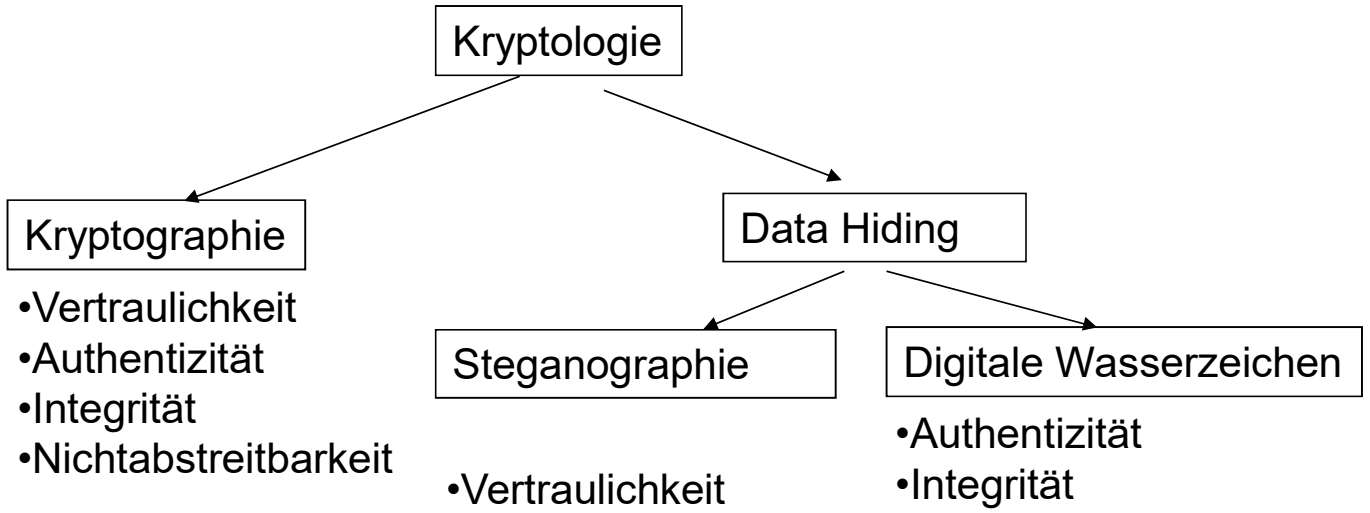
Steganographie/ Überleitung Wasserzeichen

- Herausforderung Mediensicherheit:
  - Urheberschutz
- Macht hier Steganographie Sinn?
  - Ja, wenn man zum Beweis der Urheberschaft einen Schlüssel „zückt“ und mit ihm eine Information aus dem Medium extrahiert
  - Aber:
    - K muss sicher sein
    - M muss schwer aus C entfernbar sein

- Wasserzeichenverfahren
  - Schutz durch Integration von Informationen direkt in das Datenmaterial selbst
  - Anwendung von steganographischen Techniken (geheime Nachrichten sozusagen unsichtbar machen)
  - Für Bild, Video, Audio, 3D…



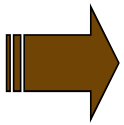
- Digitales Wasserzeichen:
  - transparentes, nicht wahrnehmbares Muster (Signal)
  - Muster/Signal repräsentiert die eingebrachte Information, meist Zufalls-Rauschsignal (pseudo-noise signal)
  - Präsenzwasserzeichen oder Codierung von Informationsbits
  - besteht in Analogie zur Steganographie aus:
    - Einbettungsprozeß E: Watermark Embedding
      - CW=E(C, W, K)
    - Abfrageprozeß/Ausleseprozeß R: Watermark Retrieval
      - W=R(CW, K)

        » K=Key (Schlüssel)
        » W=Watermark (eingebrachte Information)
        » C=Cover (Trägersignal)
        » CW= watermarked Cover (markiertes Trägersignal)

