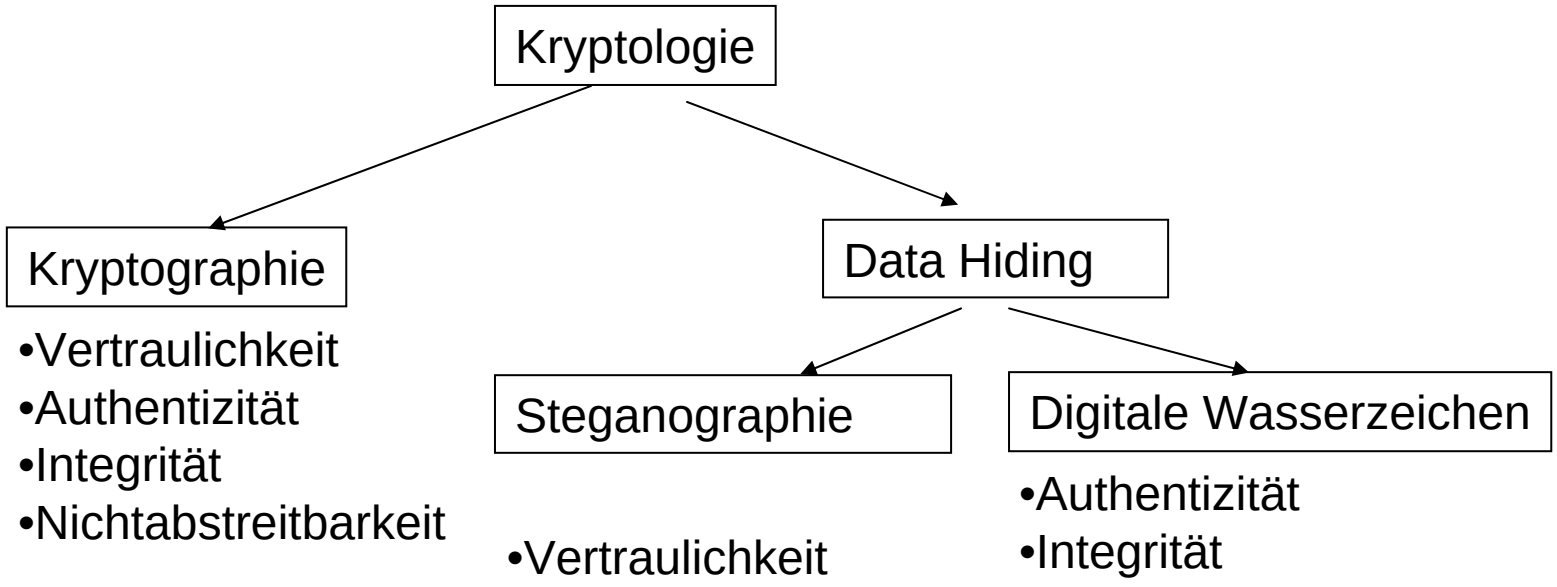
Digitale Wasserzeichen/ Einordnung

- 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…



Digitale Wasserzeichen/ Definition und Terminologie

- 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)

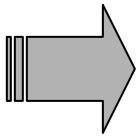
        » K=Key (Schlüssel)
        » W=Watermark (eingebrachte Information)
        » C=Cover (Trägersignal)
        » CW= watermarked Cover (markiertes Trägersignal)

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

Digitale Wasserzeichen/ Klassifikation nach Eigenschaften

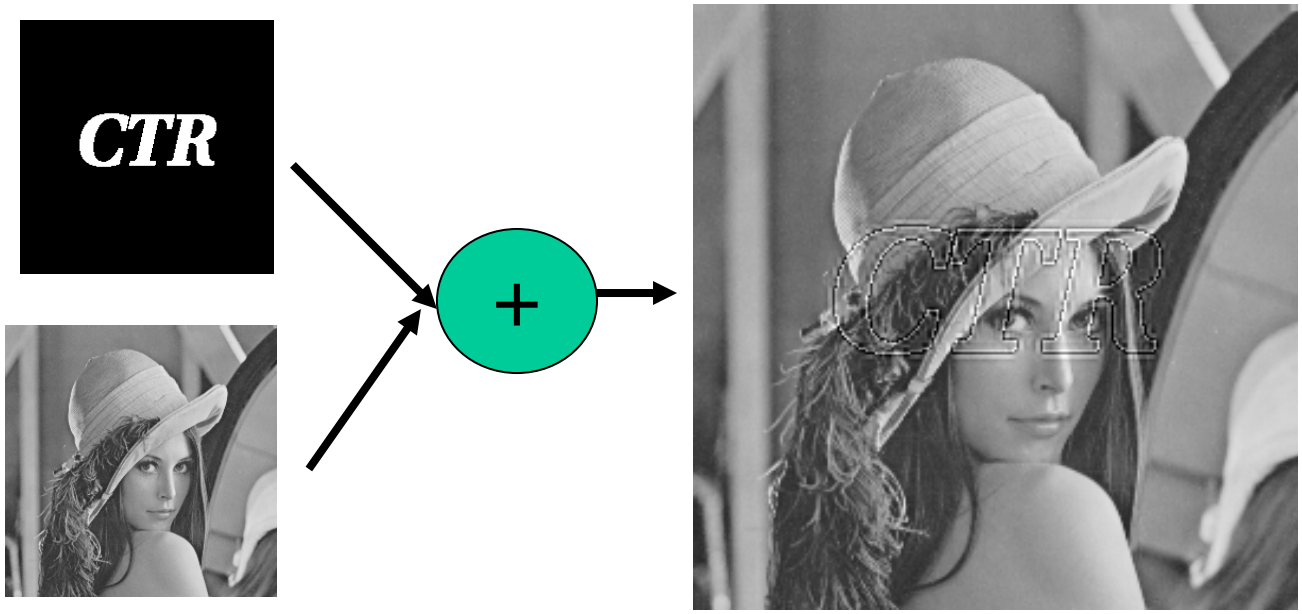
- Robustheit (robuste und fragile)
- Security (gezielte Angriffe, Invertierbarkeit)
- Detektierbarkeit (verdeckte Kommunikation)
- Wahrnehmbarkeit (Transparenz)
- Komplexität (blinde/nicht blinde)
- Kapazität (ein oder mehrere Info-Bits)
- Geheime/Öffentliche Verifikation (privat, public)
- Invertierbarkeit



