Robustness and Security of Wavelet-Based Watermarking Algorithms

Peter Meerwald,
pmeerw@cosy.sbg.ac.at

May 9, 2000

Several wavelet-based watermarking schemes and their robustness to wavelet compression attacks are discussed. Following an idea by Fridrich [3] and experiments by Kundur [8], we propose to use a parametrization of wavelet filter coefficients to bring the concept of a key-dependent transform to the wavelet domain. We demonstrate that the new technique can be easily intregrated in existing watermarking algorithms to improve security.

Model of the Watermarking Process

1. generation of a watermark W (a binary or pseudo-random sequence)

2. embedding the watermark in a host image I

   (a) transform image to a domain suitable for watermarking
   (b) modify significant coefficients to embed watermark
   (c) inverse transformation

3. circulation of the watermarked image, possible friendly (e.g. image processing, compression) and unfriendly attacks

4. extraction of the watermark $W^\star$ (blind or with utilization of the original image)

5. normalized watermark correlation

$$\delta = \frac{W^\star \cdot W}{\|W^\star\| \cdot \|W\|}$$

Watermarking in the Wavelet Domain

Xia [14] identified several advantages of watermarking in the wavelet domain:

- multiresolution characteristics, hierarchical
- superior modelling of the human visual system (HVS)
- locality
- computational efficiency

Charrier [1] outlines new requirements for the wavelet-based JPEG2000 compression standard:

- coding performance
- progressive transmission, ROI coding, scalability
- security, see `http://eurostill.epfl.ch/~ebrahimi/JPEG2000.htm`

Kim's Algorithm

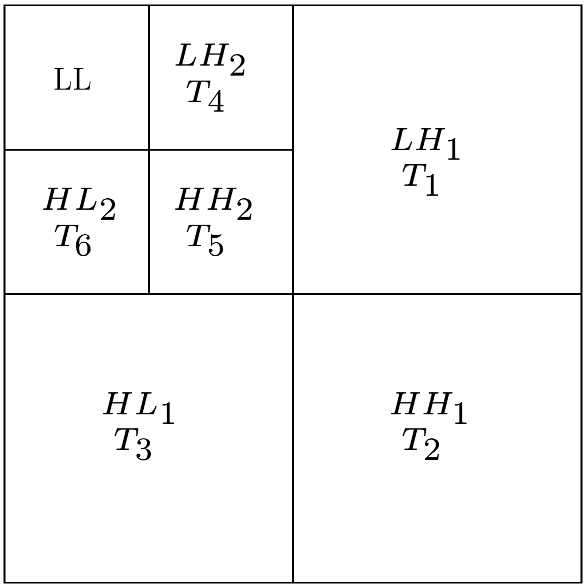
Kim [6] uses level-adaptive thresholding to embed a Gaussian distributed pseudo-random sequence in significant coefficients, similar to Cox [2]

PSNR 38.57

Wang's Algorithm

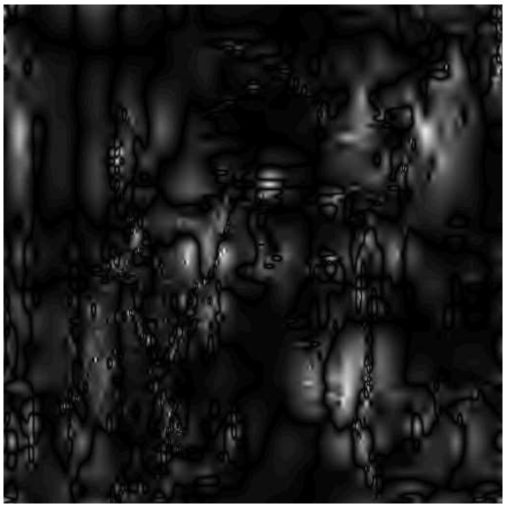
Wang [12] based on MTWC coder [11], similar to Kim

PSNR 33.28



T_s ... initial subband threshold
approximation subband (LL) not used

$T_s = \beta_s * max_s(f_s(m,n))/2$
β_s ... weighting factor for subband s
$max_s(f_s(m,n))$ ... max. coefficient in subband s

