

13. Foliensatz Computernetze

Prof. Dr. Christian Baun

Frankfurt University of Applied Sciences
(1971–2014: Fachhochschule Frankfurt am Main)
Fachbereich Informatik und Ingenieurwissenschaften
christianbaun@fb2.fra-uas.de

Lernziele dieses Foliensatzes

- Steganographie
 - Grundlagen der Steganographie
 - Semagramme
 - Zinken
 - WarChalking
 - Zielsetzungen von Steganographie
 - Rechnergestützte Steganographie
 - Grundlagen
 - LSB-Methode (*Least Significant Bit*)
 - Palettenbasierte und komprimierte Bilddaten als Trägerdaten
 - Audio- und Videodaten als Trägerdaten
 - Fragmentierung eines Dateisystems als Trägerdaten
 - Auswahl an Software-Lösungen für Steganographie
 - Angriffe auf Steganographie (*Steganalyse*)
 - Plagiatsfallen und Wasserzeichen
 - Sichtbare und unsichtbare Wasserzeichen
 - Digitaler Fingerabdruck
 - Einbettungsverfahren für digitale Fingerabdrücke
 - Fazit zur Steganographie

Grundlagen der Steganographie

- **Kryptographie** ist die **erkennbare** Benutzung eines Kryptosystems zur Chiffrierung einer Nachricht
- **Steganographie** ist der **verdeckte** Gebrauch eines Verfahrens, mit dessen Hilfe eine Botschaft versteckt wird
- Neben den Daten selbst bleibt damit im Gegensatz zu anderen Techniken auch die **Tatsache des Verschlüsseln**s selbst **geheim**

Steganographie (wörtlich übersetzt: *verdecktes Schreiben*) ist die Wissenschaft vom Verstecken von Daten

Literatur zur Steganographie

- Klaus Schmeh. **Versteckte Botschaften**. Heise Zeitschriften Verlag. 2009
- Jana Dittmann. Digitale Wasserzeichen. Springer. 2000
- Marit Köhntopp. **Steganographie als Verschlüsselungstechnik**. iX 4/1996. S.92-96
- Andreas Westfeld. **Geheime Nachrichten sicher in Bild, Text und Ton verstecken**. c't 9/2011. S.170

Klassische Formen der Steganographie

- Histiaios von Milet (ca. 500 v. Chr.)
 - Einem Sklaven den Kopf scheren und eine **Nachricht auf die Kopfhaut tätowieren**
 - Sobald die Haare wieder nachgewachsen sind, wird der Sklave zum Empfänger geschickt
 - Extrem zeitraubendes Verfahren
- Demarator von Susa (ca. 580 v. Chr.)
 - Beschrieben von Herodot (485-425 v. Chr.)
 - **Wachstafeln**, die in Wachs geritzte Botschaften enthalten
 - Die geheime Nachricht wird nicht auf das Wachs, sondern auf das Holz dahinter geschrieben
 - Dank dieses Verfahrens wurde der persische Herrscher Xerxes 580 v. Chr. von den Griechen bei Salamis entscheidend geschlagen

Weitere klassische Formen der Steganographie

- Plinius der Ältere (um 50 n. Chr.)
 - *unsichtbare* **Geheimtinte** (z.B. Zitronensaft oder Essig)
- Doppelter Boden in Paketen oder Briefumschlägen
- Hohle Absätze in Schuhen
- Emanuel Goldberg (1925)
 - **Mikropunkt** (auch Mikrat genannt)
 - Verkleinerung einer Schreibmaschinenseite auf die Größe eines mit Schreibmaschine getippten Punktes (ca. 1 mm²)

Semagramme

- Die US-Zensoren im 2. Weltkrieg, die die Post überwachten, achteten nicht nur auf seltsame Formulierungen und unsinnige Bestellungen, sondern auch auf Symbole aller Art
- Damals war es üblich, dass Verliebte ihren Liebsbriefen Kreuze als Zeichen für Küsse hinzufügen
- Die Zensoren mussten hinter den Kreuzen einen Geheimcode vermuten und diese darum entfernen
 - Wenn ein Zensor dies nicht übers Herz brachte, konnte er auch ein paar Kreuze hinzufügen
- Mit Kreuzen am Ende eines Briefes lassen sich versteckte Nachrichten übermitteln
 - Diese nennt man **Semagramme**
 - Die Anzahl und Position von Symbolen kann Buchstaben kodieren