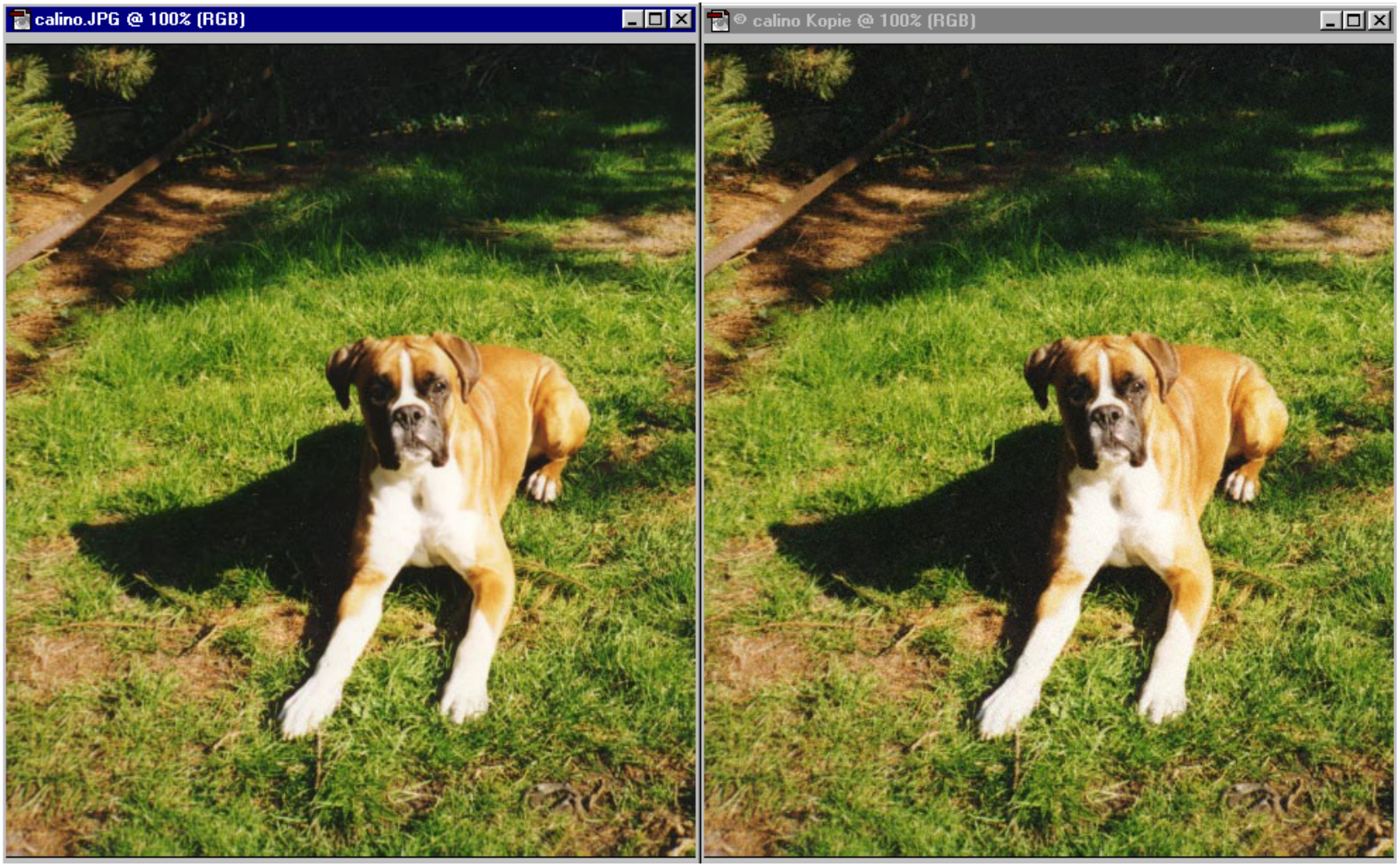
Konkurrenz der Parameter

Digitale Wasserzeichen/ Abgrenzung: Sichtbare Wasserzeichen

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

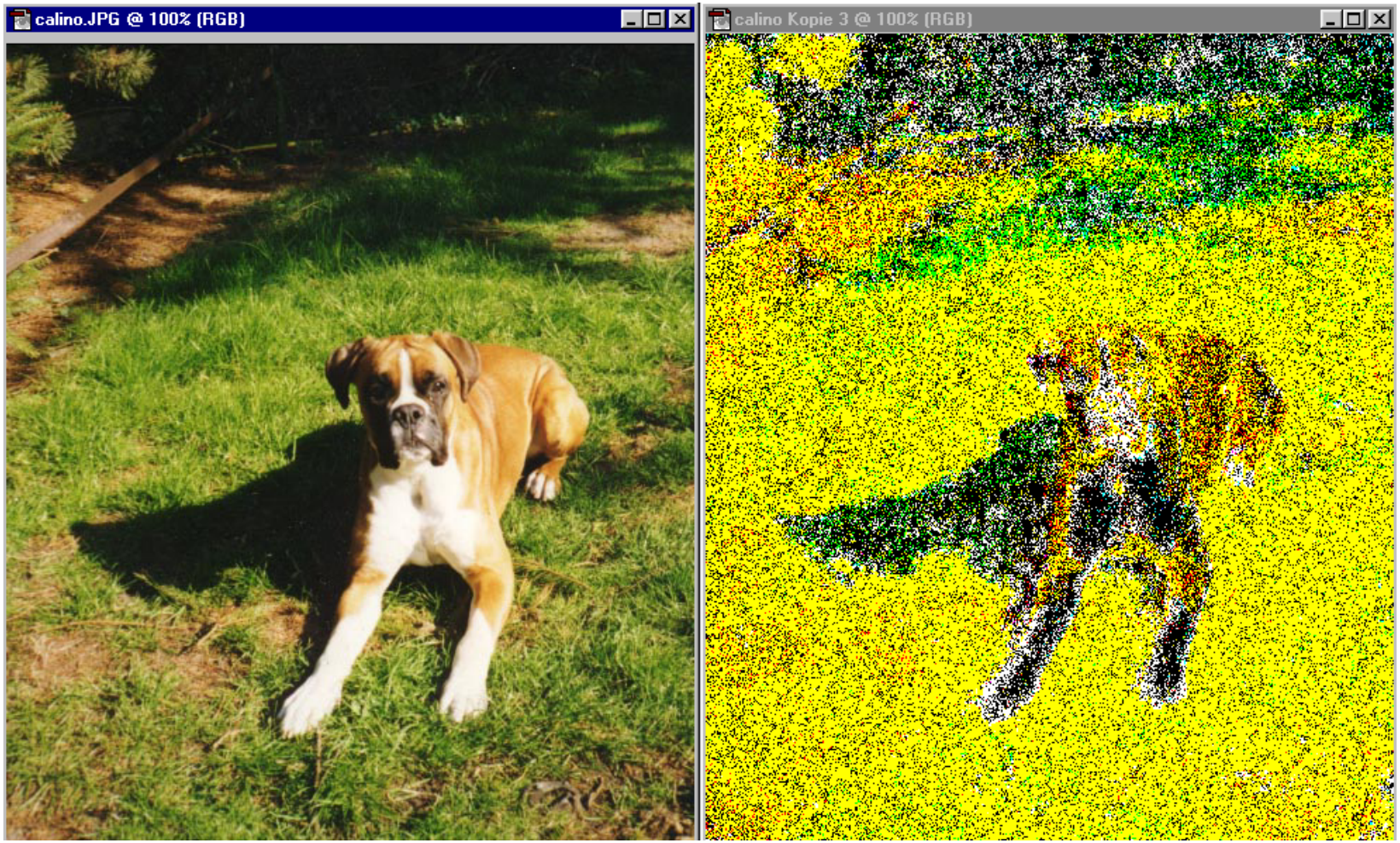


Beispiel Wasserzeichen: Digimarc

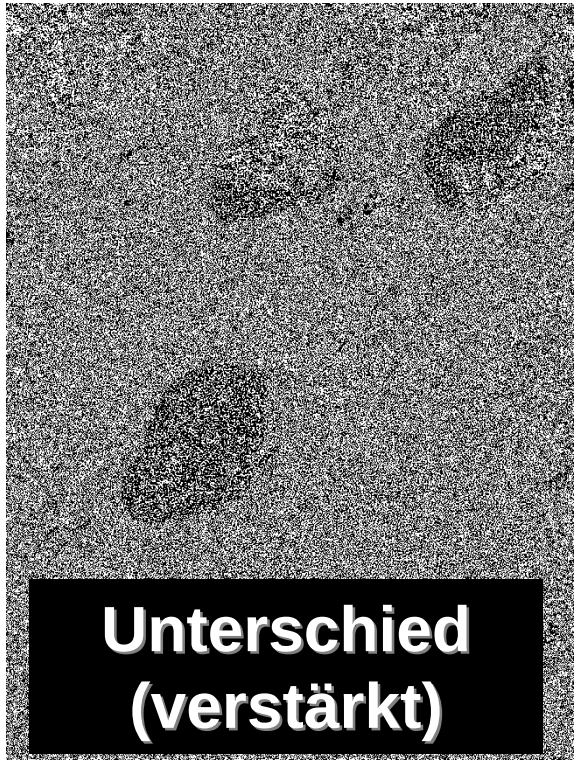


Beispiel Wasserzeichen - Zoom

Beispiel Wasserzeichen - Differenz

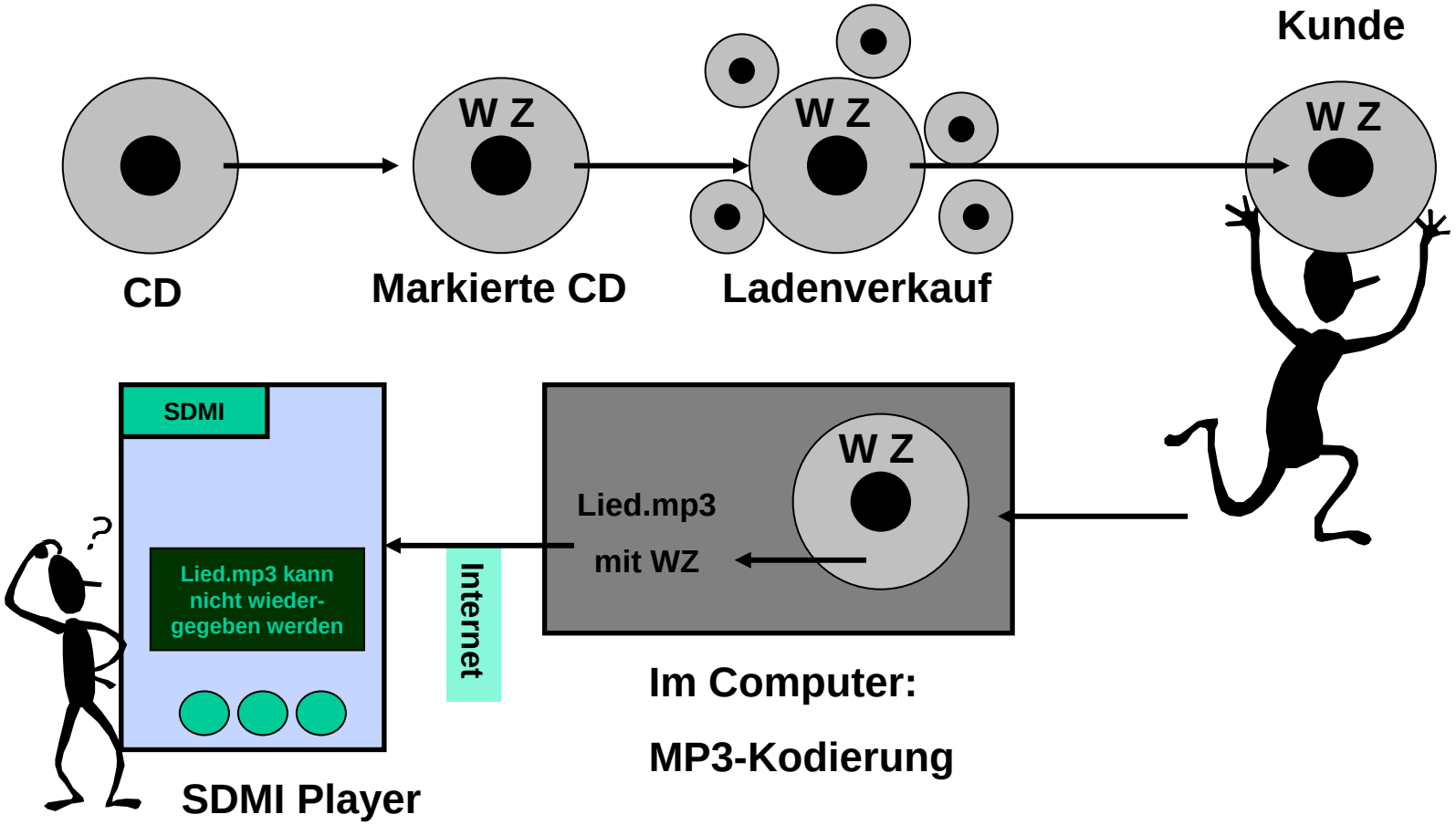


Beispiel Wasserzeichen - Differenz

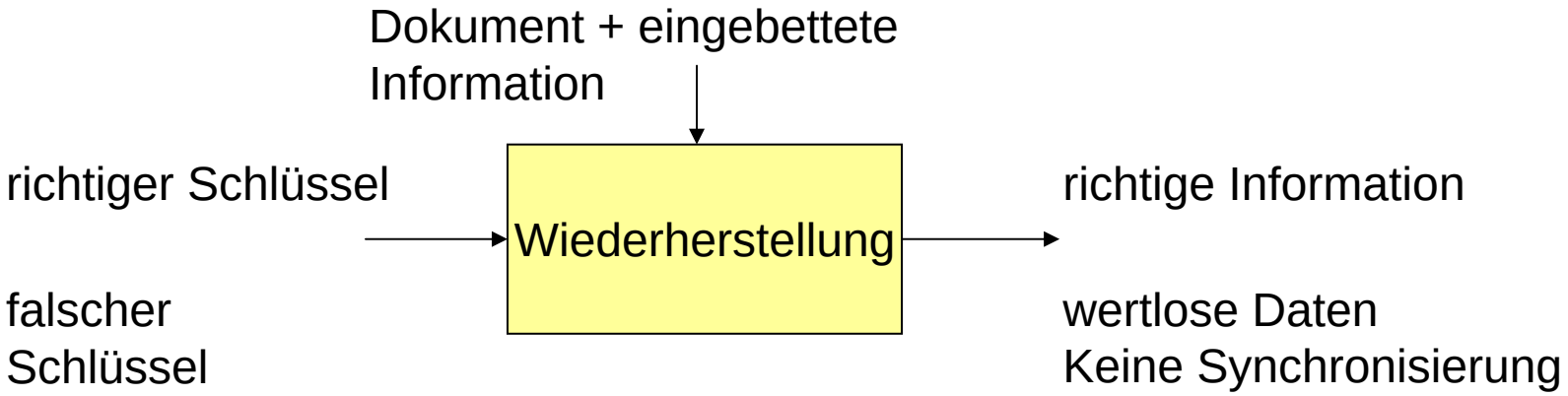


Anwendungsgebiete: Kopierschutz

Beispiel SDMI - Secure Digital Music Initiative:



- 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.



Digitale Wasserzeichen/ Sicherheit

- 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
    - Bildwasserzeichen
    - Online-Verifikation des Wasserzeichens
    - Herausforderung: Löschen des Wasserzeichens bei hoher Bildqualität

Grundlegende Prinzipien

- 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
  - Abhängig von der gewünschten Komplexität
    - Spektralwasserzeichen benötigen Transformation (FFT, DCT, Wavelet etc.)

Grundlegende Prinzipien

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

Grundlegende Prinzipien

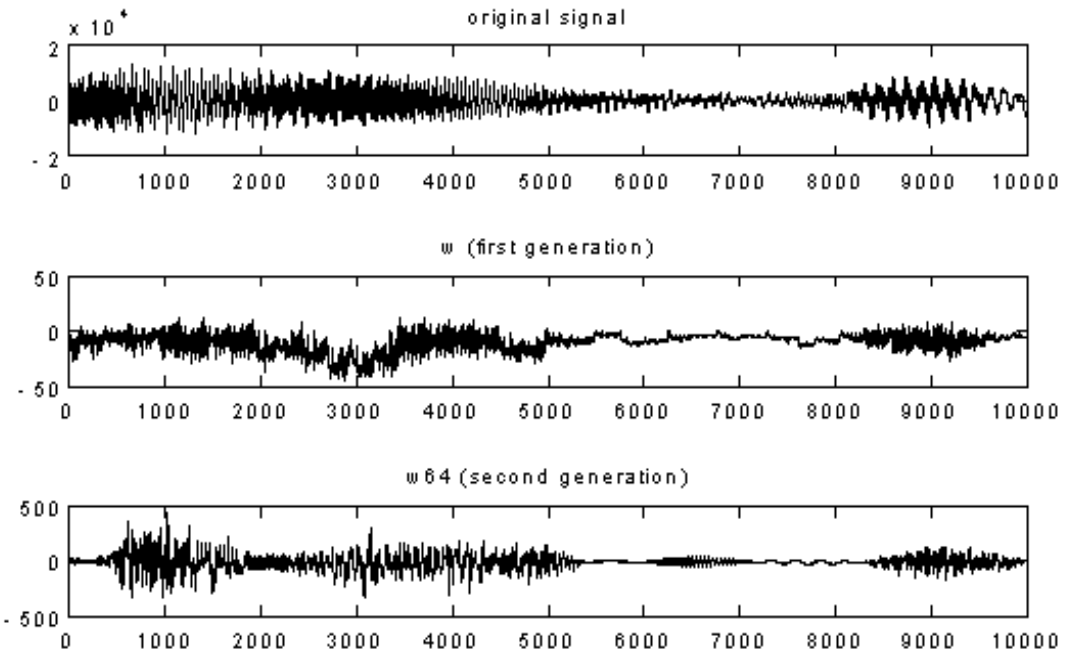
- Einbetten von Rauschen
  - Wasserzeichen wird durch Pseudorauschen dargestellt
  - Trägersignal wird „künstlich verrauscht“ durch Addition des Rauschsignals
  - Auslesen des Wasserzeichens durch Korrelation
  - Mehrere Bits einbettbar durch Verwendung mindestens zweier Pseudorauschsignale

Grundlegende Prinzipien

- 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)

Grundlegende Prinzipien

- Einbetten von Rauschen, Beispiel
- Original
- Wasserzeichen
- Wasserzeichen, mp3 gefiltert



Grundlegende Prinzipien

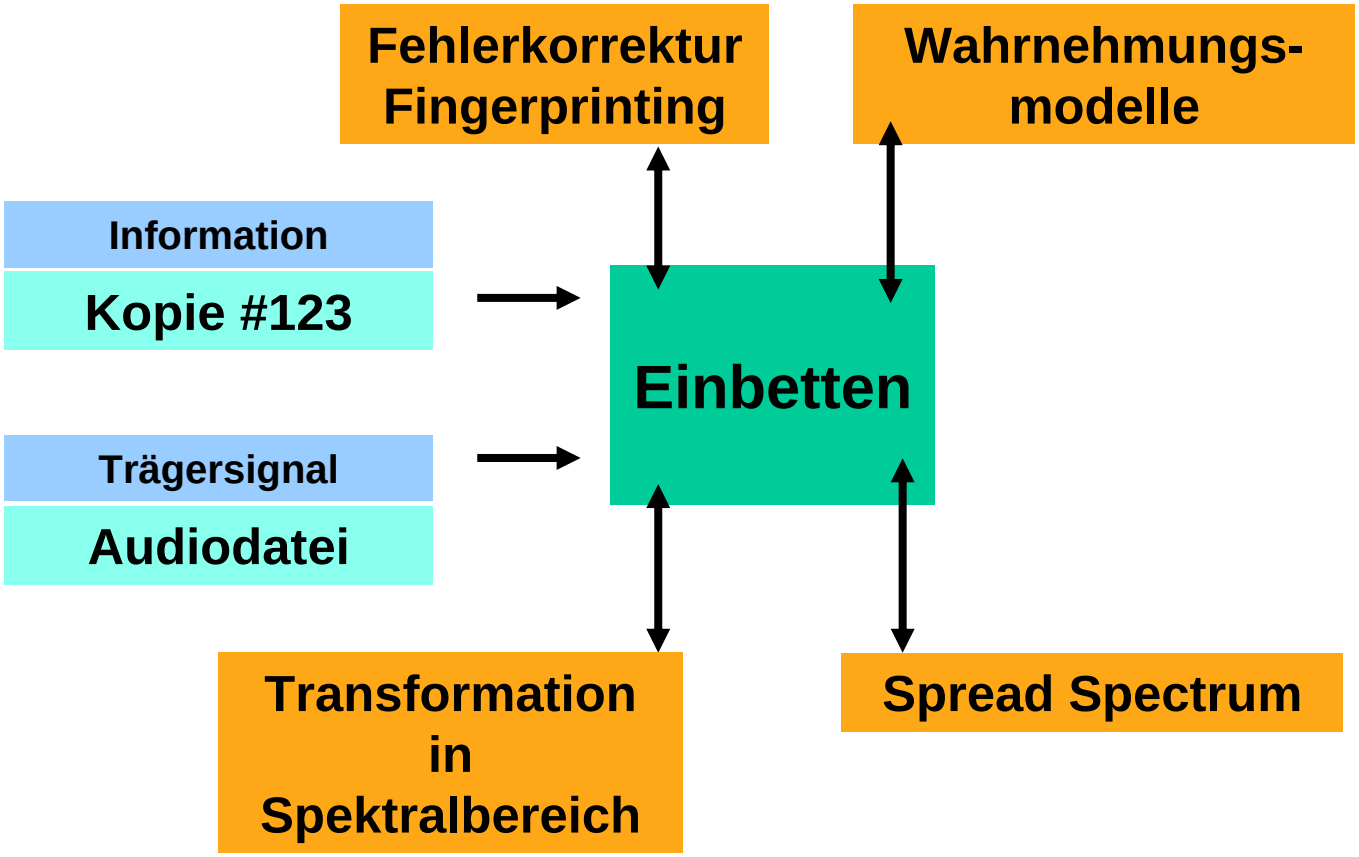
- Statistische Verfahren
  - Verändern von statistischen Eigenschaften des Trägersignals
  - Auslesen durch Prüfen dieser Eigenschaften
    - Z.B. Eigenschaft über oder unter Durchschnitt
  - Erfordert Kenntnisse über Eigenschaften des Signals
  - Oft werden Schwellwerte und logarithmische Werte verwendet,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

- Beispiel für statistisches Verfahren:
  - 10 Samples: 10, 9, 1, 5, 1, 3, 9,5, 6, 2
    - 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

Grundlegende Prinzipien

- 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

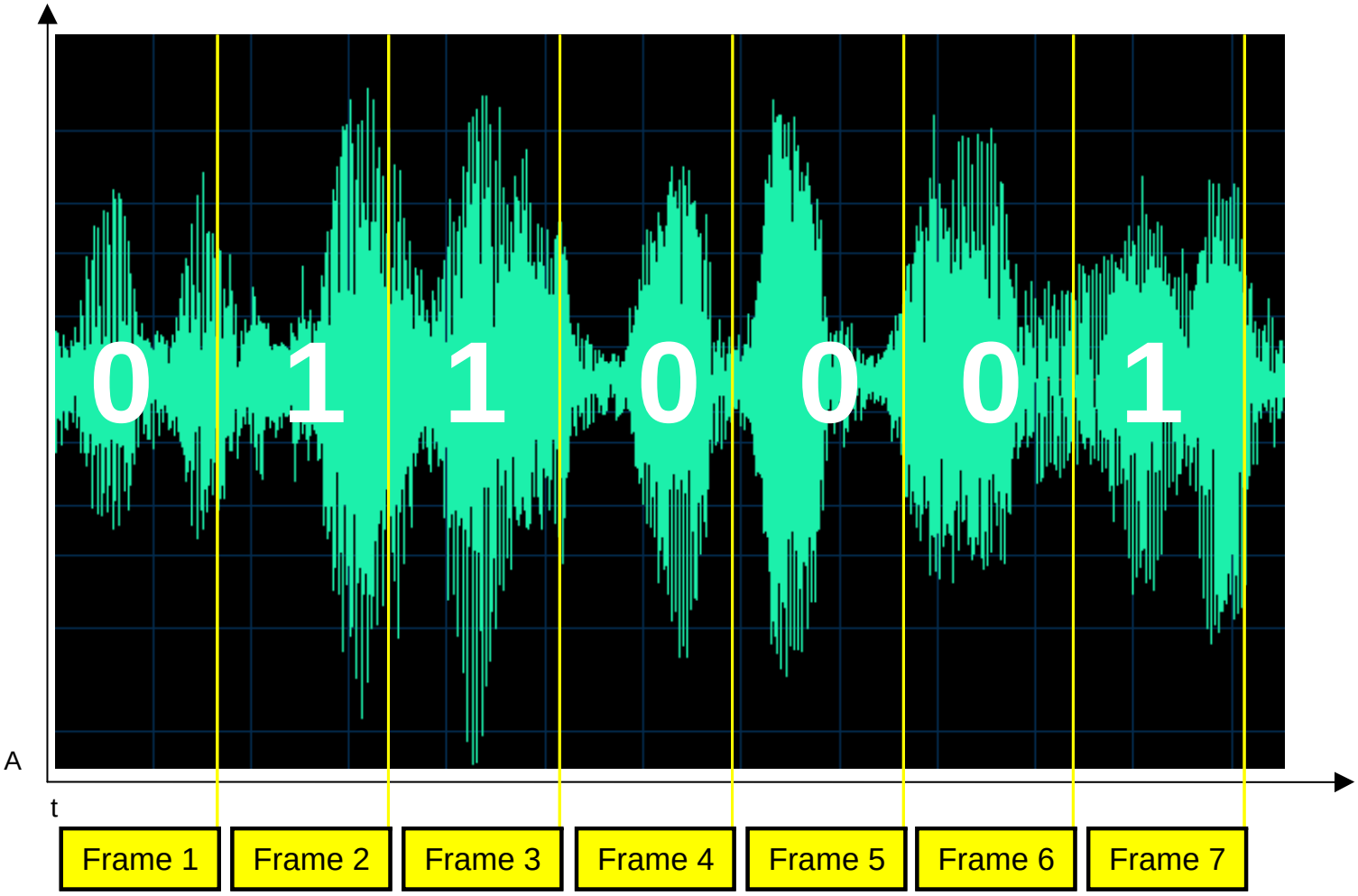
- Digitale Wasserzeichen bestehen oft aus mehreren Modulen:



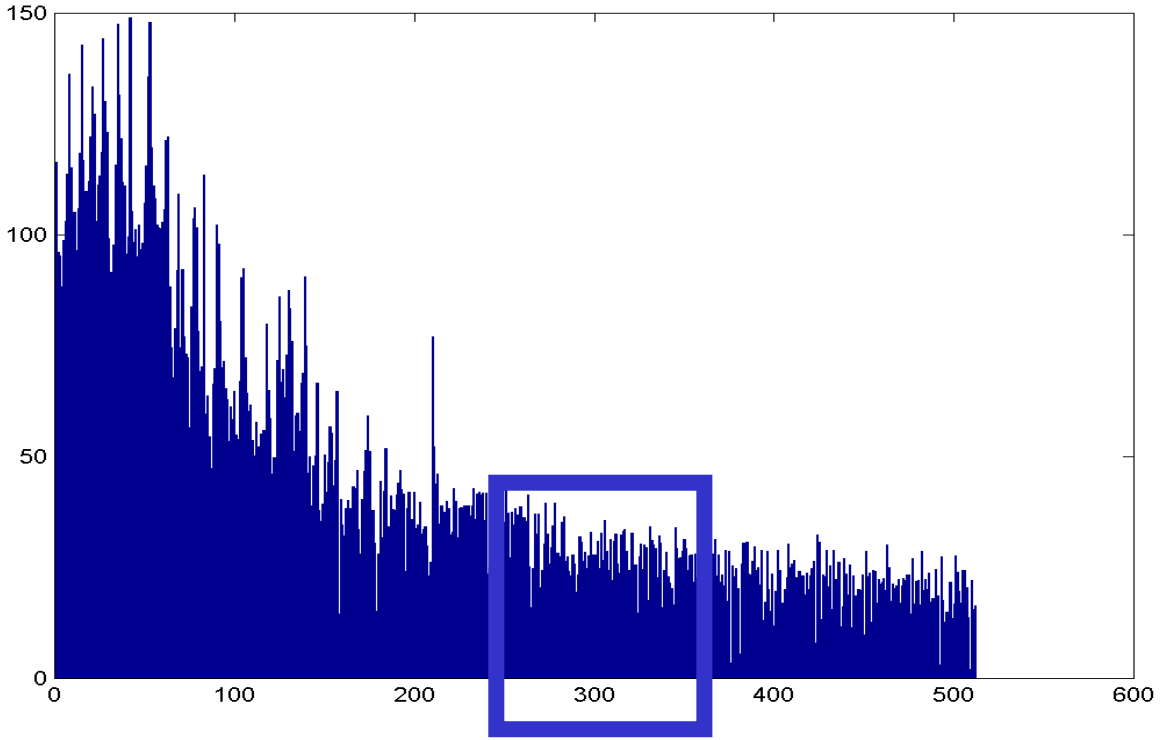
Nur gut aufeinander abgestimmte Module führen zu effizienten und zuverlässigen Verfahren