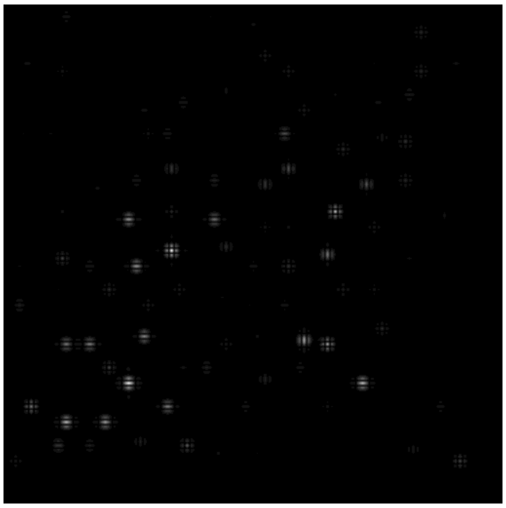



Kundur's Algorithm

Kundur [7] is quantizing the median of (LH_l, HL_l, HH_l) coefficient triples to encode a bit, l is the decomposition level

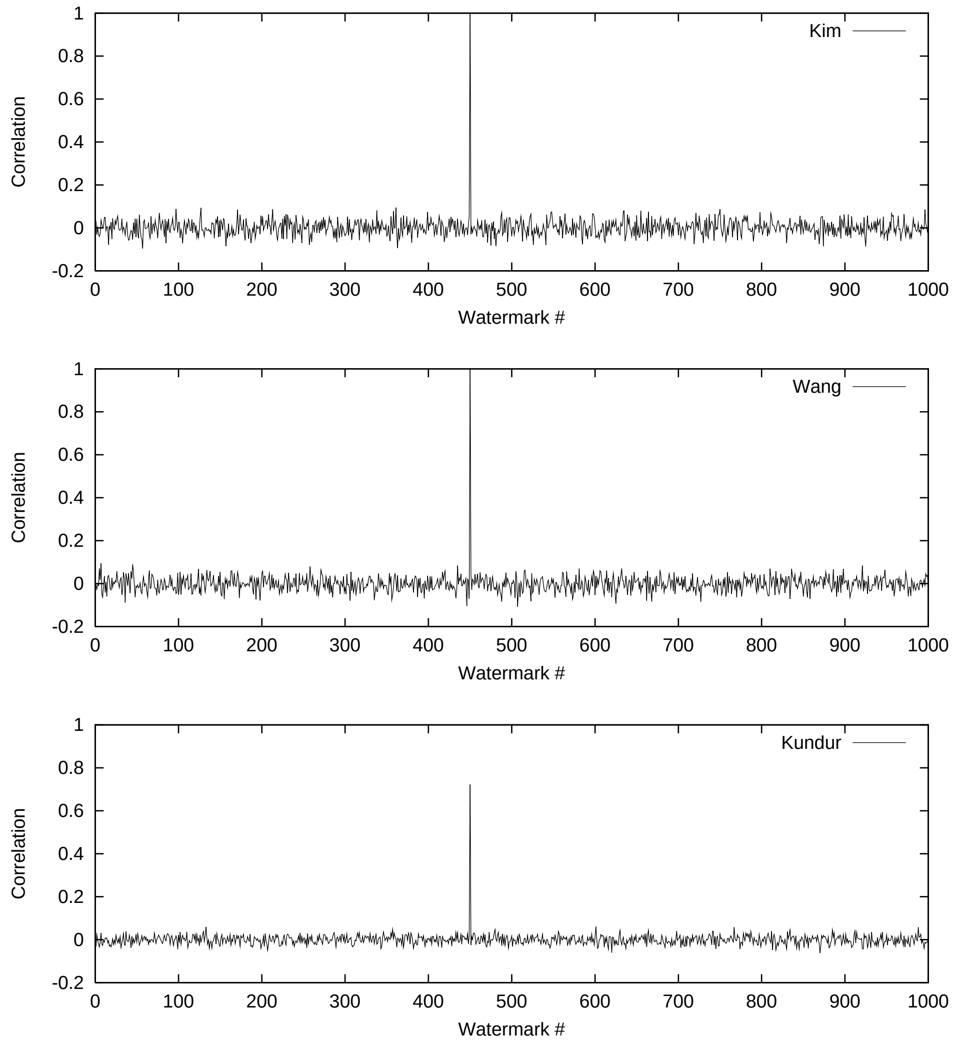
locations are pseudo-randomly selected - security?

