

# Zwei Watermarking-Verfahren im Wavelet-Bereich

---

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

22. November 1999

## Zusammenfassung

Die Watermarking-Verfahren von Wang [1] und Kundur [3] werden vorgestellt und mit ihren "historischen Vorläufern" von Cox [4] bzw. Koch [2] verglichen. Dabei wird gezeigt, welche Vorteile der Wavelet-Transformationsbereich für Watermarking-Anwendungen bietet und welche Probleme noch zu lösen sind, um die Algorithmen im Bereich des Urheberrechtes von digitalen Bildern einsetzen zu können.

# Watermarking - was ist das?

---

Einbetten von Daten in ein digitales Trägersignal, z. B. Video, Audio, Graphik, Bild [11]

verschiedene Anwendungsbereiche wie

- Urheberschutz,
- Steganographie,
- Manipulationserkennung

mit unterschiedlichen Anforderungen:

- Robustheit,
- Wahrnehmbarkeit,
- Kapazität,
- Sicherheit

# Ablauf

---

- Generieren des Watermarks  $W$  mit Länge  $n_w$
- Einbetten von  $W$  in das zu schützende Trägersignal  $I$  mit Hilfe eines Schlüssels  $K$ :  $I' = E_K(I, W)$
- Extrahieren (Nachweisen) des Watermarks aus dem (veränderten) Signal  $I^*$  unter Zuhilfenahme des Originalsignals  $I$ :  $W^* = D_K(I^*, I)$
- Korrelation des extrahierten Wasserzeichens  $W^*$  mit  $W$  um die Ähnlichkeit  $\delta(W^*, W)$  zu ermitteln

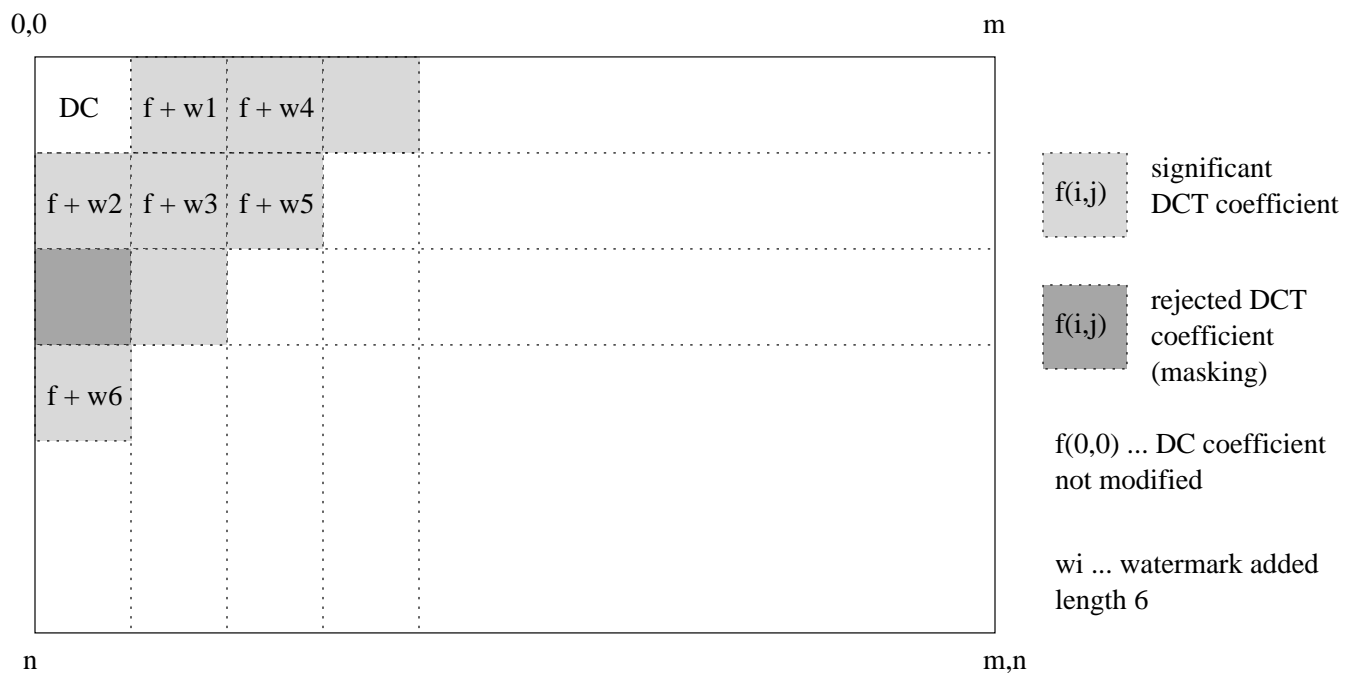
$$\delta = \frac{W^* \cdot W}{\|W^*\| \cdot \|W\|} = \frac{\sum_i w_i^* \cdot w_i}{\sqrt{\sum_i w_i^{*2} \cdot \sum_i w_i^2}}, 1 \leq i \leq n_w$$