Digitale Wasserzeichen/ Klassifizierung: Anwendungsgebiet

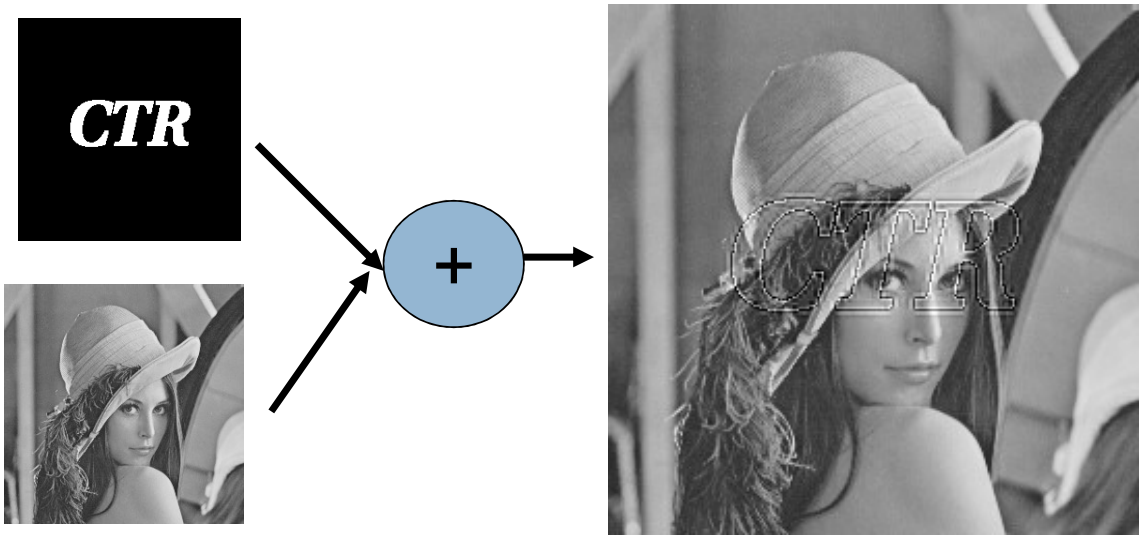
- Verfahren zur Urheberidentifizierung (Authentifizierung): Copyright Watermarks
- Verfahren zur Kundenidentifizierung (Authentifizierung): Fingerprint Watermarks
- Verfahren zur Annotation des Datenmaterials:
  Caption Watermarks
- Verfahren zur Durchsetzung des Kopierschutzes oder Übertragungskontrolle: Copy Control Watermarks oder Broadcast Watermarks
- Verfahren zum Nachweis der Unversehrtheit (Integritätsnachweis): Integrity Watermark/ Verfication Watermarks

- Robustheit (robuste und fragile)
- Security (gezielte Angriffe, Invertierbarkeit)
- Detektierbarkeit (verdeckte Kommunikation)
- Wahrnehmbarkeit (Transparenz)
- Komplexität (blinde/nicht blinde)
- Kapazität (ein oder mehrere Info-Bits)
- Geheime/Öffentliche Verifikation (privat, public)
- Invertierbarkeit