PSNR 52.37

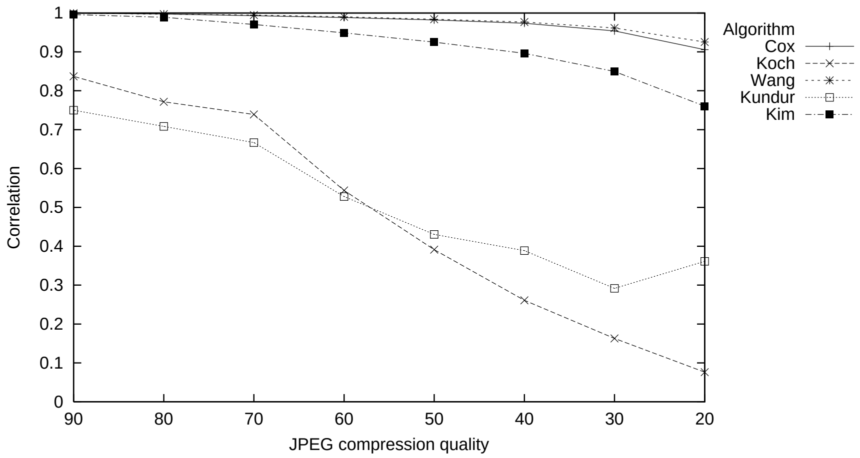


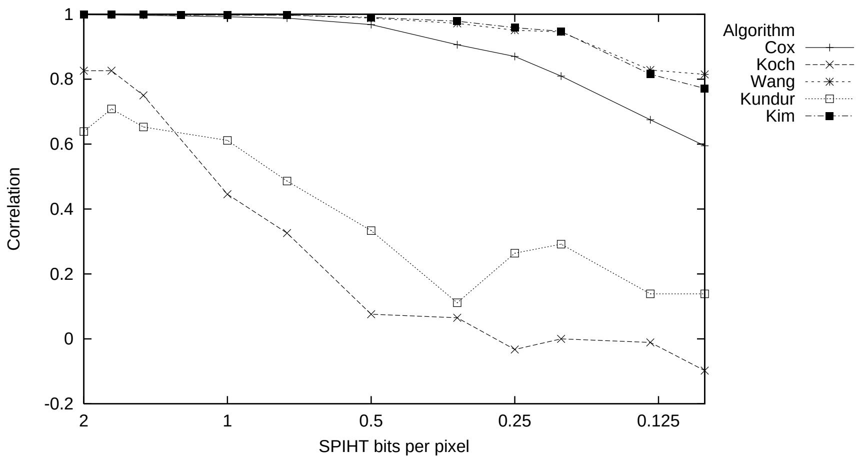
Detection of the Watermark: Confidence?

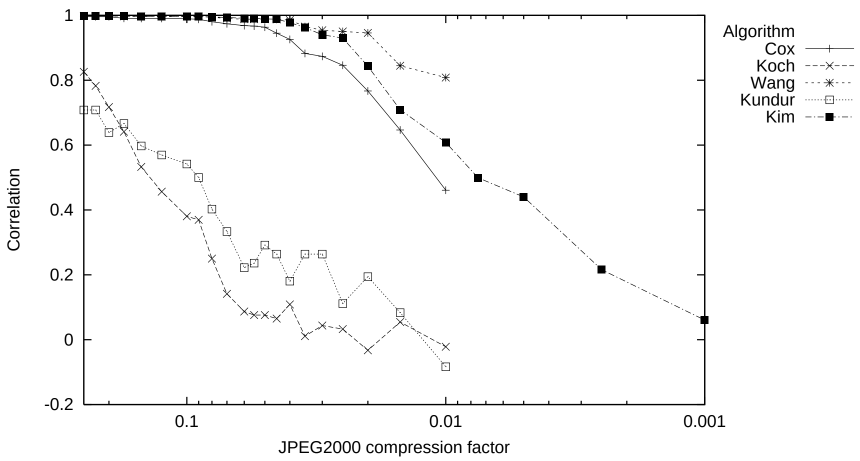
embedded a watermark #450 and trying to detect similar random watermarks #1 to #1000