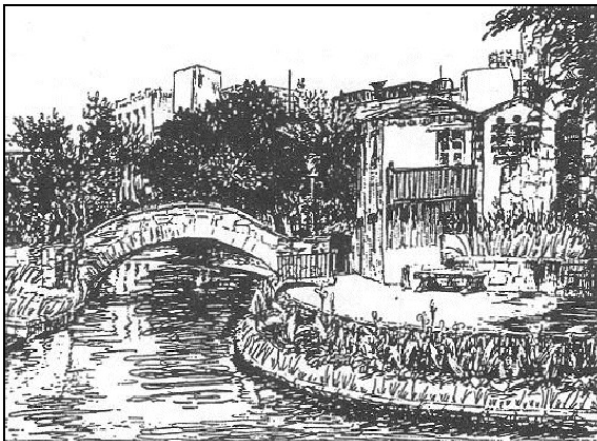
Semagramme in Bildern

- Besonders einfach und wirkungsvoll ist es, Semagramme in Bildern einzufügen
- Häufig kommt dabei der Morsecode nach Samuel Morse von 1838 zum Einsatz
- Der Morsecode ist eine effiziente Kodierung von Daten

| | | | | | |
|---|---------|---|---------|---|-----------|
| A | · — | M | — — | Y | — · — — |
| B | — . . . | N | — · | Z | — — . . |
| C | — · — · | O | — — — | 1 | · — — — — |
| D | — . . | P | · — — · | 2 | · . — — — |
| E | · | Q | — — · — | 3 | · . . — — |
| F | · . — · | R | · — · | 4 | · . . . — |
| G | — — · | S | · . . | 5 | · |
| H | · . . . | T | — | 6 | — |
| I | · . | U | · . — | 7 | — — . . . |
| J | · — — — | V | · . . — | 8 | — — — . . |
| K | — · — | W | · — — | 9 | — — — — · |
| L | · — . . | X | — . . — | 0 | — — — — — |

Semagramme in Bildern – Beispiel 1

- Wo befindet sich in dem Bild eine Nachricht versteckt?



- Das Bild wurde von den US-Zensoren zu Übungszwecken verwendet

Semagramme in Bildern – Beispiel 2

- Wo befindet sich in dem Bild eine Nachricht versteckt?
- Die Zeichnung wurde von deutschen Agenten in England erstellt



Quelle: **Nazi-Botschaften in Modezeichnungen**. Spiegel Online. 4.9.2006
<http://www.spiegel.de/panorama/0,1518,435108,00.html>

Semagramme in Bildern – Beispiel 3

- Wo befindet sich in dem Bild eine Nachricht versteckt?
- Die Zeichnung war 1977 in der französischen Zeitschrift Spirou abgedruckt



Semagramme in Bildern – Lösungen

• Beispiel 1

- Die Nachricht wird von Grashalmen am linken und rechten Flussufer dargestellt, die einen Morsecode bilden
- Ein kurzer Halm steht für einen Punkt und ein langer für einen Strich
- Am linken Ufer steht COMP LI MENTSOFCP
- Am rechten Ufer steht SAMATOURCHIEFCOLHAROLD RSHAWONHISVISITTO SANANTONIOMAY11TH1945
- Ergebnis der zusammengesetzten Nachricht mit Zwischenräumen:
COMPLIMENTS OF CPSA MA TO OUR CHIEF COL HAROLD R SHAW ON
HIS VISIT TO SAN ANTONIO MAY 11TH 1945

• Beispiel 2

- In dem Bild steht (angeblich) mit Punkte und Striche kodiert:
Massive Feindverstärkungen werden stündlich erwartet

• Beispiel 3

- In dem Bild sind 3 Morsecode-Nachrichten versteckt
 - Alle drei ergeben die Namen von Automarken
- Die Raben auf dem Baum stehen für VW, die Blumen für VOLVO und die Latten des Zauns für BUICK

Aktuelles Beispiel für ein Semagramm

- Western Digital hat in seinen „My Book“ Netzwerkplatten einen Morsecode im Gehäuse eingearbeitet
- Der Code besteht aus den Worten `personal`, `reliable`, `innovative`, `simple`, `design` und ein mal `innovateve` (ist falsch geschrieben)























Bildquelle: Wikipedia und <http://de.engadget.com>

Zinken

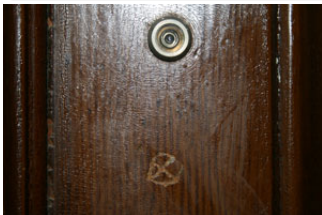
- **Geheimzeichen** von Bettlern, Einbrechern, Dieben, Hausierern, fahrendem Volk, Drucker-Kolonnen oder Vertretern
- Verständigungsmittel und Hinweis auf die Art des Empfanges in den betreffenden Wohnungen und Häusern

Quelle: <http://www.code-knacker.de/gaunerzinken.pdf>

| | | | |
|--|--|--|--|
|  Hier gibt es Geld |  Achtung, bissiger Hund |  Leute rufen Polizei |  Abhauen |
|  Die Leute sind ruppig |  Hier gibt es Essen |  Fromm tun lohnt sich |  Aufdringlich werden |
|  Nur Männer im Haus |  Vorsicht, Prügel |  Arbeit wird belohnt |  Nachtlager möglich |
|  Gefährlich: Hände weg |  Krank spielen |  Hund |  Hier wohnen alte Leute. |
|  Alleinstehende Frau |  Nur Frauen im Haus |  Hier wohnen Frauen mit weichen Herzen |  Behördenmitglied |

