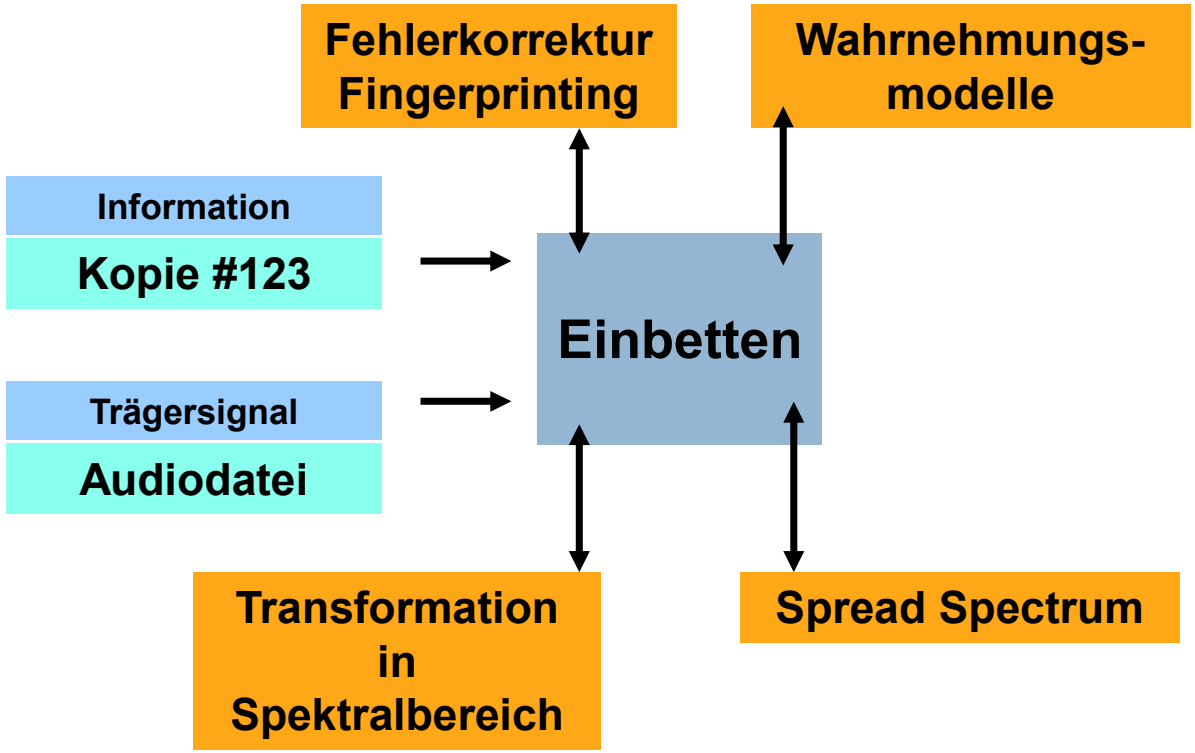
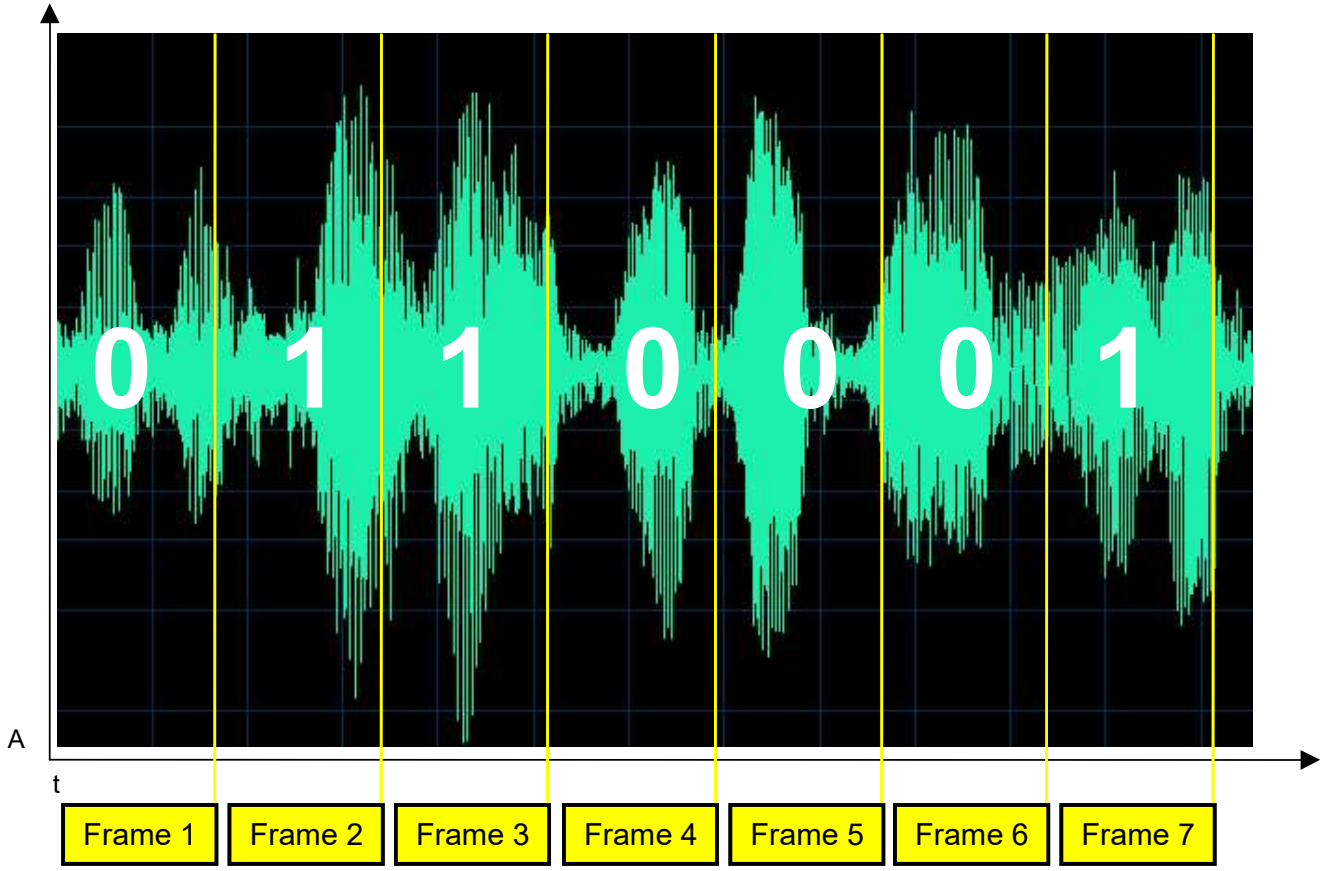
- Digitale Wasserzeichen bestehen oft aus mehreren Modulen:

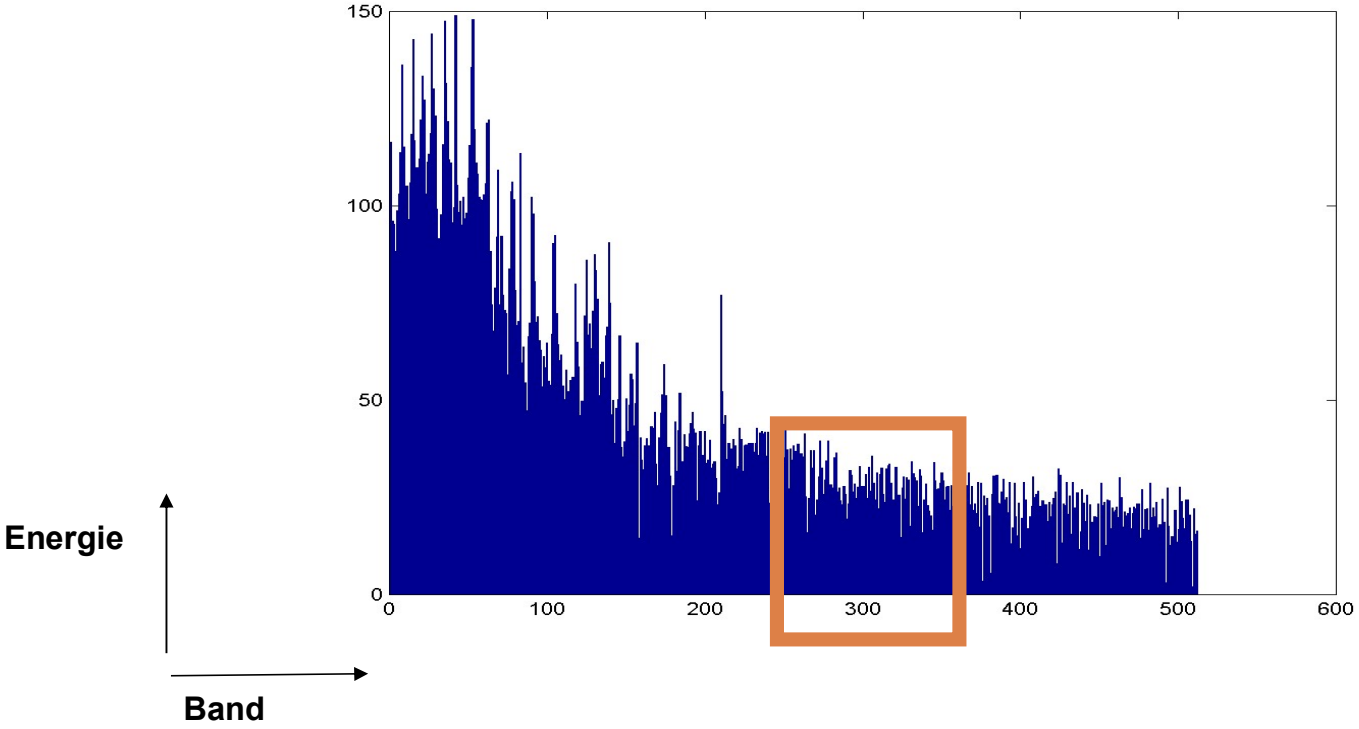


Nur gut aufeinander abgestimmte Module führen zu effizienten und zuverlässigen Verfahren

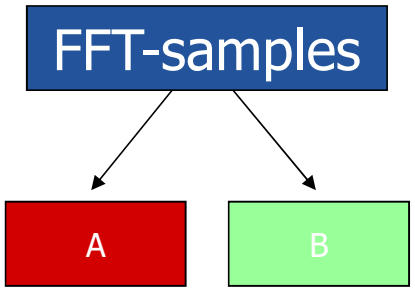
- Einbettung des Wasserzeichens in unabhängigen Abschnitten (Frames)
- Jeder Frame enthält ein Bit

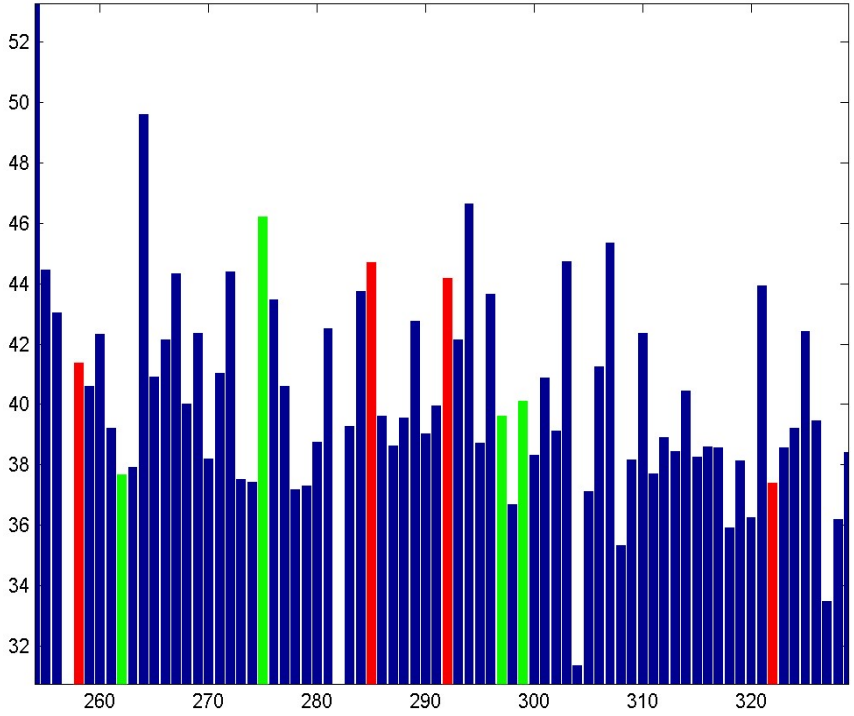


- Prinzip bei der Markierung eines einzelnen Frames:
  - Einbetten des Wasserzeichens im Frequenz-Spektrum
  - Gruppieren der Frequenzbänder