Robustness Results







Security Concerns

- watermark might be estimated in smooth areas (Fridrich)
- altering coefficients at known or guessed locations (blind algorithms)
- thwarting threshold calculation of blind adaptive schemes (Wang)
- public watermark detector (e.g. for DVD) possible? attacks by Kalker [5]

Key-dependent basis functions

an idea by Fridrich [3] to improve security and versatility, embedding a pseudo-random sequence w_i of length N

1. generate N random (key-dependent) orthogonal patterns P_i (Gram-Schmidt), smoothness (low frequency) required for robustness and imperceptability

2. calculate projections c_i of the host image I onto the patterns P_i

$$c_i = < P_i, I >$$

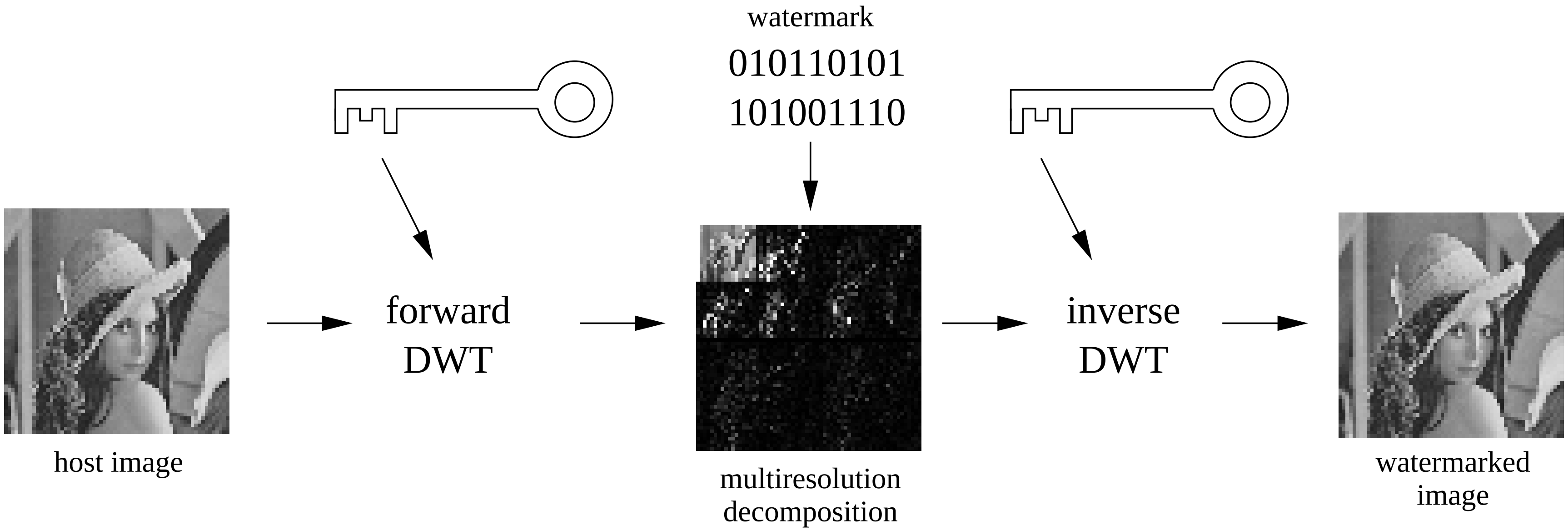
3. modify the projections to embed the watermark w_i

$$I' = I + \alpha \sum_{\mathrm{i}=1}^{N-1} w_i c_i P_i$$

high computational complexity and storage requirements

Key-dependent Wavelet Filters

wavelet transform domain accessible only with secret parameters used for filter coefficient construction