Zinken (2)

Quelle: <http://www.code-knacker.de/gaunerzinken.pdf>



Quelle: <http://derstandard.at>



Quelle: <http://diepresse.com>

| | | | |
|---------------------------------|--|---------------------------|----------------------------|
| | | | |
| Günstig zum Diebstahl | Hier ist die Polizei | Aktive Polizisten | Gefahr oder immer bewohnt |
| | | | |
| Dieser Gemeinde ausweichen | Bereits beraubt | Nichts interessantes | Unbewohntes Haus |
| | | | |
| Achtung, brutaler Hausbesitzer! | Hier lohnt sich ein Einbruch wirklich - fette Beute! | Hier ist nichts zu holen. | Ruhig aufdringlich werden. |
| | | | |
| Hier gibt's was. | Hier gibt's nichts | Am Abend kommen. | Die Polizei wird gerufen. |
| | | | |
| Hier einmal gearbeitet. | Verhaftet. | Kein Man im Haus. | Frau liebt Männer |

Moderne Zinken: WarChalking

- Markierung von an einem bestimmten Ort empfangbaren WLAN mit Kreidezeichen (englisch: *chalk* = Kreide)
 - Die Zeichen werden üblicherweise auf Häuserwänden, dem Straßenpflaster oder Laternenpfählen angebracht
- Angegeben wird teilweise sogar die SSID sowie das WEP-Kennwort
- Ziel: Kostenlos im Internet surfen
- Ist heute auch schon wieder veraltet
- Kostenfreies Internet weckt heute kaum noch Begehrlichkeiten, da vielerorts (z.B. in Hotels, Restaurants und Kneipen) legal vorhanden

| let's warchalk..! | |
|--------------------------------|---------------------------------------|
| KEY | SYMBOL |
| OPEN NODE | ssid bandwidth |
| CLOSED NODE | ssid |
| WEP NODE | ssid access contact bandwidth |
| blackbeltjones.com/warchalking | |



Quelle: <http://www.wired.com/gadgets/wireless/news/2002/07/53638>

Zielsetzungen von Steganographie

- Man unterscheidet 2 Zielsetzungen von Steganographie

① Unsichtbarkeit

- Geheime Nachrichten werden in anderen Nachrichten versteckt

② Markieren

- Seriennummern oder andere eindeutige (Urheber-)Informationen werden in Dokumente oder sonstige Daten hineincodiert
- So können illegale Kopien zurückverfolgt und Urheberrechtsverletzungen nachgewiesen werden
- Diese **digitalen Fingerabdrücke** oder **Wasserzeichen** können sich z.B. bei Texten aus minimal veränderten Wort- oder Zeilenabständen oder Schriftmodifikationen und bei Bildern oder PDF-Dokumenten aus veränderten Pixelwerten ergeben

Beispiel: Daten in Texten verstecken

- Ein unverdächtiger Postkartentext:

Liebe Kolleginnen! Wir genießen nun endlich unsere Ferien auf dieser Insel vor Spanien. Wetter gut, Unterkunft auch, ebenso das Essen. Toll! Gruß, M. K.

- Entzifferung der versteckten Botschaft:
 - Zeichen (einschließlich Satzzeichen) bis zum nächsten Leerzeichen zählen
 - Anzahl ungerade \Rightarrow 0
 - Anzahl gerade \Rightarrow 1
 - Die ersten 8 Wörter ergeben 01010011
 - Das entspricht dezimal 83
 - Nach der ASCII-Tabelle ergibt das den Buchstaben S
 - Die nächsten 8 Wörter ergeben 01001111 (79, Buchstabe O)
 - Die letzten 8 Wörter ergeben wieder 01010011 (83, Buchstabe S)
- Die geheime Nachricht ist also SOS

Rechnergestützte Steganographie – Grundlagen

- Computerdaten, in denen sich eine versteckte Nachricht befindet, nennt man **Trägerdaten** oder **Cover**
- Für die Wahl einer geeigneter Trägerdaten ist das Prinzip der **glaubhaften Abstreitbarkeit** wichtig
 - Existenz oder Ursprung von Informationen soll nicht nachweisbar sein
 - Besonders bei Bildern oder Videos als Trägerdaten sollten diese unverfänglich sein und keinen Verdacht erwecken
- Beispiele für Trägerdaten, die rechnergestützt steganographisch verändert werden:
 - Textdaten
 - Bilddaten
 - Audiodaten
 - Videodaten
 - Dateisystem-Fragmentierungen

Rechnergestützte Steganographie – einfaches Verfahren (1)