Digitale Wasserzeichen/ PCM Audiowasserzeichen

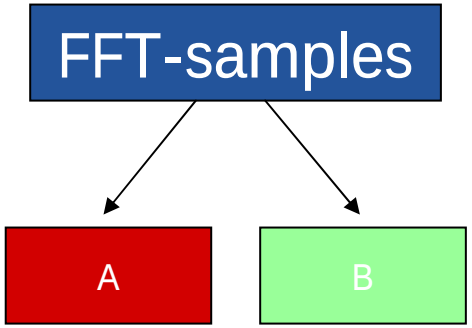
- Einbettung des Wasserzeichens in unabhängigen Abschnitten (Frames)
- Jeder Frame enthält ein Bit

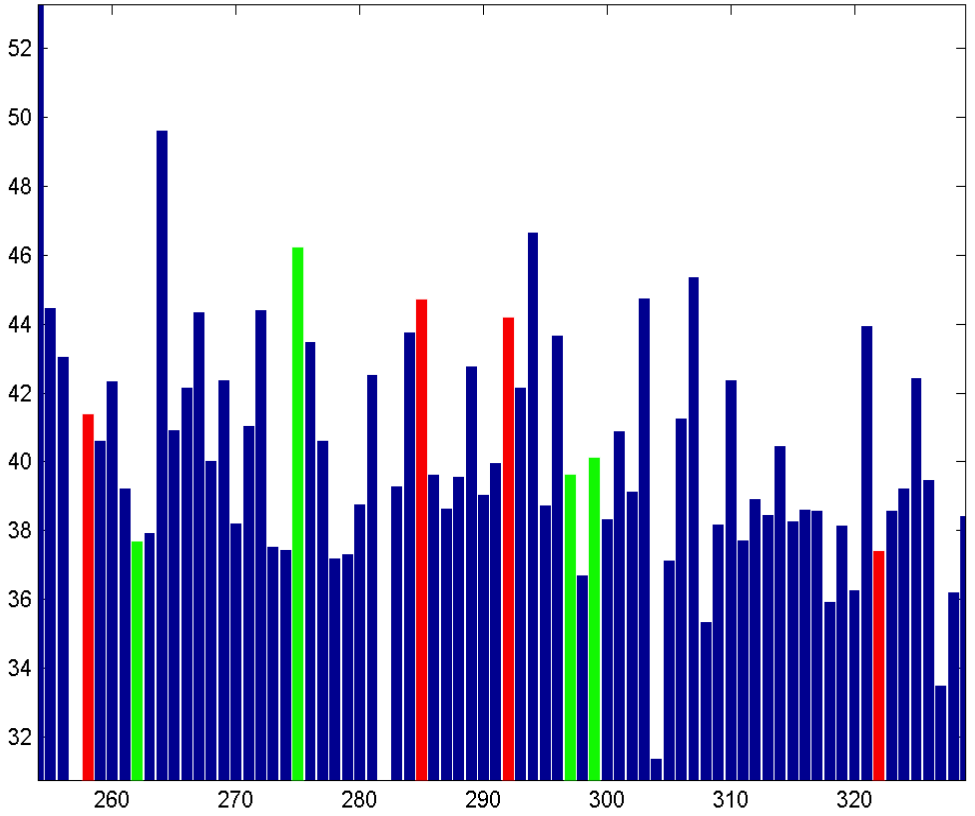


- Prinzip bei der Markierung eines einzelnen Frames:
  - Einbetten des Wasserzeichens im Frequenz-Spektrum
  - Gruppieren der Frequenzbänder



- Prinzip:
- Pseudozufälliges Aufteilen eines Teils der Frequenzbändern in zwei Gruppen A und B





Digitale Wasserzeichen/ PCM Audiowasserzeichen

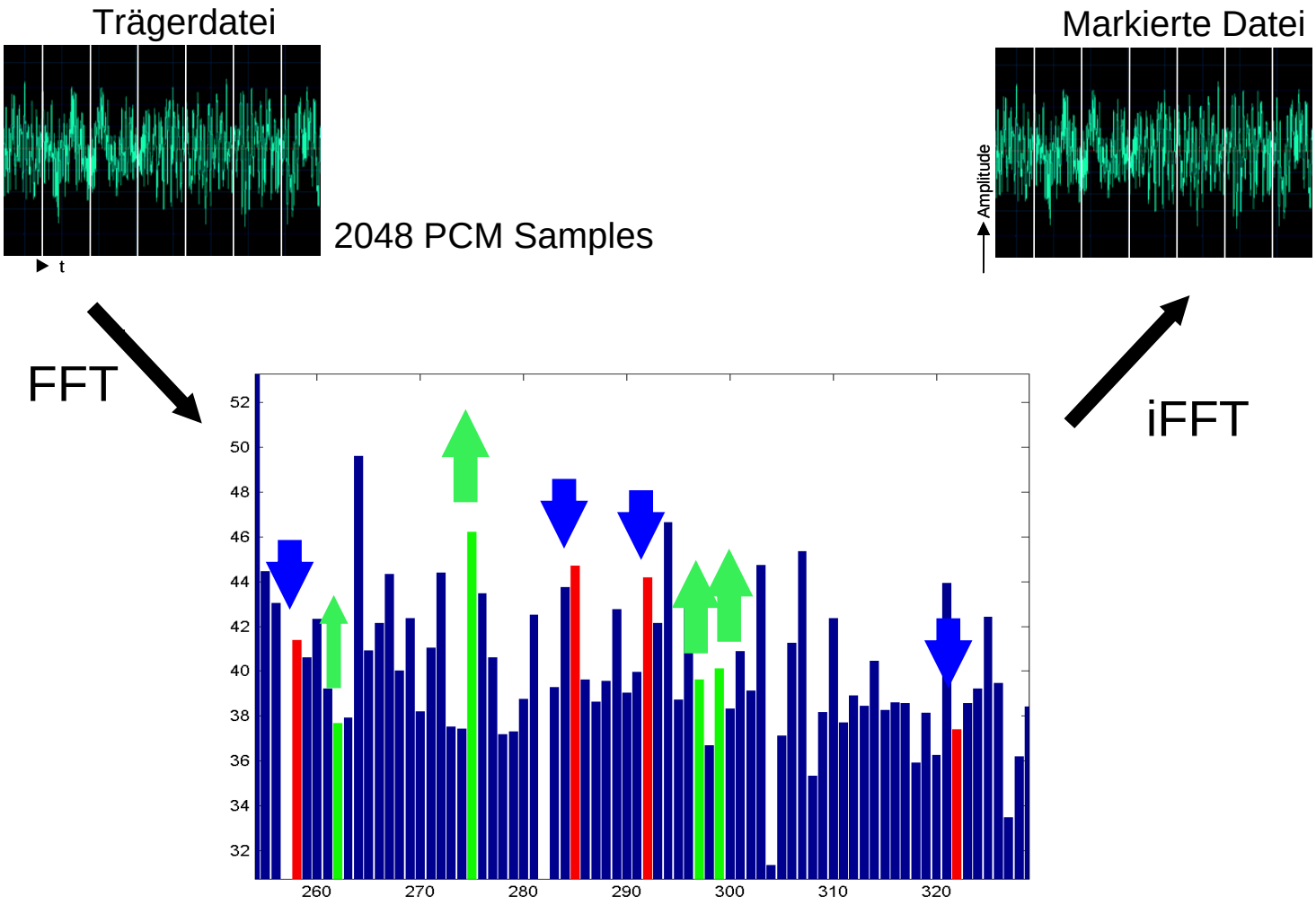
- Prinzip:
  - In unmarkiertem Material: ausgewählte statistische Eigenschaften für Gruppen A und B in der Regel gleich (z.B. Gesamtenergie)
  - Einbettungsprozess: gezielte minimale Erhöhung bzw. Erniedrigung der Energien in den Frequenzbändern, Erzwingen von signifikanter Abweichung der statistischen Eigenschaften in Gruppen A und B
  - Auslese-Prozess: Detektieren von eingebetteter „0“ oder „1“ durch Interpretation des Verhältnisses der Gesamtenergie in Gruppen A und B

Digitale Wasserzeichen/ PCM Audiowasserzeichen

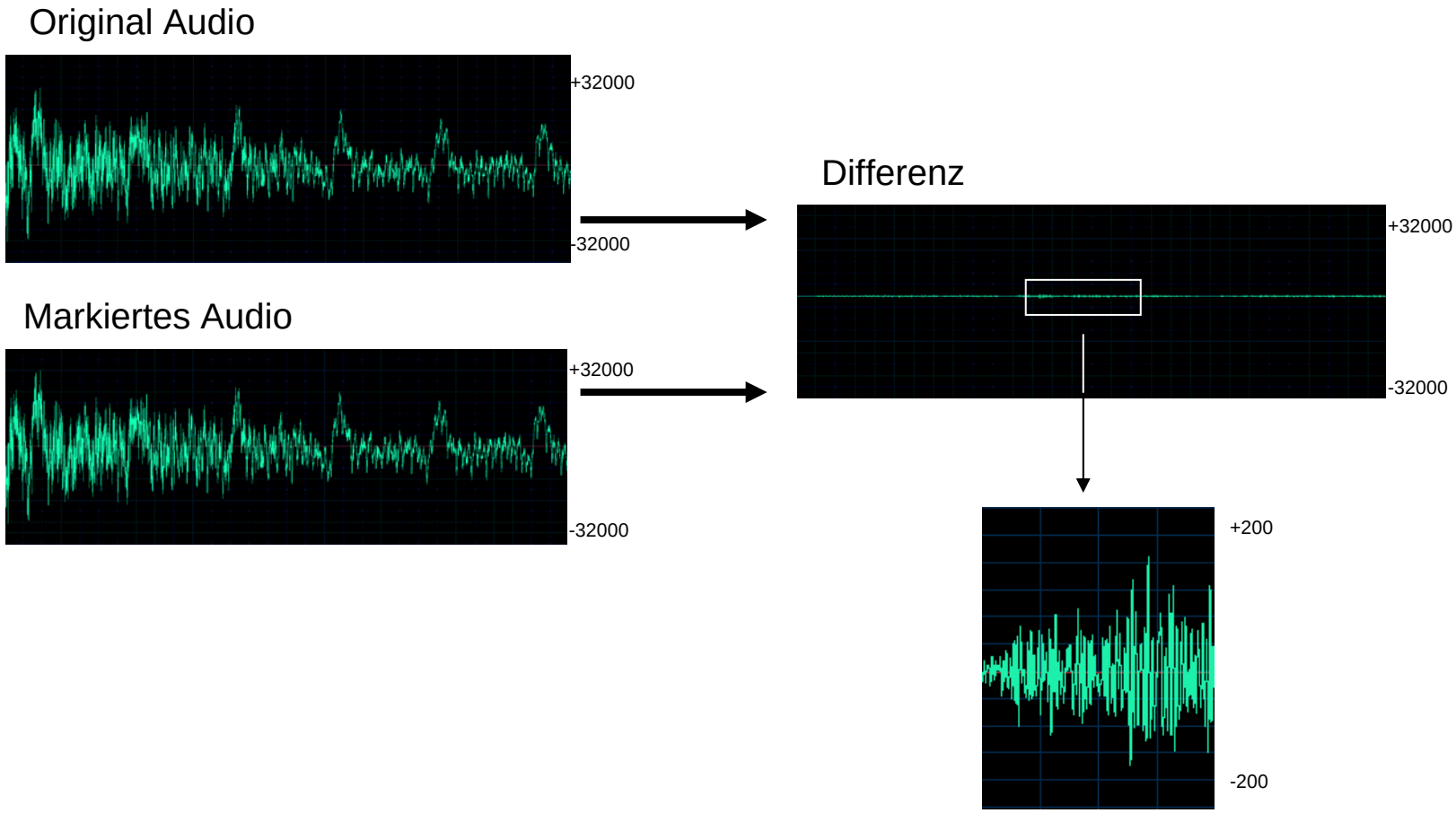
- Prinzip:

WZ-Bit	Gruppe A	Gruppe B
0	Erhöhen	Erniedrigen
1	Erniedrigen	Erhöhen

Digitale Wasserzeichen/ PCM Audiowasserzeichen

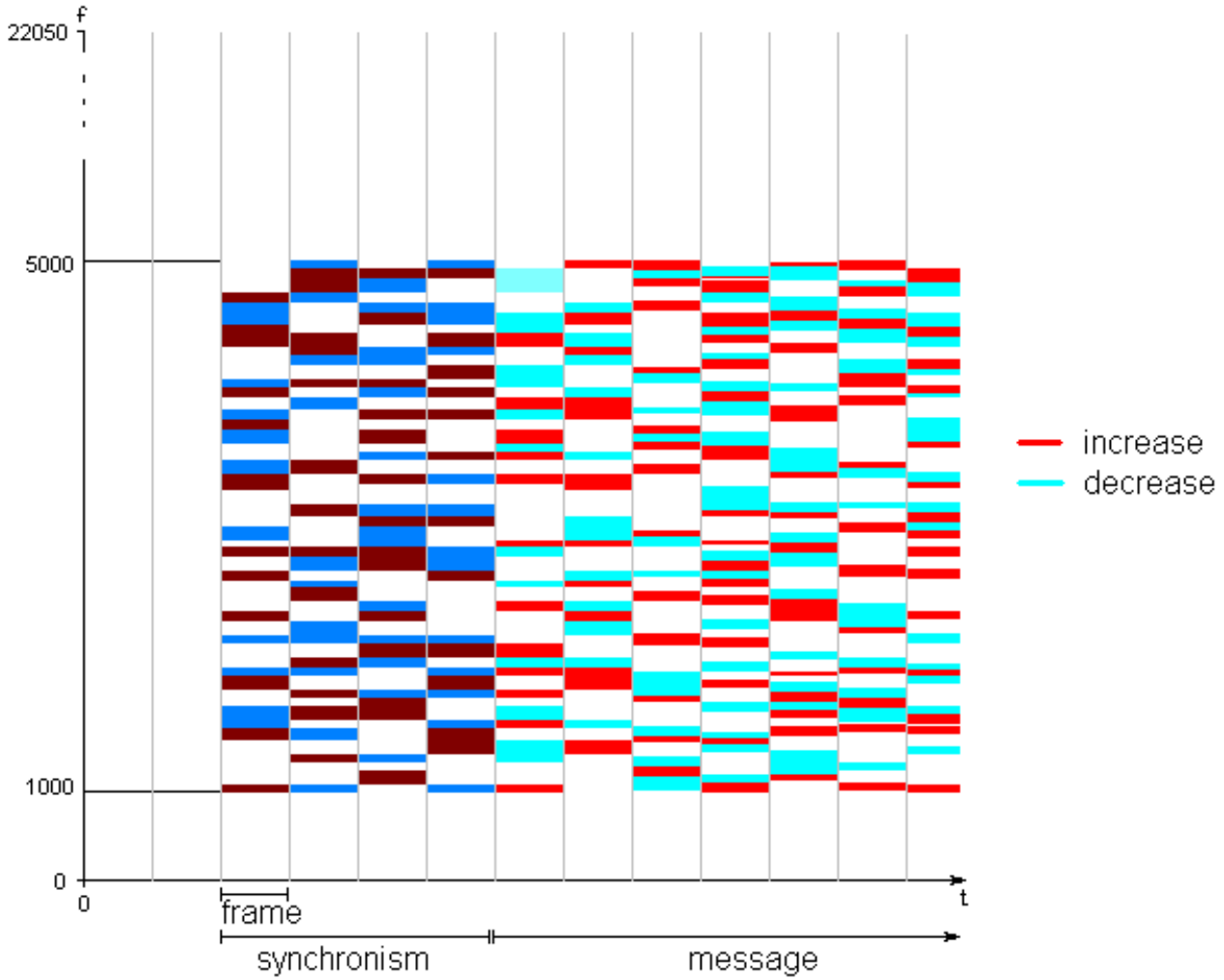


Digitale Wasserzeichen/ PCM Audiowasserzeichen



Differenzsignal besitzt nur sehr geringe Energie

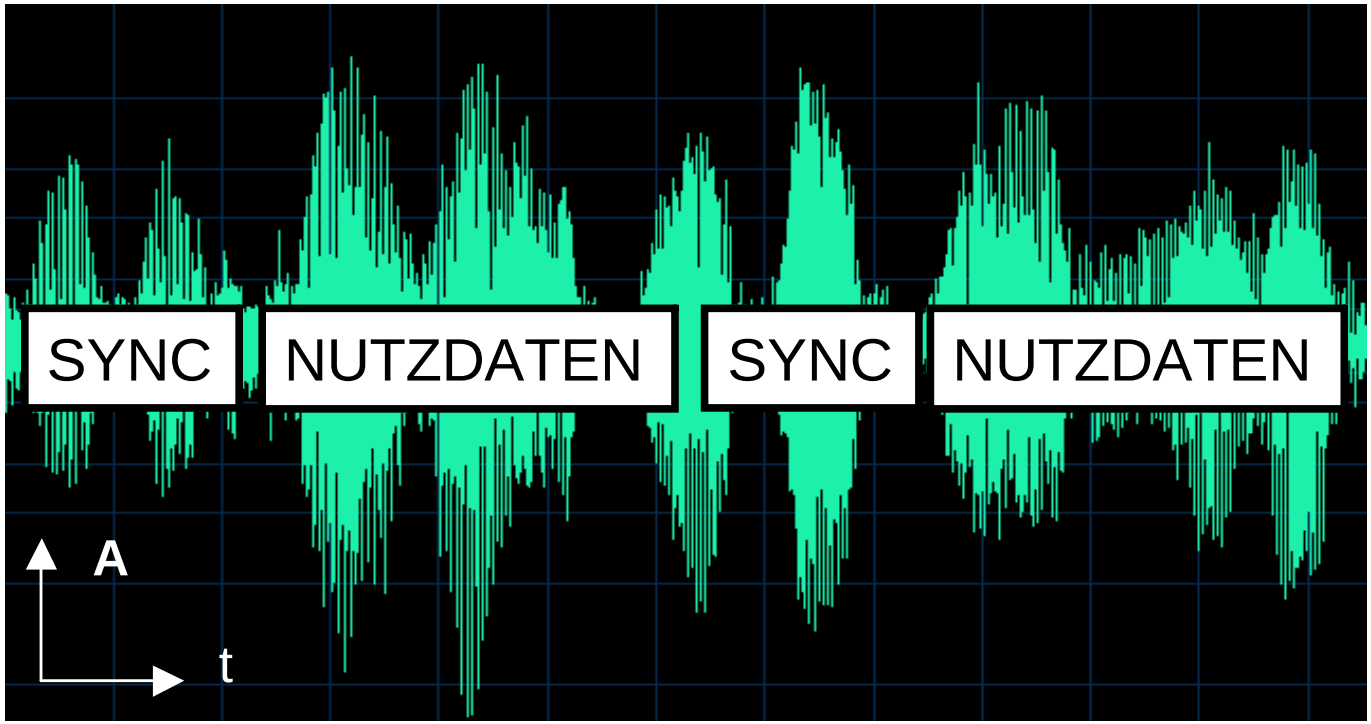
Digitale Wasserzeichen/ PCM Audiowasserzeichen



