Watermarking mit parametrisierten Wavelet-Filtern

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

7. Juni 2000

Zusammenfassung

Es werden einige Wavelet-basierte Watermarking-Algorithmen und deren Robustheit gegenüber Wavelet-Kompressions-Attacken diskutiert. Einer Idee von Fridrich [4] und Kundur [9] folgend, schlagen wir vor, eine Parametrisierung der Wavelet-Filter-Koeffizienten zu verwenden, um dadurch das Konzept der schlüsselabhängigen Transformation auf den Wavelet-Bereich übertragen zu können. Wir zeigen, daß mit diesem neue Verfahren leicht die Sicherheit bestehender Watermarking-Algorithmen verbessern werden kann.

Watermarking im Wavelet-Bereich

Xia [17] sieht folgende Vorteile für Wasserzeichen im Wavelet-Bereich:

- Multiresolution-Eigenschaften, hierarchische Zerlegung
- geeignete Modellierung des menschlichen Sehapparates (HVS)
- Lokalität
- effizeint berechenbar

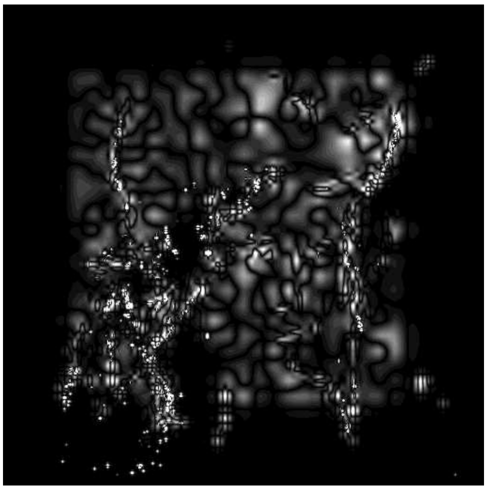
Charrier [1] beschreibt folgende Anforderungen für den kommenden Wavelet-basierenden JPEG2000-Kompressionsstandard:

- effiziente Kodierung, gute Qualität bei geringer Datenmenge
- progressive Übertragung, region-of-interest coding, Skalierbarkeit
- Sicherheit, siehe `http://eurostill.epfl.ch/~ebrahimi/JPEG2000.htm`

Kim's Algorithmus

Kim [7] verwendet der Zerlegungsstufe angepaßte Schwellwerte um eine normalverteilte Folge von pseudo-zufälligen Zahlen in signifikante Koeffizienten einzubetten, ähnlich dem Algorithmus von Cox [2]

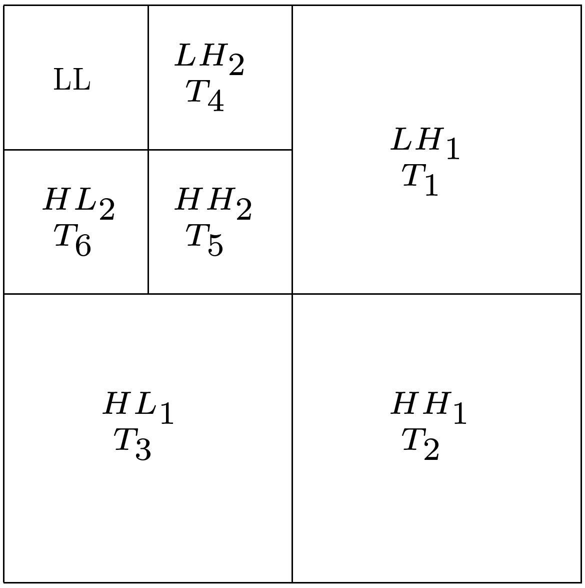
PSNR 38.57



Wang's Algorithmus

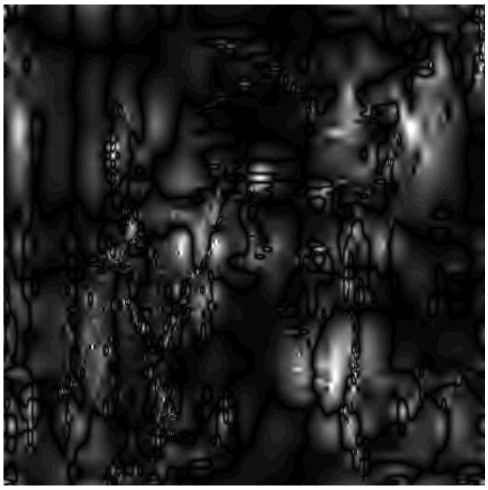
Wang [15] basiert auf dem MTWC Coder [14], ähnlich dem Verfahren von Kim