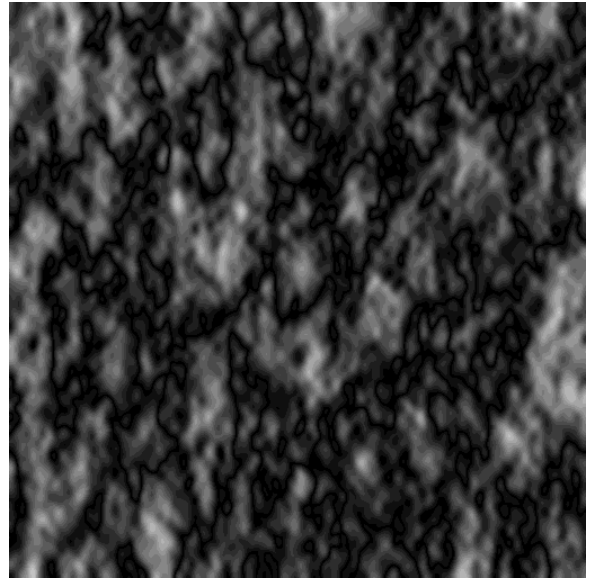
## Zwei klassische Verfahren. . .

Cox [4] und Koch [2], beide arbeiten im DCT-Bereich, beide verändern für die Wahrnehmung signifikante Koeffizienten um das Wasserzeichen robust zu machen

**Cox:** zu den 1000 größten DCT-Koeffizienten<sup>1</sup>  $f(m, n)$  wird eine eben so lange um 0 normalverteilte Folge von Zufallszahlen  $w_i$  addiert

$$f'(m, n) = f(m, n)(1 + \alpha w_i)$$





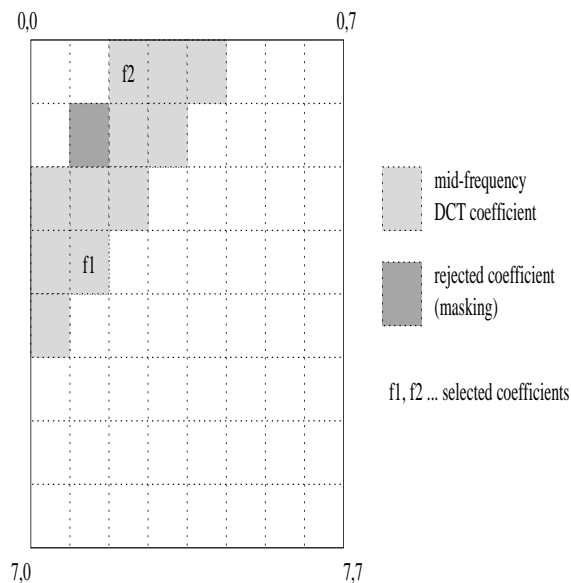
Parameter	Beschreibung
$n_w = 1000$	Länge des Watermarks
$\alpha = 0.1$	Intensität der Einbettung

**Koch:** in zufällig gewählten 8x8 DCT Block  $b$  wird die Beziehung zwischen 2 (oder  $3^2$ ) Koeffizienten im mittleren Frequenzbereich verändert, um pro Block ein Bit an Information  $w_i$  einzubetten