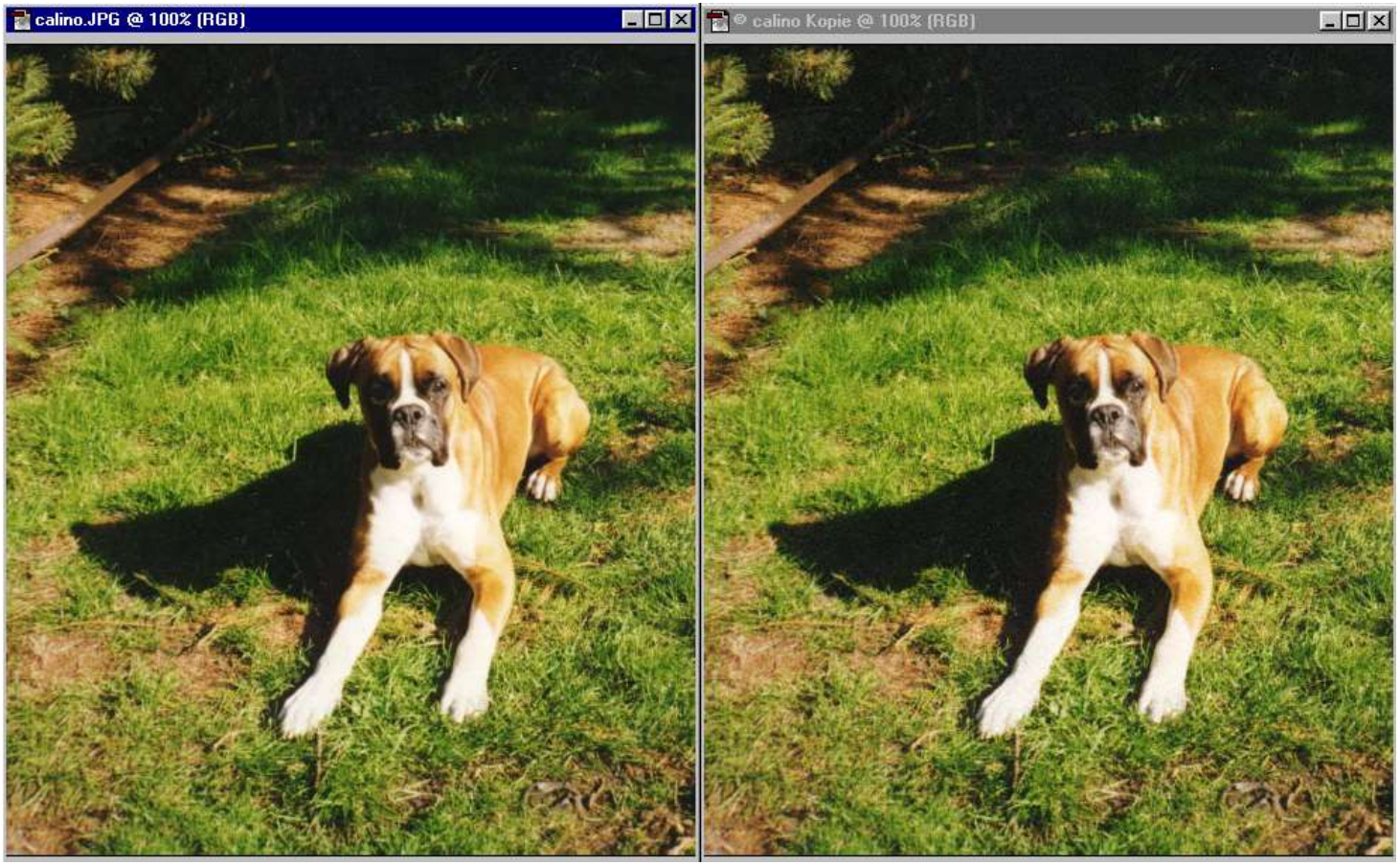


Konkurrenz der Parameter

- deutlich sichtbares Symbol im Bild
  - Fernsehrsender: Logo in oberen Ecke
  - Bilddatenbanken