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

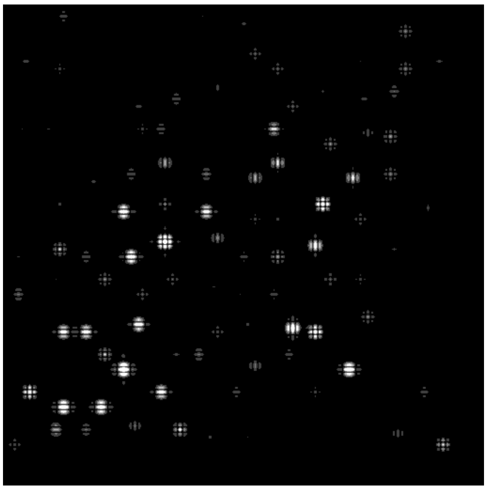


Kundur's Algorithmus

Kundur [8] quantisiert den Mittelwert eines Koeffizeinten-Trippels (LH_l, HL_l, HH_l) um ein Bit einzubetten, l ist die Zerlegungsstufe

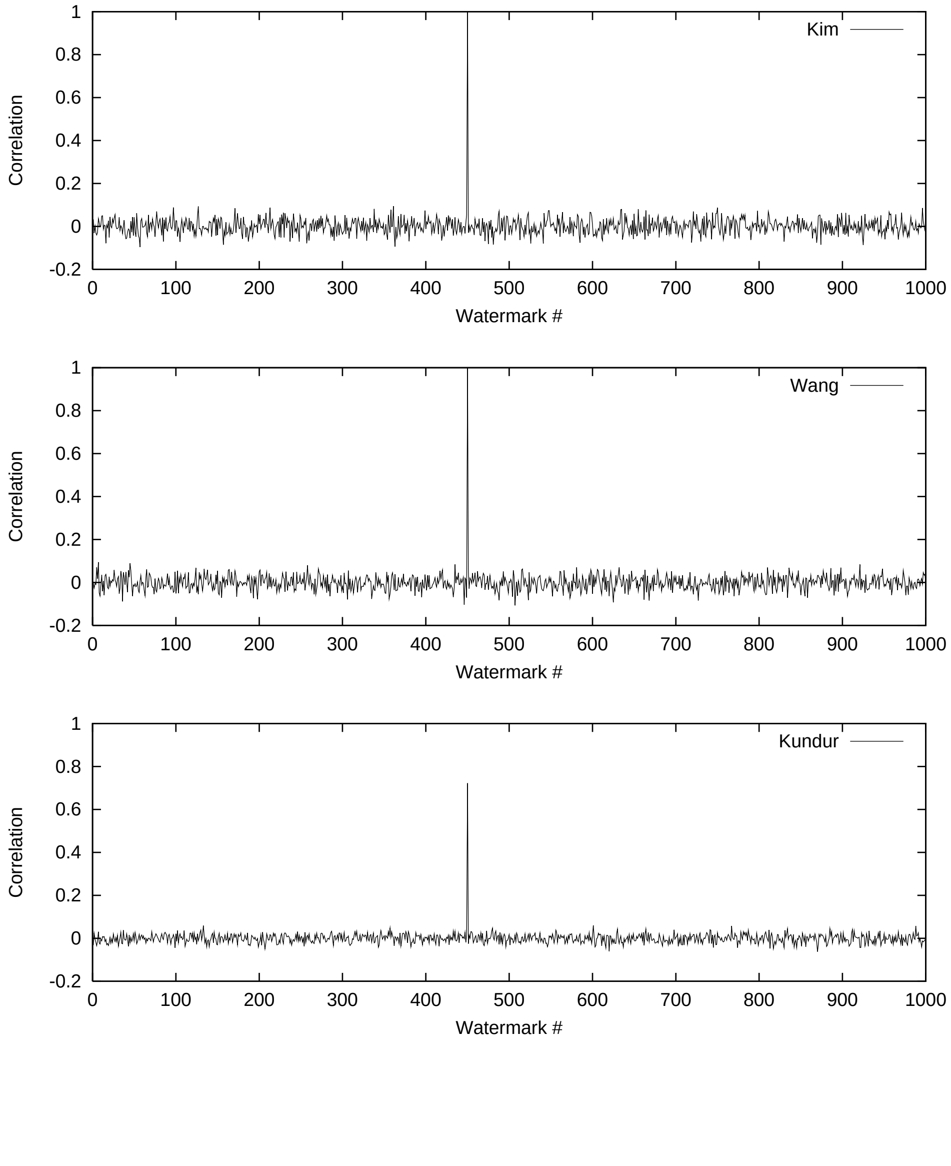
die Positionen der Einbettung werden pseudo-zufällig ausgewählt - Sicherheit?