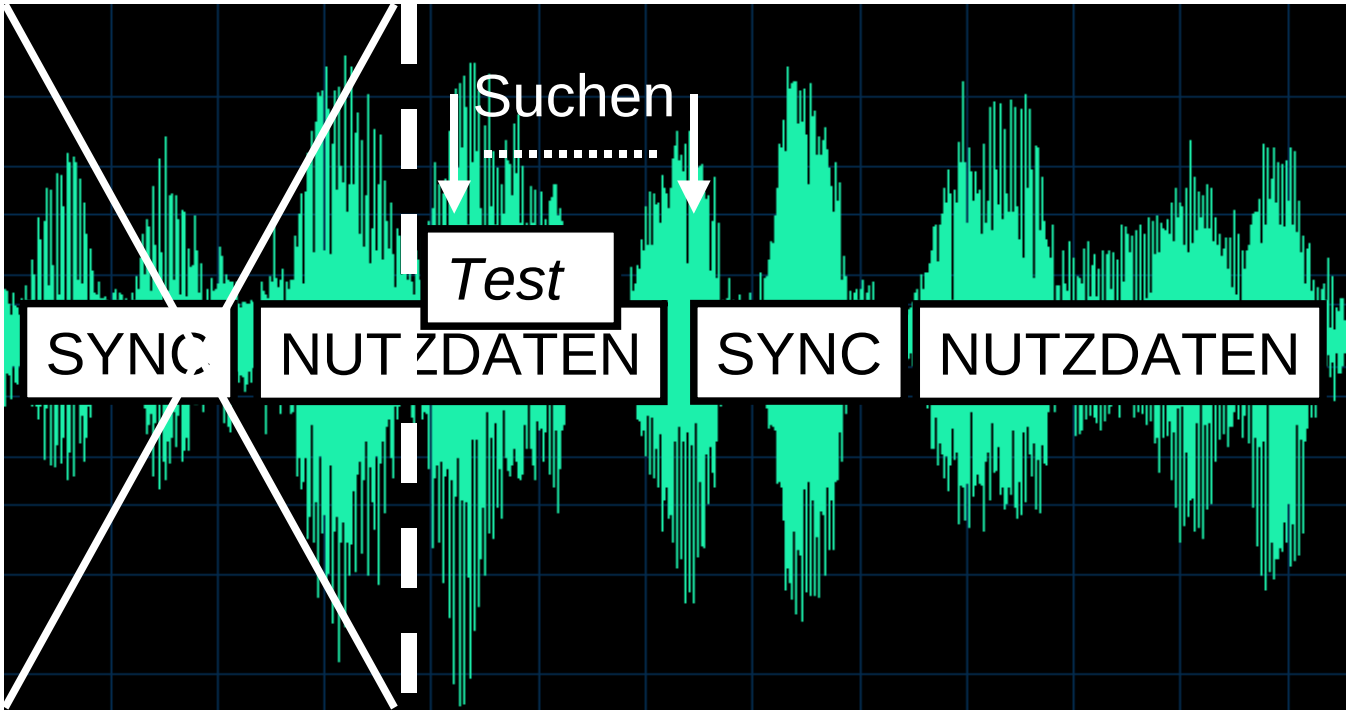
Veränderte Frequenzbänder werden variiert (geheimer Wasserzeichen-Schlüssel)

Digitale Wasserzeichen/ PCM Audiowasserzeichen

- Sychronisierung:
- Sync und Nutzdaten werden abwechselnd eingebettet
- Sync signalisiert Start eines neuen Wasserzeichens



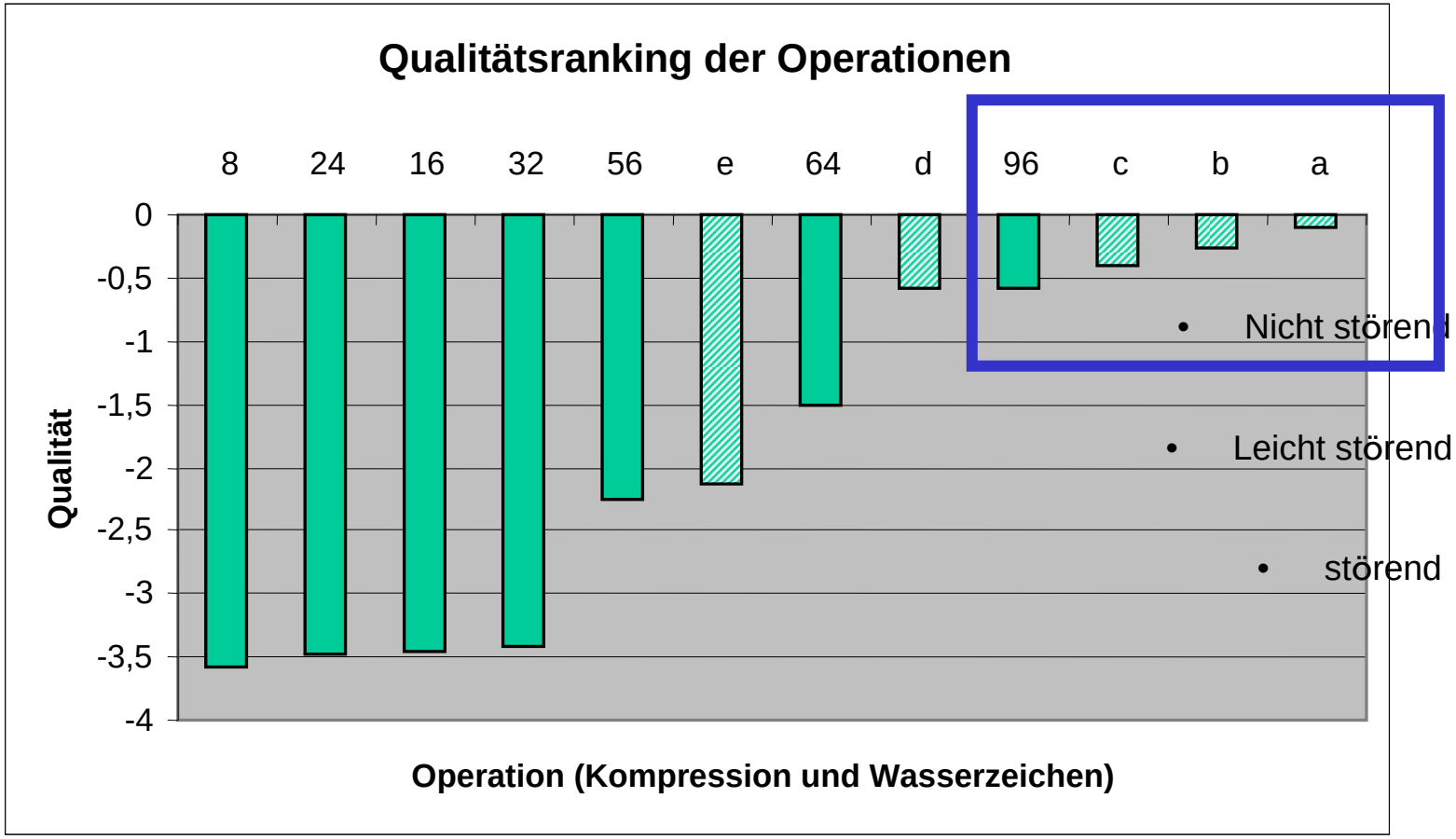
- Nach dem Löschen von Daten kann das Wasserzeichen ab dem nächsten Sync wieder ausgelesen werden
- Robustheit gegen Schneiden des Materials



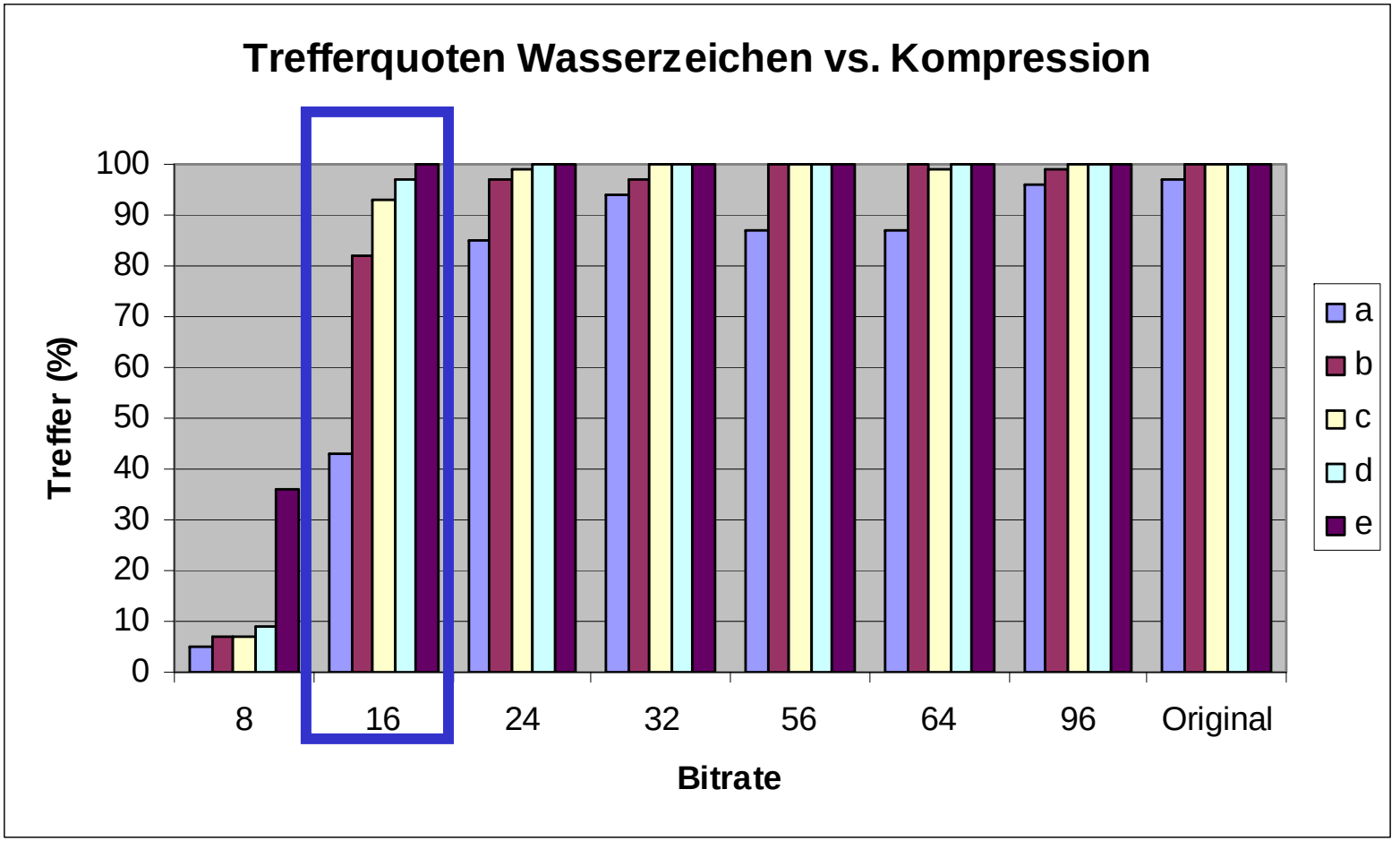
Digitale Wasserzeichen/ PCM Audiowasserzeichen

- Anmerkungen
  - Verschiedene Operationen zum Verändern  der Energie in den Frequenzbändern möglich
  - typischerweise Potenzieren der Energiewerte: Verträglichkeit mit üblichen psychoakustischen Modellen
  - Wo darf der Algorithmus wie stark verändern?
    - Psychoakustische Modelle steuern Einbetten
    - Einbetten in mittleres Frequenzspektrum (z.B. 1000 – 5000 Hz)
    - Typische technische Einstellungen:
      - 180 potentielle Frequenzbänder
      - davon 30 / 30 auswählen
      - Redundanz 3-6 aufeinanderfolgende Frames pro Bit
      - Kapazität: 1 – 10 Bit/s

- Wahrnehmbarkeit - Transparenz
- Vergleich MP3 Kompression (8…96 kBit/s Mono) mit Wasserzeichen bei verschiedenen Stärken (a…e)



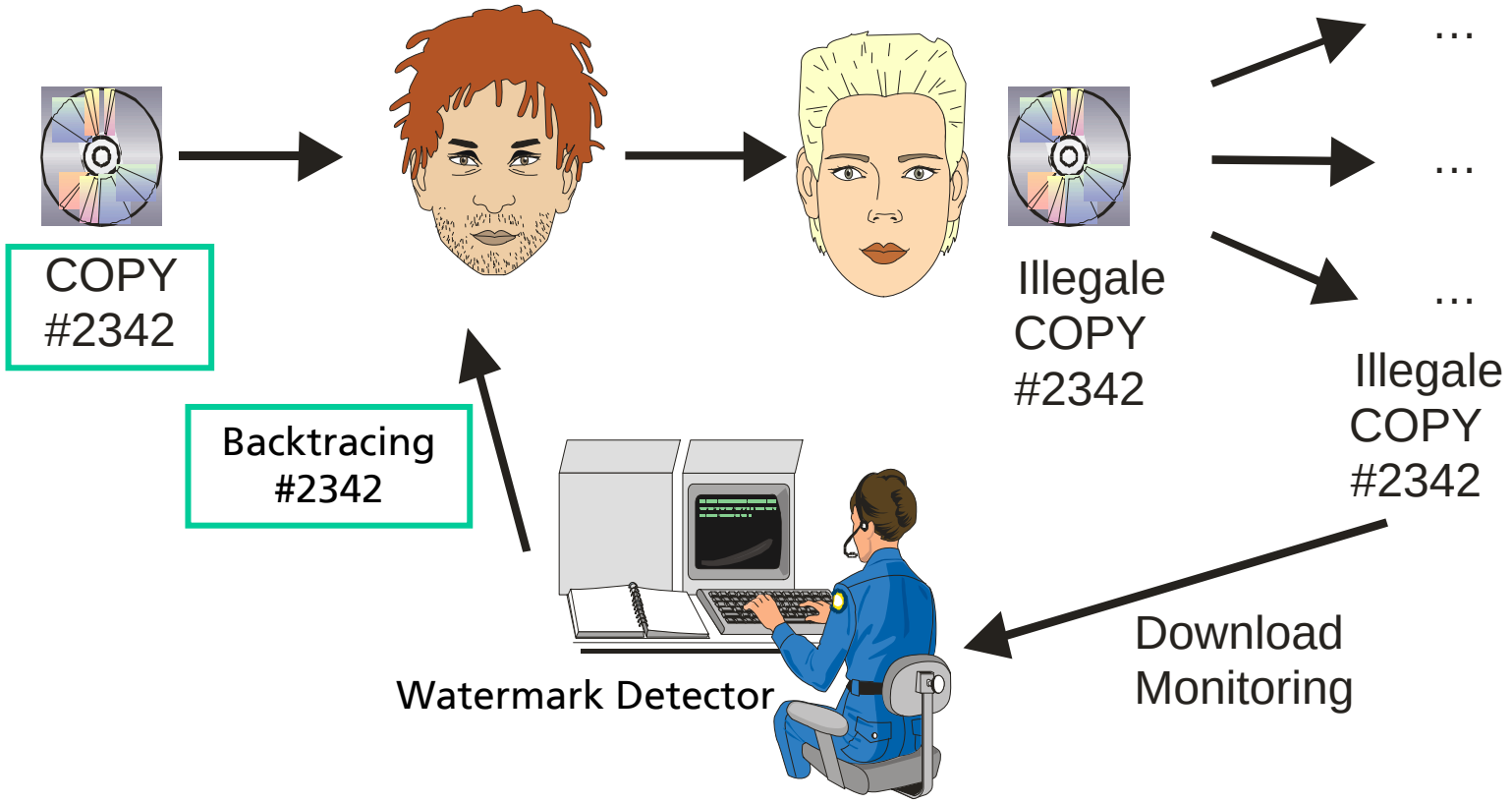
- Robustheit gegenüber MP3-Kompression



- Wasserzeichenstärke, die einem MP3 mit 96 kBit Mono entspricht übersteht MP3 Wandlung nach 16 kBit/s