$$\Delta_b(m_1, n_1, m_2, n_2) = |f_b(m_1, n_1)| - |f_b(m_2, n_2)|$$

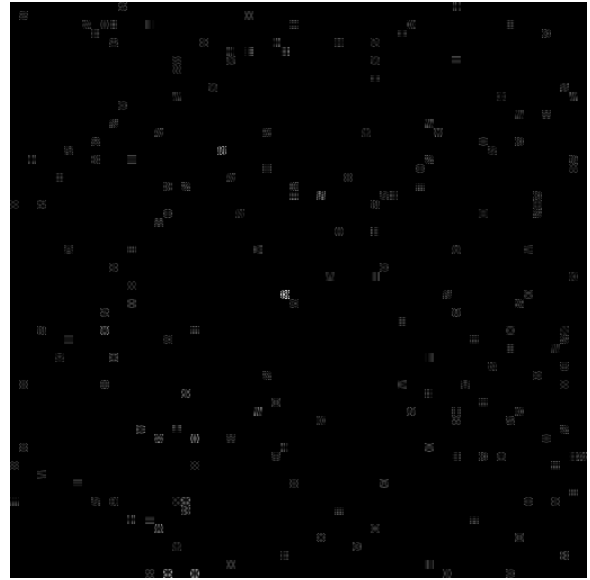
wollen

$$\Delta_b(m_1, n_1, m_2, n_2) = \begin{cases} \geq q & \text{for } w_i = 1 \\ \leq -q & \text{for } w_i = 0 \end{cases}$$



<sup>1</sup>ausgenommen DC-Koeffizient

<sup>2</sup>Erweiterung Benham [10]



Parameter	Beschreibung
$n_w = 184$	Länge des Watermarks
$q = 1.0$	Intensität der Einbettung
$Q = 10$	Quantisierungsfaktor

## . . . und ihre Probleme

### **Cox:**

Umkehrbarkeit der Einbettung (siehe Craver [5])

Originalbild notwendig, um Wasserzeichen auszulesen (non-blind)

Rechenaufwand für DCT

nimmt nicht auf Human Vision System (HVS) Bezug (siehe Erweiterung Bartolini [12])

### **Koch:**

Block-Artefakte durch 8x8 DCT

Sicherheit beruht auf Auswahl der Blöcke

HVS wird nicht ausgenutzt

Entfernen eines Watermarks durch Mitteln mehrerer Kopien eines Bildes möglich (Collusion attack)



# Warum nun im Wavelet-Bereich?

Xia [8] sieht folgende Vorteile:

- multiresolution-Eigenschaft und hierarchisch, spart Aufwand bei der Erkennung des Signals, speziell bei Videos
- HVS nicht besonders empfindlich gegenüber Kanten und Texturen welche in den detail subbands repräsentiert sind
- zukünftige Kompressionsverfahren werden Wavelet-basiert sein - Vorteil? siehe Wolfgang<sup>3</sup>[7] und Kundur<sup>4</sup>[9]

weitere:

- Transformation effizienter zu rechnen als  $M \times N$  DCT
- lokalisiert

---

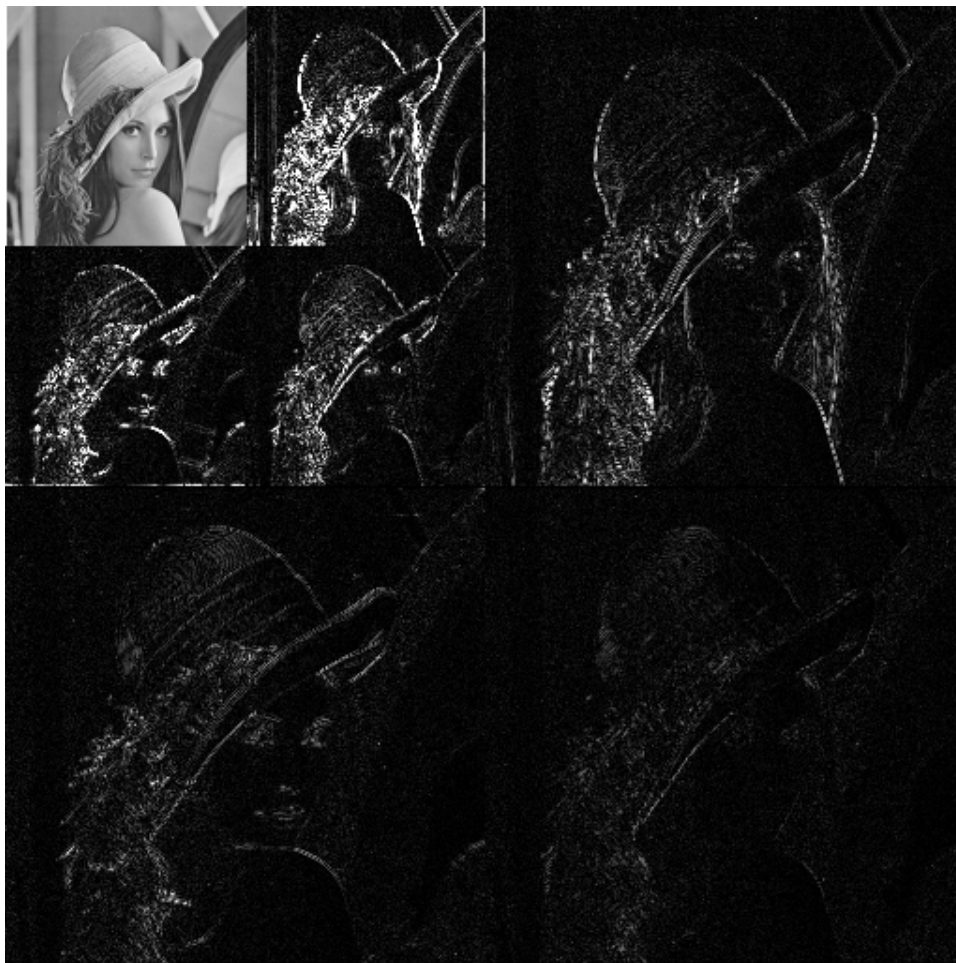
<sup>3</sup>Based on our experiments, we find that at low data rates it is beneficial to match the transform framework of the watermarking scheme to the transform framework of the compression scheme.