PSNR 52.37

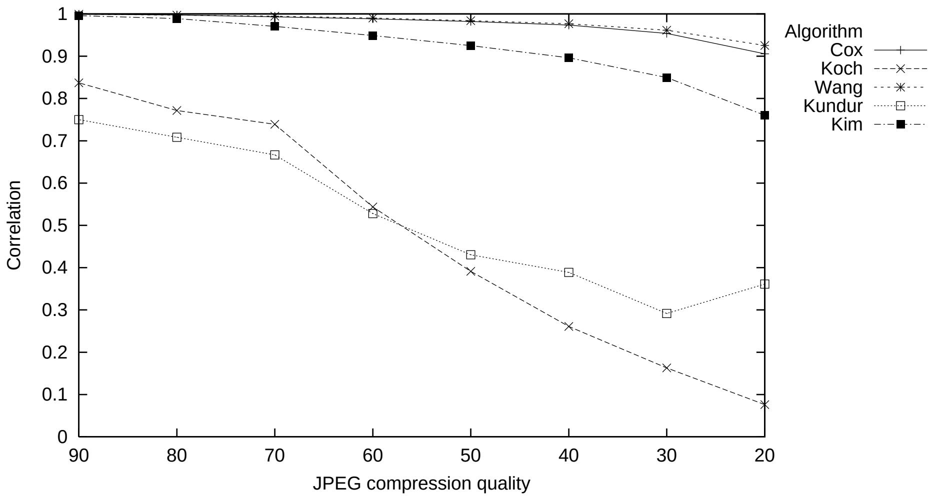


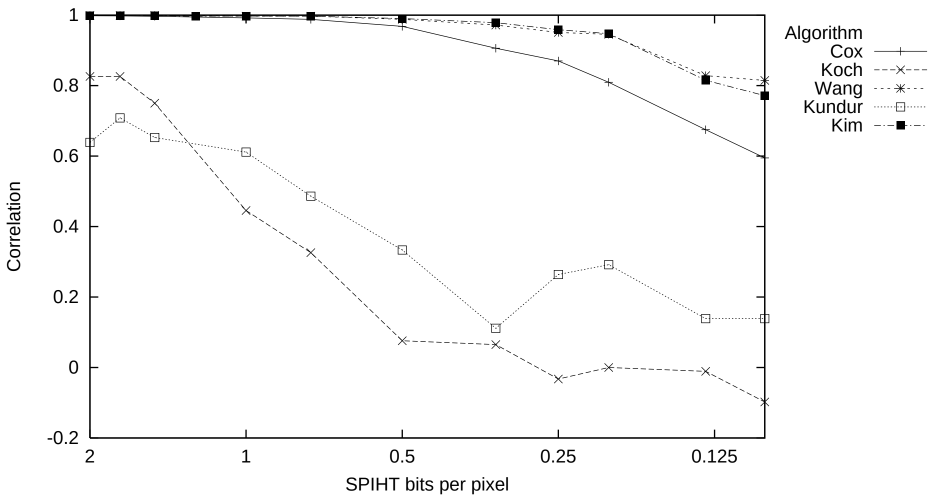
Erkennen der Wasserzeichen

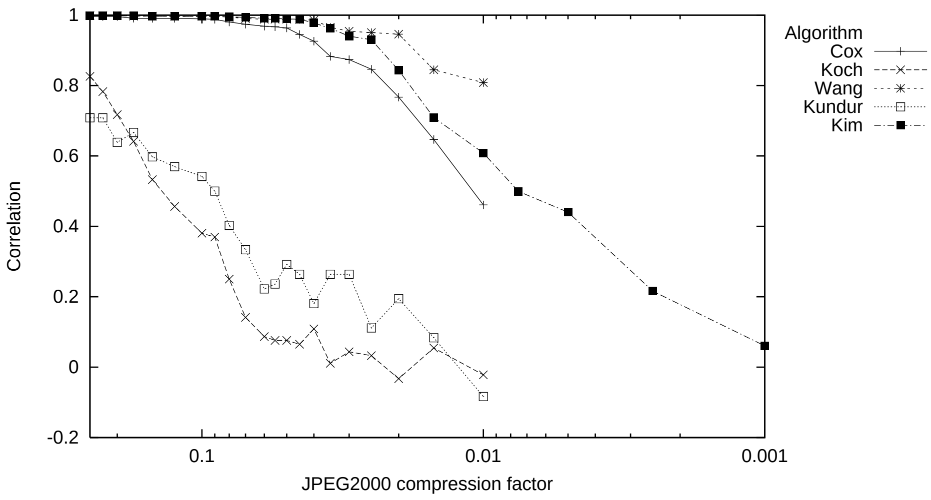
das Wasserzeichen #450 wurde eingebettet, daraufhin wurde versucht ähnliche, zufällig erzeugte Wasserzeichen #1 bis #1000 auszulesen