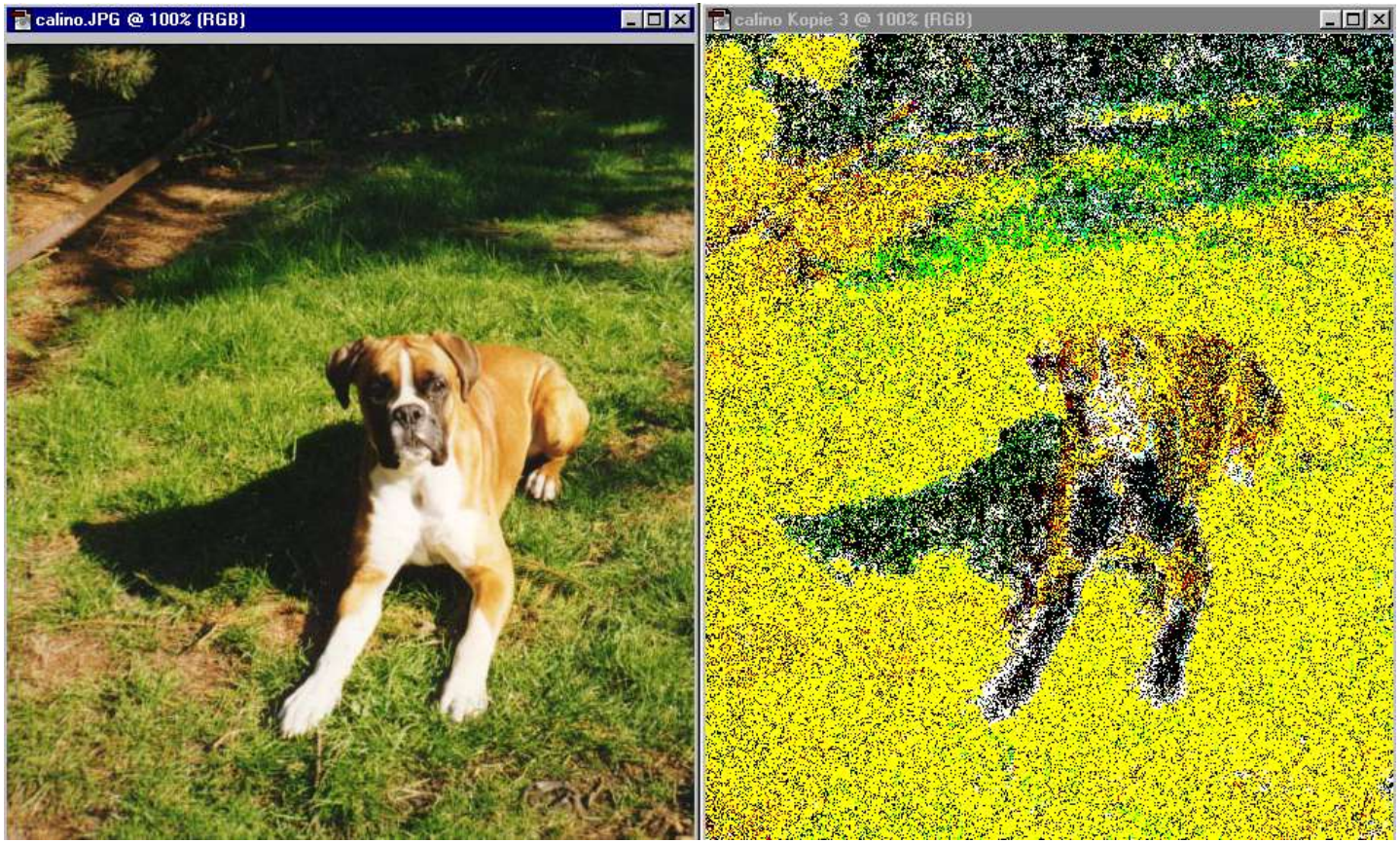


Beispiel Wasserzeichen: Digimarc

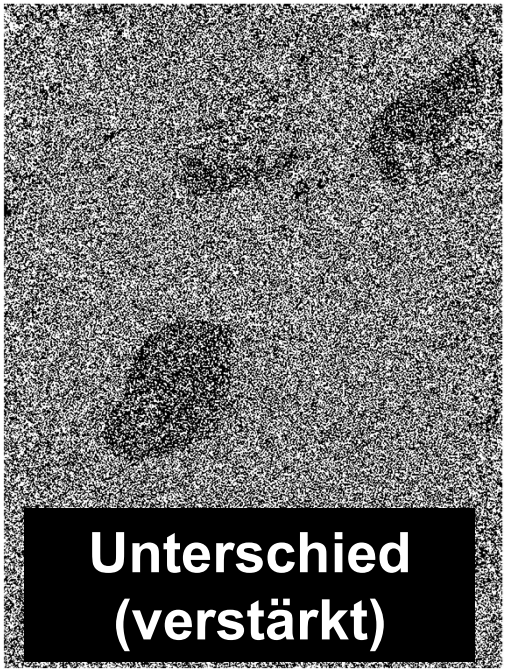


Beispiel Wasserzeichen - Zoom

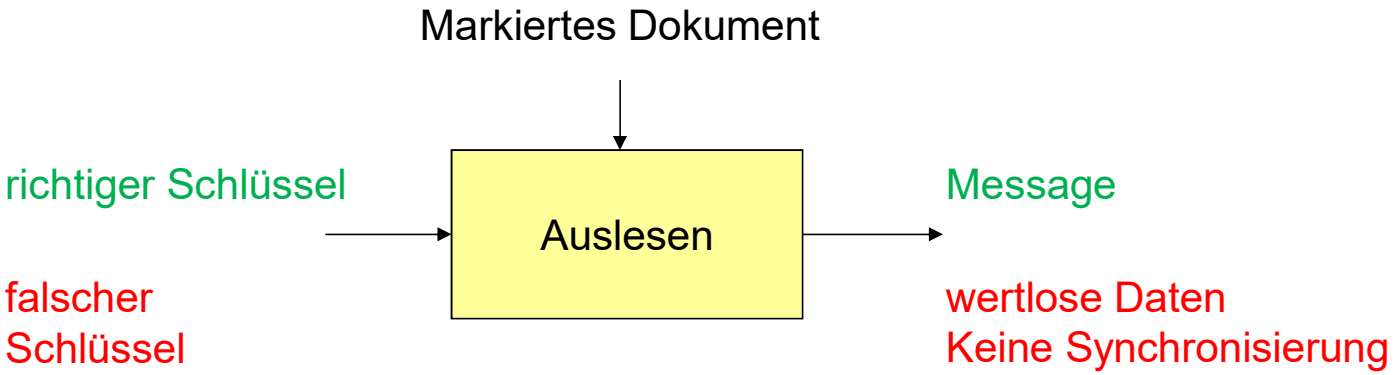
Beispiel Wasserzeichen - Differenz



Beispiel Wasserzeichen - Differenz

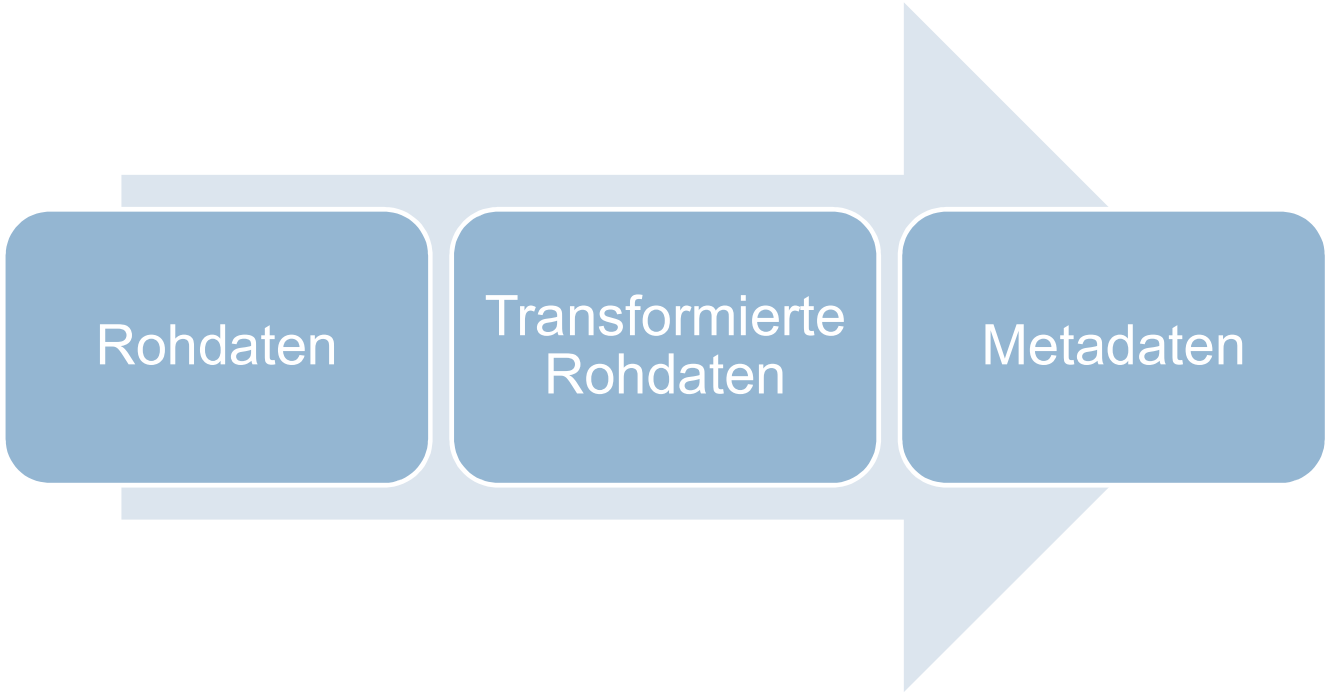