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



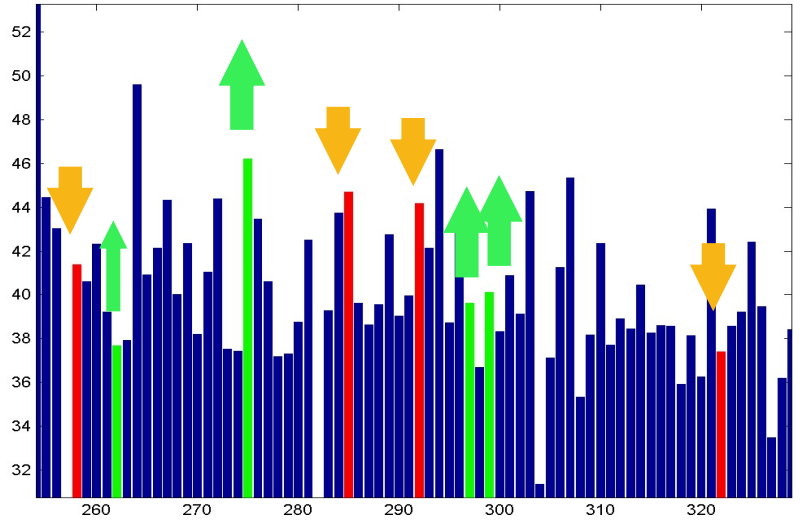


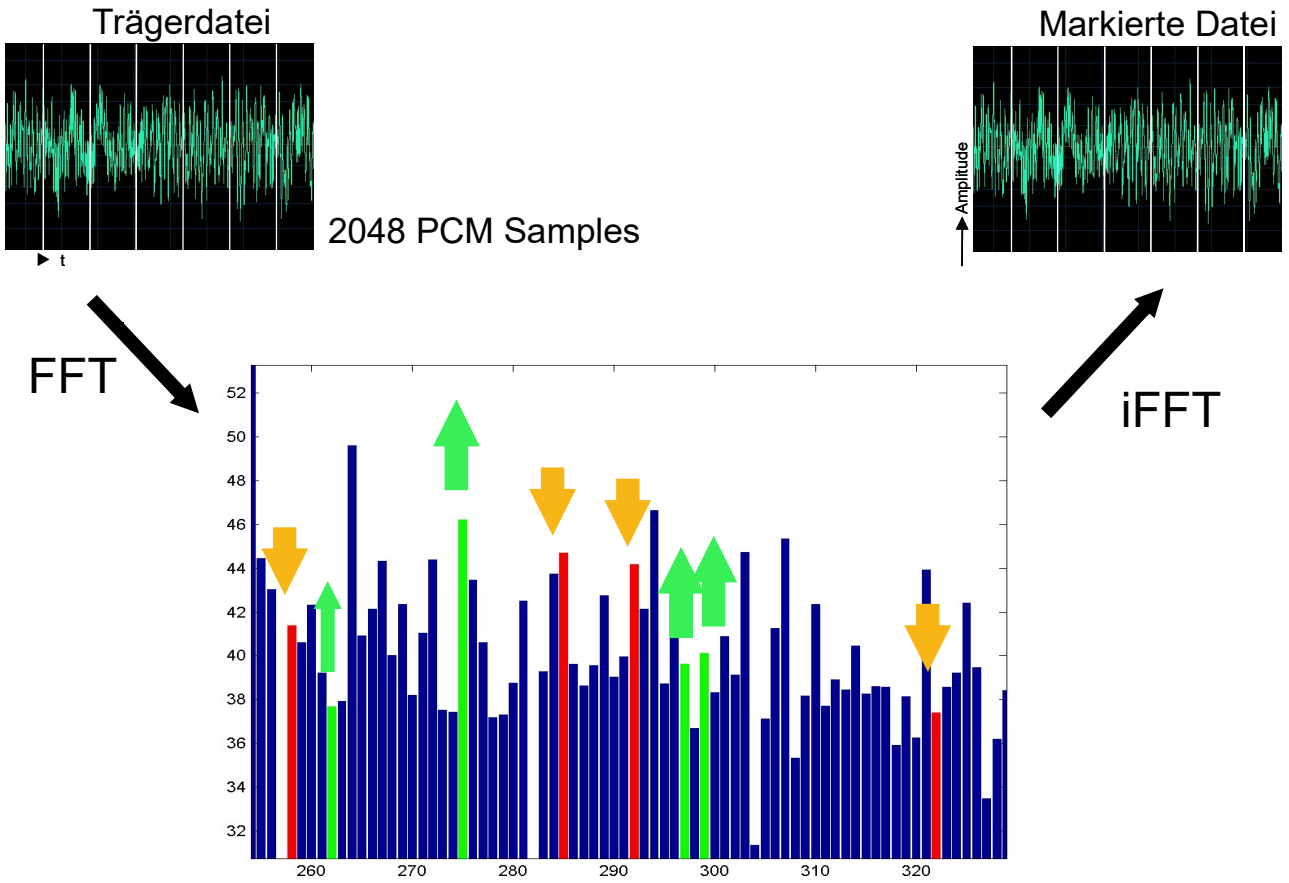
- Prinzip:
  - In unmarkiertem Material: ausgewählte statistische Eigenschaften für Gruppen A und B in der Regel gleich (z.B. Gesamtenergie)
  - Einbettungsprozess: gezielte minimale Erhöhung bzw. Erniedrigung der Energien in den Frequenzbändern, Erzwingen von signifikanter Abweichung der statistischen Eigenschaften in Gruppen A und B

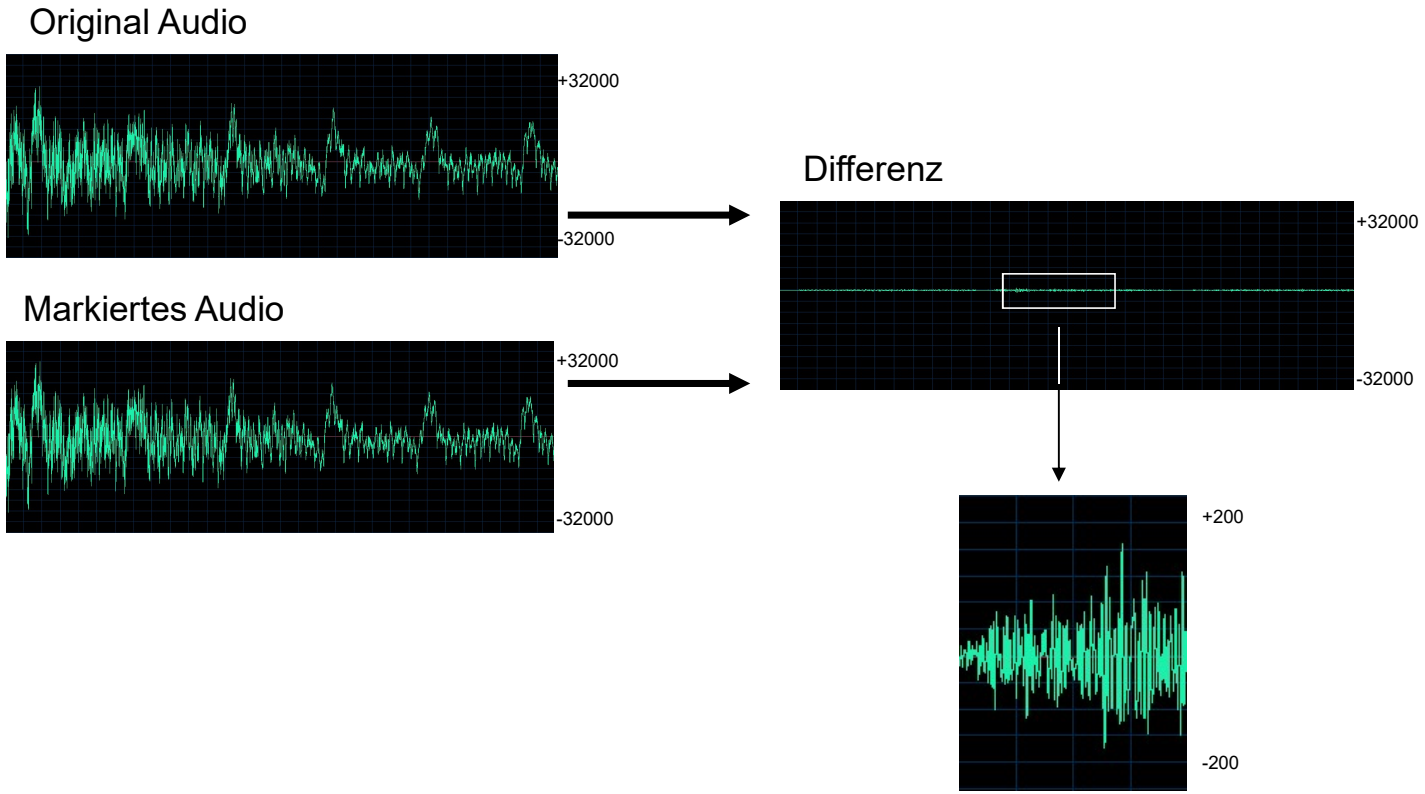
WZ-Bit	Gruppe A	Gruppe B
0	Erhöhen	Erniedrigen
1	Erniedrigen	Erhöhen

  - Auslese-Prozess: Detektieren von eingebetteter „0“ oder „1“ durch Interpretation des Verhältnisses der Gesamtenergie in Gruppen A und B

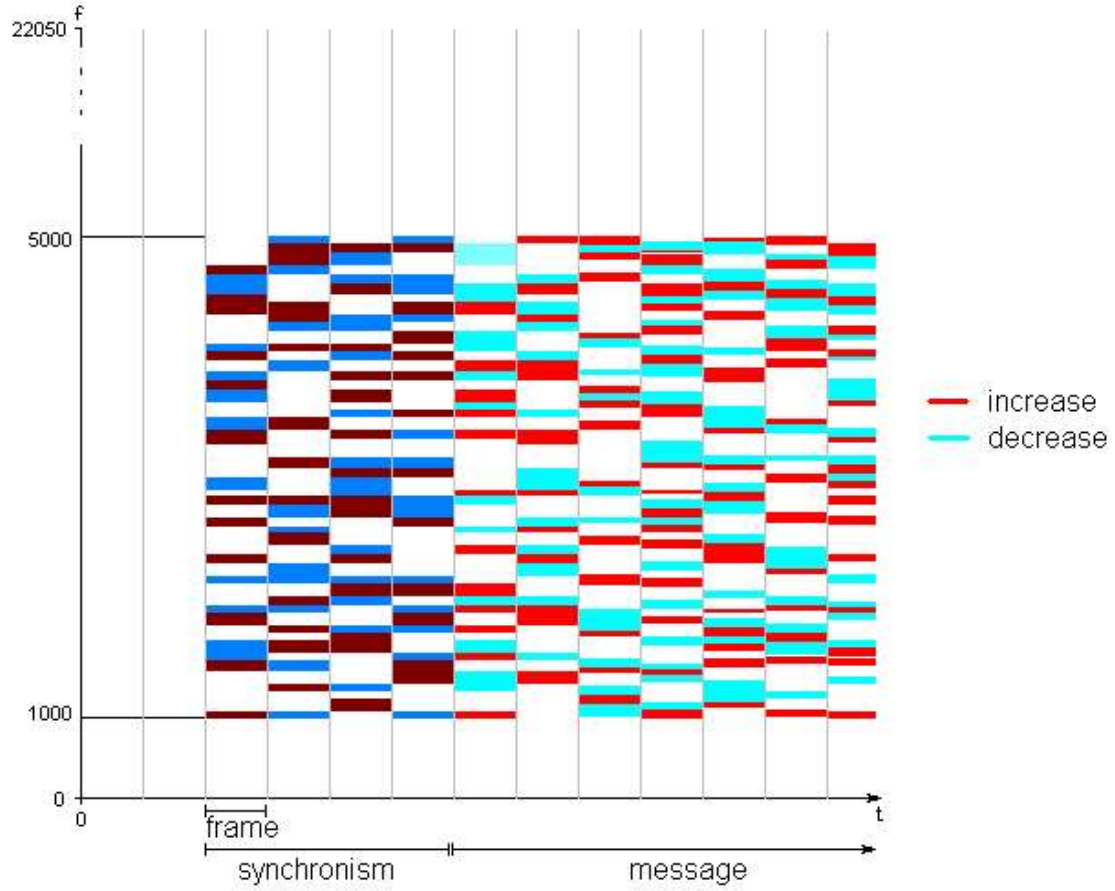
- Bänder werden individuell gestärkt oder geschwächt
  - Ein Parameter gibt die gewünschte Stärke der Änderung an
  - Ein weiterer das erlaubte Überschreiten der Maskierungsschwelle
- Maskierung gilt ebenfalls individuell pro Band
  - Wird errechnet durch Psychoakustik
- Stark maskierte Bändern enthalten viel Wassserzeichen-Energie
- Schwach maskierte Bänder entsprechend wenig