Robustheit der Wasserzeichen







Bedenken bezüglich der Sicherheit

- das Wasserzeichen könnte in glatten Flächen erraten werden (Fridrich)

- verändern von Koeffizienten an bekannten Stellen (blind algorithms)

- behindern der korrekten Schwellwert-Berechnung (Wang)

- ist ein öffentlicher Apparat zur Erkennung von Wasserzeichen (z.B. für DVD) möglich? siehe die Angriffe von Kalker [6]

Schlüsselabhängige Basisfunktionen

eine Idee von Fridrich [4] um die Sicherheit und Flexibilität zu erhöhen, eingebettet wird eine pseudo-zufällige Folge w_i der Länge N

1. generiere N zufällige (schlüsselabhängige) orthogonale Muster P_i (Gram-Schmidt), Glattheit ist erforderlich, um das Muster beständig und unauffällig einbetten zu können

2. berechne Projektionen c_i der Muster auf das Träger-Bild I

$$c_i =< P_i, I >$$

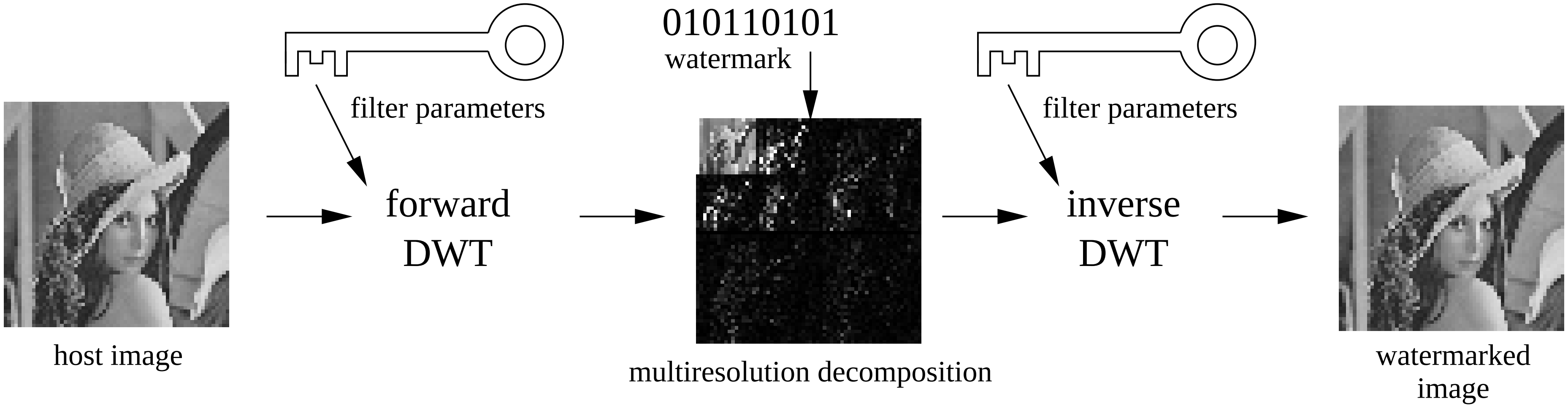
3. verändere die Projektionen, um das Wasserzeichen w_i einzubetten

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

das Verfahren erfordert hohe Rechenleistung und viel Speicherplatz

Schlüsselabhängige Wavelet-Filter

der Wavelet-Transformationsbereich soll nur mit den passenden Parametern, die für die Erzeugung der Filter-Koeffizienten benutzt wurden, zugänglich sein



Konstruktion von Wavelet-Filtern durch Parametrisierung

Parametrisierungen von orthogonalen und bi-orthogonalen Filtern sind verfügbar, z.B. Pollen [11], Zou [18], Resnikoff [12]

Suche nach Lösungen $c_k \in \mathbb{R}$ für die Dilationsgleichung

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

unter Einhaltung von zwei Bedingungen (siehe Daubechies [3])