<sup>4</sup>It follows that complementary perceptual models should be used for watermarking and coding to increase robustness which is in direct contrast to other research in the area.

# Wavelet-Transformation

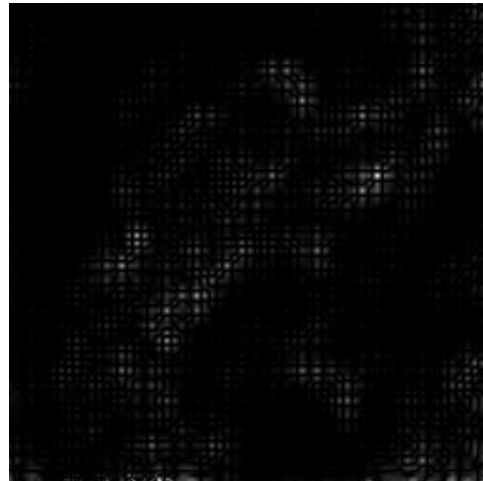
LL	$LH_1$ (horizontal)
$HL_1$ (vertical)	$HH_1$ (diagonal)

LL	$LH_2$	$LH_1$ (horizontal)
$HL_2$	$HH_2$	
$HL_1$ (vertical)		$HH_1$ (diagonal)



# HH weg, trotzdem. . .

---



gelöschtes Subband	PSNR
HH1	43.70
HH2	38.94
HH3	34.78
HH4	31.97

# Wang: Multi-Threshold

---

ähnlich Cox, allerdings im Wavelet-Bereich, baut auf MTWC [6]

berechnen einer anfänglichen Signifikanz-Schwelle für jedes Subband  $s$ :  $T_s = \beta_s * \max_s(f_s(m, n))/2$

LL $T_4$	$LH_2$ $T_4$	$LH_1$ $T_1$
$HL_2$ $T_6$	$HH_2$ $T_5$	
$HL_1$ $T_3$		$HH_1$ $T_2$

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

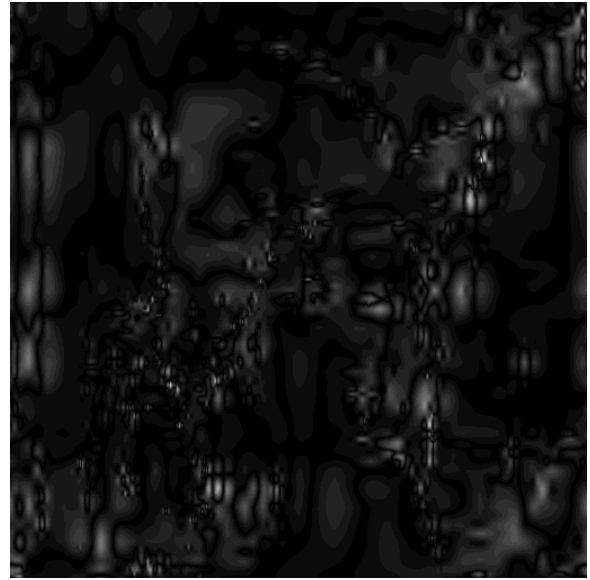
$$T_s = \beta_s * \max_s(f_s(m, n))/2$$

$\beta_s$  ... weighting factor for subband  $s$

$\max_s(f_s(m, n))$  ... max. coefficient in subband  $s$

im Subband mit dem größten Schwellenwert werden alle Koeffizienten  $f_s(m, n) > T_s$  mit einem Watermark  $w_i$  versehen:  $f'_s(m, n) = f_s(m, n) + \alpha_s \cdot \beta_s \cdot T_s \cdot w_i$ , dabei werden schlüsselabhängig Koeffizienten ausgelassen

nach der Bearbeitung eines Subbands  $s$  wird der Schwellenwert  $T'_s = T_s/2$  angepaßt