Trägerdatei
t
2048 PCM Samples
Markierte Datei
Amplitude
FFT
iFFT
52
50
48
46
44
42
40
38
36
34
32
260
270
280
290
300
310
320

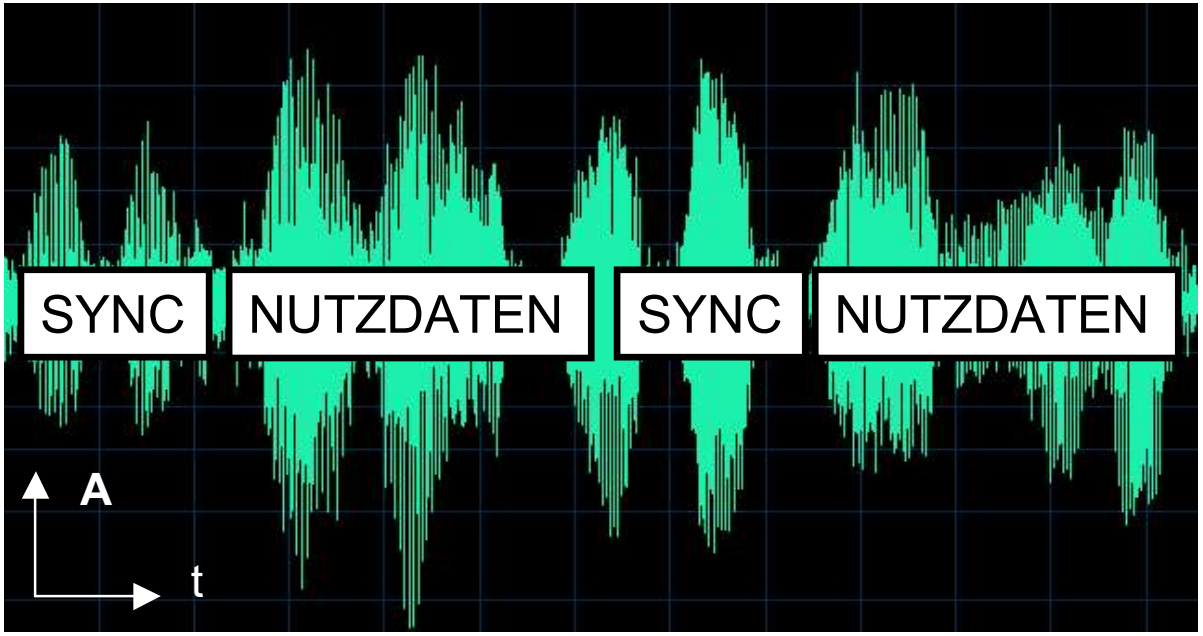


Differenzsignal besitzt nur sehr geringe Energie

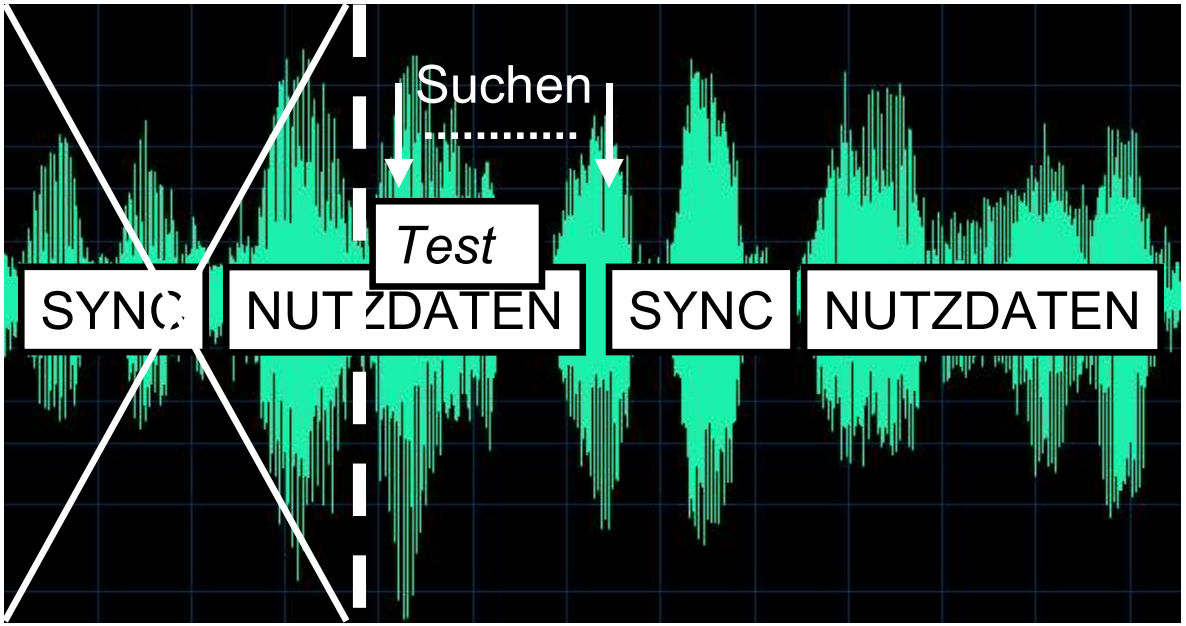


Veränderte Frequenzbänder werden variiert (geheimer Wasserzeichen-Schlüssel)

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

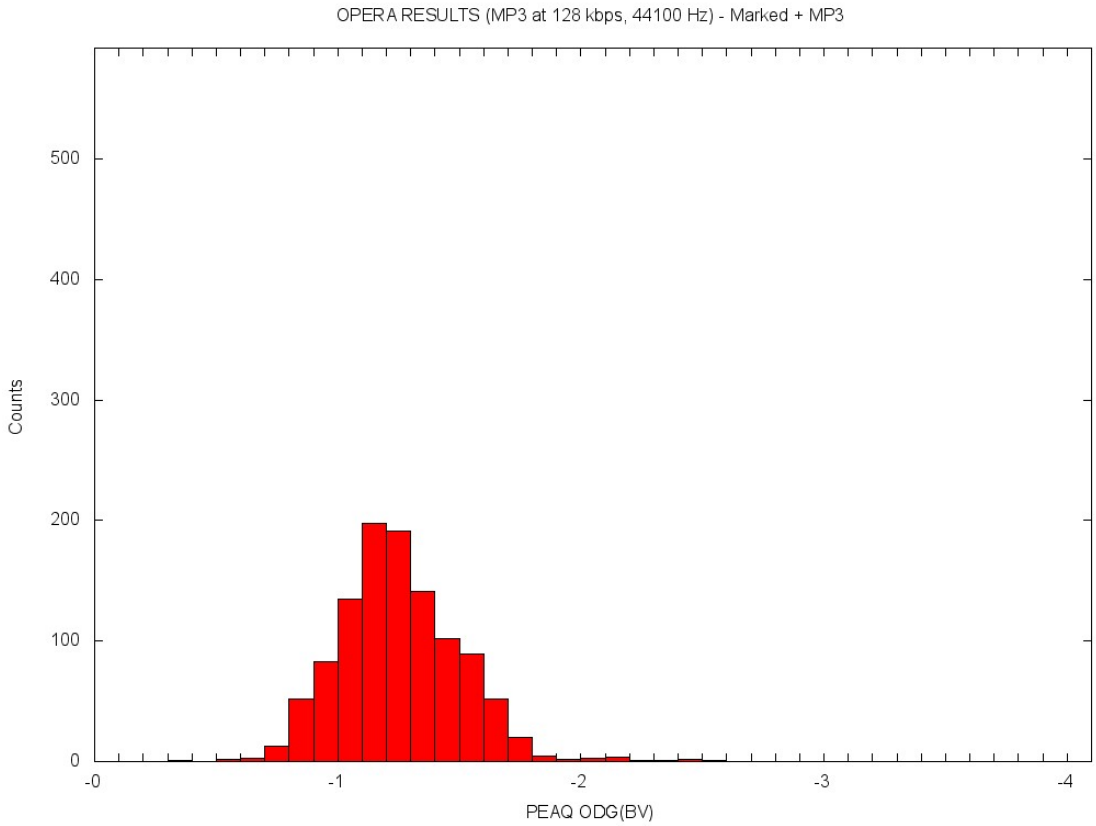


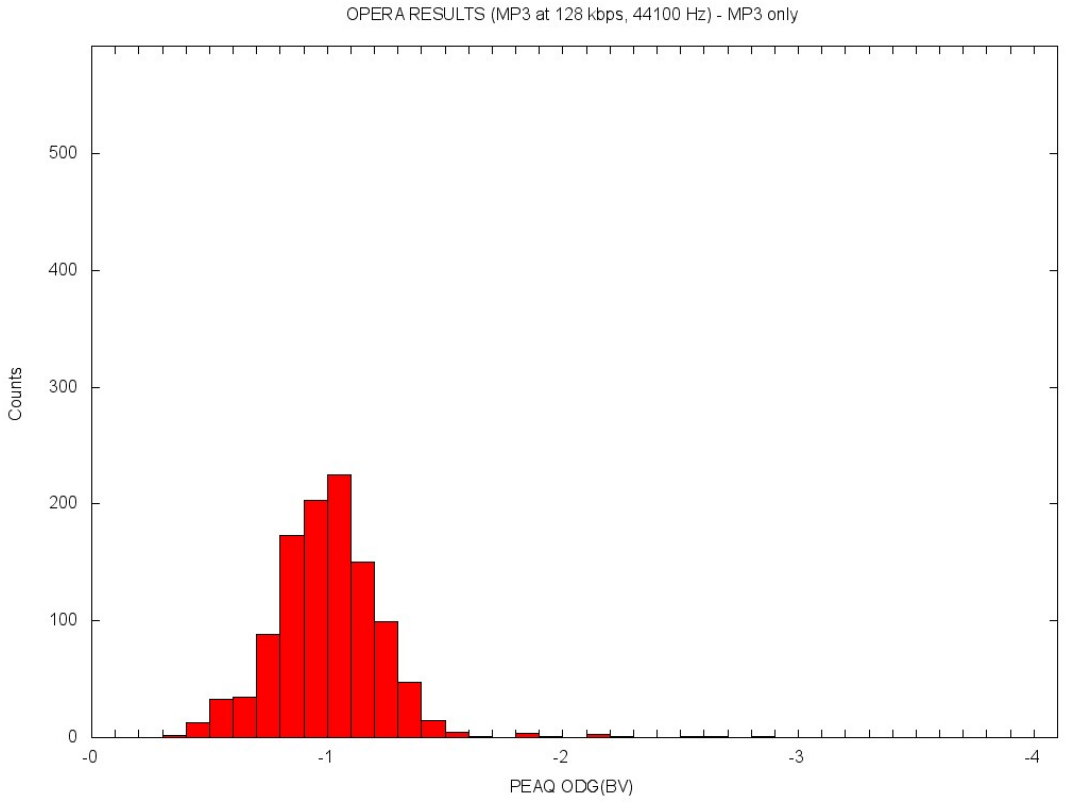
- Nach dem Löschen von Daten kann das Wasserzeichen ab dem nächsten Sync wieder ausgelesen werden
- Robustheit gegen Schneiden des Materials