- Informationen können nicht ermittelt, gelesen und/oder von unberechtigten Dritten abgeändert werden.
- Die Sicherheit liegt in der Verborgenheit des Schlüssels, nicht in der Verborgenheit des Algorithmus.



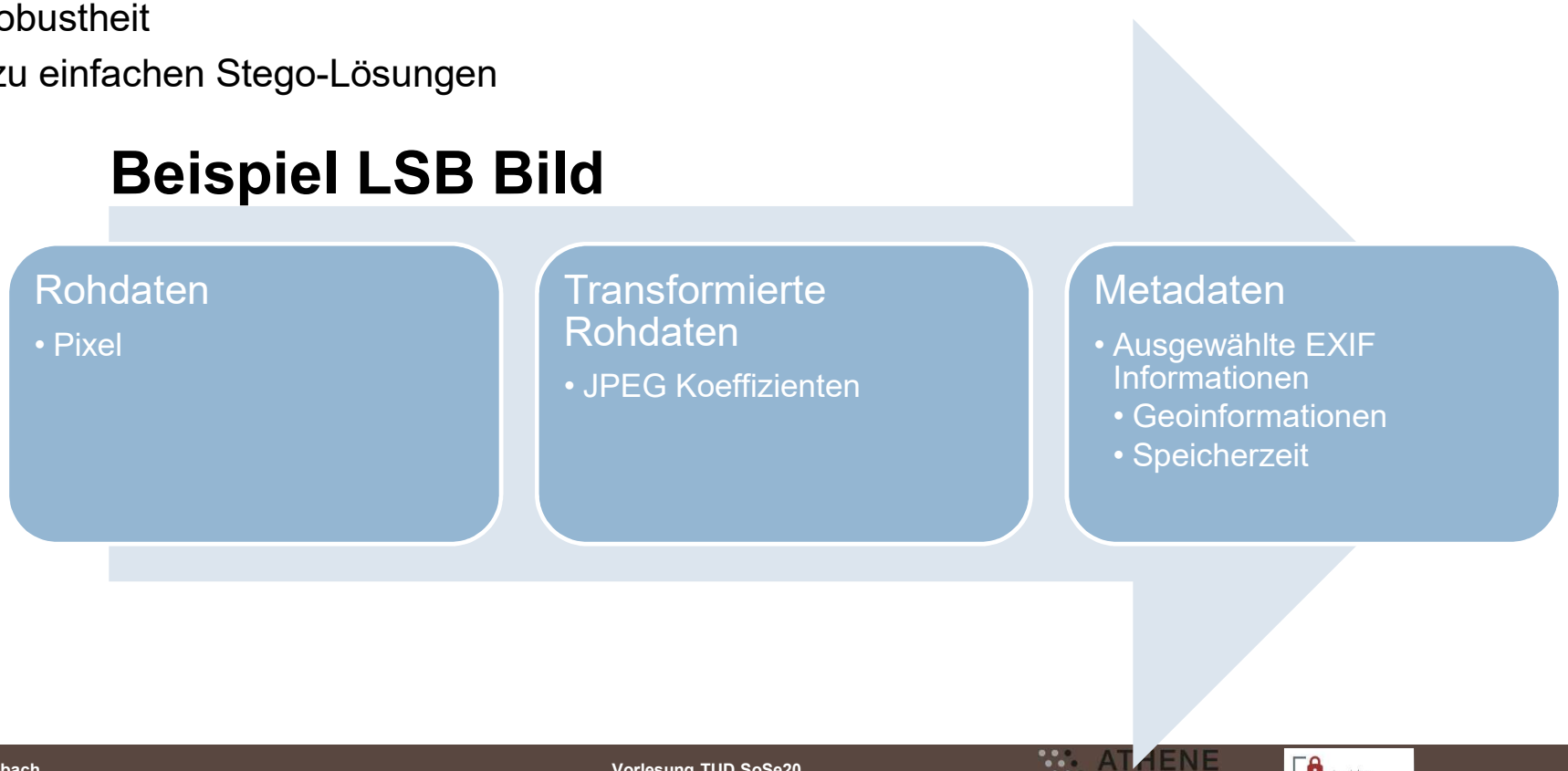
- Problem
  - Sicherheit für Wasserzeichen nur im Bildbereich teilweise erforscht
  - Forscher vertreten teilweise die Meinung, sichere Wasserzeichen seien nicht möglich
  - Kommerzielle Verfahren werden nicht veröffentlicht
    - Unsicherheit beim Kunden
  - Sicherheit verschiedener Verfahren konnte gebrochen werden
  - Beispiel: BOWS-Contest
    - http://bows2.ec-lille.fr
    - Bildwasserzeichen
    - Online-Verifikation des Wasserzeichens
    - Herausforderung: Löschen des Wasserzeichens bei hoher Bildqualität
  - Wasserzeichen wurden erfolgreich angegriffen
  - Orakel ermöglichte ein SNR von über 50dB
  - Codeanalyse und 10.000 Beispielbilder als Training erlaubten ähnliche Angriffe
  - Reine Bildmanipulation brachte nur 20dB