Parameter	Beschreibung
$\alpha_s = 0.125$	Intensität der Einbettung
$\beta_s = 1$	Gewichtung der Subbands
$n_w = 1000$	Länge des Watermarks

# Kundur: Multi-Resolution

---

ähnlich Koch, allerdings im Wavelet-Bereich

auf Grund eines Schlüssels werden 3 Koeffizienten aus den 3 Detail-Subbands einer Ebene  $l$  gewählt und aufsteigend sortiert:

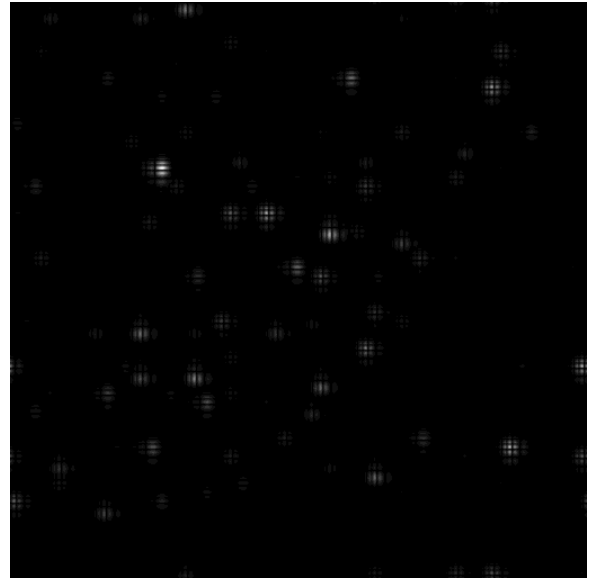
$$f_{k1,l}(m, n) \leq f_{k2,l}(m, n) \leq f_{k3,l}(m, n)$$

$LL$	$LH_2$	$LH_2$ $f_{k2,1}$ 4.15 ●
$HL_2$	$HH_2$	
$HL_1$ $f_{k3,1}$ 15.66 ●		$HH_1$ $f_{k1,1}$ 0.53 ●

der mittlere Koeffizient  $f_{k2,l}(m, n)$  wird entsprechend dem Watermark-Bit  $w_i$  verändert:

$$f'_{k2,l} = \begin{cases} f_{k1,l} + \Delta \cdot (2p + 1) & w_i = 1 \\ f_{k1,l} + \Delta \cdot 2p & w_i = 0 \end{cases}$$

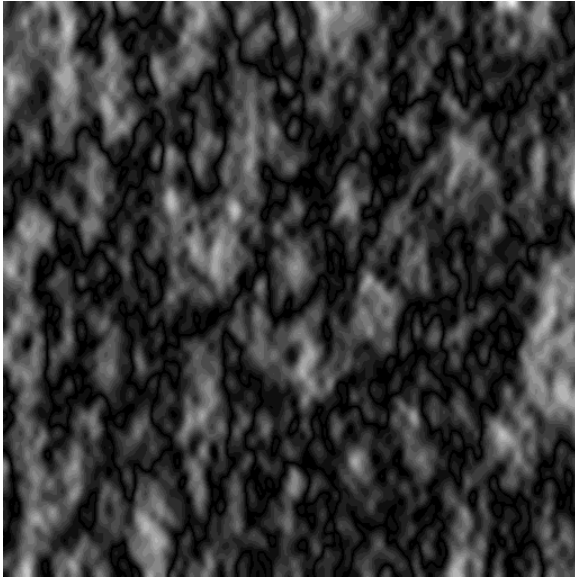
to embed  $w_i = 1$   
 to embed  $w_i = 0$   
 $\Delta$  ... bin width