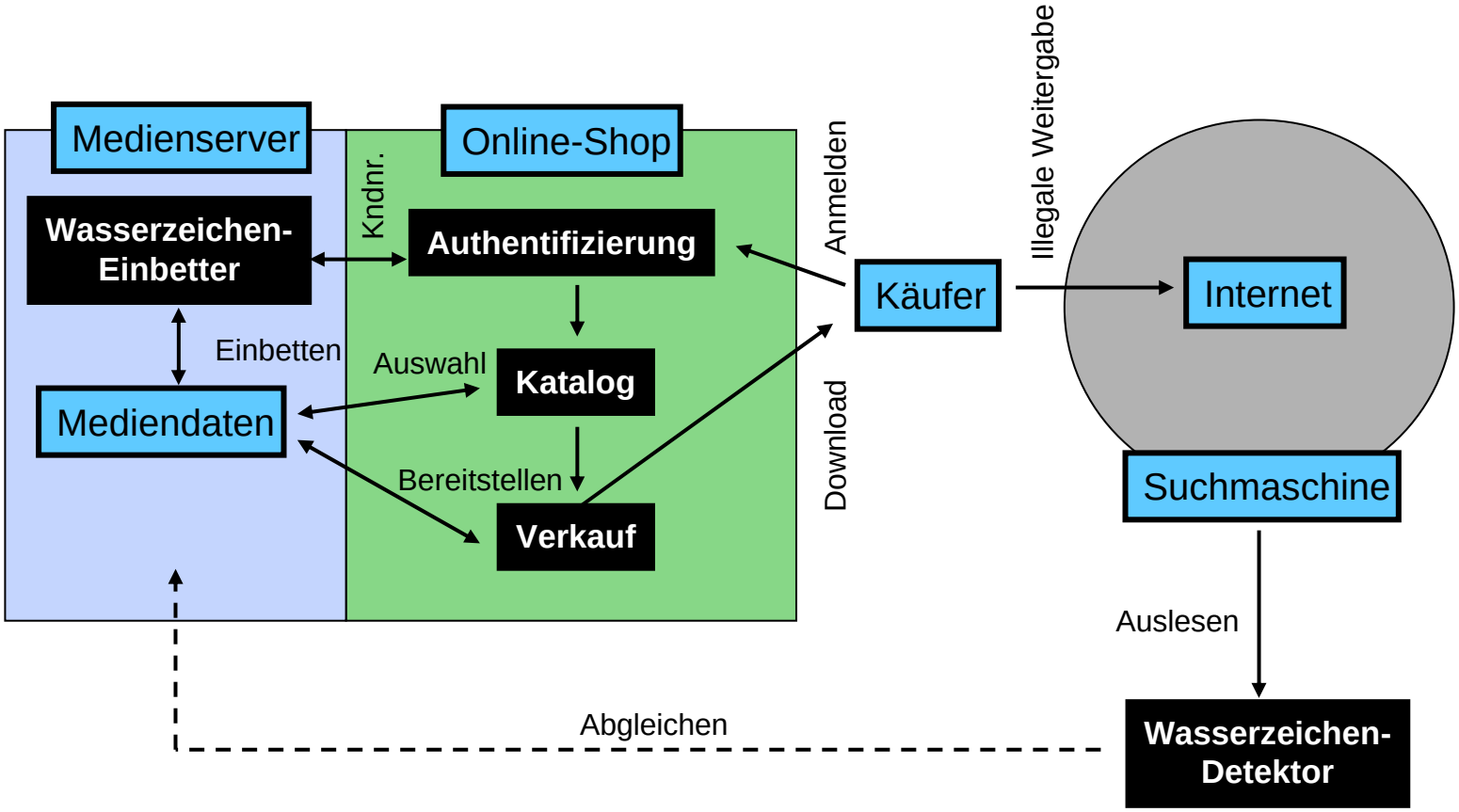
Anwendungsgebiete: Kundenverfolgung

Markierte Kopien können zurückverfolgt werden



Anwendungsgebiete: Kundenverfolgung

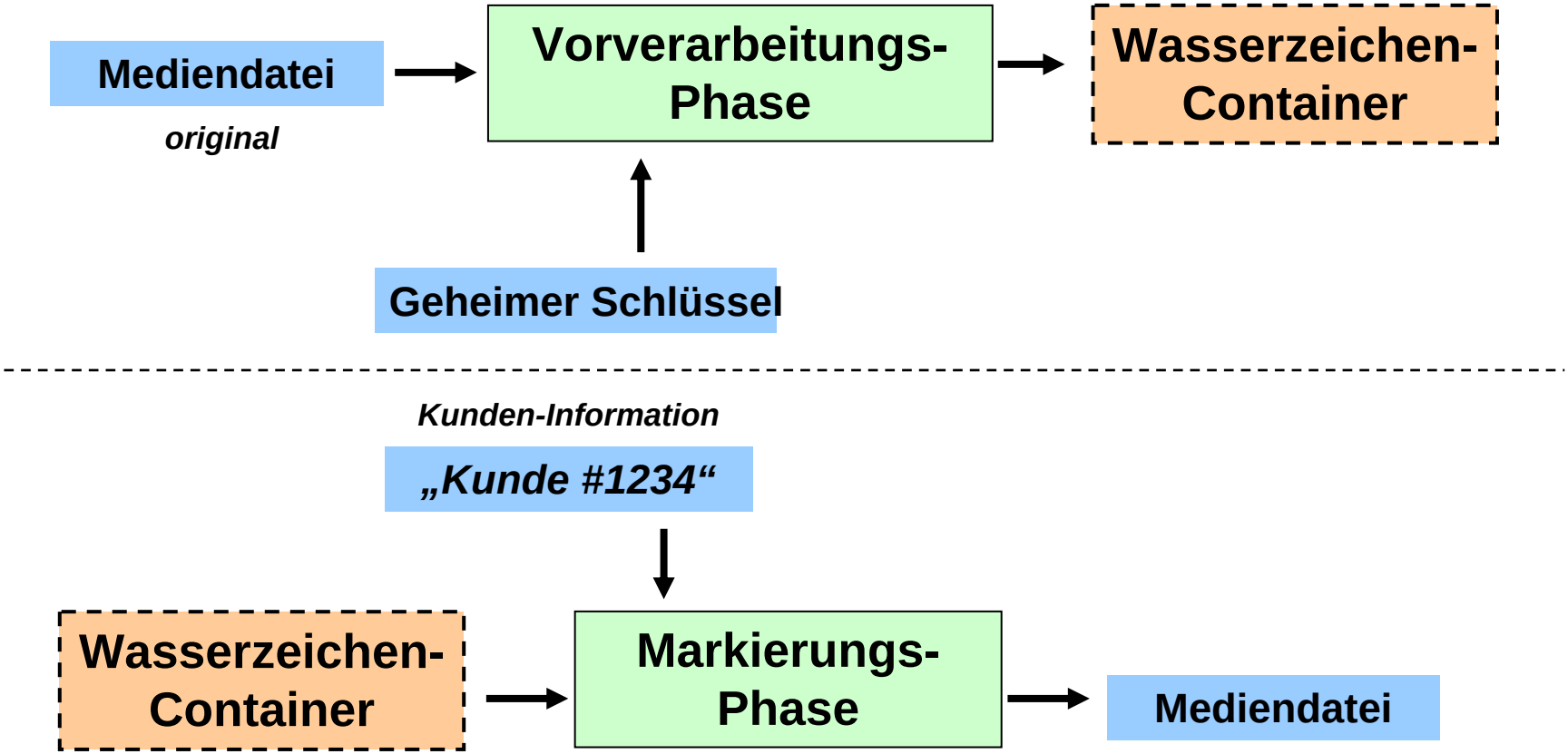
- Online-Shops/ Download-Portale (Transmark Szenario)



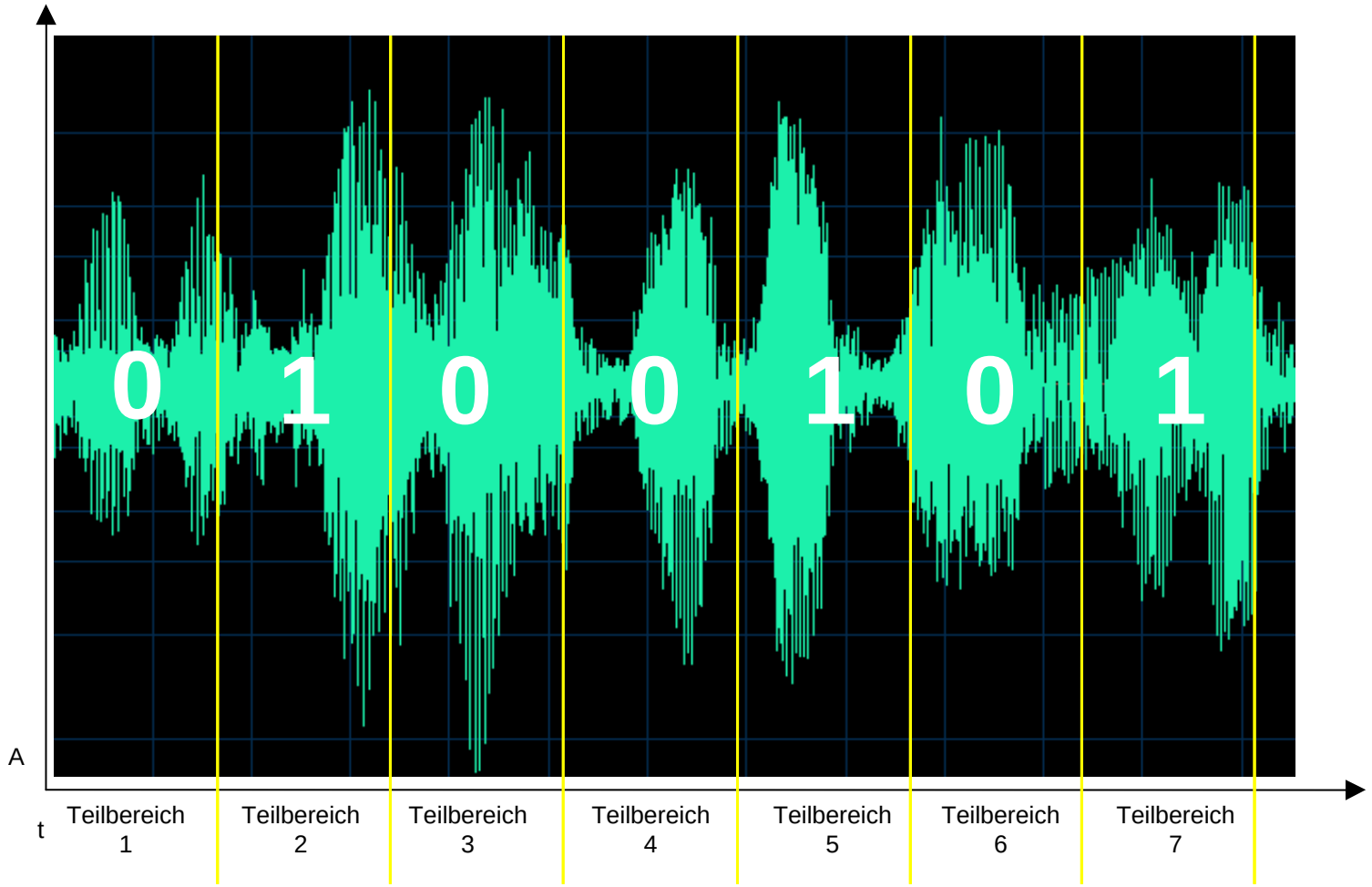
Anwendungsgebiete: Kundenverfolgung

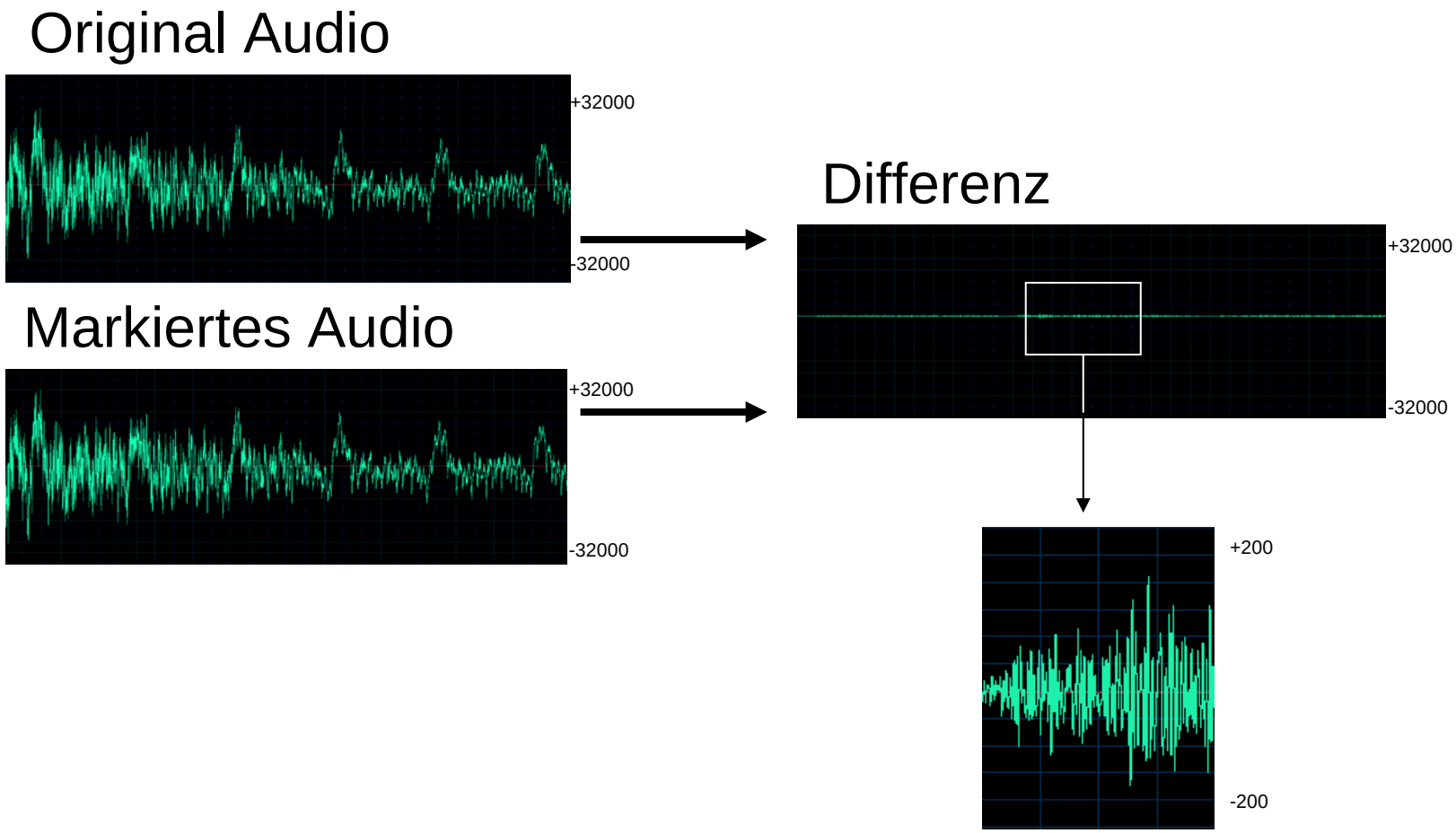
- Anforderungen :
  - Hohe Transparenz
  - Hohe Robustheit
  - Wünschenswert: Sicherheit gegen Koalitionsangriffe
    - Kann hohe Kapazität erfordern

- Steigerung der Einbettungsgeschwindigkeit bei vielen individuell markierten Kopien
- PCM Wasserzeichen z.B. 70 x Echtzeit

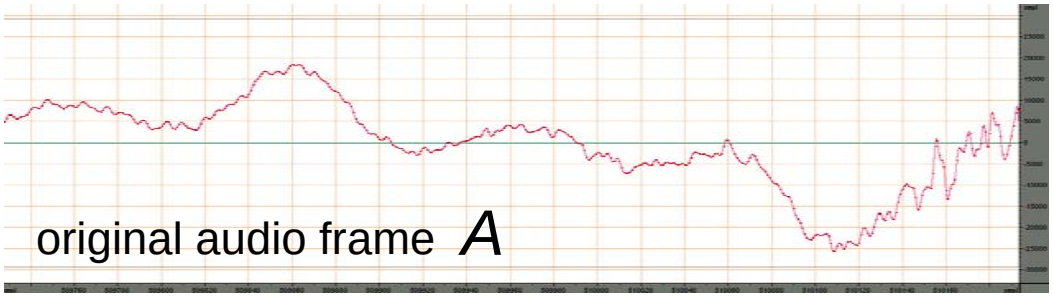


PCM Audio Watermarking

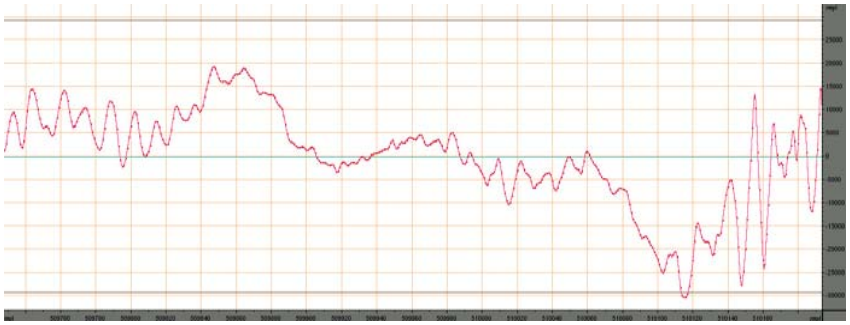



Original Audio
+32000
-32000
Markiertes Audio
+32000
-32000
Differenz
+32000
-32000
+200
-200

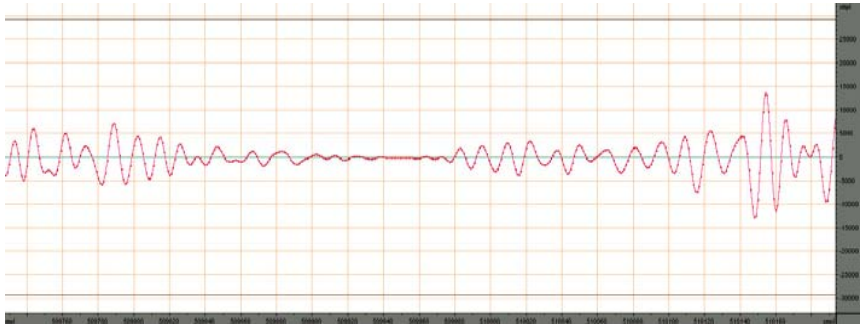
PCM Audio Watermarking / Container Pre-Processing