Construction of Wavelet Filters by Parametrization

readily available for orthogonal and bi-orthogonal filter types, e.g. Pollen [9], Zou [15], Resnikoff [10]

Pollen's parametrization for constructing 6-tap orthogonal filter coefficients:

$$a_{-2} = ((1 + \cos\alpha + \sin\alpha) * (1 - \cos\beta - \sin\beta) + 2 * \sin\beta * \cos\alpha)/4$$

$$a_{-1} = ((1 - \cos\alpha + \sin\alpha) * (1 + \cos\beta - \sin\beta) - 2 * \sin\beta * \cos\alpha)/4$$

$$a_0 = (1 + \cos(\alpha - \beta) + \sin(\alpha - \beta))/2$$

$$a_1 = (1 + \cos(\alpha - \beta) - \sin(\alpha - \beta))/2$$

$$a_2 = 1 - a_{-2} - a_0$$

$$a_3 = 1 - a_{-1} - a_1$$

two parameters $-\pi \leq \alpha, \beta < \pi$ can be kept secret

Application to Watermarking

keeping α and β secret to construct secret wavelet filters

secret transform domain? keyspace?

✔ no additional computational cost

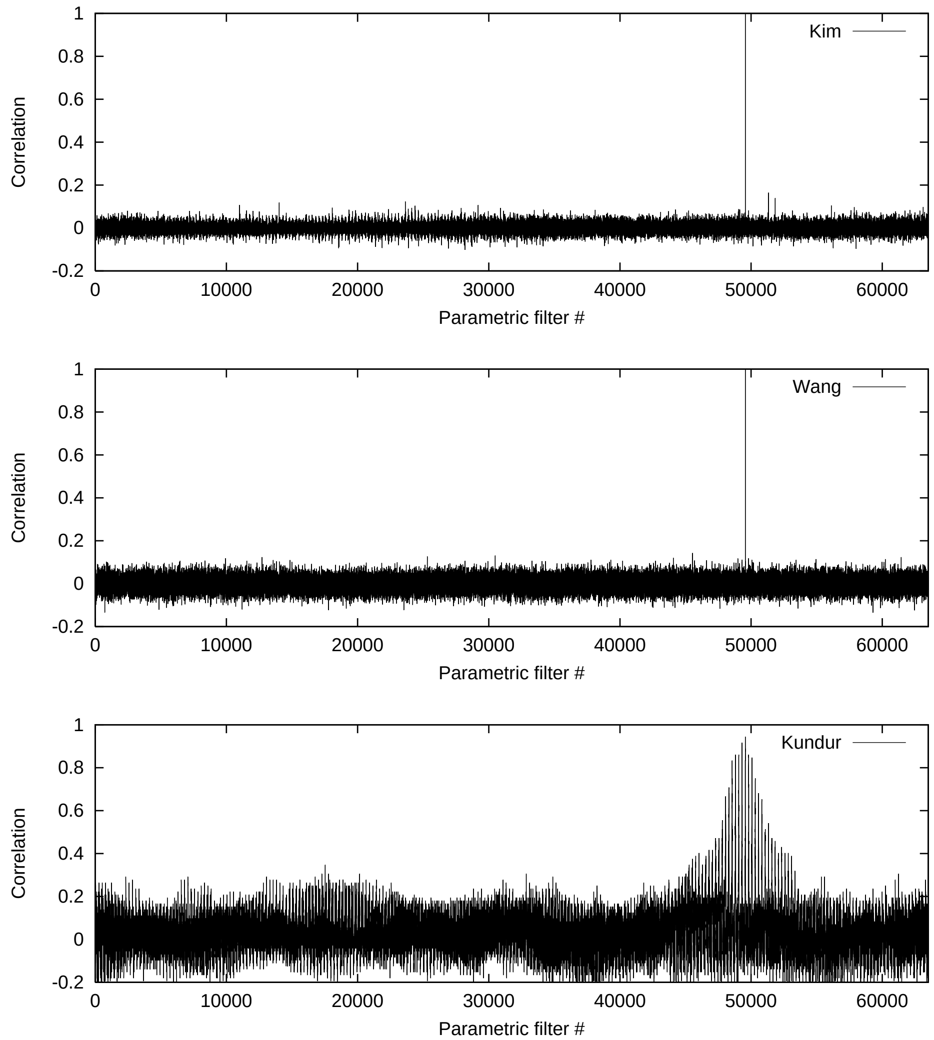
✔ coefficient skipping not necessary for security reasons, more watermark locations for blind schemes