- Einfache Möglichkeit zum Verbergen von Daten in Bildern:
 - Schwarz-Weiß-Bilder, deren Bildpunkte (Pixel) mit einem Wert von 0 bis 255 dargestellt werden
 - 0 steht für schwarz und 255 für weiß
 - Die Werte dazwischen repräsentieren die Grautöne
 - Verschiebt man die Grautöne um einen Zähler, kann das menschliche Auge das nicht wahrnehmen
- Das Verfahren bezeichnet man als **LSB-Methode** (*Least Significant Bit*) weil immer das **niederwertigste Bit** als Datenversteck genutzt wird
 - Das niederwertigste Bit hat den kleinsten Einfluss auf den Gesamtwert
- Man kann pro Bildpunkt 1 Bit geheime Informationen speichern
- Bei Farbbildern wird jeder Bildpunkt mit 3 Farbwerten (RGB) zwischen 0 und 255 dargestellt
 - Die Nachrichtenlänge, die in ein Bild passt, verdreifacht sich so
 - Allerdings verdreifacht sich auch die Dateigröße gegenüber S/W
- Problem: Das LSB-Verfahren funktioniert nur bei **unkomprimierten Bildformaten** wie MS-Bitmap (BMP)

Rechnergestützte Steganographie – einfaches Verfahren (2)

- In der Praxis ist die **LSB**-Methode meist nicht anwendbar, weil unkomprimierte Dateiformate für Bilder zu groß sind
- Komprimierte Dateiformate wie JPG, PNG und GIF sind populärer

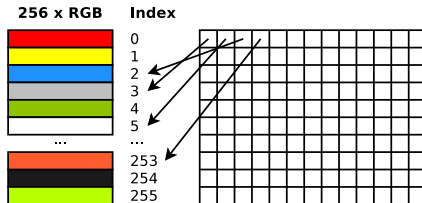
Quelle: Klaus Schmeih. Versteckte Botschaften. Heise. 2009

„Komprimierung ist der natürliche Feind der computerbasierten Steganographie, denn das Komprimieren hat den Zweck, überflüssige Datenteile zu entfernen. Gerade diese überflüssigen Teile sind es jedoch, die sich steganografisch nutzen lassen.“

- Es existieren auch andere Möglichkeiten um Informationen in Bildern zu verstecken
 - Diese Verfahren bieten aber eine geringere Informationsdichte als LSB
- Die Informationsdichte an versteckten Daten, die man erreichen kann, hängt von der Menge des tolerierten Rauschens in diesen Daten ab
 - Bild- und Audiodaten haben einen hohen tolerablen Rauschanteil
 - Eine Veränderung des Rauschens fällt nicht auf

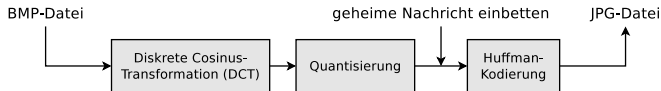
Palettenbasierte Bilddaten als Trägerdaten

- BMP-Bilder sind schnell einige MB groß und sind als E-Mail-Anhang sperrig und verdächtig groß
 - Darum sind sie als Trägermedium ungeeignet
- Einige Bildformate (z.B. GIF und PCX) arbeiten mit **indizierten Farben**
- Das bedeutet, dass sie palettenbasiert arbeiten
 - Sie speichern nur die 256 wichtigsten Farben in einer eigenen Tabelle
 - Ein bestimmter Wert innerhalb einer Bilddatei steht nicht für eine festgelegte Farbe, sondern für ein Feld in der Tabelle (der Farbpalette), in der ein Farbwert eingetragen ist
- Verschiedene Felder in der Palette können die gleiche Farbe repräsentieren
- Das bedeutet, dass sie palettenbasiert arbeiten
 - Diese doppelten Einträge lassen sich für Steganographie nutzen



Komprimierte Bilddaten als Trägerdaten

- Der JPEG-Algorithmus wandelt mit der diskreten Kosinustransformation (DCT) Bildpunkte vom Pixelbereich in einen Frequenzraum um
 - Dabei entstehen genauso viele Frequenzkoeffizienten wie Bildpunkte vorhanden sind
 - Da diese gerundet (quantisiert) werden, entstehen geringe Bildveränderungen (Verluste)
 - Dabei entstehen positive und negative ganze Zahlen
 - Am häufigsten entsteht der Wert 0, da die meisten Frequenzen mit einem nahezu verschwindenden Anteil auftreten
 - Die Koeffizienten lassen sich wegen der vielen Nullen verlustfrei und besonders platzsparend abspeichern
 - Nachrichten werden deshalb nach diesem Schritt versteckt
 - Die niederwertigsten Bits dieser Koeffizienten werden überschrieben