Parametrisierung nach Scheid [13], Pollen [11], Zou [18]

N Parameter-Werte mit $-\pi \le \alpha_i \le \pi$, $0 \le i < N$, die Rekursion

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

liefert die Koeffizienten c_k^N, $0 \le k < 2N + 2$

Pollen-Parametrisierung

Parametrisierung von Pollen zur Erzeugung von orthogonalen Filtern der Länge 6:

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

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

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

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

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

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

die zwei Parameter $-\pi \leq \alpha, \beta < \pi$ bleiben geheim

Anwendung für Watermarking

die Parameter α und β zur Erzeugung der Wavelet-Filterkoeffizienten bleiben geheim

wird wirklich ein geheimer Transformationsbereich erzeugt? wie viele Schlüsselwerte existieren?

Vorteile

- ✔ keine zusätzliche Rechenarbeit
- ✔ Auslassen von Koeffizienten beim Einbetten nicht mehr erforderlich, um das Verfahren sicher zu machen
- ✔ ein vom Watermarking-Algorithmus unabhängiger Sicherheitsrahmen
- ✔ es ist möglich, die Filter auch anhand von Eigenschaften des Träger-Bildes zu wählen um z. B. die Robustheit zu erhöhen

Eignung der parametrisierten Transformation

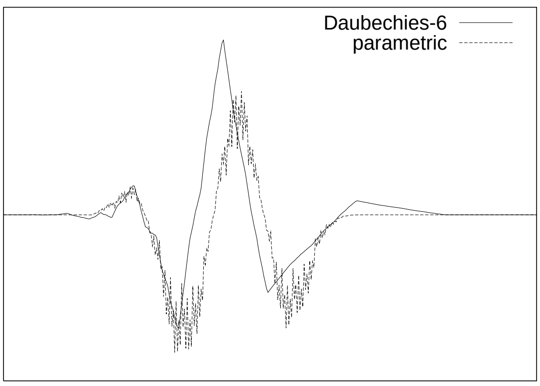
Frequenz-Zerlegung der Transformation geht teilweise verloren

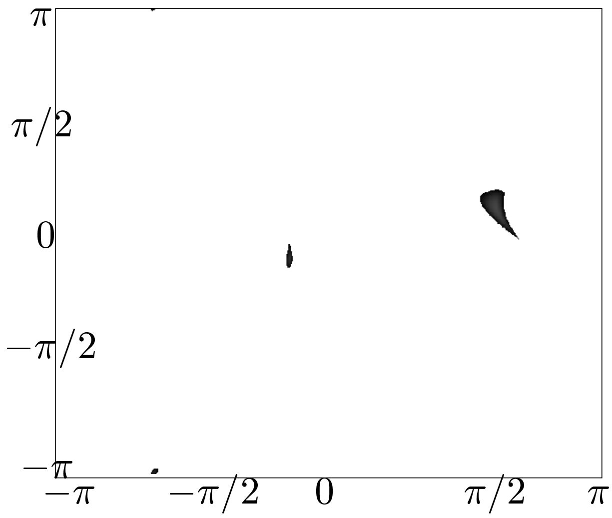
wählen Glattheit der Wavelet-Koeffizienten-Folge als Maß für die Eignung des Filters (Differenz 2. Ordnung) [10]

$$V_\phi^{(2)} = \sum_n \left| g_n^{(J)} - g_{n-1}^{(J)} + g_{n-2}^{(J)} \right|$$