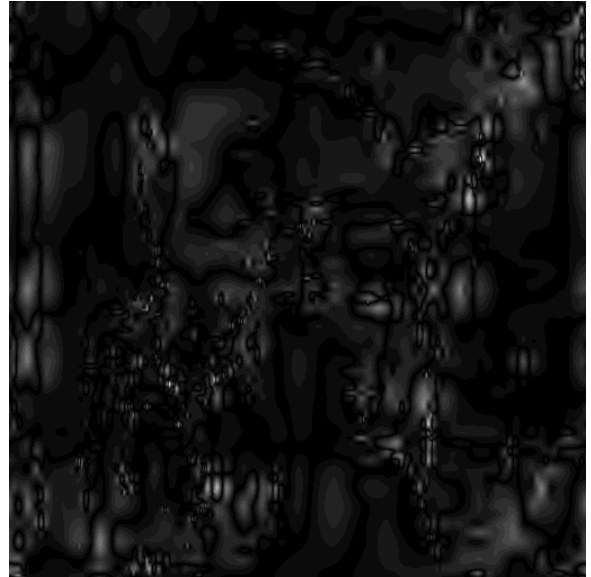
Parameter	Beschreibung
$\Delta = 2$	'bin width' Quantisierung
$L = 3$	DWT decomposition level
$n_w = 96$	Länge des Wasserzeichens

# Vergleich der Verfahren: Differenzbild

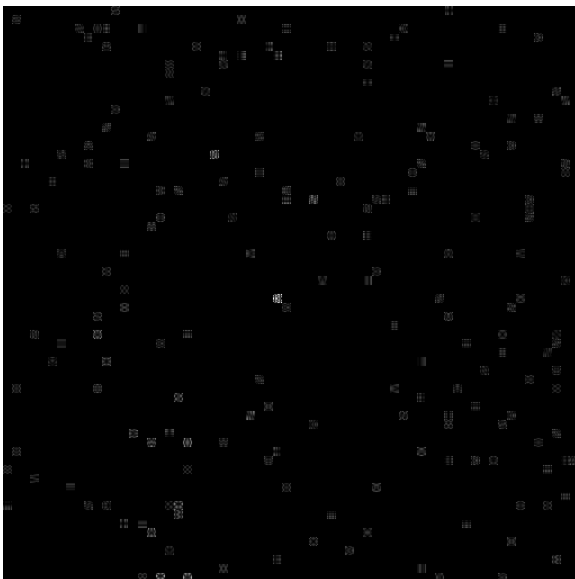
---



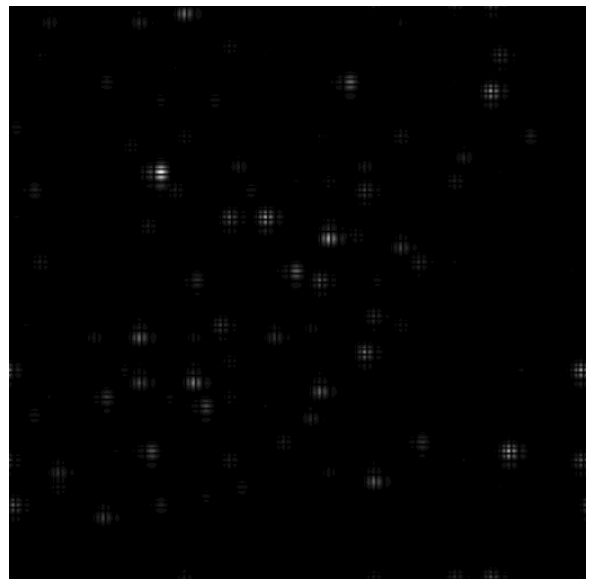
(a) Cox



(b) Wang



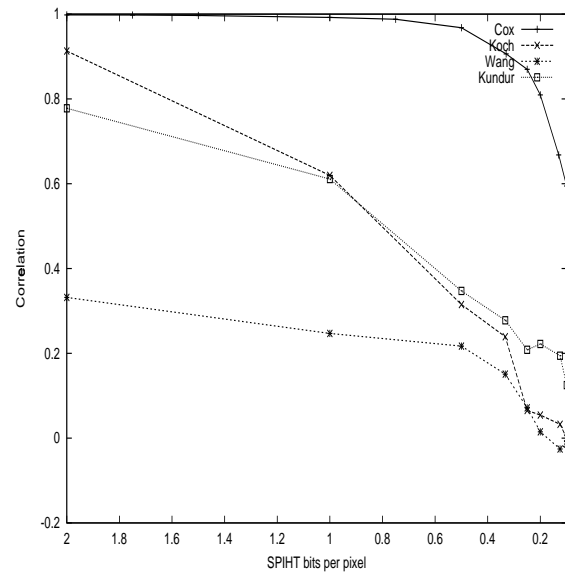
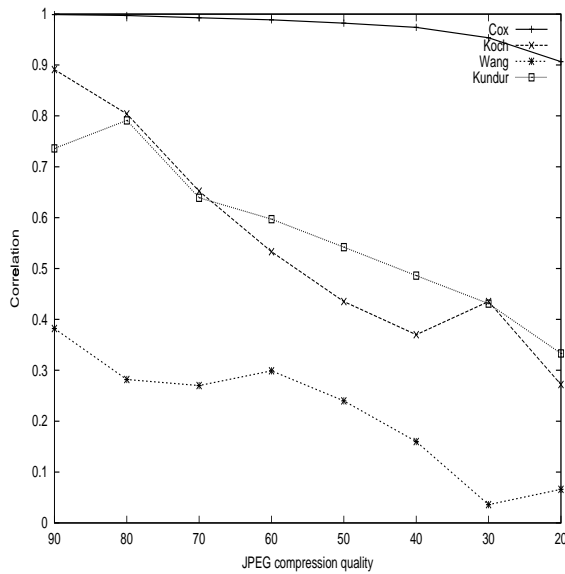
(c) Koch