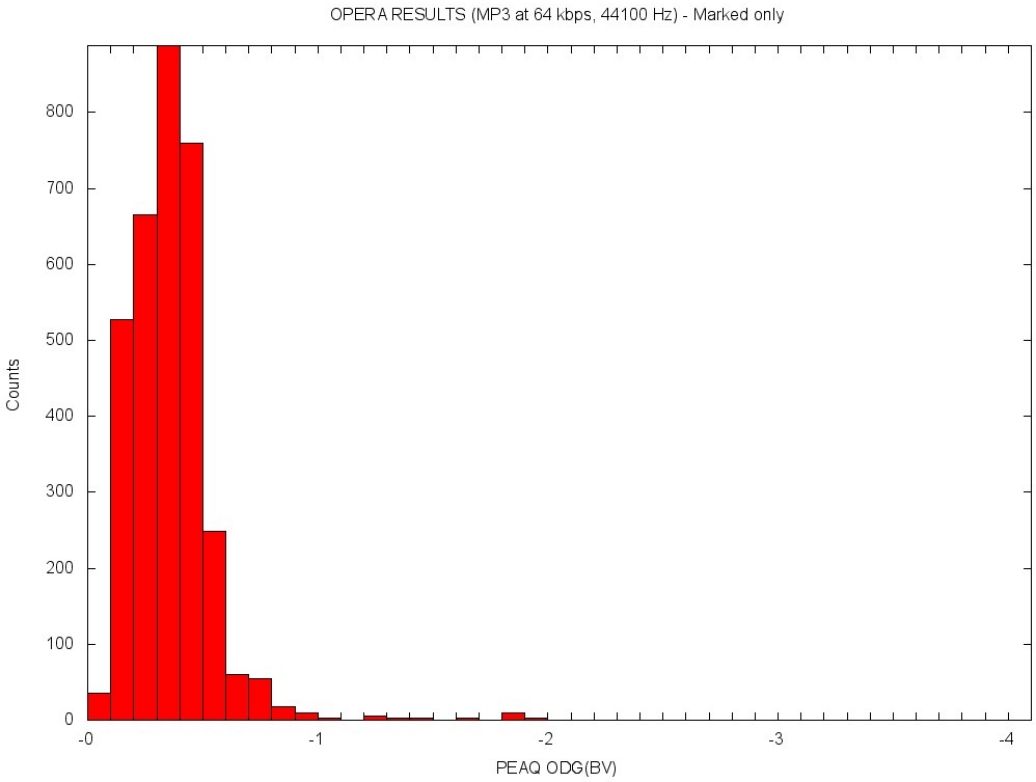
- Anmerkungen
  - Verschiedene Operationen zum Verändern  der Energie in den Frequenzbändern möglich
  - typischerweise Potenzieren der Energiewerte: Verträglichkeit mit üblichen psychoakustischen Modellen
  - Wo darf der Algorithmus wie stark verändern?
    - Psychoakustische Modelle steuern Einbetten
    - 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

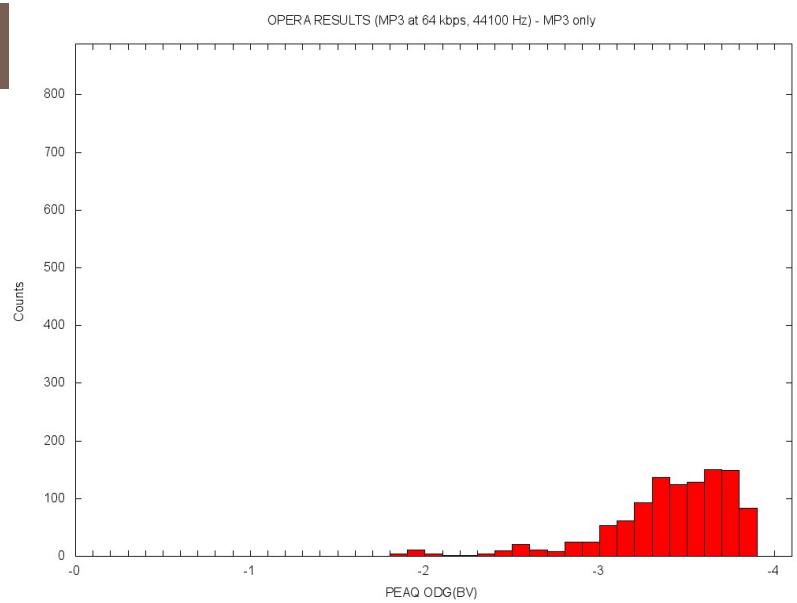
- Ergebnisse: Audioqualität

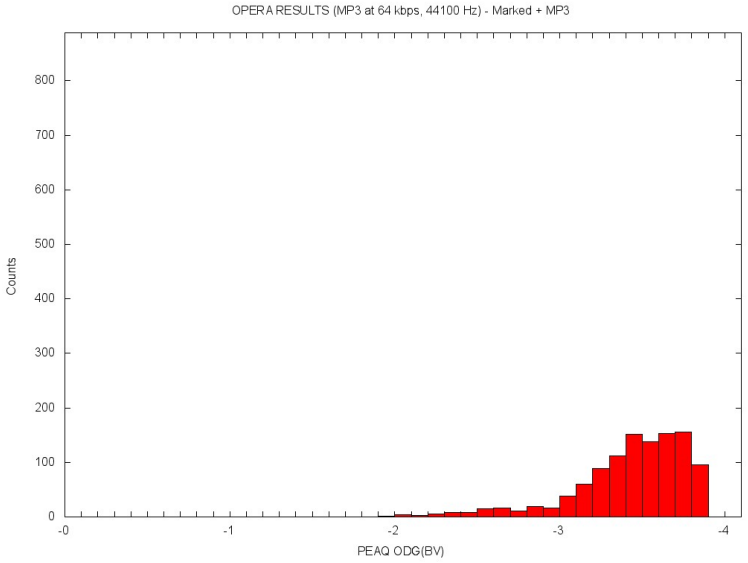




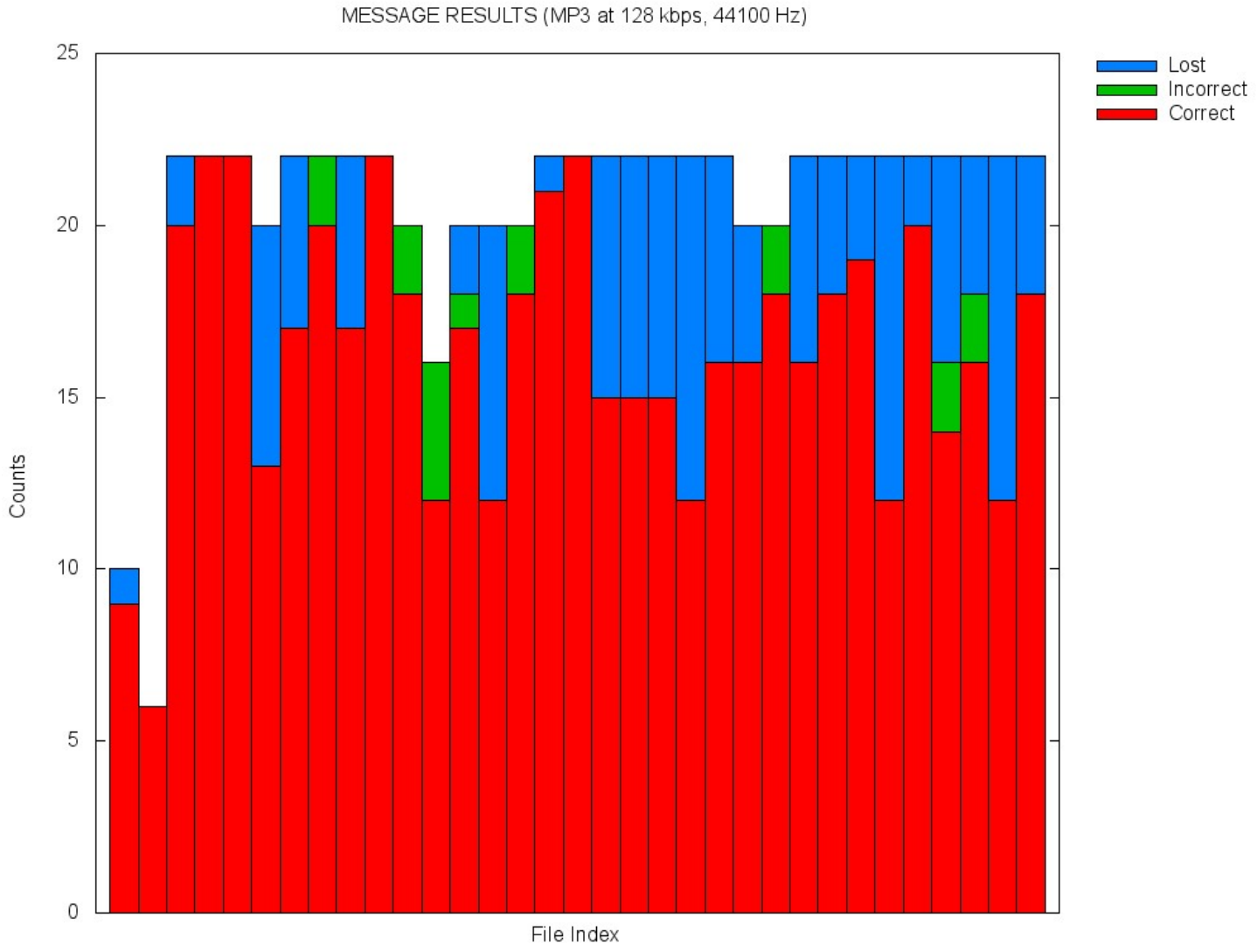
- Ergebnisse: Audioqualität



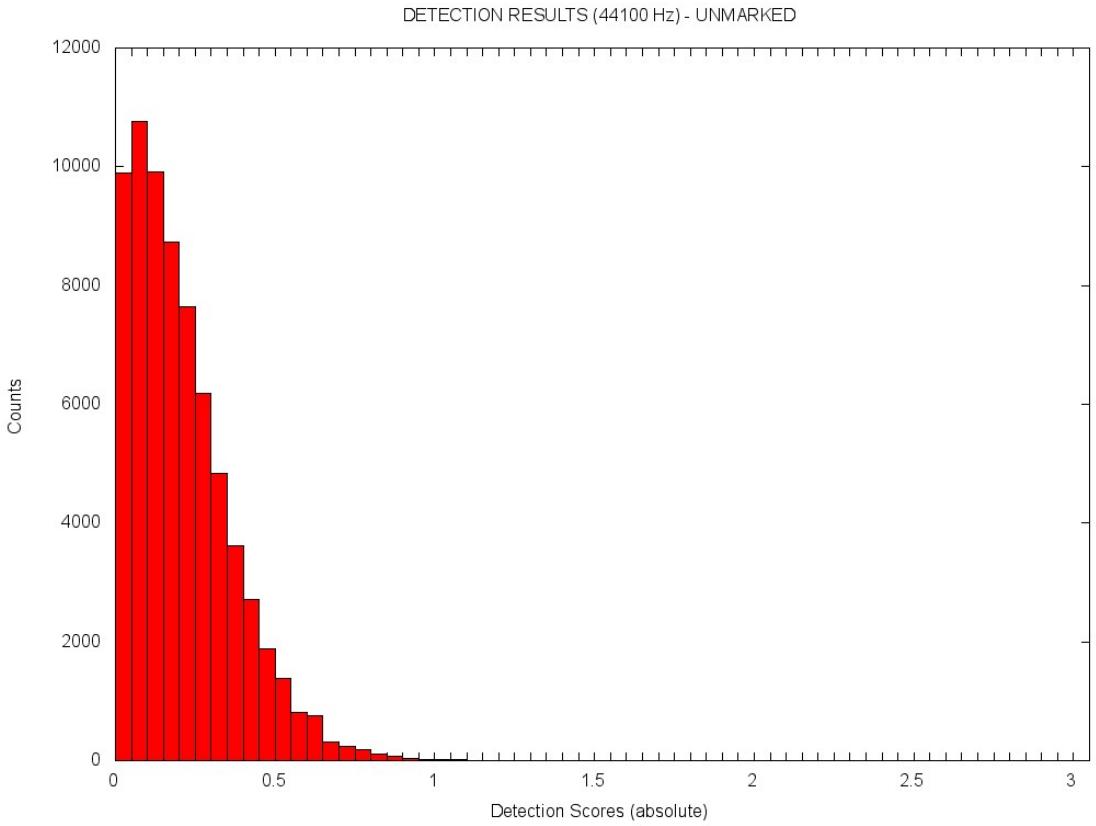


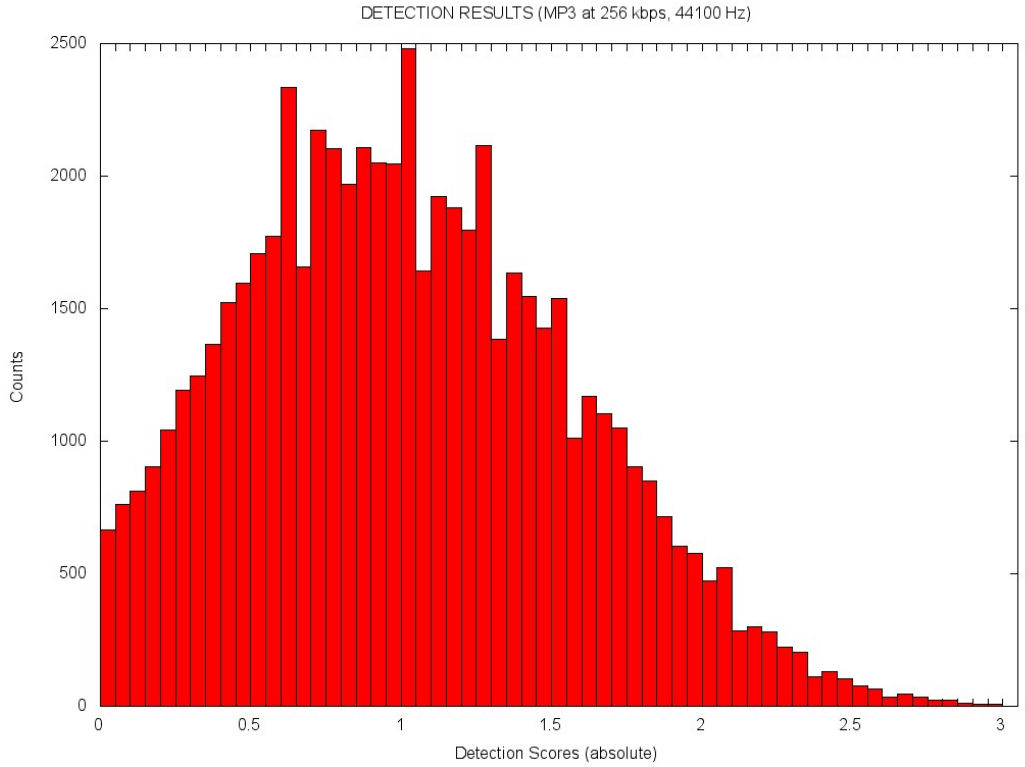


- Ergebnisse: Detektion

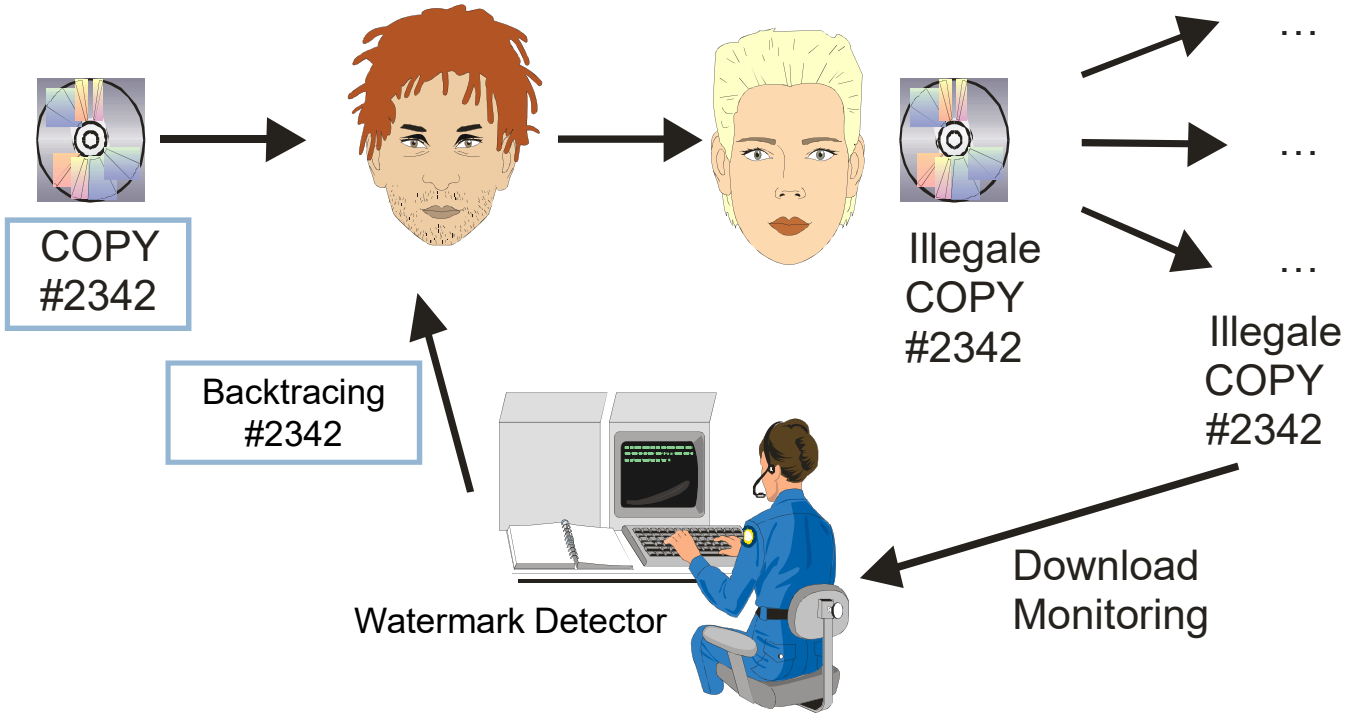


- Ergebnisse: Detektion

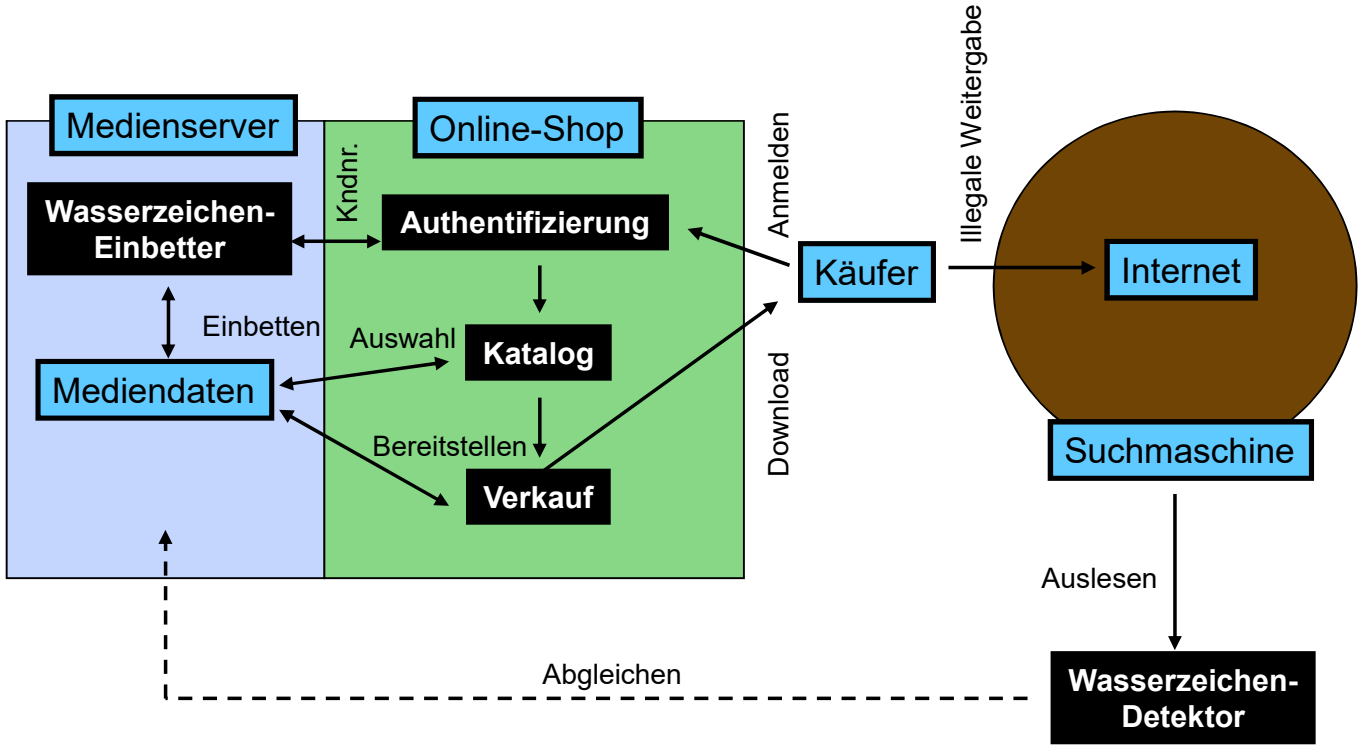




Markierte Kopien können zurückverfolgt werden



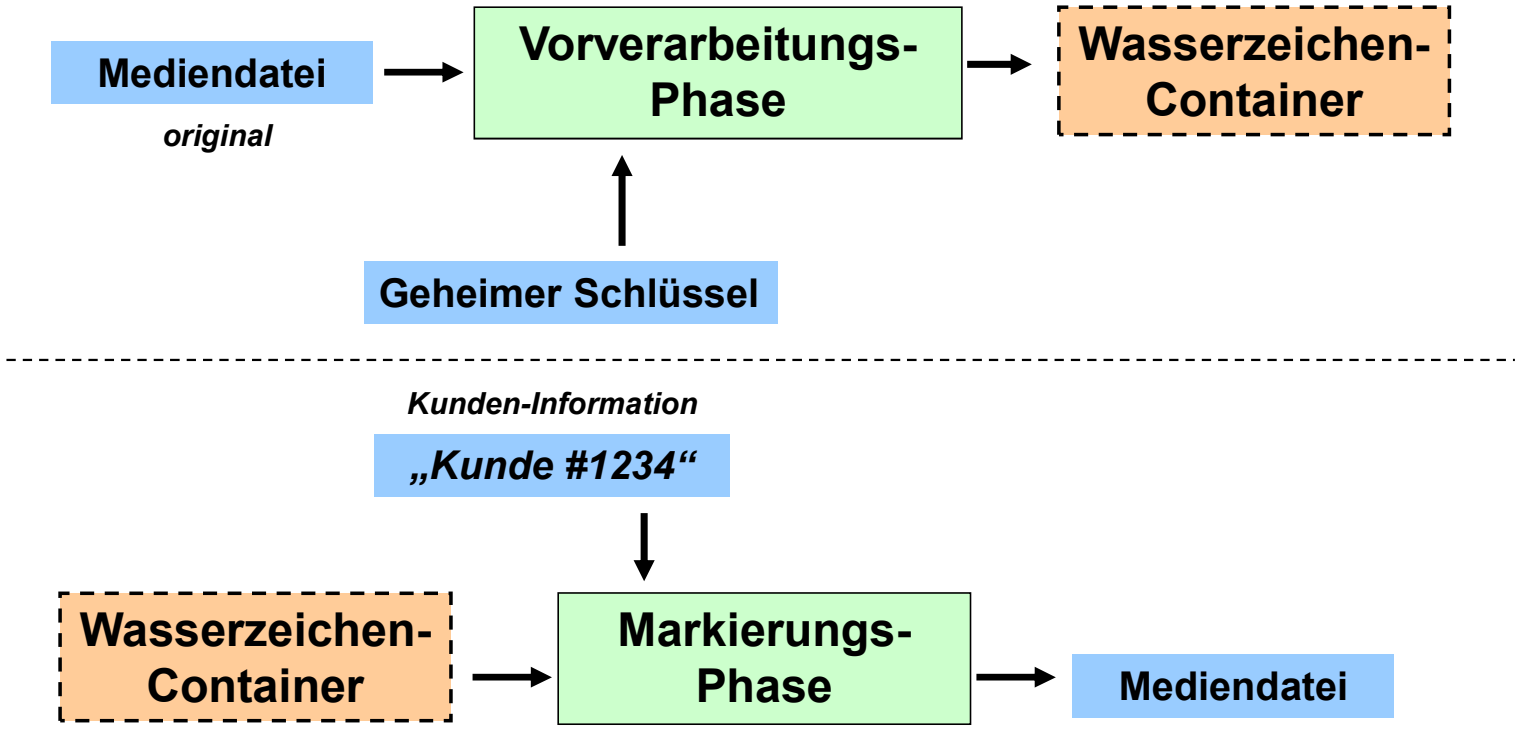
- Online-Shops/ Download-Portale (Transmark Szenario)

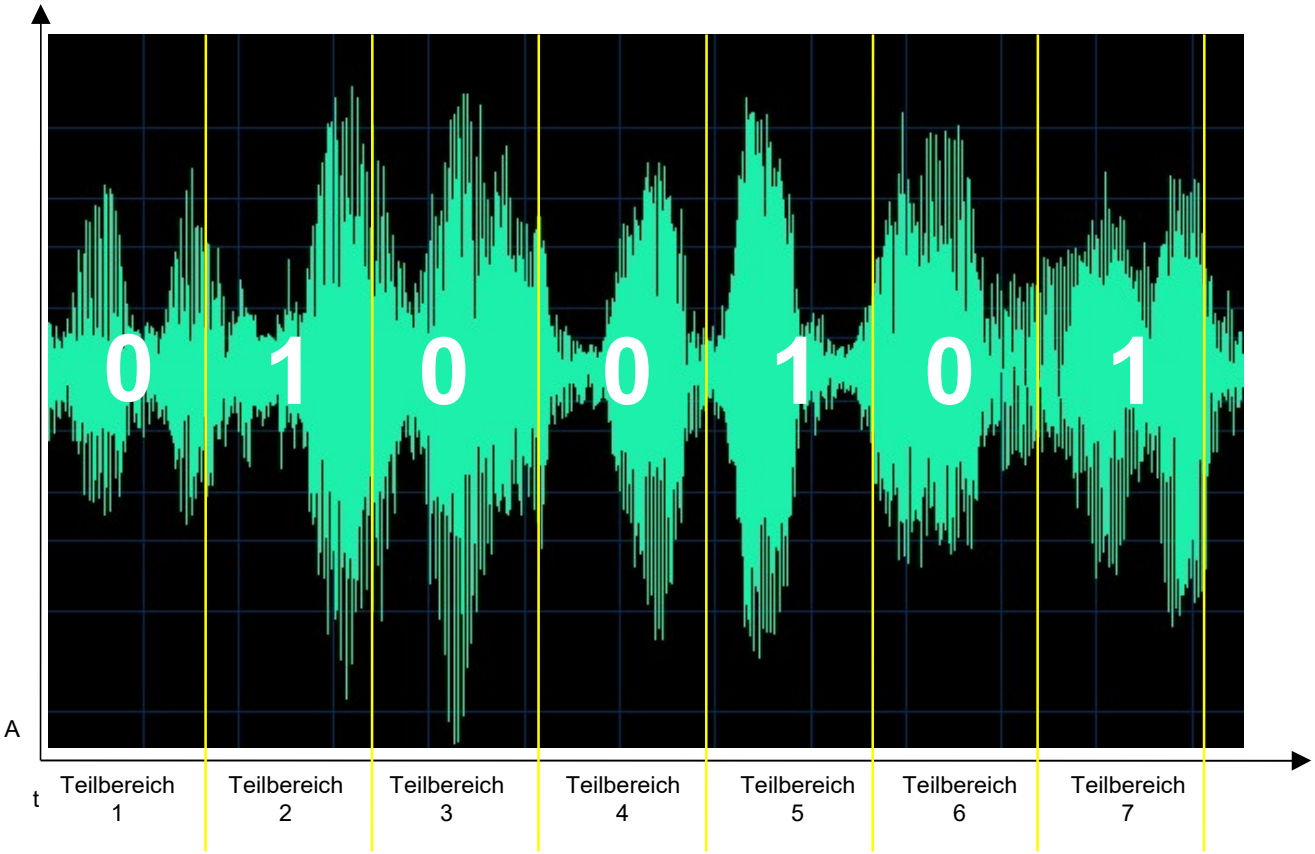


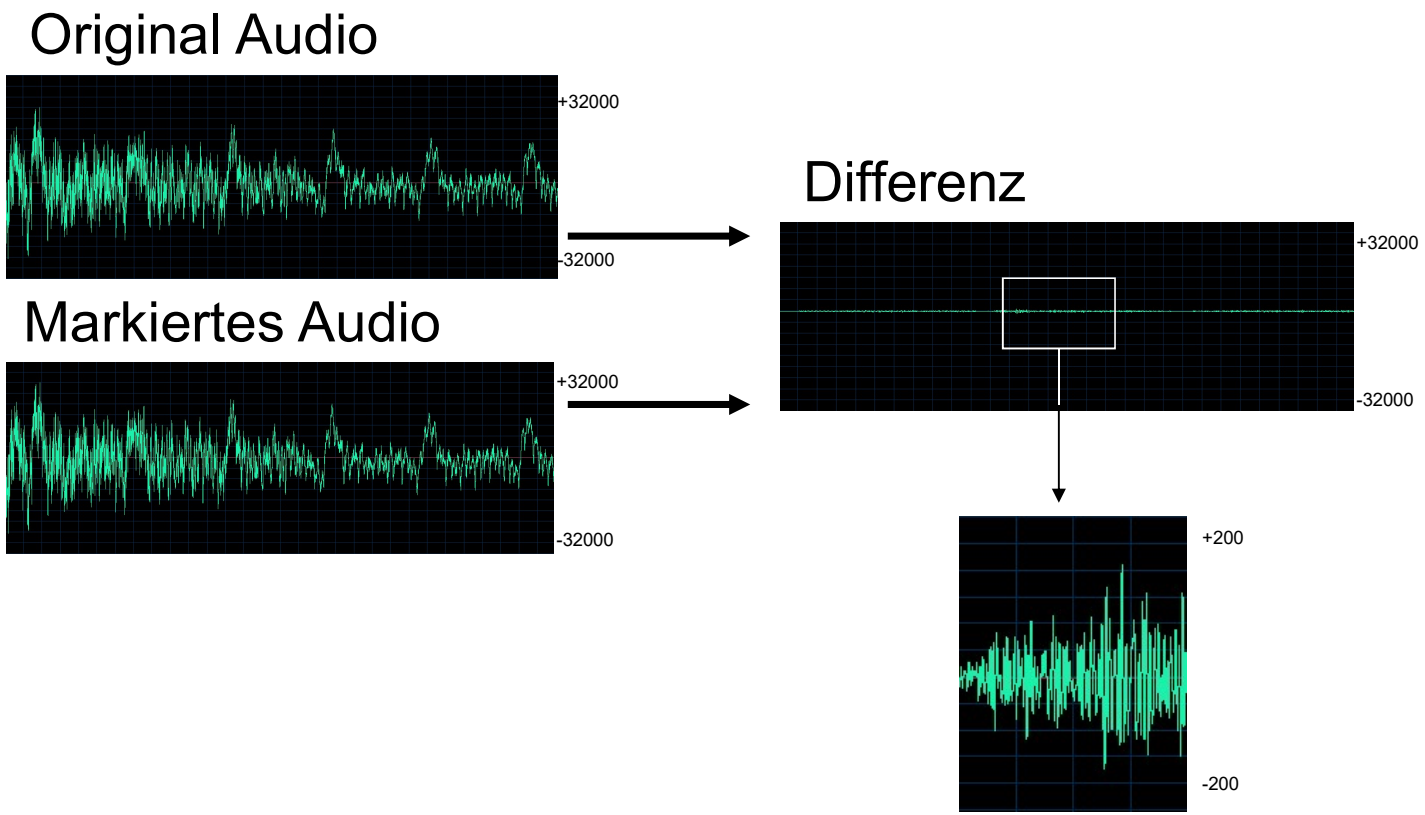
Anwendungsgebiete: Kundenverfolgung

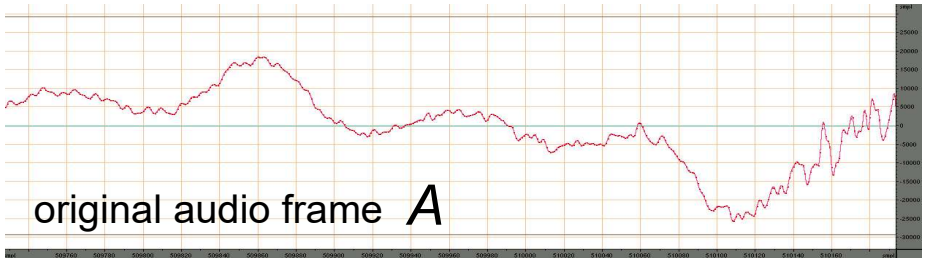
- Anforderungen :
  - Hohe Transparenz
  - Hohe Robustheit
  - Wünschenswert: Sicherheit gegen Koalitionsangriffe
    - Kann hohe Kapazität erfordern

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



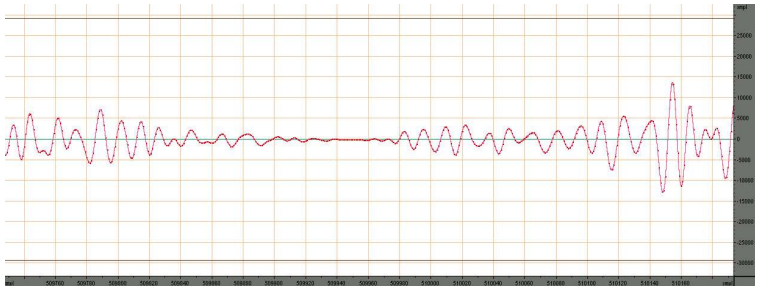

0
1
0
0
1
0
1
A
t
Teilbereich 1
Teilbereich 2
Teilbereich 3
Teilbereich 4
Teilbereich 5
Teilbereich 6
Teilbereich 7


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

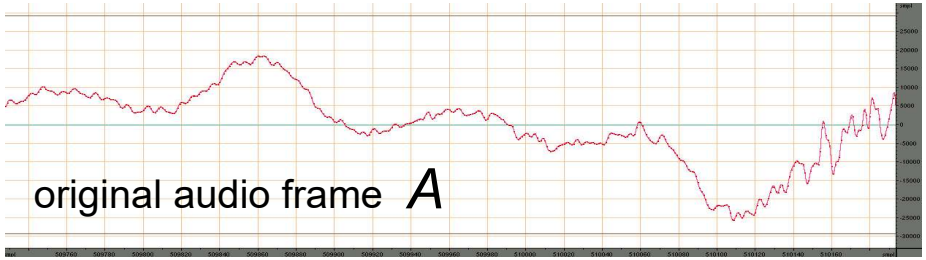


original audio frame A

Frame mit eingebetteter „0“ A_0

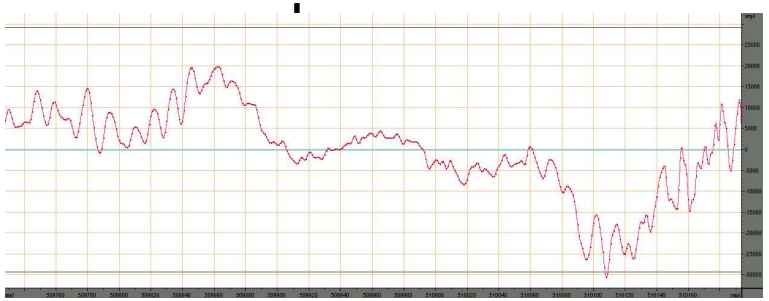


Differenzsingnal $D_0 = A - A_0$

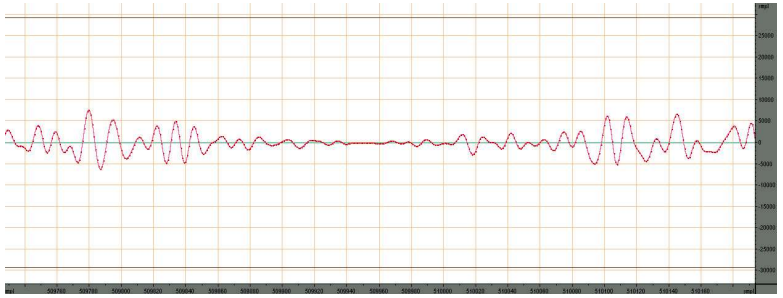


original audio frame A

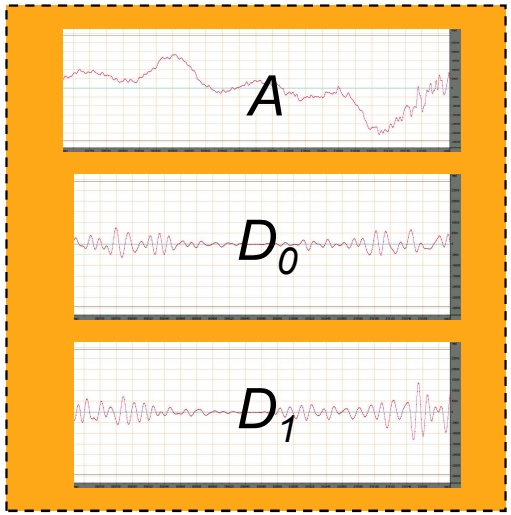
Frame mit eingebetteter „1“ A_1



Differenzsignal $D_1 = A - A_1$



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

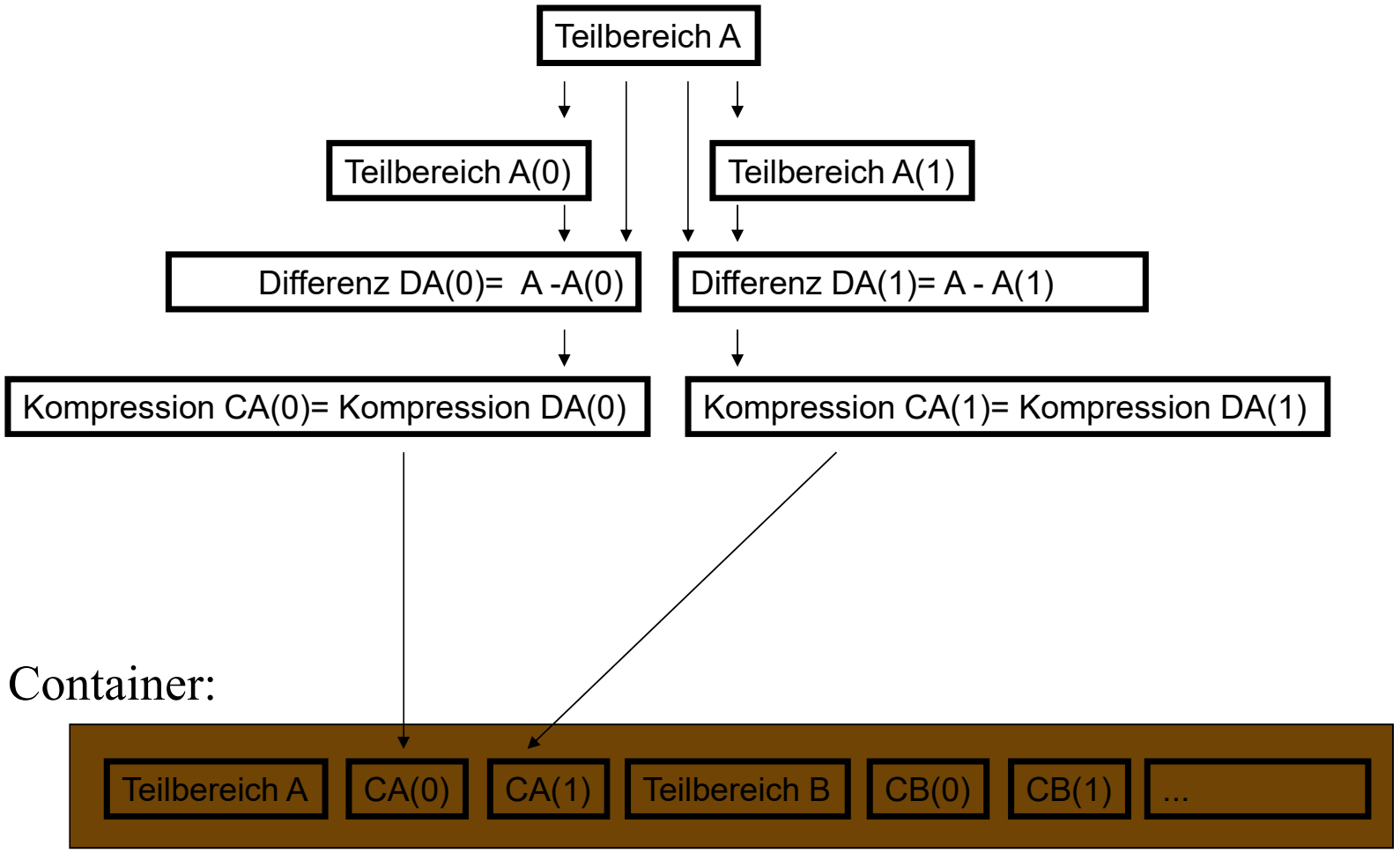


@ Rendering stage

$A_0 = A - D_0$

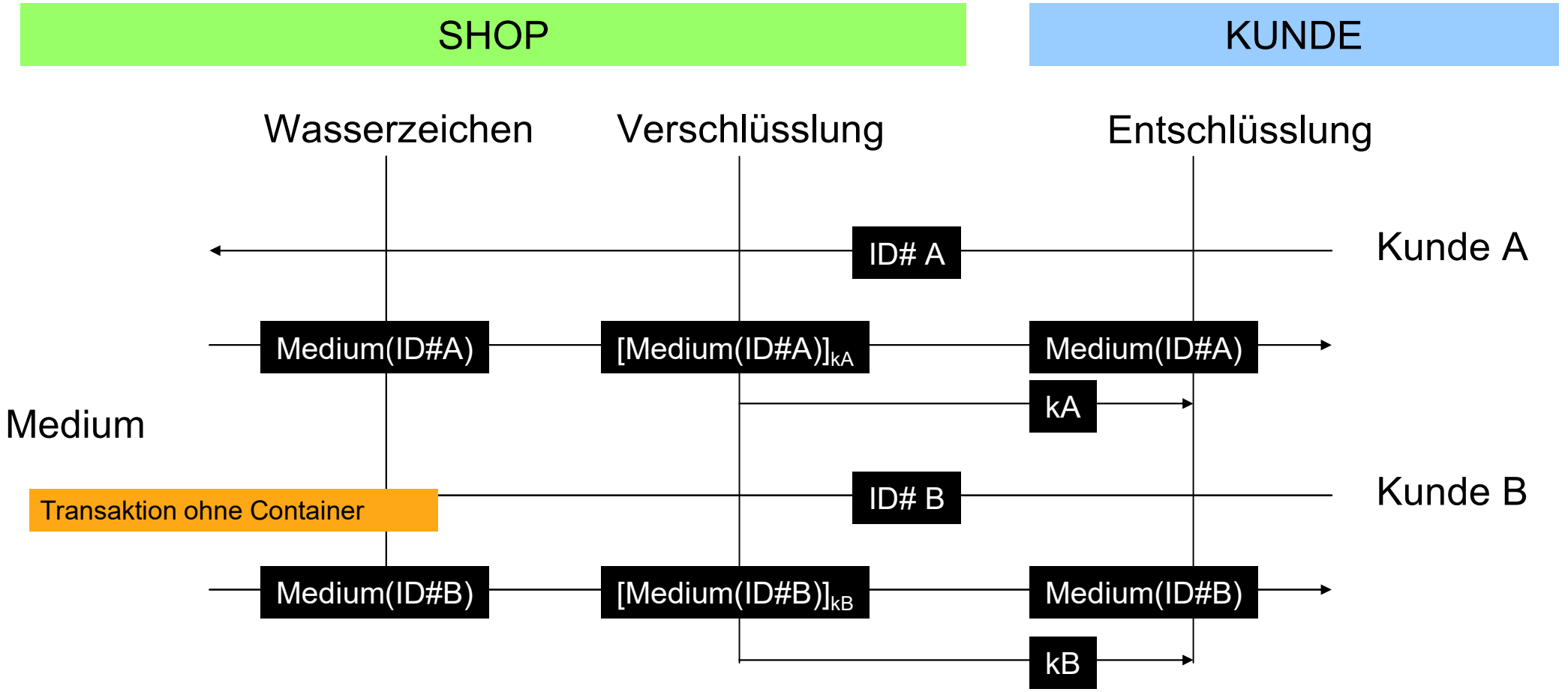
$A_1 = A - D_1$

- 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

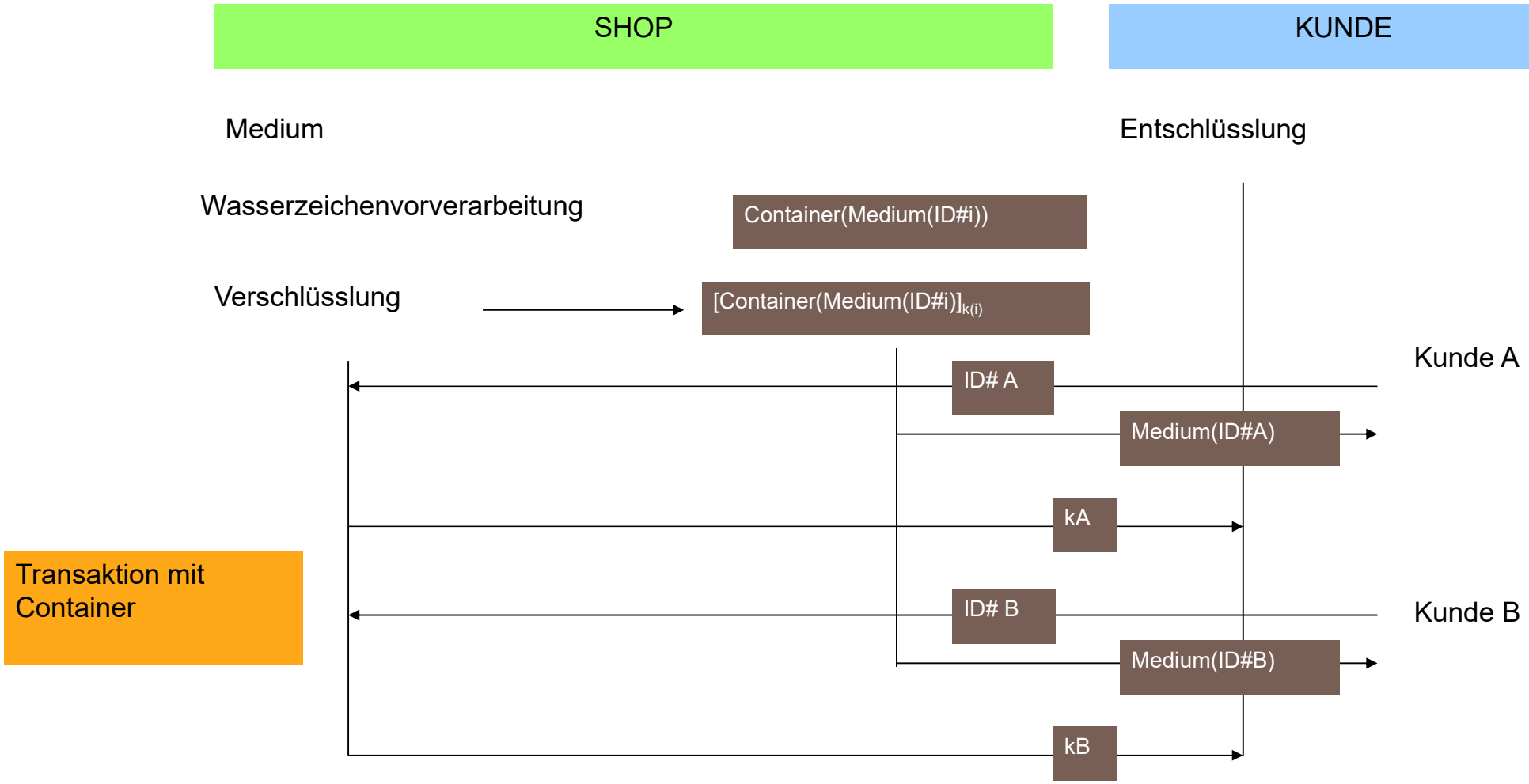

Teilbereich A
Teilbereich A(0)
Teilbereich A(1)
Differenz DA(0)= A -A(0)
Differenz DA(1)= A - A(1)
Kompression CA(0)= Kompression DA(0)
Kompression CA(1)= Kompression DA(1)
Container:
Teilbereich A
CA(0)
CA(1)
Teilbereich B
CB(0)
CB(1)
...

Kryptographisch geschützte Wasserzeichencontainer

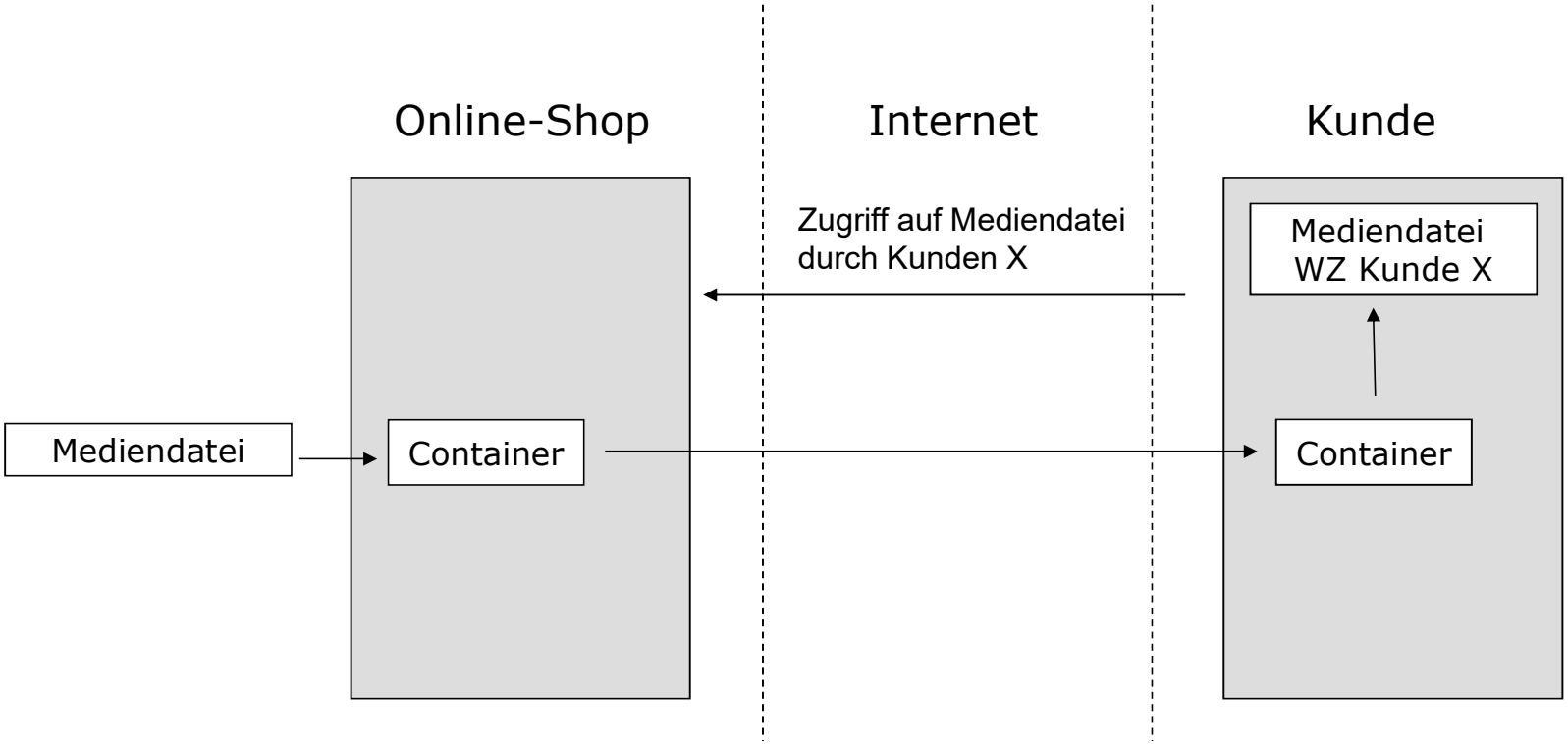
- Digitale Wasserzeichen werden in der Praxis zum Schutz von Urheberrechten eingesetzt
- Transaktionswasserzeichen sind hier eine verbreitete Strategie
  - Jeder Download wird individuell markiert
  - Markierte Kopien können zurückverfolgt werden
- Wasserzeichen-Container ermöglichen sehr schnelles Markieren
- Problem: Jeder Kunde erhält eine individuelle Datei
  - Caching
  - Verschlüsslung bei Übertragung


SHOP
KUNDE
Wasserzeichen
Verschlüsslung
Entschlüsslung
ID# A
Kunde A
Medium(ID#A)
[Medium(ID#A)]kA
Medium(ID#A)
kA
Medium
Transaktion ohne Container
ID# B
Kunde B
Medium(ID#B)
[Medium(ID#B)]kB
Medium(ID#B)
kB

Kryptographisch geschützte Wasserzeichencontainer



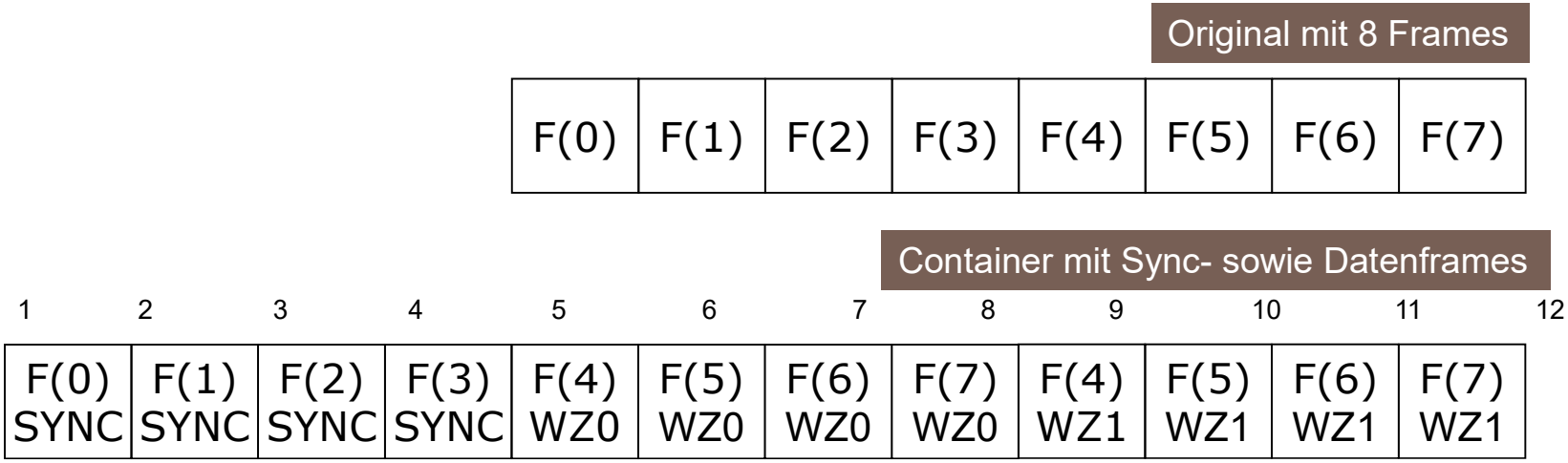
Kryptographisch geschützte Wasserzeichencontainer



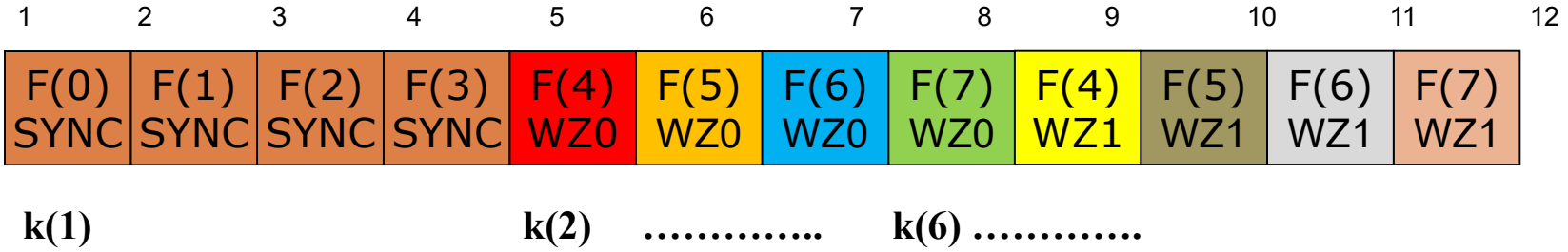
Herausforderung: Konzept, welches zwei Prinzipien vereint:

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

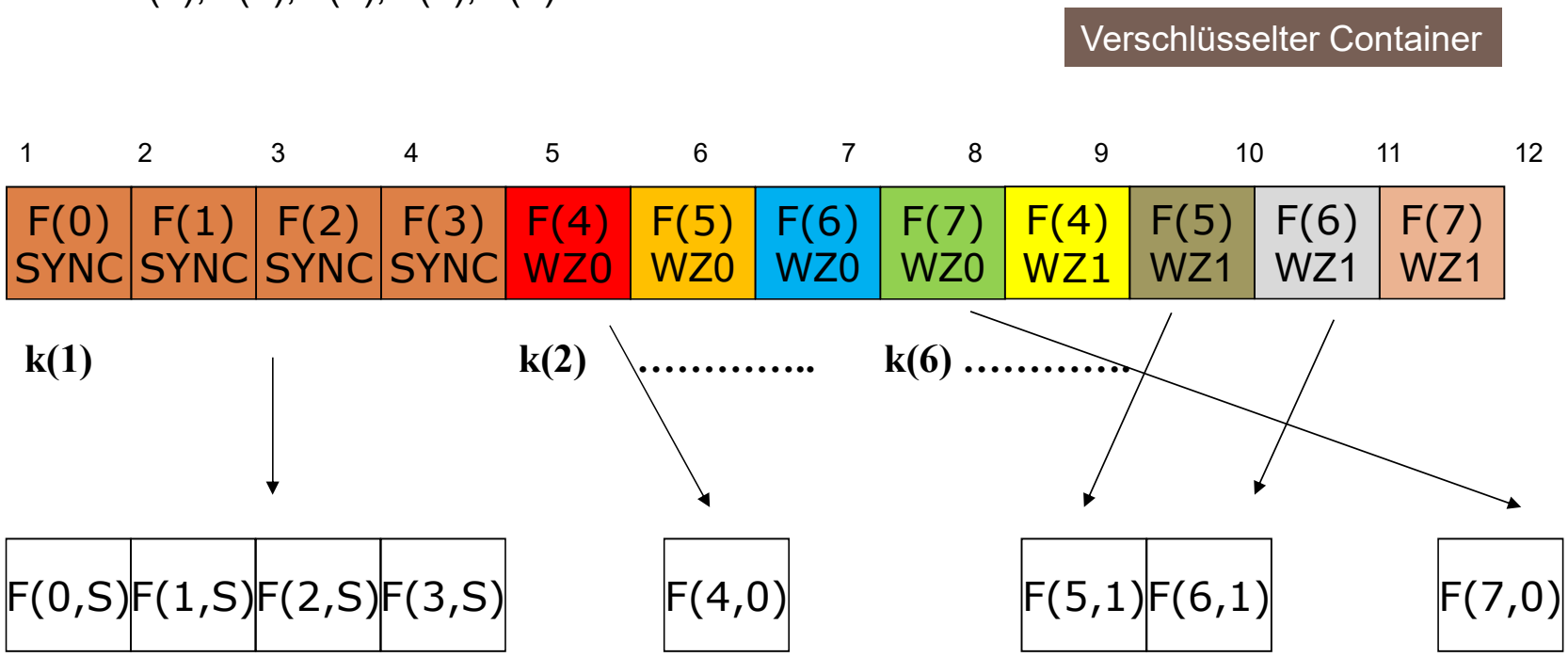
- Beispiel kurze Audiodatei
- Unterteilt in 8 Frames
- Jedes Frame kann ein Bit enthalten: SYNC, WZ0, WZ1



- Nachricht Länge n
- Verschlüsselung
  - k(1) SYNC
  - k(2) WZM Pos 1, Wert 0
  - k(3) WZM Pos 2, Wert 0
  - k(4) WZM Pos 3, Wert 0
  - ….
  - k(n+2) WZM Pos 1, Wert 1
  - …
- (Länge*2)+1 Schlüssel



- Nachricht Länge 0110
  - Kunde erhält k(1), k(2), k(7), k(8), k(6)



Kryptographisch geschützte Wasserzeichencontainer/ System