algorithms. Contrasting to these results, parameterization has found not to be suited for non-blind quantization based watermarking schemes [3].



(a) 2-dim. parameter space

Figure 2: Detection results using wrong parametrized filters.

Considering the blind additive algorithm considered in this work we notice in Figs. **??** and 2(a) large regions in parameter space centered around the correct parameters which indicate watermark detection. The detection strength decreases continuously, but not very fast. This behaviour is shown for 1 and 2 dimensional parameter spaces.

3.1 Analysis

There is a fundamental difference between the blind algorithm considered here and the non-blind ones used in previous work [2, 3, 8]. The current algorithm does not order the wavelet coefficients by their size. Using slightly wrong filterparameters leads to slightly wrong wavelet coefficients. While this can result in multiplication of the coefficient $C_{x_i y_i}$ with an different watermark value $W_{x_k y_k}$ in order sensitive algorithms, the current algorithm always multiplies the coefficient C_{xy} with its corresponding watermark value W_{xy}. Since wavelet coefficient values are continuously depending on the parameters of the filter, the method of parametrization is not suited to add key-dependency to the blind algorithm proposed by Dugad et al.

4. WAVELET PACKETS

Wavelet Packets [13] represent a generalization of the method of wavelet decomposition. Recursive decomposition is applied not only to the approximation subband, but to all subbands. For the forward wavelet transformation we use a secret wavelet packet tree and embed the watermark in the generated wavelet coefficients. After embedding we apply the inverse transformation using the same wavelet packet tree to generate the watermarked image. The wavelet packet tree is generated by a random process that depends on a secret seed number. We embed a watermark in the well known picture 'Lena' with an embedding strength that results in 40 dB PSNR. Then we try to detect the mark while we vary the following parameters:

1. Tree Decompositions
   First we do a one level decomposition into the HH_1, HL_1, LH_1 and LL_1 subbands. For further levels we use two types of random tree decomposition strategies.
   In Decomposition 1 each subband has a probability of 0.5 to be decomposed.
   In Decomposition 2 each Subband has a probability of 0.9 to be decomposed at the second level. At the third an fourth level the probability is 0.5. At deeper levels the probability is 0.2 for the approximation subband and 0.5 for all others.
   Both decompositions do not limit the number of possible trees but they result in different average decompositions depths (ADD). The average decompositions depths of the both decompositions depending on a maximum decomposition depth can be computed using equation (1) and (2) respectively. We assume an undecomposed image has a decompositions depth of 1.

$$ADD_{D1}(n) = 2 + \sum_{i=0}^{n} 0.5^i \tag{1}$$

$$\begin{aligned} ADD_{D2}(n) &= 2 + 0.9 + 0.9 * 0,5 + 0.9 * 0.5^2 \\ &+ \sum_{i=5}^{n} (0.9 * 0.5^{i-2} * (1 - \frac{1}{4^i}) \\ &+ 0.9 * 0.5^2 * 0.2^{i-4} * \frac{1}{4^i}) \end{aligned} \tag{2}$$

   To give an example, at a maximum of 7 levels decomposition 1 has an expected average depth of 2.98 while decomposition 2 has 3.78. We assume that deeper decompositions are less likely to generate false positive detections of the watermark.

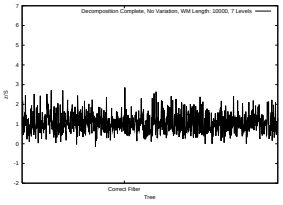
2. Watermark Length
   In general, longer watermarks are more sensitive to attacks, since they are embedded in more small coefficients than a short watermark, which is embedded in major coefficients only. These small coefficients can be attacked more easily. We use the Threshold T_1 in [6] to determine the number of modified wavelet coefficients. Three different thresholds were used to watermark 0.38%, 3.8%, and 76% of the coefficients.

3. Maximum Levels
   This Parameter regulates the maximum decomposition depth. A higher value results in a higher average decomposition depth. For our tests 4 and 7 levels were used.

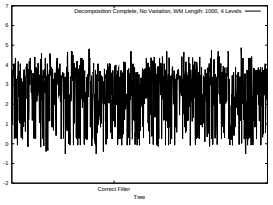
Only a certain subset of the results looks promising with respect to use the method of wavelet packets as key-dependency scheme for the algorithm by Dugad et al. Figs. 3(a) to 3(d) show typical results. While 3(b) shows no clear peak at all, 3(a) at least has its maximum correlation at the correct parameter value (i.e. decomposition structure). Figs. 3(c) and 3(d) look very promising and exhibit a distinct peak at the right decomposition structure.