Audiodaten als Trägerdaten

- Geheime Informationen können im Hintergrundrauschen versteckt werden
- Auch die **LSB**-Methode kann mit Audio-Dateien angewendet werden
 - Am einfachsten geschieht das mit unkomprimierten Audio-Daten (WAV-Dateien)
 - Jede Audio-Datei hat eine Abtastung (englisch: *sampling*)
 - Von jedem Sample-Wert kann das niederwertigste Datenbit durch die Bits einer geheimen Nachricht ersetzt werden
 - Die Sample-Werte umfassen 8 oder 16 Bit
 - Also können diese Dateien ca. 1/8 oder 1/16 ihrer Größe an steganographischen Daten aufnehmen
 - Dieses Verfahren übersteht aber keine verlustbehaftete Kompression mit MP3 oder OGG Vorbis

Videodaten als Trägerdaten

- In Videodaten lassen sich ähnliche stenographische Verfahren anwenden wie bei unbewegten Bildern
- Auch die Bildübergänge bieten Möglichkeiten, um Informationen zu verstecken
- Bei Videokonferenzen kann auch ein stenographischer Kanal erzeugt werden

Andreas Westfeld. **Steganographie in komprimierten Videosignalen**. Diplomarbeit. TU Dresden. 1997

Fragmentierung eines Dateisystems als Trägerdaten (1)

- Man kann Daten durch gezielte Fragmentierung der Cluster einer Datei im FAT-Dateisystem (File Allocation Table) verstecken
 - Die FAT (Dateizuordnungstabelle) ist eine Tabelle fester Größe, in der die belegten und freien Cluster im Dateisystem erfasst sind
 - Ein Cluster besteht aus mehreren Sektoren auf dem Speichermedium und ist die kleinste Zuordnungseinheit, die von einer Datei belegt werden kann
 - Für jeden Cluster im Dateisystems existiert ein Eintrag in der FAT mit folgenden Informationen über den Cluster:
 - Cluster ist frei oder das Medium an dieser Stelle beschädigt
 - Cluster ist von einer Datei belegt und enthält die Adresse des nächsten Clusters der Datei oder ist der letzte Cluster der Datei (EOF)
 - Die belegten Cluster einer Datei bilden eine verkettete Liste (Clusterkette)
- Die Abstände der Cluster ergeben die Binärfolge der versteckten Daten
 - Zwei (numerisch) direkt aufeinanderfolgende Cluster bedeuten, dass das folgende Bit dem vorhergehenden gleich ist
 - Ist der Abstand zum nächsten Cluster größer, bedeutet dies, dass das neue Bit nicht mehr dem vorhergehenden entspricht

Fragmentierung eines Dateisystems als Trägerdaten (2)

- Die Folge von Clustern einer Datei ergibt einen bestimmten Bitstrom
- Kennt man den richtigen Zustand des Startbits, ergibt sich der Bitstrom
- In der Abbildung ist der Datenstrom 110011 versteckt
- 20 MB lassen sich auf einem Medium mit 160 GB bei 2 KB Clustergröße verstecken
- Da es keine offensichtlich verschlüsselten Daten gibt, kann der Anwender abstreiten, dass das Speichermedium geheime Daten enthält
- Problem: **Defragmentierung** führt zum Verlust der versteckten Daten
- Das Verfahren wurde 2010 entwickelt und 2011 veröffentlicht

Directory entry table (date, time
& file attributes are not shown)

| Name | Start | Size |
|----------|--------|-------|
| data.dat | 526241 | 20482 |
| asd.txt | 526243 | 1028 |
| ... | ... | ... |
| fat.fs | 526246 | 2046 |

FAT structure

| | | | |
|---|--------|--------|---|
| 1 | : | : | |
| | 526241 | 526242 | |
| | 526242 | 526244 | 1 |
| | 526243 | EOF | 0 |
| | 526244 | 526245 | |
| | 526245 | 526247 | 0 |
| | 526246 | EOF | 1 |
| | 526247 | 526248 | |
| | 526248 | EOF | 1 |
| | 526244 | 0 | |
| | : | : | |

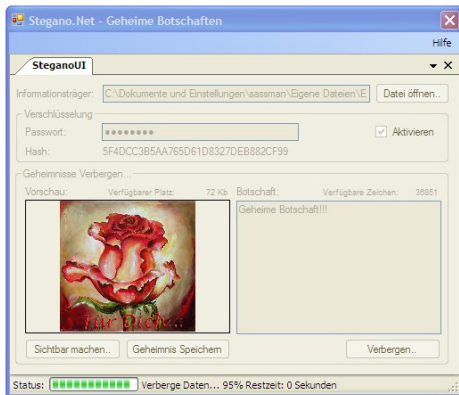
Auswahl an Software-Lösungen für Steganographie (1)