können Parameter beschränken auf Werte, die "glatte" Wavelets produzieren

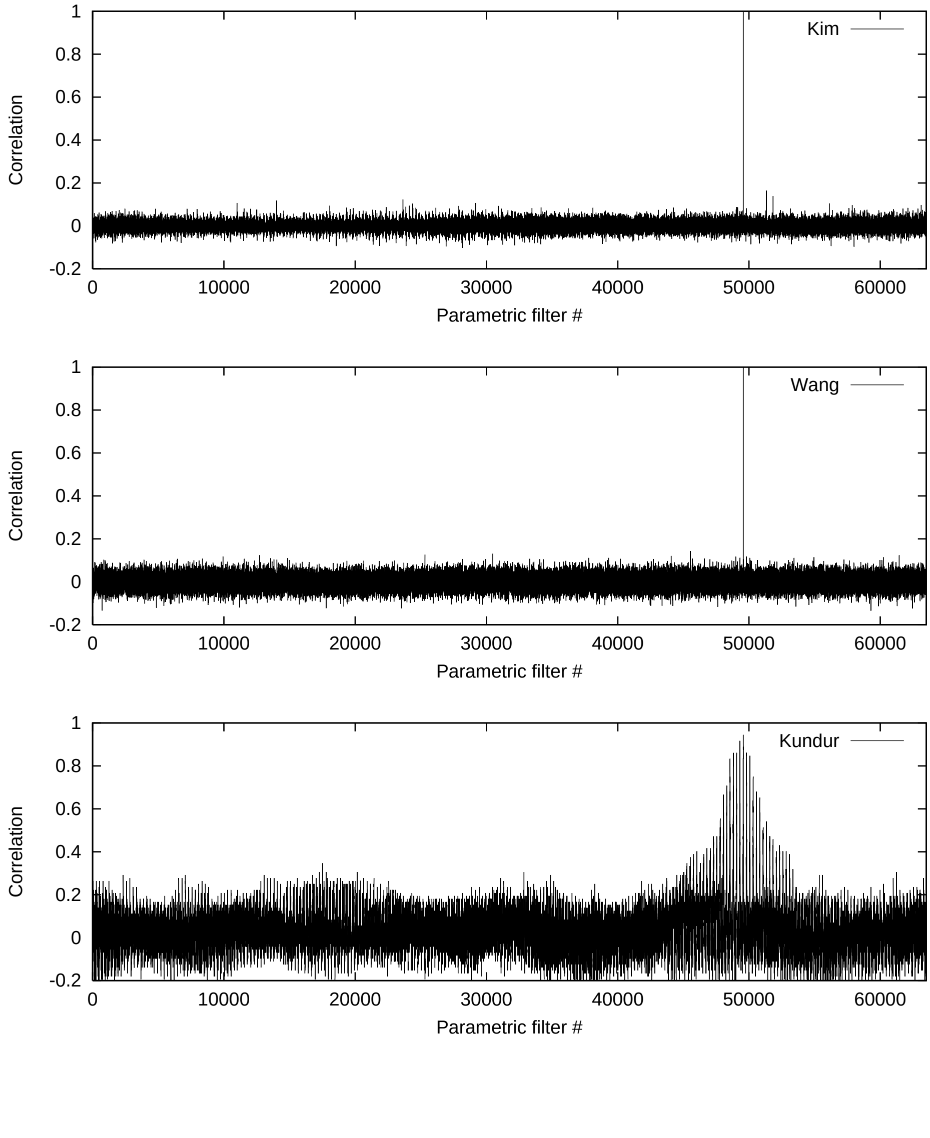
Maßstab ist die Glattheit des Haar-Wavelets $V_H^{(2)}$, also wollen Wavelets mit $V_{\phi_\alpha}^{(2)} < V_H^{(2)}$