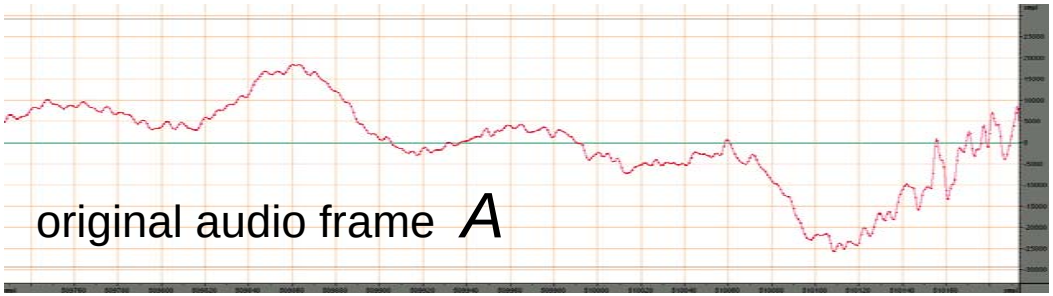
original audio frame A



Frame mit eingebetteter „0“ A_0

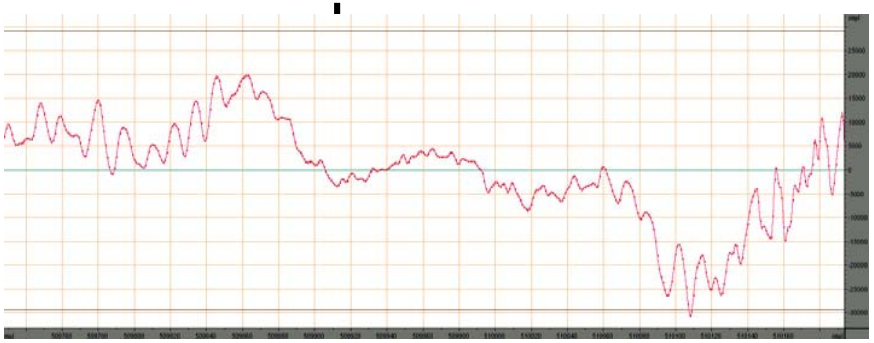


Differenzsingnal $D_0 = A - A_0$

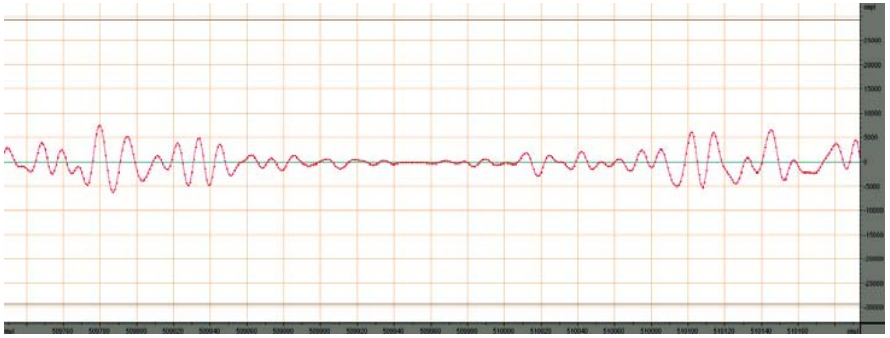


original audio frame A

Frame mit eingebetteter „1“ A_1

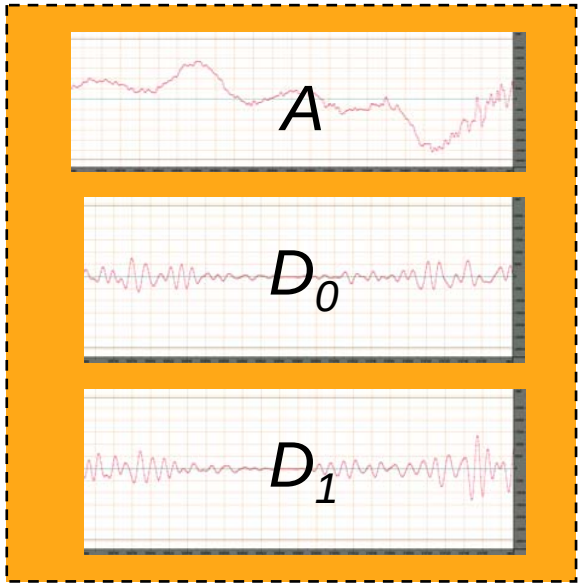


Differenzsignal $D_1 = A - A_1$



PCM Audio Watermarking / Container Pre-Processing

- Container File:
- Original Frame + Differenzsignale „1“ und „0“



@ Rendering stage

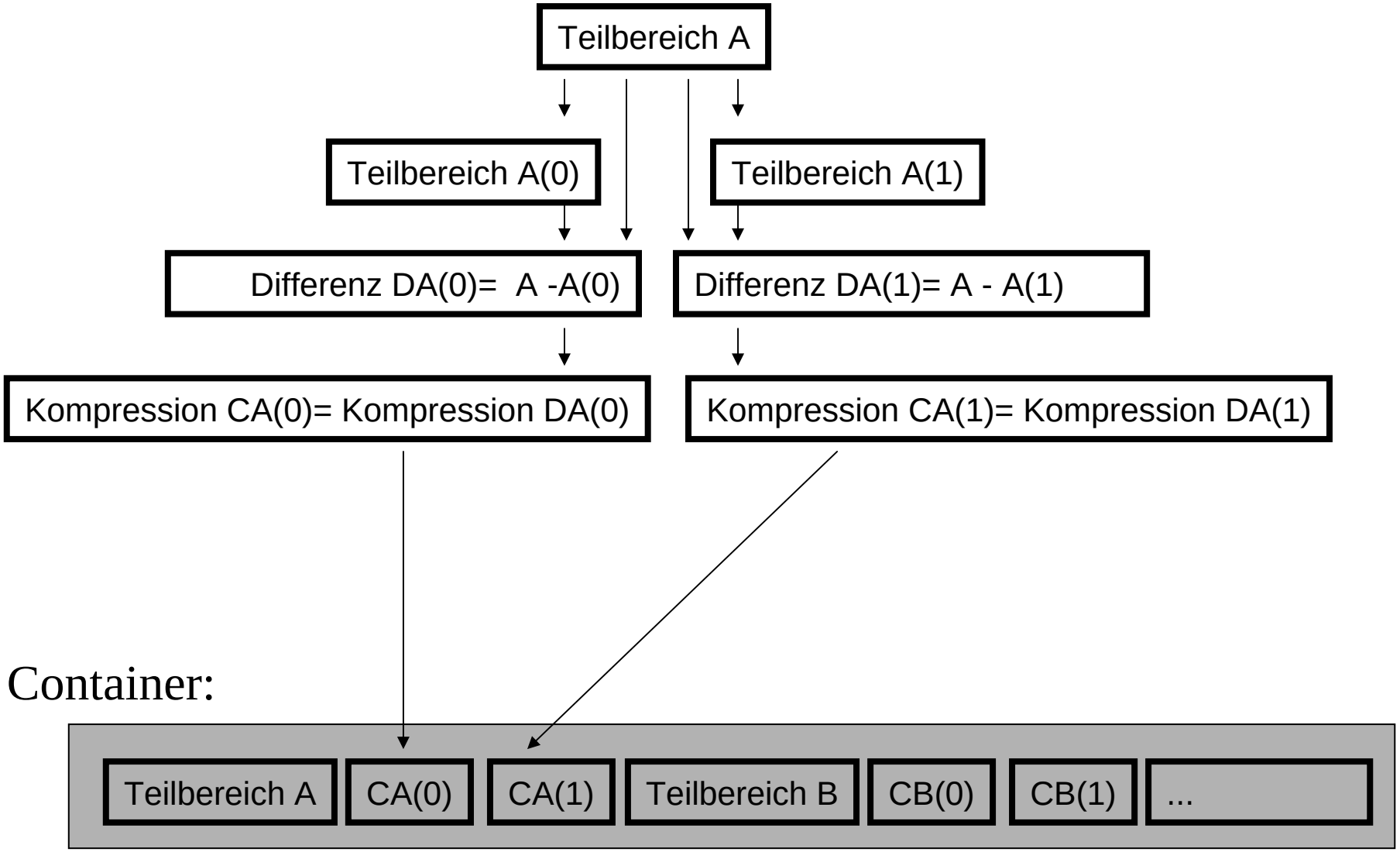
$A_0 = A - D_0$

$A_1 = A - D_1$

PCM Audio Watermarking / Container Pre-Processing

- Im Vergleich zum Trägersignal haben die Differenzsignale nur wenig Energie
- Trotzdem wird ihnen als PCM Information eine Dynamik von 16 Bit zugeordnet
- Diese wird nicht ausgenutzt
- Kompression bietet sich an
  - Gebräuchlich für Audio: ADPCM
    - Adaptive Differential Pulse Code Modulation
  - Idee: Speichern der Differenz des nächsten zum aktuellen PCM Wert
  - Niedrige Dynamik = Geringe Wechsel
  - Gute Repräsentation des Signals mit wenigen Bit
  - In der Praxis: 4 statt 16 Bit
  - Dementsprechend:
    - Original 100% (16 Bit)
    - Differenz A 25% (4 Bit)
    - Differenz B 25% (4 Bit)
      - > Container = 150% des Originals

PCM Audio Watermarking / Container



Kryptographisch geschützte Wasserzeichencontainer

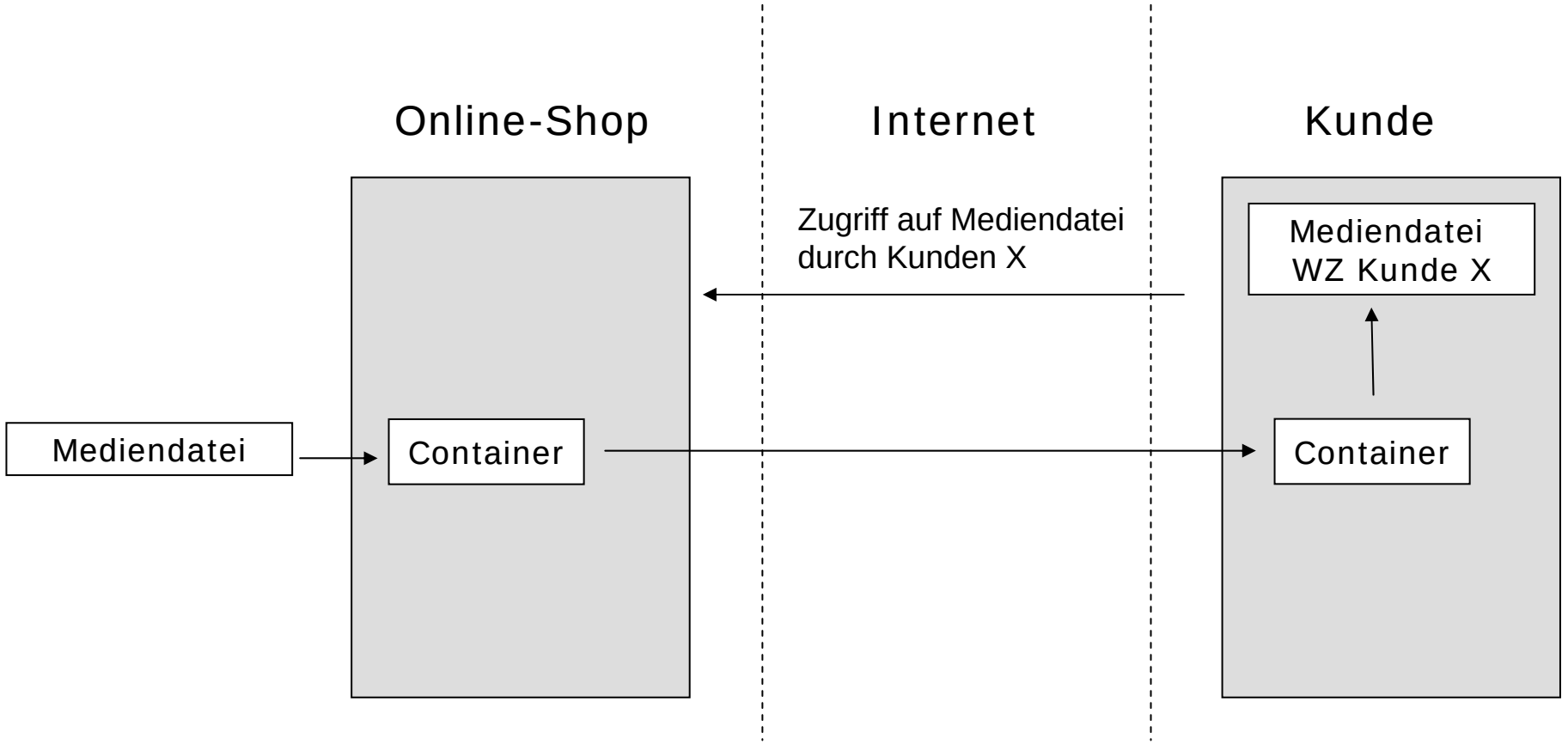
- Digitale Wasserzeichen werden in der Praxis zum Schutz von Urheberrechten eingesetzt

- Transaktionswasserzeichen sind hier eine verbreitete Strategie
  - Jeder Download wird individuell markiert
  - Markierte Kopien können zurückverfolgt werden

- Wasserzeichen-Container ermöglichen sehr schnelles Markieren

- Problem: Jeder Kunde erhält eine individuelle Datei
  - Caching
  - Verschlüsslung bei Übertragung

Kryptographisch geschützte Wasserzeichencontainer

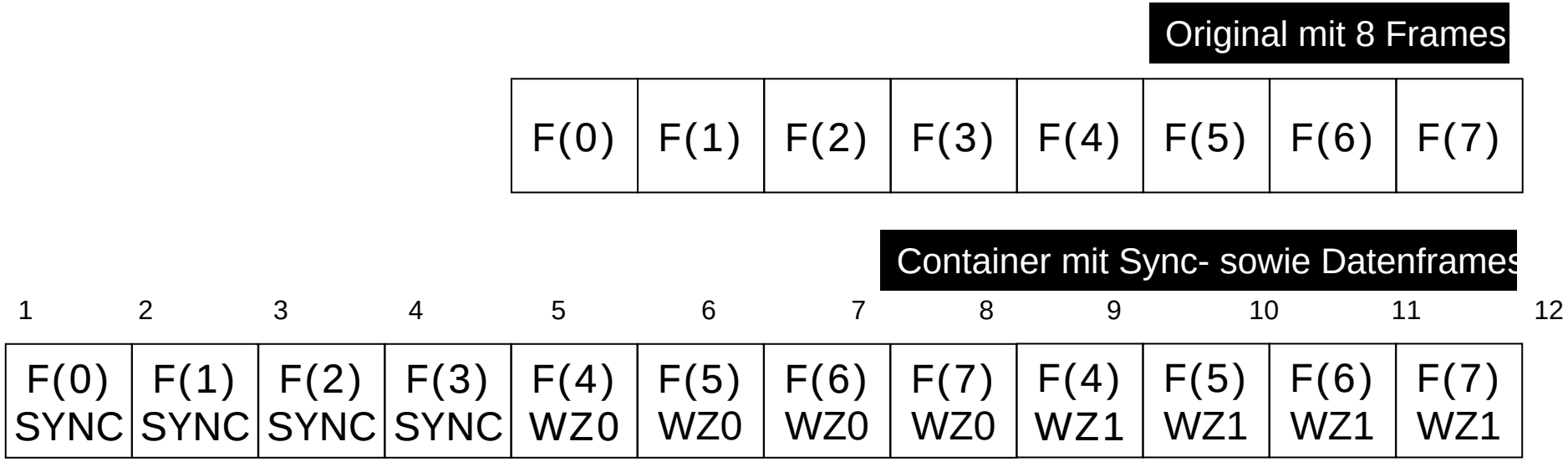


Herausforderung: Konzept, welches zwei Prinzipien vereint:

- Einheitliche Datei für den Download bei allen Kunden
- Individuelle Markierung

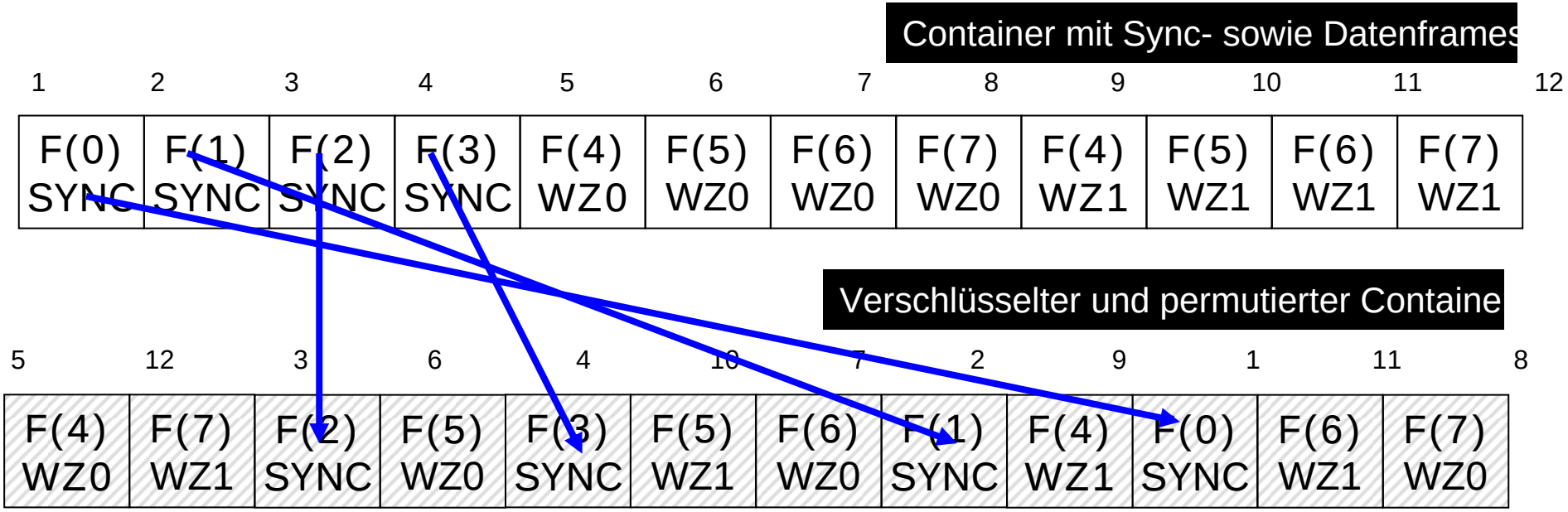
Kryptographisch geschützte Wasserzeichencontainer/ Konzept