(d) Kundur



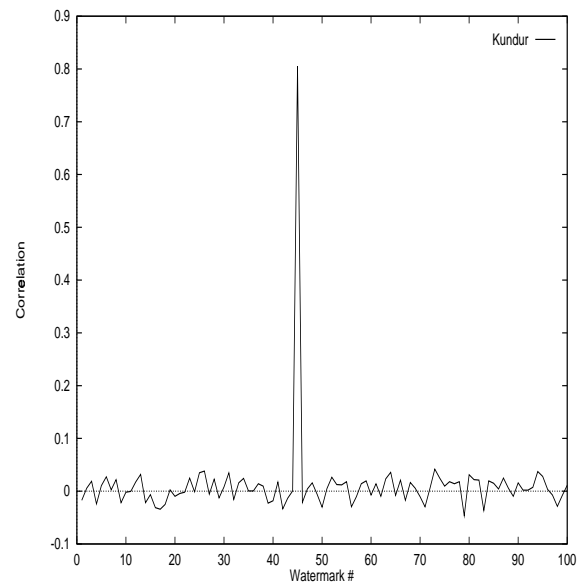
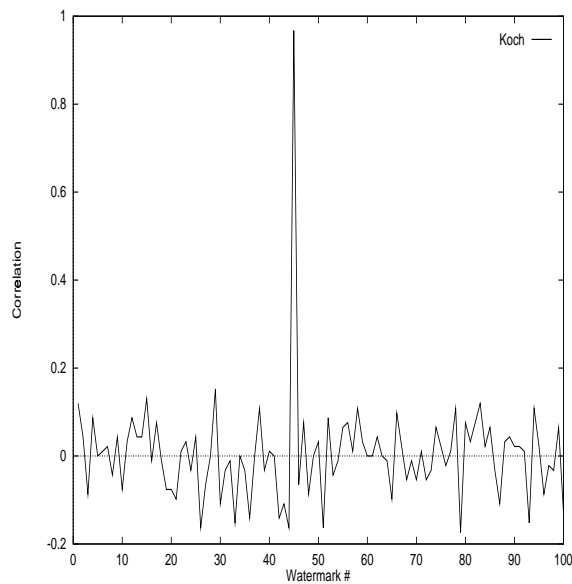
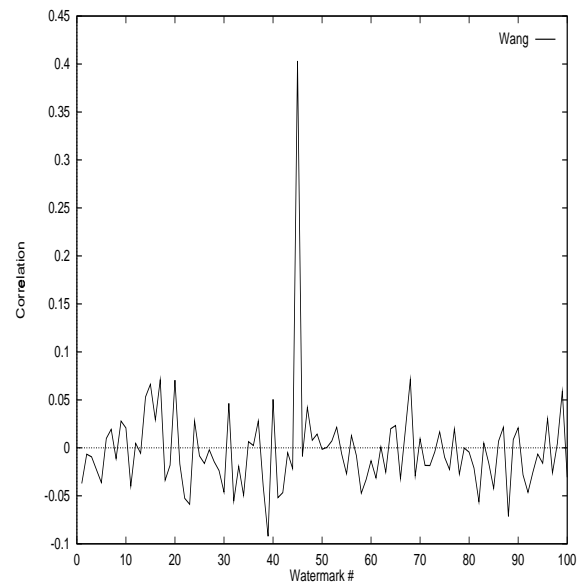
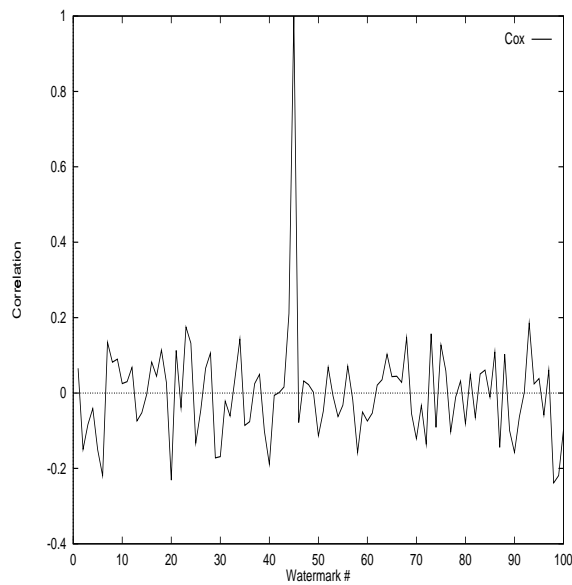
# Vergleich der Verfahren: Robustheit