✔ security framework for existing watermarking algorithms, only have to adapt thresholds

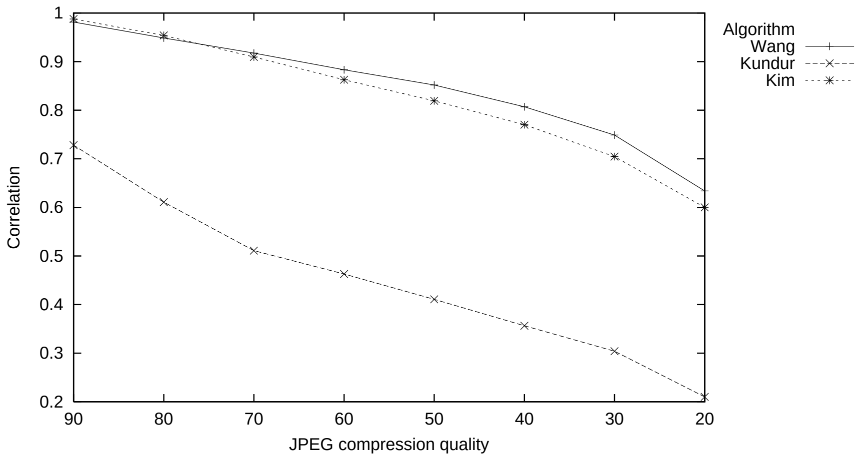
✔ possibility to chose filters in an image-adaptive way