- Beispiel kurze Audiodatei
- Unterteilt in 8 Frames
- Jedes Frame kann ein Bit enthalten: SYNC, WZ0, WZ1



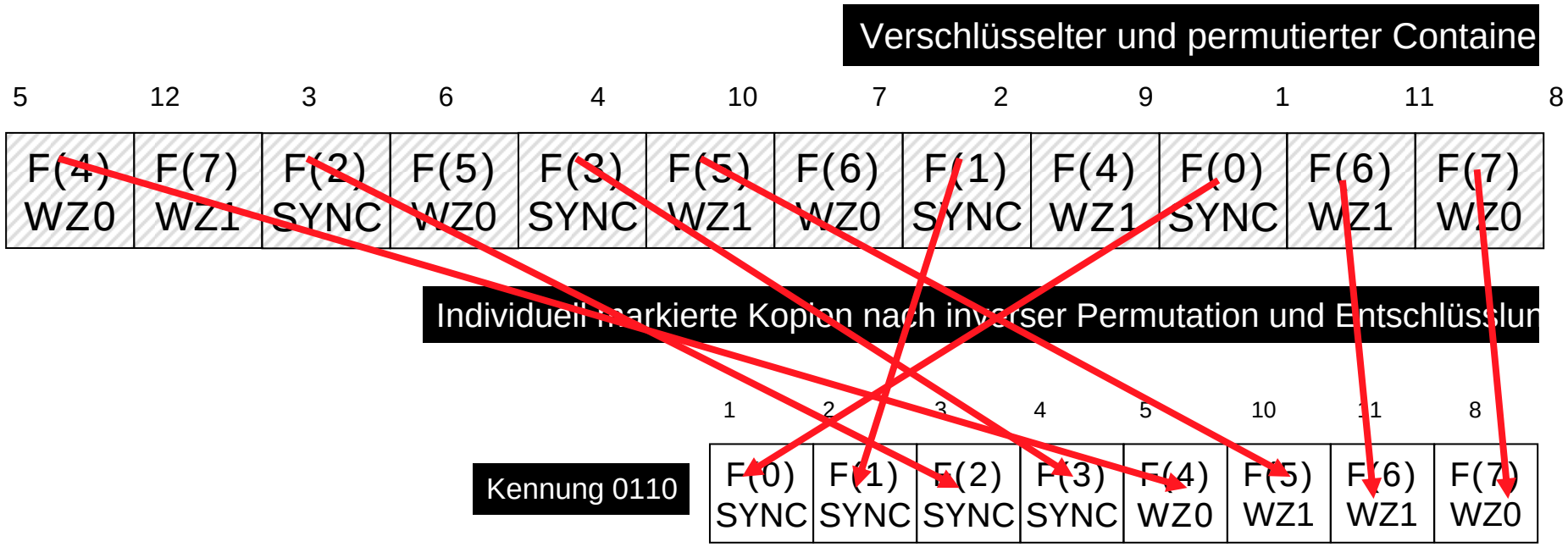
Kryptographisch geschützte Wasserzeichencontainer/ Konzept

- Erstellen eines verschlüsselten Containers

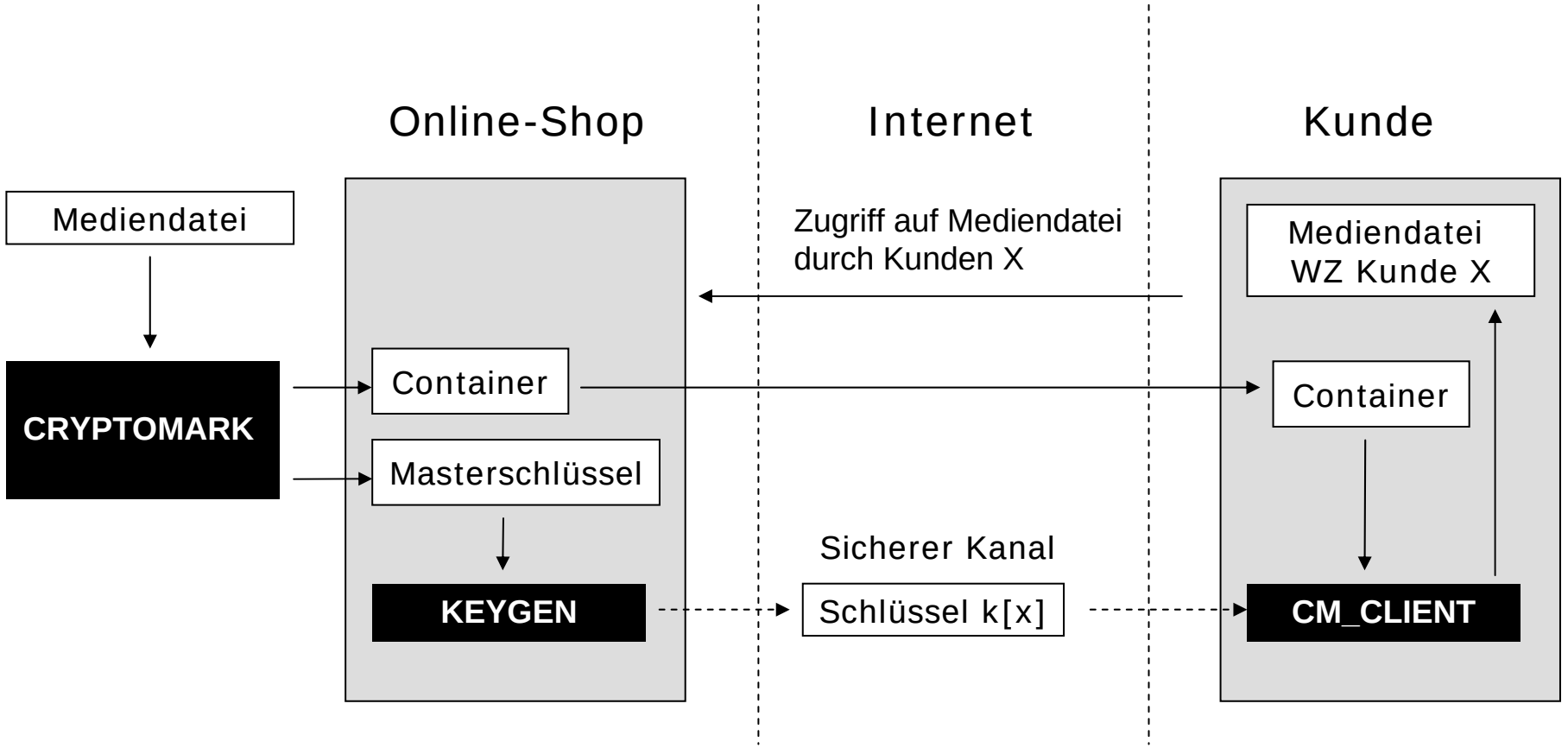


Kryptographisch geschützte Wasserzeichencontainer/ Konzept

- Erstellen individuell markierter Kopien



Kryptographisch geschützte Wasserzeichencontainer/ System

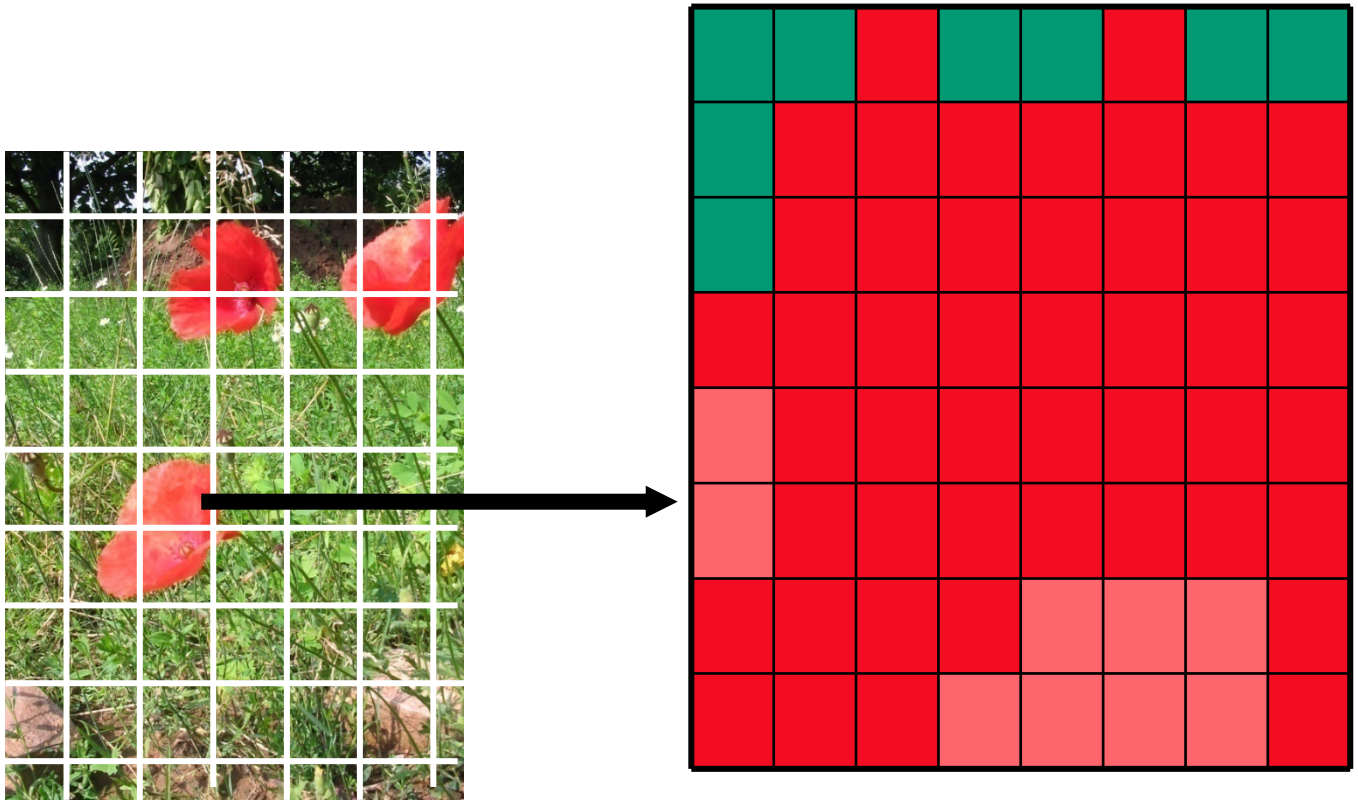


Kryptographisch geschützte Wasserzeichencontainer/ System

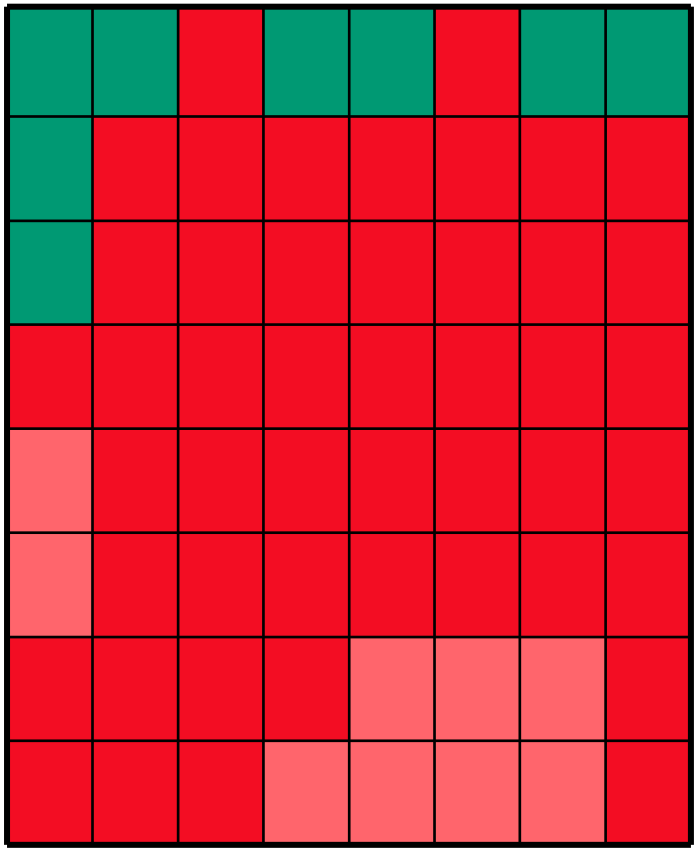
- Original: WAV file, 4 min 20 s, mono, 22440 KB
- 48 Bit Wasserzeichen eingebettet
- Größenzuwachs des Containers: 6,75% (23912 KB)
- Master Key : 7 KB
  - 3DES Verschlüsslung
- Kundenschlüssel: 3 KB
  - berechnet in < 1s
- Zeit zur Entschlüsslung: 35 sec auf Minimal-PC

Beispiel Bildwasserzeichen

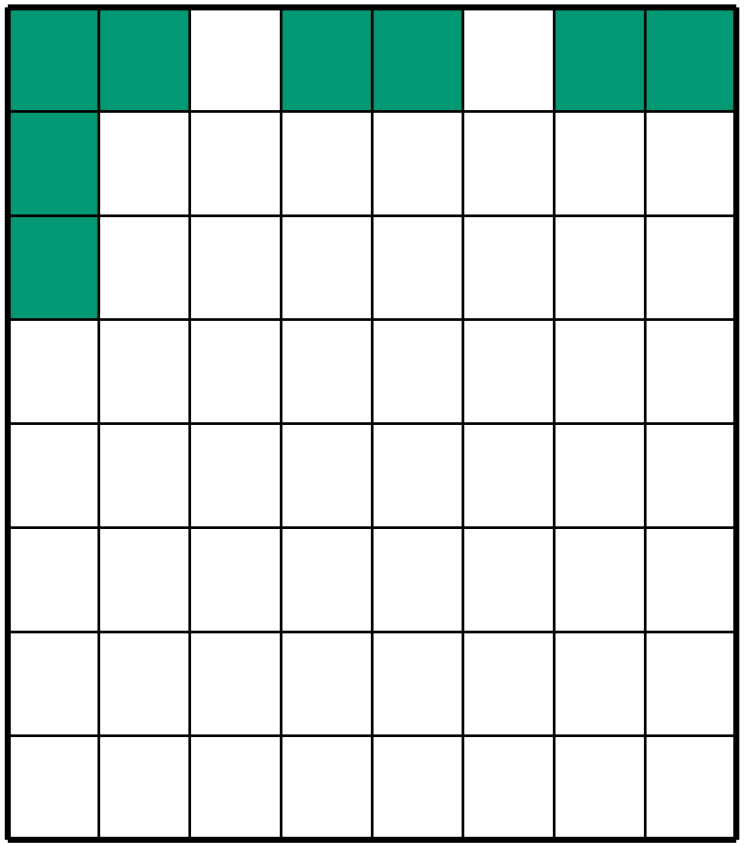
- Übertragen das Audiowasserzeichen-Prinzips
- “Patchwork Watermarking”
- DCT-Domain
- Grünkanal