- Es existieren verschiedene Software-Lösungen, um Texte in Bildern, Videos oder Audio-Dateien zu verstecken
- Wichtig ist, dass der Quellcode der Software verfügbar ist
- **S-Tools 4.0**
 - Unterstützt Audio (WAV) und Bilder (BMP, GIF)
 - Die geheimen Informationen werden via AES, DES 3DES oder MDC verschlüsselt
 - Arbeitet nach der LSB-Methode (Datenversteck = niederwertigstes Bit)
 - Freeware von Andy Brown – Quellcode wird vom Autor verkauft
 - <http://www.securitytube.net/video/908>
- **Hide and Seek**
 - Arbeitet nach der LSB-Methode (Datenversteck = niederwertigstes Bit)
 - Die geheimen Informationen werden via AES verschlüsselt
 - Unterstützt Bilder (GIF)
 - Sehr alte Software
 - <http://www.jjtcc.com/Security/stegtools.htm>

Auswahl an Software-Lösungen für Steganographie (2)

• Stegano.Net

- Unterstützt Bilder (JPG, PNG)
- Freeware von Sven Assmann – Quellcode nicht verfügbar
- <http://svenomenal.net/devel/steganoV2>



Auswahl an Software-Lösungen für Steganographie (3)

• **Steganography Demo**

- Von Andrew S. Tanenbaum
- <http://www.cs.vu.nl/~ast/books/mos2/zebras.html>

• **Steghide**

- Unterstützt Audio (WAV, AU) und Bilder (JPG, BMP)
- Erweitertes LSB-Verfahren
- Die geheimen Informationen werden via AES verschlüsselt
- Eine Sequenz von Bildpunkt-Positionen bzw. Audio-Samples wird mit Hilfe einer Pseudo-Zufallszahl ausgewählt
 - Der Pseudo-Zufallszahlengenerator wird mit einer Benutzereingabe (Passphrase) initialisiert
- Kommandozeilenanwendung
- GNU General Public License (GPL)
- <http://steghide.sourceforge.net>
- <http://wiki.ubuntuusers.de/Steghide>

-
- no data available
 ● domestic controls
 ● new demanding decryption
 ● small and special controls
 ● decryption order and special controls
 ● unclear
 ● no domestic controls
- DOMESTIC CRYPTO REGULATIONS**
 (c) Bert-Jaap Koops
 July 2010

Angriffe auf Steganographie – Steganalyse

- **Steganalyse** ist die Analyse von Verfahren der Steganographie
- Steganalyse geht in 2 Schritten vor:
 - ① Herausfinden, ob in einem Medium eine steganographische Information enthalten sein kann
 - ② Analysieren, Erkennen und Extrahieren der steganographischen Information
- Man unterscheidet u.a. **visuelle** und **statistische Angriffe**
- Besonders bei Bildern kann man beim LSB-Verfahren bisweilen ein Rauschen mit bloßem Auge erkennen \implies visueller Angriff
- Der statistische Angriff beurteilt die Farbverteilung in einer Bilddatei
- Eine weitere Möglichkeit der Analyse ist, indem man das Originalmedium ausfindig macht

Die Steinlaus – eine Plagiatsfalle

Bildquelle: sueddeutsche.de/Pschyrembel

- Die Steinlaus (*Petrophaga lorioti*) ist eine von Lorient erfundene und 1976 vorgestellte Tierart
- Seit 1983 enthält das klinische Wörterbuch Pschyrembel die Steinlaus als fingierten Lexikonartikel (Nihilartikel)
- Die Steinlaus ist nicht nur ein Klassiker des wissenschaftlichen Humors, sondern auch ein Beispiel für Steganographie
- Der ursprüngliche Zweck des Lexikonartikels war es nämlich, Abschreiber zu überführen
- Eine solche Vorgehensweise wird **Plagiatsfallen** genannt
 - Plagiatsfallen sind absichtlich eingebaute harmlose Fehler an unverfänglicher Stelle in Datenbeständen



Steinlaus:
Gemeine S. (*Petrophaga lorioti*).

Weitere Beispiele für Plagiatsfallen

- Die Österreichische Telekom fügt für jeden Vorwahlbereich eine nicht existierende Telefonnummer im Telefonbuch ein
 - Taucht eine dieser Telefonnummern in Telefon-CDs auf, kann wegen Urheberrechtsverletzung gegen den Herausgeber vorgegangen werden
- In kartografischen Werken werden als Plagiatsfalle fiktive Straßen eingebunden
- In der Musik-Enzyklopädie „Die Musik in Geschichte und Gegenwart“ von 1999 ist ein Eintrag zum erfundenen Komponisten Otto Jägermeier
- In der 1990 erschienenen 9.Auflage des Chemie-Lexikons Römpp findet man als Erklärung für die KKK-Regel (eigentlich Kälte, Katalysator, Kern): *Regel, nach der sich mit Chemie beschäftigte weibliche Personen eher um Küche, Kinder u. Kirche kümmern sollten...*
- Im psychologischen Wörterbuch von Häcker, Stapf und Dorsch aus dem Jahr 2004 (14.Auflage) ist der Elchtest aufgeführt