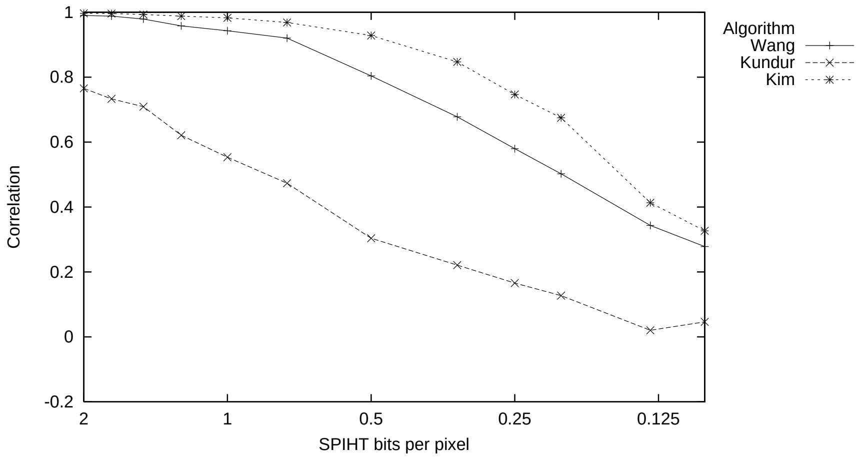
Detection of the Secret Watermark

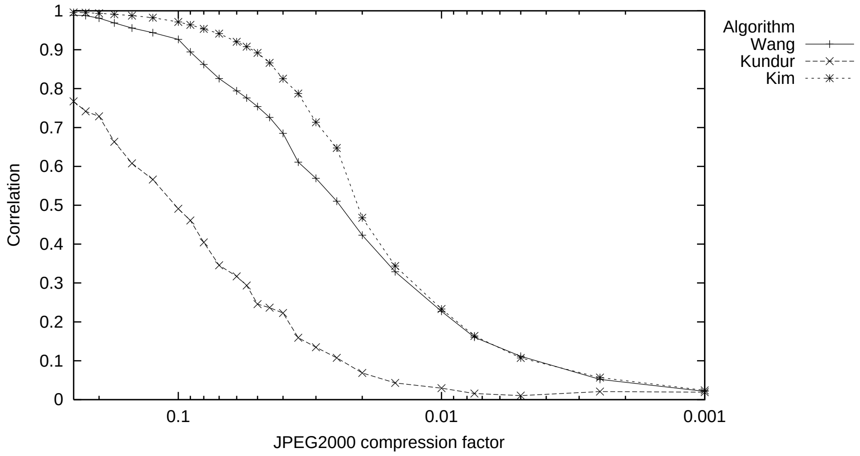
embedded a watermark using parametric filter #49560 and detecting the same watermark by trying filter parametrizations #1 to #63504



Robustness of the Secret Watermark







Matching watermarking and compression domain?

dispute by Kundur [8] and Wolfgang [13]: does matching the watermarking and compression domain result in better or worse robustness?

requirements for compression filter and watermarking filter different, Hsu [4]

evaluating different transforms, different wavelet filters

few analysis of unfriendly attacks (exploiting knowledge of the algorithm) so far

security analysis require open algorithms

References

[1] Maryline Charrier, Diego Santa Cruz, and Mathias Larsson. JPEG2000, the next millennium compression standard for still images. In *Proceedings of the IEEE ICMCS '99*, volume 1, pages 131 – 132, Florence, Italy, June 1999.

[2] 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, 1997.

[3] Jiri Fridrich, Arnold C. Baldoza, and Richard J. Simard. Robust digital watermarking based on key-dependent basis functions. In David Aucsmith, editor, *Information hiding: second international workshop*, volume 1525, Portland, OR, USA, April 1998.

[4] Chiou-Ting Hsu and Ja-Ling Wu. Multiresolution watermarking for digital images. *IEEE Transactions on Circuits and Systems II*, 45:1097 – 1101, August 1998.

[5] Ton Kalker, Jean-Paul Linnartz, Geert Depovere, and Maurice J. J. J. B. Maes. On the reliability of detecting electronic watermarks in digital images. In *9th European Signal Processing Conference EUSIPCO '98*, Island of Rhodes, Greece, September 1998.

[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] Deepa Kundur and Dimitrios Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. In *Proceedings of IEEE ICASSP '98*, volume 5, pages 2969 – 2972, Seattle, WA, USA, May 1998.

[8] Deepa Kundur and Dimitrios Hatzinakos. Mismatching perceptual models for effective watermarking in the presence of compression. In *Proceedings of the SPIE Conference on Multimedia Systems and Applications II*, volume 3845, Boston, MA, USA, September 1999.

[9] David Pollen. Parametrization of compactly supported wavelets. Technical report, Aware Inc., USA, 1989.

[10] Howard L. Resnikoff, Jun Tian, and Raymond O. Wells. Biorthogonal wavelet space: parametrization and factorization. *SIAM Journal on Mathematical Analysis*, August 1999.

[11] Houng-Jyh Wang and C.-C. Jay Kuo. High fidelity image compression with multithreshold wavelet coding (MTWC). In *SPIE's Annual meeting - Application of Digital Image Processing XX*, San Diego, CA, USA, August 1997.

[12] Houng-Jyh Wang and C.-C. Jay Kuo. Watermark design for embedded wavelet image codec. 1998.

[13] Raymond B. Wolfgang, Christine I. Podilchuk, and Edward J. Delp. The effect of matching watermark and compression transforms in compressed color images. In *Proceedings of the IEEE International Conference on Image Processing, ICIP '98*, Chicago, IL, USA, October 1998.

[14] Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce. Wavelet transform based watermark for digital images. *Optics Express*, 3:497, December 1998.

[15] H. Zou and Ahmed H. Tewfik. Parametrization of compactly supported orthonormal wavelets. *IEEE Transactions on Signal Processing*, 41:1423 – 1431, March 1993.