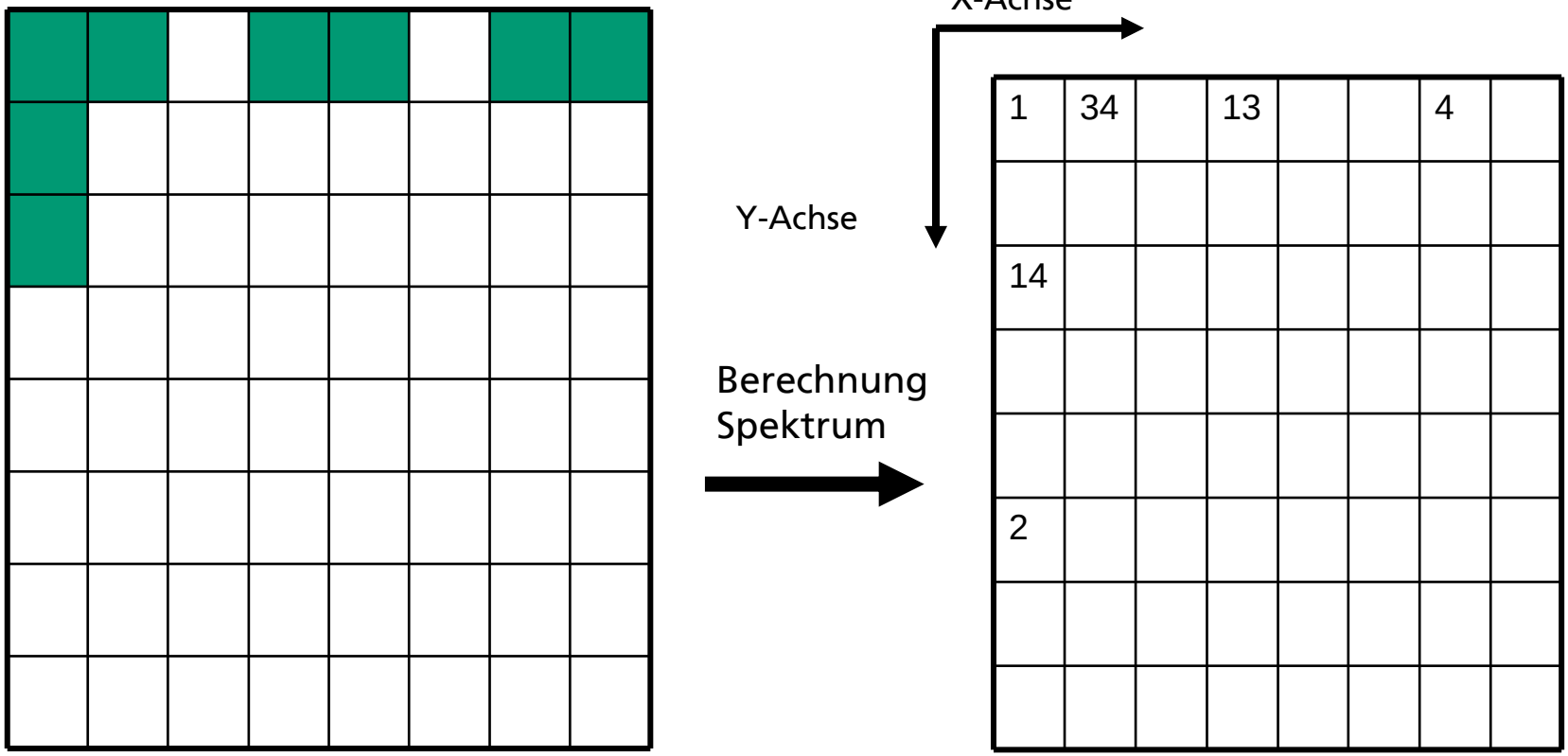
Beispiel Bildwasserzeichen



Auswahl
Grünkanal

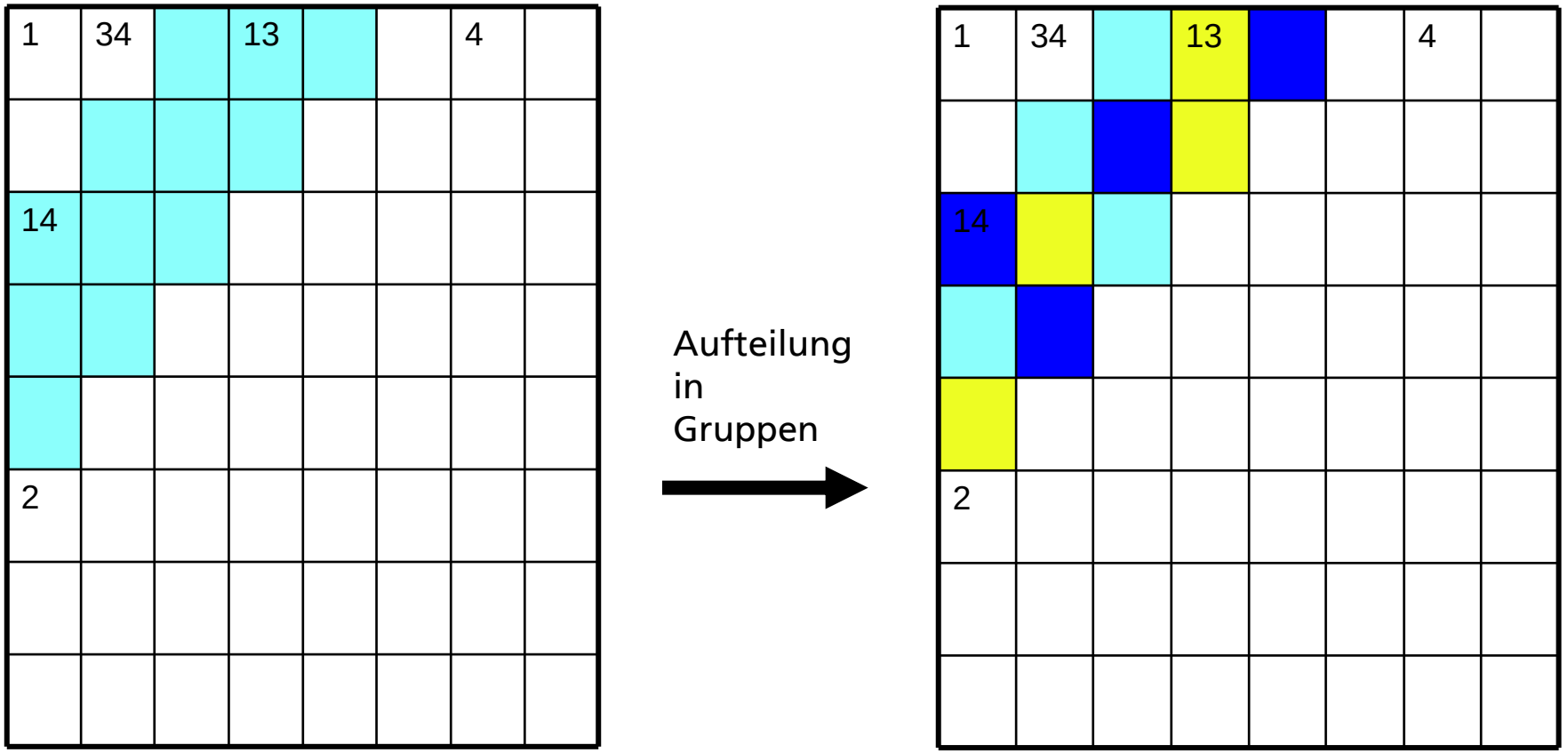


Beispiel Bildwasserzeichen

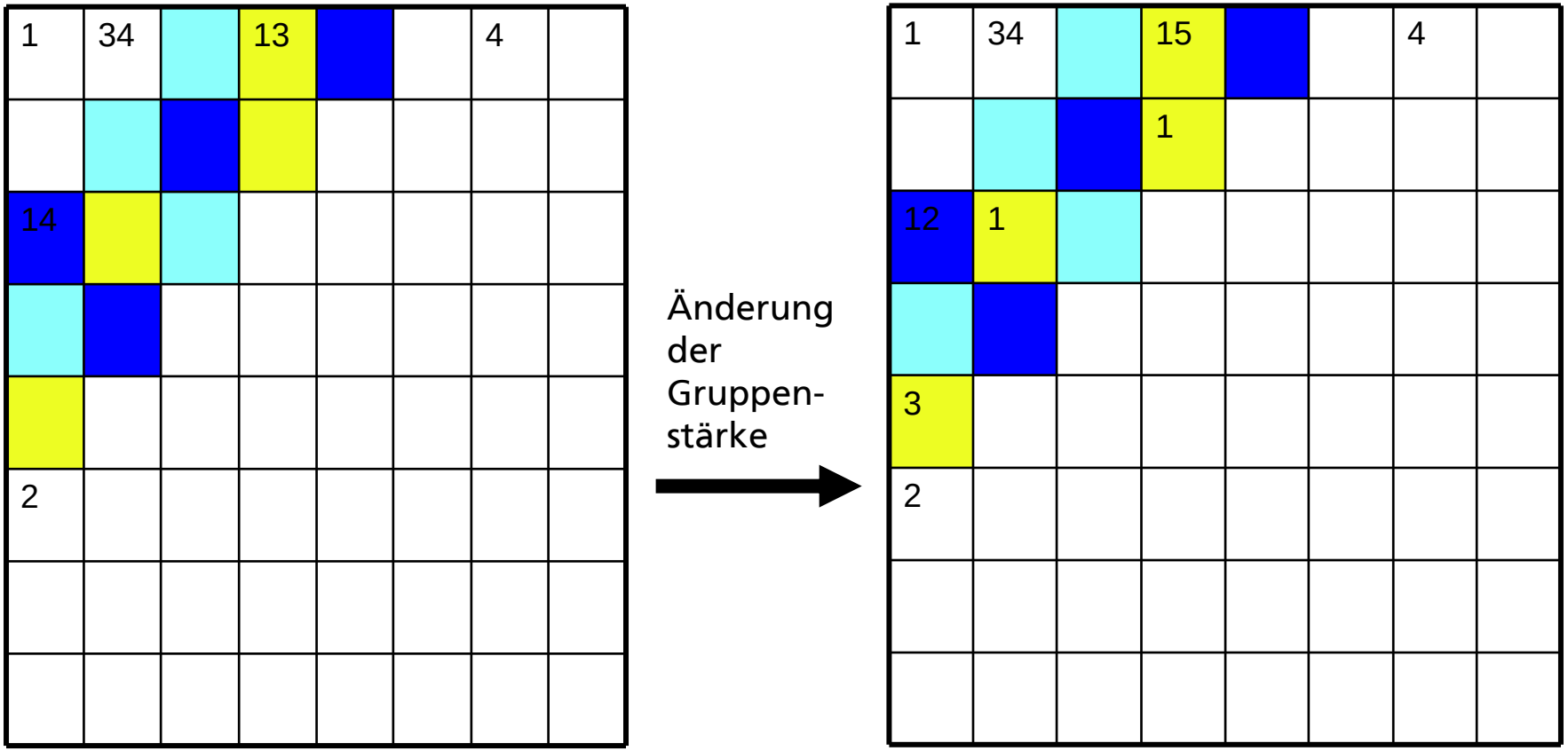


Intensität von Helligkeit und Wechsel

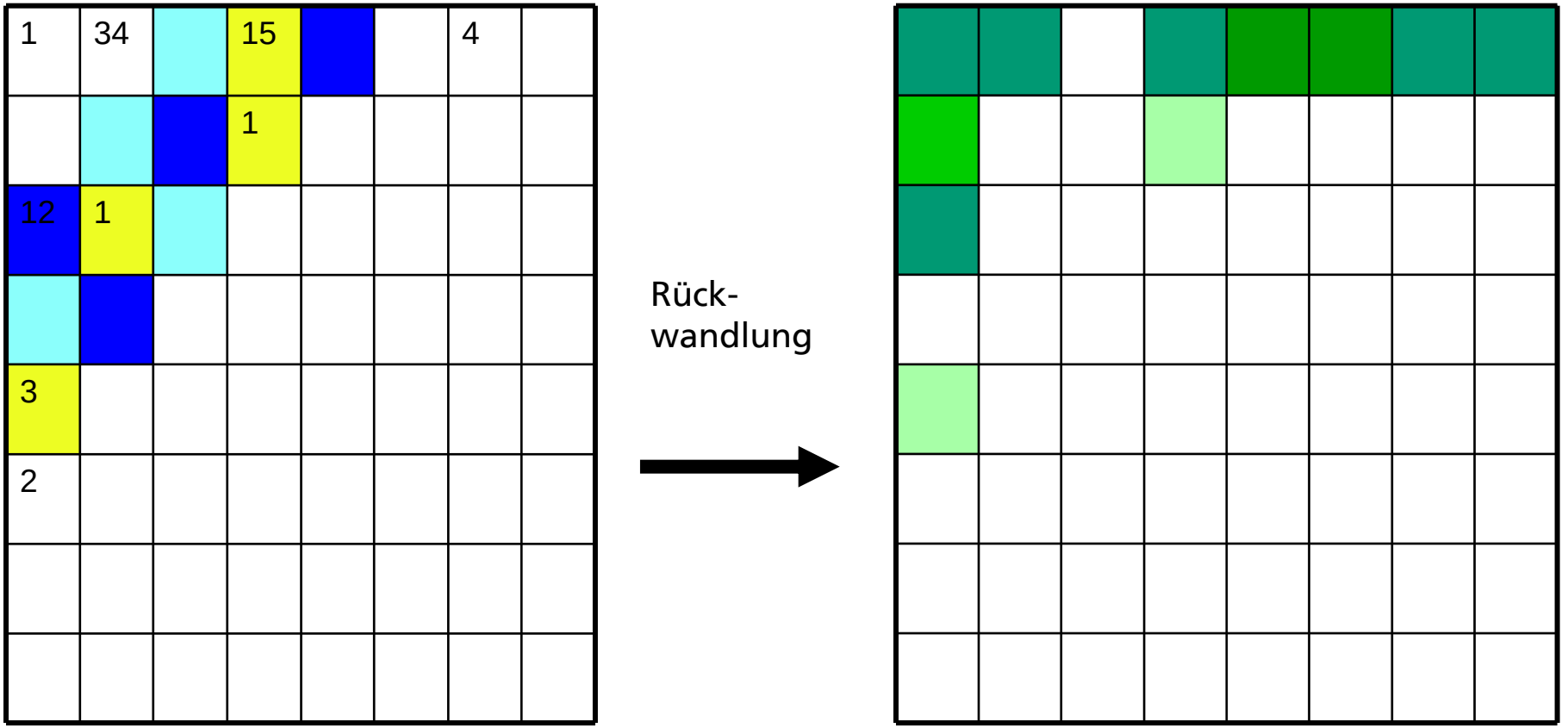
Beispiel Bildwasserzeichen



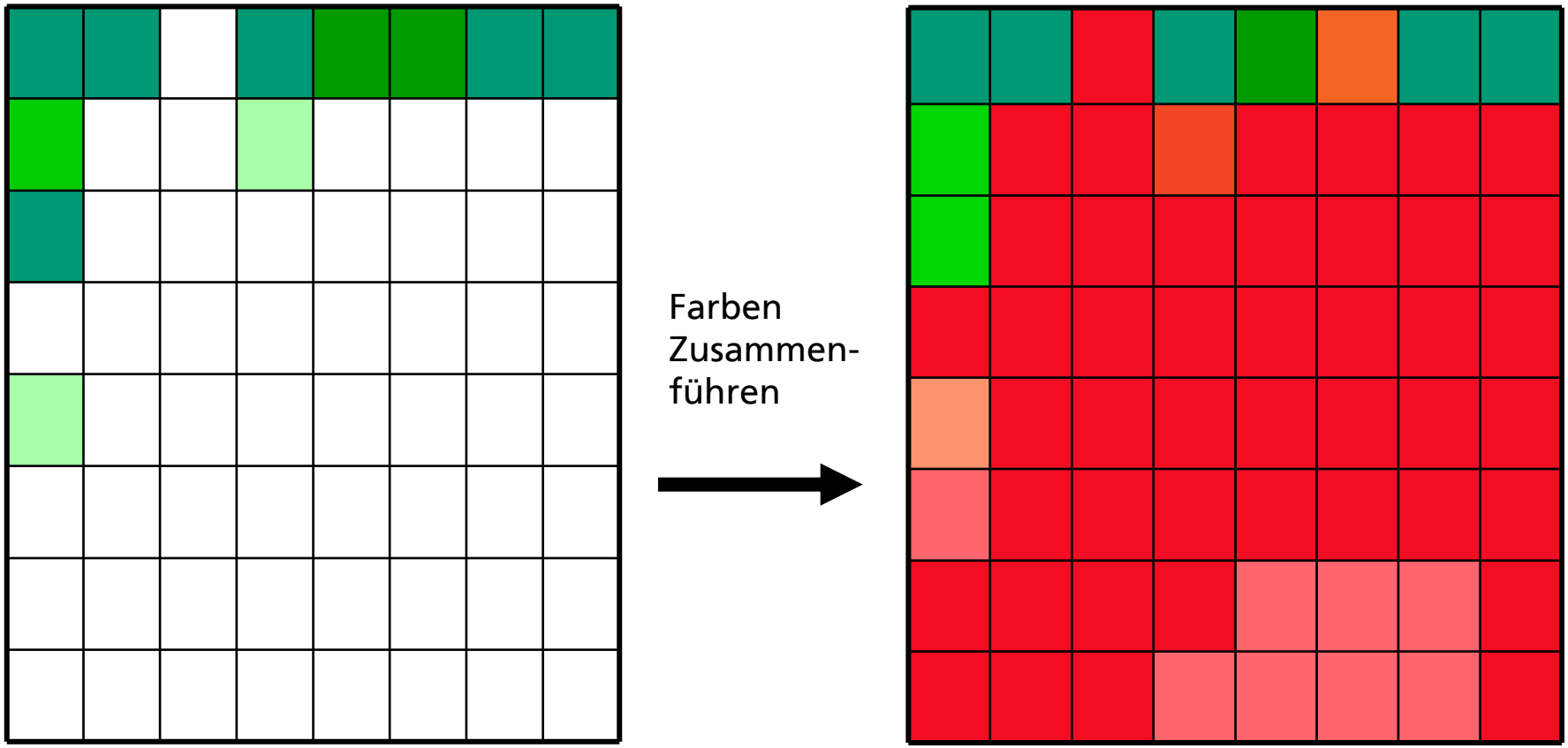
Beispiel Bildwasserzeichen



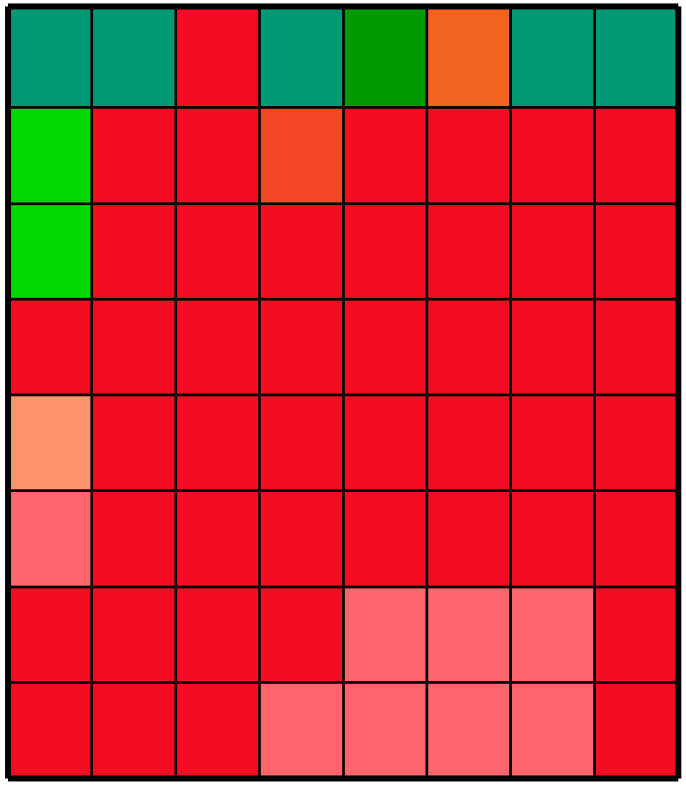
Beispiel Bildwasserzeichen



Beispiel Bildwasserzeichen



Beispiel Bildwasserzeichen



Einfügen