4.1 Parameter Analysis

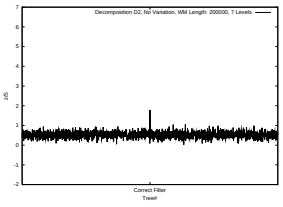
To systematically analyse which parameters have an influence on the quality of the peaks we process the results by the following scheme:
First we classify all values which resulted from the test into two groups differing only by the value of a certain parameter.



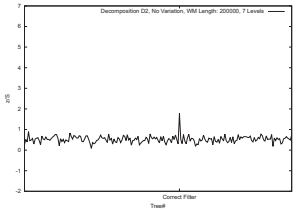
(a) Decomp. 1, 3.8 % mod. coeff., 7 Levels



(b) Decomp. 1, 0.38 % mod. coeff., 4 Levels



(c) Decomp. 2, 76 % mod. coeff., 7 Levels

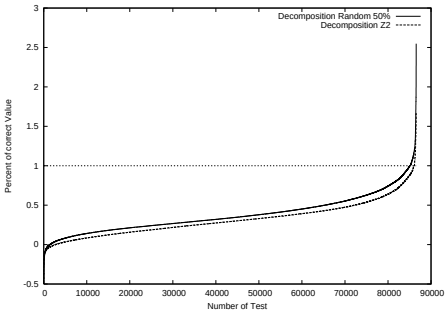


(d) Decomp. 2, 76 % mod. coeff., 7 Levels

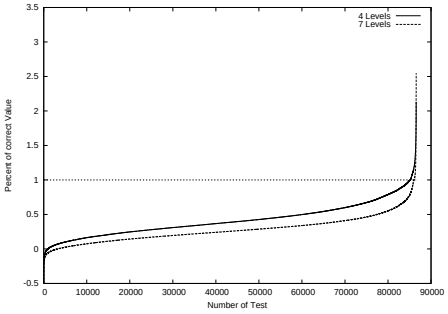
Figure 3: Wrong decompositions compared to correct one

For each value S/z there exists a associated value $S/z_{correct}$, which is the detection strength when we apply the correct decomposition for the host image S/z belongs to.
We then calculate the fraction $p = \frac{S/z}{S/z_{correct}}$.
This will result in $p = 1$ for the correct decomposition and in $p \leq 1$ for wrong decompositions. Unfortunately there are also $p \geq 1$ which means that a certain decomposition yields to a detection, although it is incorrect (i.e. false positives). Finally we order the fraction values by their size and look at the resulting graph. A lower graph indicates that the single fractions are lower on the average, meaning the peaks are better distinguishable.

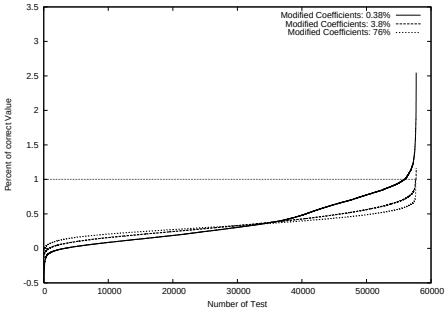
It can be seen clearly that all three parameters have an influence on the quality of the peaks. Decomposition strategy 2 (leading to a larger number of "deep" decomposition structures) and a higher value for the maximal decomposition depth are shown to give superior results in Figs. 4(a) and 4(b). The results in Fig. 4(c) also show the importance of the watermark length (e.g. the number of modified coefficients). While 0.38% and 3.8% are too few modified coefficients, 76% modified coefficients yield good results.
To get an idea of the necessary number of modified coefficients, at which the peaks are clearly distinguishable from values of S/z of incorrect decompositions, we took three different decompositions at random and looked at their maximum percentage at a wrong decomposition versus the number of modified coefficients. (Figure 5). Here it can be seen that 30000 out of 262144 (11.5 %) modified coefficients are sufficient for a clear peak when we set a threshold ≥ 0.8 of the correct value. For 70000 (27 %) and more modified coefficients a detection threshold ≥ 0.6 is achievable.