Wasserzeichen

- Um rechnergestützt Plagiate eigener Werke beweisen zu können, sind digitale **Wasserzeichen** hilfreich
- Wie bei der Steganographie sollen auch Wasserzeichen mit bloßem Auge nicht sichtbar sein
- Die wichtigste Eigenschaft digitaler Wasserzeichen ist, dass sie nur **schwer entfernbar** sein sollen
 - Man spricht hier von der **Robustheit** des Wasserzeichens
- Man unterscheidet **robuste** und **fragile** Wasserzeichen
 - Robuste Wasserzeichen verwendet man zum **Schutz der Urheberrechte** digitaler Werke
 - Fragile Wasserzeichen verwendet man zur **Integritätssicherung** digitaler Werke
- Fragile Wasserzeichen sollen bei Manipulationen *zerbrechen*
 - Sie dienen als Nachweis der Unversehrtheit
 - Manipulationen am Datenmaterial können festgestellt werden, ohne dass ein Vergleich mit dem Original erforderlich ist

Sichtbare und unsichtbare Wasserzeichen

- Man unterscheidet auch **sichtbare** und **unsichtbare** Wasserzeichen
- Bei digitalen Bildern soll das sichtbare Wasserzeichen die kommerzielle Weiternutzung unmöglich machen.
- Beispiele für derartige Wasserzeichen sind in jeder Fernsehsendung, in der zumeist ein Symbol des Fernsehsenders in einer Bildecke zu sehen ist
- Beispiele für sichtbare Wasserzeichen:
Google Earth und Corbis Datenbank
- Das Bild zeigt eine Luftaufnahme der San Francisco Bay Area und ist aus der Corbis Datenbank



Quelle: <http://homepages.thm.de/~hg10013/>

Beispiele für digitale Wasserzeichen

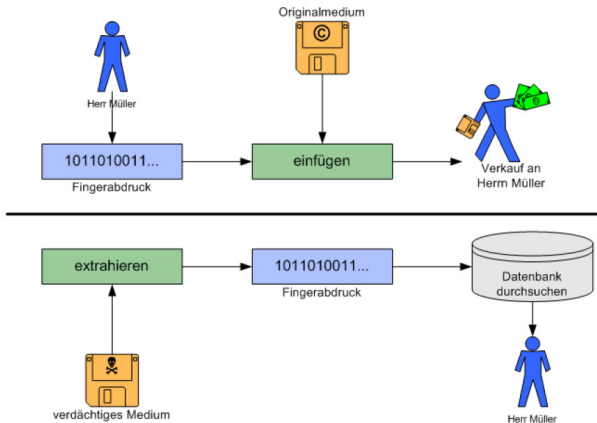
- Apple fügt seit 2007 auf iTunes den Namen und die E-Mail-Adresse des Kunden in die Musikdateien ein
- In den Videos, die die etwa 5.800 Oscar-Juroren vorab erhalten, sind seit 2005 Wasserzeichen enthalten
 - Grund: Einige Juroren-DVDs von 2004 waren in Tauschbörsen erschienen
 - In einem Fall konnte so das Leck ermittelt werden
 - Der Juror wurde zu \$600.000 Strafe verurteilt
 - Die undichte Stelle wurde (leider) nicht bekannt gegeben

Digitaler Fingerabdruck (1)

- Verfahren zur **Kundenidentifizierung**
- Kundenspezifische Markierungen (Fingerabdrücke) werden in das Datenmaterial eingebracht
 - Unterschiedliche Kunden erhalten also unterschiedliche Kopien des Datenmaterials mit einem einzigartigen digitalen Fingerabdruck
- Die Markierungen dienen zum Nachweis legaler Kundenkopien
- Zudem lassen sich illegale Kopien bis zum Verursacher der Urheberrechtsverletzung zurückverfolgen
 - Aus gefundenem Datenmaterial, welches das Urheberrecht verletzt, wird der digitale Fingerabdruck extrahiert und nach der Kundeninformation in den Einträgen der Datenbank des Herausgebers gesucht
 - Das Vorgehen wird **Traitor Tracing** genannt
- Problem (für den Herausgeber): Vergleicht man mehrere markierte Dokumente, lassen sich die Fingerabdrücke aufspüren und beseitigen

Digitaler Fingerabdruck (2)

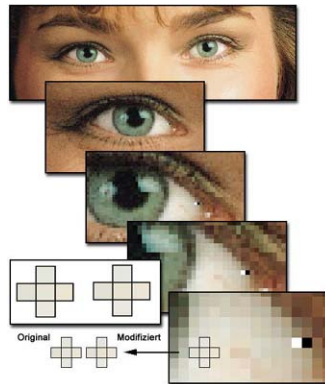
- Die Abbildung veranschaulicht das Traitor Tracing



Quelle: André Calliess, Kristine Jetzke, Sylvia Richter, Jan Schwenzien. **Digitale Wasserzeichen**. Universität Potsdam. 2006

Einbettungsverfahren für digitale Fingerabdrücke (1)

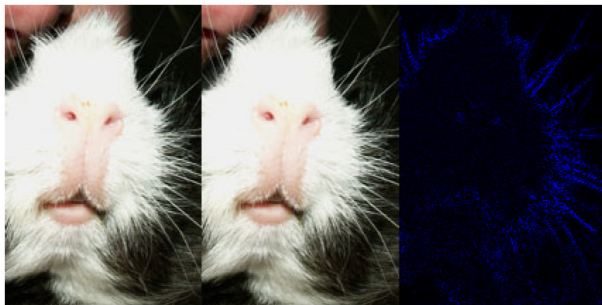
- Man kann auch mit dem Bildraumverfahren (Patchworkverfahren) bei zufällig ausgewählten Paaren kleiner Bildteile (Patches) einen Bildteil abdunkeln und einen anderen aufhellen
- Im Bild wurden die Blauanteile des RGB-Bildes im Fadenkreuz verändert (außen um den Wert 3 erhöht, im Mittelpunkt um 3 gesenkt)
- Selbst die schwarz-weiße Kennzeichnung wäre in der Originalgröße kaum zu erkennen



Quelle: <http://homepages.thm.de/~hg10013/Lehre/MMS/SS02/Hlawatsch/text.htm>

Einbettungsverfahren für digitale Fingerabdrücke (2)

- Bestimmte Farbtöne, wie z.B. der Blaubereich, werden von Menschen schlechter wahrgenommen als andere Farben



- Zudem werden vorwiegend Kanten mit großen Helligkeitsunterschieden verwendet, um dort Farbwerte zu verändern

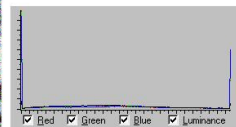
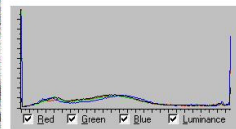
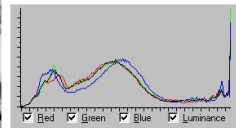
Quelle: André Calliess, Kristine Jetzke, Sylvia Richter, Jan Schwenzien. **Digitale Wasserzeichen**. Universität Potsdam. 2006

Einbettungsverfahren für digitale Fingerabdrücke (3)

- Der JPEG-Algorithmus wandelt mit der diskreten Kosinustransformation (DCT) Bildpunkte vom Pixelbereich in einen Frequenzraum um
 - Statt durch Einzelpixel wird sich jedes Bild als Signal im Frequenzbereich mit Hilfe der Frequenzkomponenten beschreiben
 - Hohe (oder schnelle) Frequenzen stehen für Bildteile, die hohe Änderungen in Kontrast oder Helligkeit beinhalten
 - Tiefere (oder langsamere) Frequenzanteile repräsentieren eher gleichmäßige Bildflächen
- Das letzte Bit der Farbdefinition wird für das Wasserzeichen verwendet
- Man verwendet einen Code, der die eher schmalbandige Information des Wasserzeichens in ein sehr breitbandiges Signal umsetzt
 - Das breitbandige Signal ähnelt einem Rauschen und lässt sich unauffällig zum Bild addieren
- Rauschen an sich stellt in der Regel redundante Information dar und trägt normalerweise nicht viel zum Bildeindruck bei

Einbettungsverfahren für digitale Fingerabdrücke (4)

- Die Abbildung zeigt ein Bild mit überlagertem Rauschen
- Deutlich erkennbar ist die Verbreiterung des Spektrums
- Ein Problem sind sichtbare Artefakte, wenn die Einstellungen zu Gunsten einer höheren Robustheit gewählt werden
- Je robuster ein Wasserzeichen sein soll, desto mehr zusätzliche Informationen müssen in das Bild eingebracht werden



Quelle: <http://homepages.thm.de/~hg10013/Lehre/MMS/SS02/Hlawatsch/text.htm>

Fazit zur Steganographie

- Steganographie ist ein wirksames Werkzeug für zensurresistenten Informations- und Datenaustausch
- Die Entwicklung der Werkzeuge zur Steganographie hat sich in den letzten 10 Jahren stark verlangsamt
 - Die Entwicklung vieler ehemals populärer Werkzeuge wie z.B. S-Tools ist eingeschlafen
 - Kommerzielle Produkte wie z.B. von Steganos existieren nur wenige
 - Einige Werkzeuge wie z.B. Steghide werden nach wie vor aktiv weiterentwickelt
- Digitale Wasserzeichen/Fingerabdrücke sind ein wirksames Werkzeug zum Schutz der Urheberrechte
 - Allerdings empfinden die Benutzer/Kunden diese häufig als störend und einengend
- Es existieren viele verschiedene Steganographie-Verfahren
 - Die Auswahl des am besten geeigneten Verfahrens hängt immer vom Anwendungszweck und der Art der Trägerdaten (*Cover*) ab