- Es existieren verschiedene Strategien zum Einbetten von Wasserzeichen
  - Viele unterschiedliche Medientypen (Video, Audio, Bild, Text etc.)
  - Viele unterschiedliche Dateiformate (MPEG, JPEG, GIF, WMA, PDF, DOC etc.)
  - Abhängig vom Trägersignal
    - Kein echtes Rauschen in Textdaten
    - Wenige Freiheitsgrade in MIDI-Daten



- Least significant bit (LSB) Wasserzeichen
  - Einbetten der Information durch Ersetzen des LSB
  - Hohe Datenrate
  - Niedrige Komplexität
  - Keine Robustheit
  - Analog zu einfachen Stego-Lösungen

Beispiel LSB Bild

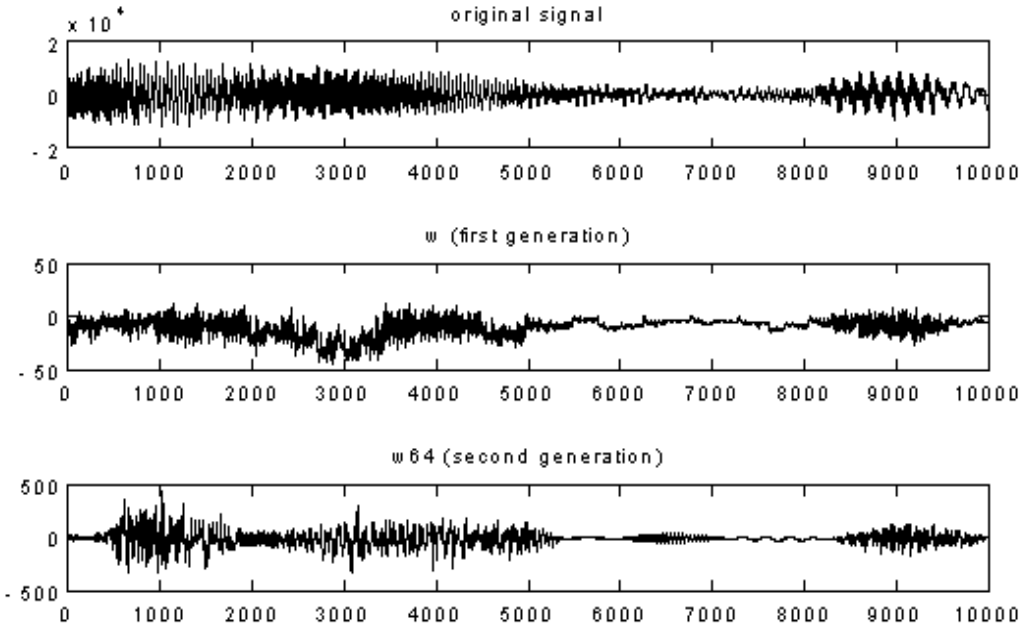


Grundlegende Prinzipien

- Einbetten von Rauschen
  - Wasserzeichen wird durch Pseudorauschen dargestellt
  - Trägersignal wird „künstlich verrauscht“ durch Addition des Rauschsignals
  - Auslesen des Wasserzeichens durch Korrelation
  - Mehrere Bits einbettbar durch Verwendung mindestens zweier Pseudorauschsignale

- Einbetten von Rauschen, Beispiel
  - Boney, Tewfik and Hamdy Laurence Boney, Ahmed H . Tewfik , and Khaled N. Hamdy, Digital Watermarks for Audio Signals, 1996 IEEE Int. Conf. on Multimedia Computing and Systems June 17-23, Hiroshima, Japan, p. 473-480
  - PCM Audio Verfahren
  - Verwendet MPEG Psychoakustik
  - Nicht-Blind (Original wird zum Auslesen benötigt)

- Original
- Wasserzeichen
- Wasserzeichen, mp3 gefiltert



Boney, Tewfik and Hamdy Laurence Boney, Ahmed H . Tewfik , and Khaled N. Hamdy, Digital Watermarks for Audio Signals, 1996 IEEE Int. Conf. on Multimedia Computing and Systems June 17-23, Hiroshima, Japan, p. 473-480

Grundlegende Prinzipien

- Statistische Verfahren
  - Verändern von statistischen Eigenschaften des Trägersignals
  - Auslesen durch Prüfen dieser Eigenschaften
    - Z.B. Eigenschaft über oder unter Durchschnitt
  - Erfordert Kenntnisse über Eigenschaften des Signals
  - Oft werden Schwellwerte und logarithmische Werte verwendet, um Robustheit zu erreichen

- (Naives) Beispiel für statistisches Verfahren:
  - 10 Samples: 10, 9, 1, 5, 1, 3, 9,5, 6, 2
  - Pseudozufällige Auswahl von je 4 Samples in Gruppe A und B (Auswahl=rot)
    - A: 10, 9, 1, 5, 1, 3, 9,5, 6, 2 = 25
    - B: 10, 9, 1, 5, 1, 3, 9,5, 6, 2 = 24
    - Ungefähr gleich, kein WZ zu entdecken
  - Regel: A > B => „0“, B > A => „1“
  - „1“ Einbetten
  - B muss größer A werden

- Beispiel:
  - A reduzieren, B erhöhen
    - A: 10, 8, 1, 4, 1, 3, 8,5, 6, 1 = 21
    - B: 10 (!), 9, 1, 5, 1, 4, 9,6, 7, 2 = 28
  - B deutlich größer als A
  - Geringe individuelle Änderungen
  - Resultierende Samples:
    - 10, 8, 1, 4, 1, 4, 8, 6, 7,1

10	9	1	5	1	3	9	5	6	2	**Ausgangssamples**
B	A	-	A	-	B	A	B	B	A	**Pseudozufällige Auswahl**
+1 / -	-1	-	-1	-	+1	-1	+1	+1	-1	**Veränderung**
10	8	1	4	1	4	8	6	7	1	**Resultierende Samples**