Algorithm	PSNR
Cox	35.35
Koch	48.36
Wang	41.53
Kundur	55.86

# Vergleich der Verfahren: Sicherheit

---



# Verbesserungsmöglichkeiten und Ausblick

---

- Sicherheit durch schlüsselabhängige Wahl der Wavelet-Transformation
- Ausnutzen der Schwächen des HVS, erhöhen der Robustheit
- Verbesserte Korrelation durch zusätzliches Referenz-Watermark (siehe Kundur)
- Protokolle, Standards, . . .

# Literatur

- [1] Wang, H.-J., Su, P.-C., und Kuo, C.-C.,  
Wavelet-Based Digital Image Watermarking, Optics  
Express, Volume 3, Nummer 12, Dezember 1998.
  
- [2] Koch, E., und Zhao, J., Towards Robust and  
Hidden Image Copyright Labeling, Proceedings of  
the IEEE International Workshop on Nonlinear  
Signal and Image Processing, p. 452 - 455,  
Halkidiki, Greece, pp. 452 - 455, Juni 1995.
  
- [3] Kundur, D., und Hatzinakos, D., Digital  
Watermarking Using Multiresolution Wavelet  
Decomposition, Proceedings of the IEEE  
International Conference on Acoustics, Speech and  
Signal Processing ICASSP '98, Volume 5, pp.  
2969 - 2972, Mai 1998.
  
- [4] Cox, I. J., Kilian, J., Leighton, T., und Shamoon,  
T., Secure Spread Spectrum Watermarking for  
Images, Audio and Video, Proceedings of the IEEE  
International Conference on Image Processing,  
pp. 243 - 246, September 1996.

- [5] Craver, S., Memon, N., Yeo, B.-L., Yeung, M. M.,  
On the Invertability of Invisible Watermarking  
Techniques, Proceedings of the IEEE International  
Conference on Image Processing ICIP '97, p. 540,  
Santa Barbara, USA, Oktober 1997.
  
- [6] Wang, H.-J., Kuo, C.-C., High fidelity image  
compression with multithreshold wavelet coding  
(MTWC), SPIE's Annual Meeting - Application of  
Digital Image Processing XX, San Diego, USA,  
July 27 - August 1, 1997.
  
- [7] Wolfgang, R. B., Podilchuk, C. I., und Delp, E. J.,  
The effect of matching watermark and compression  
transforms in compressed color images, Proceedings  
of the IEEE International Conference on Image  
Processing ICIP '98, Chicago, USA, October 1998.
  
- [8] Xia, X.-G., Boncelet, C. G., und Arce, G. R.,  
Wavelet transform based watermark for digital  
images, Optics Express, Volume 3, Nummer 12,  
Dezember 1998.
  
- [9] Kundur, D., und Hatzinakos, D., Attack  
characterization for effective watermarking,

Proceedings of the IEEE International Conference on Image Processing ICIP '99, 1999.

- [10] Benham, D., Memon, N., Yeo, B.-L., und Yeung, M. M., Fast Watermarking of DCT-based Compressed Images, Proceedings of the International Conference on Image Science, Systems and Technology CISST '97, Juni 1997.
- [11] Busch, C., Funk, W., und Wolthusen, S., Digital Watermarking: From Concepts to Real-Time Video Applications, IEEE Computer Graphics and Applications Journal, Jänner/Februar 1999
- [12] Bartolini, F., Barni, M., Cappellini, V., und Piva, A., Mask building for perceptually hiding frequency embedded watermarks, Proceedings of the IEEE International Conference on Image Processing ICIP '98, Chicago, USA, p. 450 - 454, Oktober 1998.