(a) Method of decomposition



(b) Maximum decomposition depth



(c) Watermark length

Figure 4: Influence of the parameters on the quality of the peak

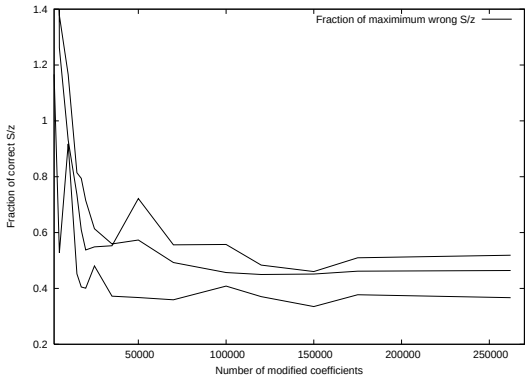


Figure 5: Quality of the peaks versus number of modified coefficients

5. CONCLUSIONS

We showed that key-dependency with wavelet packet decomposition can be successfully achieved when using the blind algorithm by Dugad et al., contrasting to the filter parametrization approach. With wavelet packets no watermark will be detected if the decomposition is unknown. We also showed that the chosen embedding parameters have to satisfy some minimum requirements. If they do, detection results in a clear, distinguishable peak at the correct decomposition parameter value. These are promising results to use the algorithm of Dugad et al. in a multiple watermark system. Future work will focus on detection strength and collision free detection using this algorithm in the context of multiple watermarks.

6. REFERENCES

[1] I. Daubechies. *Ten Lectures on Wavelets*. Number 61 in CBMS-NSF Series in Applied Mathematics. SIAM Press, Philadelphia, PA, USA, 1992.

[2] W. Dietl, P. Meerwald, and A. Uhl. Key-dependent pyramidal wavelet domains for secure watermark embedding. In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents V*, volume 5020, pages 728–739, Santa Clara, CA, USA, Jan. 2003. SPIE.

[3] W. Dietl, P. Meerwald, and A. Uhl. Protection of wavelet-based watermarking systems using filter parametrization. *Signal Processing (Special Issue on Security of Data Hiding Technologies)*, 83:2095–2116, 2003.

[4] W. Dietl and A. Uhl. Watermark security via secret wavelet packet subband structures. In A. Lioy and D. Mazzocchi, editors, *Communications and Multimedia Security. Proceedings of the Seventh IFIP TC-6 TC-11 Conference on Communications and Multimedia Security*, volume 2828 of *Lecture Notes on Computer Science*, pages 214–225, Turin, Italy, Oct. 2003. Springer-Verlag.

[5] W. M. Dietl and A. Uhl. Robustness against unauthorized watermark removal attacks via key-dependent wavelet packet subband structures. In *Proceedings of the IEEE International Conference on Multimedia and Expo, ICME '04*, Taipei, Taiwan, June 2004. To appear.

[6] R. Dugad, K. Ratakonda, and N. Ahuja. A new wavelet-based scheme for watermarking images. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'98)*, Chicago, IL, USA, Oct. 1998.

[7] J. R. Kim and Y. S. Moon. A robust wavelet-based digital watermark using level-adaptive thresholding. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'99)*, page 202, Kobe, Japan, Oct. 1999.

[8] P. Meerwald and A. Uhl. Watermark security via wavelet filter parametrization.

[9] F. C. Mintzer and G. W. Braudaway. If one watermark is good, are more better? In *Proceedings of the 1999 International Conference on Acoustics, Speech and Signal Processing (ICASSP'99)*, volume 4, pages 2067–2070, Phoenix, AZ, USA, Mar. 1999.

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

[11] N. P. Sheppard, R. Safavi-Naini, and P. Ogunbona. On multiple watermarking. In *Proceedings of the 9th ACM Multimedia 2001 Conference*, pages 3–6, Ottawa, Ontario, Canada, Sept. 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*, volume 3460, pages 388–398, San Diego, CA, USA, July 1998.

[13] M. Wickerhauser. *Adapted wavelet analysis from theory to software*. A.K. Peters, Wellesley, Mass., 1994.

[14] X.-G. Xia, C. G. Boncelet, and G. R. Arce. Wavelet transform based watermark for digital images. *Optics Express*, 3(12):497, Dec. 1998.

[15] H. Zou and A. H. Tewfik. Parametrization of compactly supported orthonormal wavelets. *IEEE Transactions on Signal Processing*, 41(3):1423–1431, Mar. 1993.

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability