Copyright & Co:

Digitale Wasserzeichen

Norman Hendrich
Universität Hamburg, Fachbereich Informatik, TECH

Inhalt

Einführung digitale Wasserzeichen

- Konzept
- Angriffe

Markierung von Audiodateien:

- EQ und Filtern
- LSB-Verfahren
- Spread-Spectrum
- Echo-Verfahren

Zusammenfassung

Literatur

Begriffe

Kryptographie

- Nachricht komplett verschlüsseln
- gute Verfahren bekannt

Steganographie

- geheime Nachricht in offener Nachricht verbergen
- Morsecode mit {i,j} {f,t}
- Binärcode mit space, tab

Wasserzeichen ("watermark")

- Sichern des Urheberrechts, Angaben des Käufers, etc.
- offen oder versteckt

Das Problem

- Riesenmarkt: USA sales in 1997: CDs 9.915 M$, CCs 1.523 M$ (IBM)

Analogtechnik:

- Masterbänder altern
- jede Kopie schlechter als die Vorlage
- schlechte Qualität bei Consumertechniken (VHS, CC, ...)

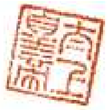
Digitaltechnik:

- alle Kopien identisch mit Vorlage
- Alterung durch Kopieren kompensierbar
- bisheriger Kopierschutz sinnlos (S/PDIF copy-bit)
- auch billige Geräte/Recorder bieten 1:1 Kopien
- extrem gutes Preis/Leistungsverhältnis

=> "Raubkopieren" nimmt zu

Wasserzeichen

Wasserzeichen:



- Monogramm/Logo auf/in jedem Blatt
- seit etwa 1500
- als Qualitätsnachweis des Papiers

- oder zur Authentifizierung (Banknoten, Ausweis, Fahrkarten, etc)
- Fälschung stark erschwert
- Entfernung praktisch unmöglich

digitale Wasserzeichen:

- sichtbare oder unsichtbare Markierung von Daten
- bisherige Verfahren wenig robust

Anforderungen an Wasserzeichen

Wasserzeichen:

- ausreichende Datenrate für Kennzeichnung
- Beispiel ISBN: 10 Dezimalstellen
- keine oder geringe Beeinträchtigung des Nutz- (Audio-) Signals
- "user friendly"

Robustheit:

- gegen elementare Signalverarbeitung
- gegen psychoakustische Signalverarbeitung
- gegen möglichst viele "Angriffe"
- Entfernung nur bei gleichzeitiger Verschlechterung des Nutzsignals
- gegen Fälschung

Wasserzeichen für Textdateien

Textdateien sind besonders schwer zu sichern:

- hinzugefügte Zeichen zerstören die Nutzinformation
- Wasserzeichen nur über Formatierung

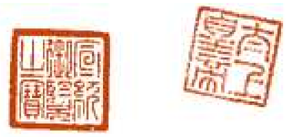
- Tab/Space - Verfahren
- Zeilenabstände oder Wortabstände modulieren (~1/300)
- modifizierte Fonts

- fällt normalerweise nicht auf
- übersteht Vergrösserung, mehrfaches Kopieren
- übersteht Drucken, Scannen, OCR

- ASCII-Export zerstört die Info

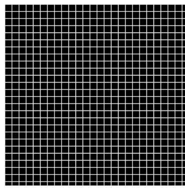
this page intentionally left blank

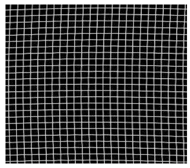
typische Angriffe



einfache Angriffe:

- einfache digitale Filter
- Mischen mehrerer Signale oder mit Rauschen
- Lautstärkeänderung, Dynamikänderung
- sample-rate conversion
- A/D-D/A Konvertierung
- Tempoänderung, pitch-shifting
- MP3-Kodierung usw.
- Kombination mehrerer Verfahren (StirMARK)





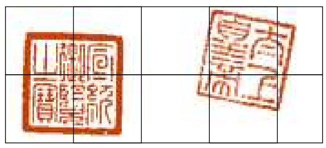
gezielte Angriffe möglich, sobald Algorithmus bekannt:

- Angreifer kann sehr viel Rechenzeit investieren
- praktisch nicht zu verhindern

Mosaic-Attack

"Mosaic-Attack":

- Wasserzeichen erfordert Mindestlänge der Nutzdaten
- lange Dateien in viele kurze zerlegen
- Wasserzeichen wird verstümmelt



- für Bilddaten bereits Tools verfügbar
- Verfahren eignet sich auch für Audio

Interpretation-Attack

"Interpretation-Attack":

- die meisten Algorithmen sind "additiv"
- auch verschiedene Verfahren kombinierbar
- Angreifer fügt eines Wasserzeichen hinzu

=> Priorität der Urheberschaft?!

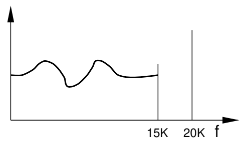
Original:	d
Original + Wasserzeichen:	d + w
Pirat:	d + w + x
Pirat behauptet:	d + w -x ist das Origial

this page intentionally left blank

Radio: mit Kopierschutz und Marken . . .

auch Radiosender brauchen "personality":

- Jingles
- besondere EQ-Einstellungen



trotz zweifelhafter Qualität:

Mitschneiden unmöglich:

- Moderator spricht in Anfang und Ende jedes Songs
- Titel werden nicht ausgespielt
- Titel werden überblendet
- usw.

externe Marken

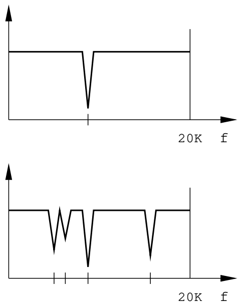
Wasserzeichen im Header/in Kommentaren:

- einfachste Realisierung, etwa zustäzlicher Chunk im WAV-Format
- Nutzdaten werden nicht gestört
- trivial entfernbar (s. S/PDIF Copy-Bit) und fälschbar
- aber Kombination mit digitaler Signatur möglich

`file.wav`	`header`	`chunk-x`	`mark`	`samples`	`sig`

`copy.wav`	`header`	`chunk-x`	`samples`

Notch-Filter



Signal mit Bandsperren (notchfilter) bearbeiten

- sehr schmale Notchfilter (1/100 Oktave)
- kaum hörbar
- mit FFT sofort erkennbar
- evtl. mehrere Bänder sperren

- skaliert nicht auf hohe Anzahl verschiedener Wasserzeichen
- sehr leicht entfernbar
- sehr leicht fälschbar

LSB-Techniken

Wasserzeichen im LSB der Nutzdaten kodieren:

```
sample[t] = sample[t] & 0xfffe
          + mark[t] & 0x0001;
```

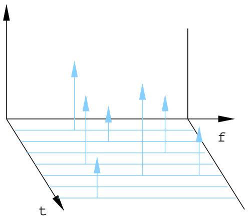
- sehr einfach zu realisieren
- fällt in Popmusik nicht auf
- aber in leisen Passagen hörbar
- sehr hohe Bitrate für das Wasserzeichen möglich

- Konflikt mit Dithering-Verfahren
- anfällig gegen Rauschen
- sehr leicht entfernbar, evtl. fälschbar
- bei 24-bit (DVD-Audio) auch mehrere Bits nutzbar

Spread-Spectrum

schmalbandiges Signal in breitbandigem Signal verstecken

- Nutzsignal wird auf mehrere Frequenzbänder aufmoduliert
- Frequenzbänder werden ständig gewechselt
- Auswahl der Frequenzbänder pseudozufällig
- Sender und Dekoder verwenden gleiche Zufallszahlen



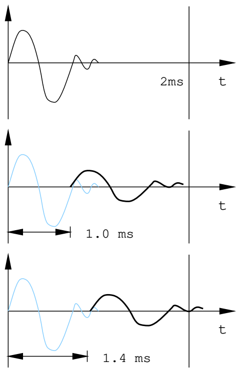
- seit WW2 militärisch genutzt
- GSM, DECT Mobiltelefone, GPS, usw.

- ohne Kenntnis der Zufallszahlen nicht detektierbar
- Nutzsignal detektierbar, auch wenn << Rauschen
- unempfindlich gegen einfache Angriffe

- sehr empfindlich gegen Timing-Veränderungen

Echo-Marking

Wasserzeichen als Echo im Signal verstecken:



- kurze Echos sind kaum wahrnehmbar
- eignen sich damit als Kennzeichnung:
- Bit 1: 1.0 msec Echo
- Bit 0: 1.4 msec Echo

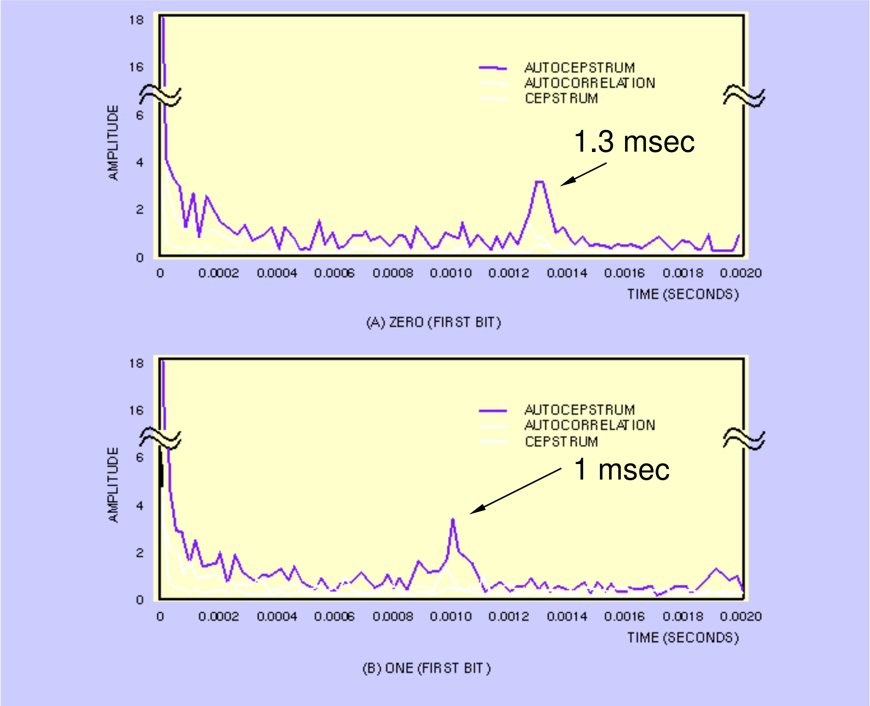
- Detektion erfordert Analyse der Echos
- sehr robust gegen alle einfachen Angriffe

- Entfernung des Echos sehr aufwendig
- aber machbar ...

http://www.research.ibm.com/journal/sj/mit/sectiona/bender.html

Echo-Marking

Figure 28 Result of autocepstrum and autocorrelation for (A) "zero" and (B) "one" bits



Literatur

- Proceedings of the IEEE, special issue on "identification and protection of multimedia information", July 1999
- Lecture notes in computer science, LNCS 1174, "information hiding", Cambridge 1996, K-INF-23262
- Cambridge security group, www.cl.cam.ac.uk
- `www.research.ibm.com/journal/sj/mit/sectiona/bender.html`
- diverse Firmen und Organisationen, u.a.:

  `www.smdi.org`

  `www.musicode.com`

  `www.audiotrack.com`