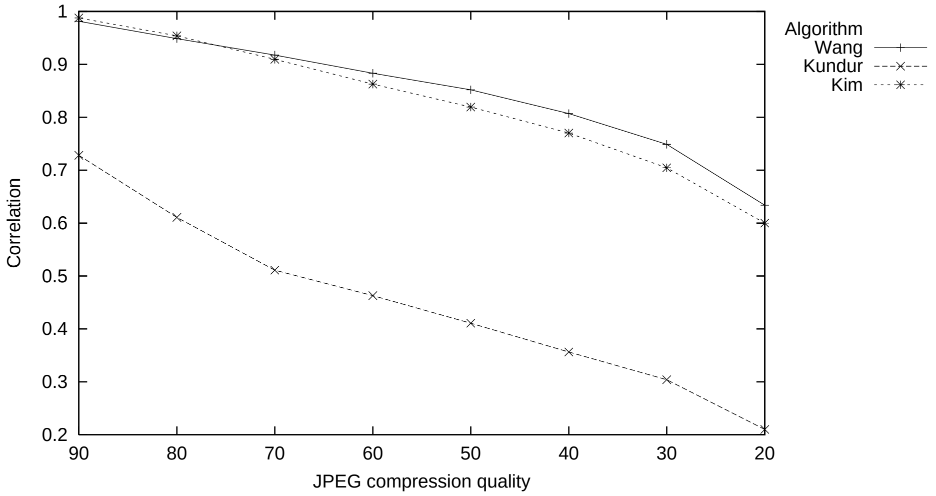


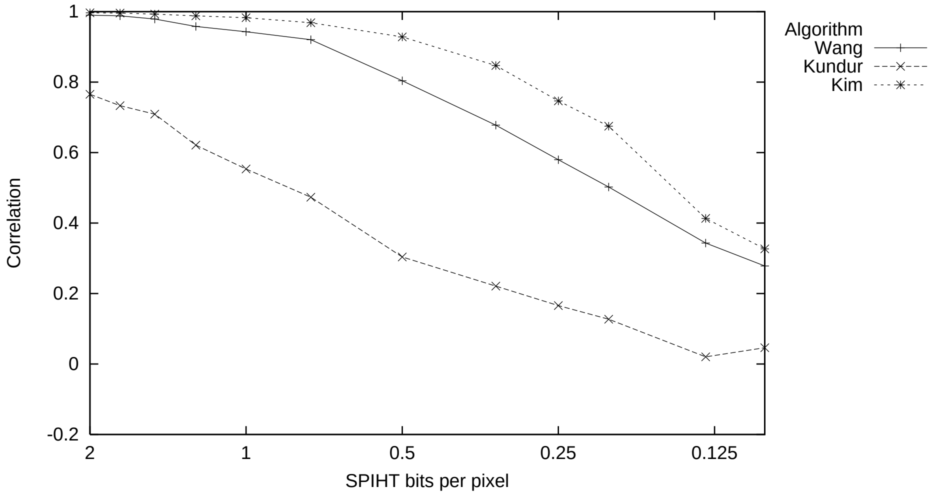
Erkennen der sicheren Wasserzeichen

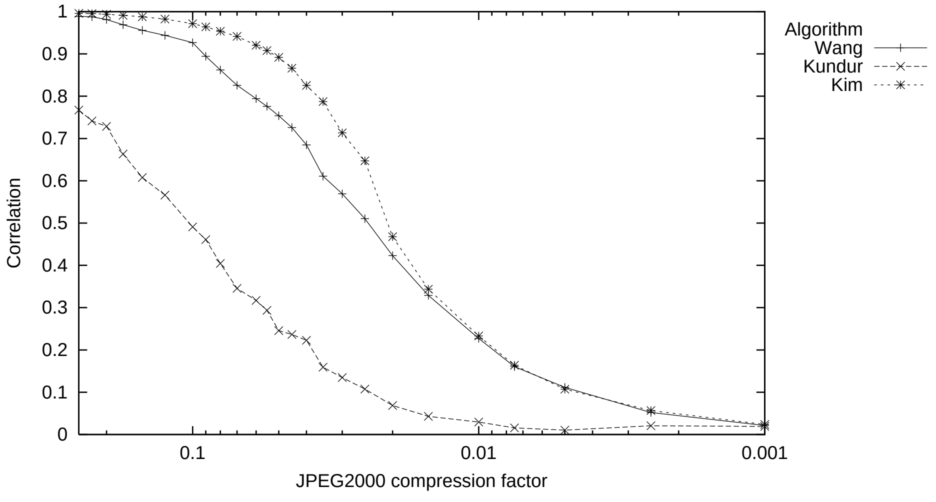
es wurde ein Wasserzeichen mit dem parametrisierten Filter #49560 eingebettet, danach wurde versucht, das gleiche Wasserzeichen, allerdings unter Verwendung der Filter #1 bis #63504, wieder auszulesen



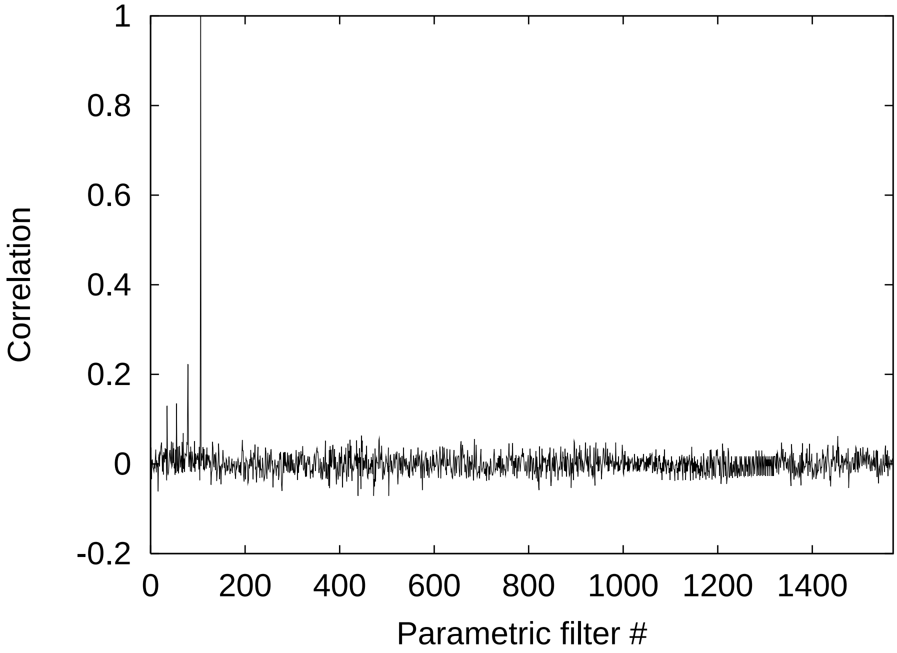
Robustheit sicherer Wasserzeichen

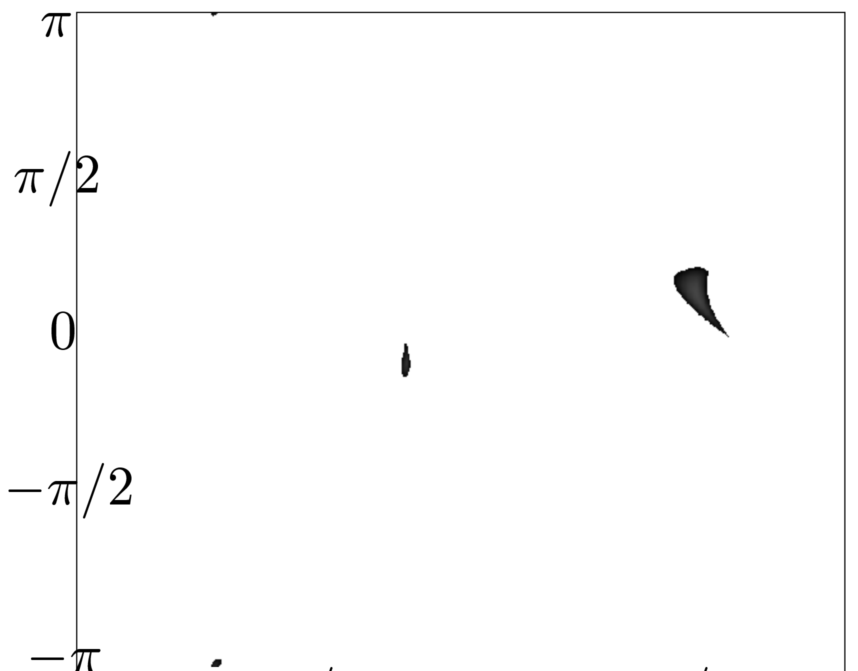






Erkennen des sicheren Wasserzeichens (glatte Wavelets)





Muß der Transformationsbereich für Watermarking und Kompression übereinstimmen?

- widersprüchliche Meinungen von Kundur [9] und Wolfgang [16]: ermöglicht der gleiche Transformationsbereich für Watermarking und Kompression ein robusteres Wasserzeichen?

- die Anforderung an die Wavelet-Filter für Kompression und Watermarking sind unterschiedlich, Hsu [5]

- es müssen verschiedene Transformationen und Wavelet-Filter getestet werden

- bis jetzt kaum Analysen von unfreundlichen Attacken (solche, die Wissen um den verwendeten Algorithmus ausnützen)

- Analyse der Sicherheit erfordert offene Wasserzeichen-Algorihmen

Literatur

[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] Ingrid Daubechies. *Ten lectures on wavelets*. SIAM Press, 1992.

[4] 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, pages 143 – 157, Portland, OR, USA, April 1998.

[5] Chiou-Ting Hsu and Ja-Ling Wu. Multiresolution watermarking for digital images. *IEEE Transactions on Circuits and Systems II*, 45(8):1097 – 1101, August 1998.

[6] 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 *Proceedings of the 9th European Signal Processing Conference EUSIPCO '98*, Island of Rhodes, Greece, September 1998.

[7] 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.

[8] 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.

[9] 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.

[10] S. Maslakovic, I. R. Linscott, M. Oslick, and J. D. Twicken. Smooth orthonormal wavelet libraries: design and application. In *Proceedings of IEEE ICASSP '98*, Seattle, WA, USA, May 1998.

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

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

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

[14] 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.

[15] Houng-Jyh Wang and C.-C. Jay Kuo. Watermark design for embedded wavelet image codec. In *Proceedings of the SPIE's 43rd Annual Meeting, Applications of Digital Image Processing*, San Diego, CA, USA, July 1998.

[16] 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.

[17] Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce. Wavelet transform based watermark for digital images. *Optics Express*, 3(12):497, December 1998.

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