Steganographie

Ein Vortrag von

Ibrahim Günaydin & Stefan Kaulingfrecks

Steganographie (1)

- Information unsichtbar verbergen.
- Die Steganographie benutzt harmlose Daten als Überträger.

Steganographie(2)

- Geheimbotschaft mit Sklaven als Trägermedium übertragen.
- unsichtbare Tinte
- Kleinpunkttechnologie "microdots"

Steganographie (3)

Zwei Arten von Steganographie

– Semagramm

- Die Nachrichten werden in andere Daten eingebettet.
- Sichtlich getarnte Geheimschriften.

2. Steganogramm

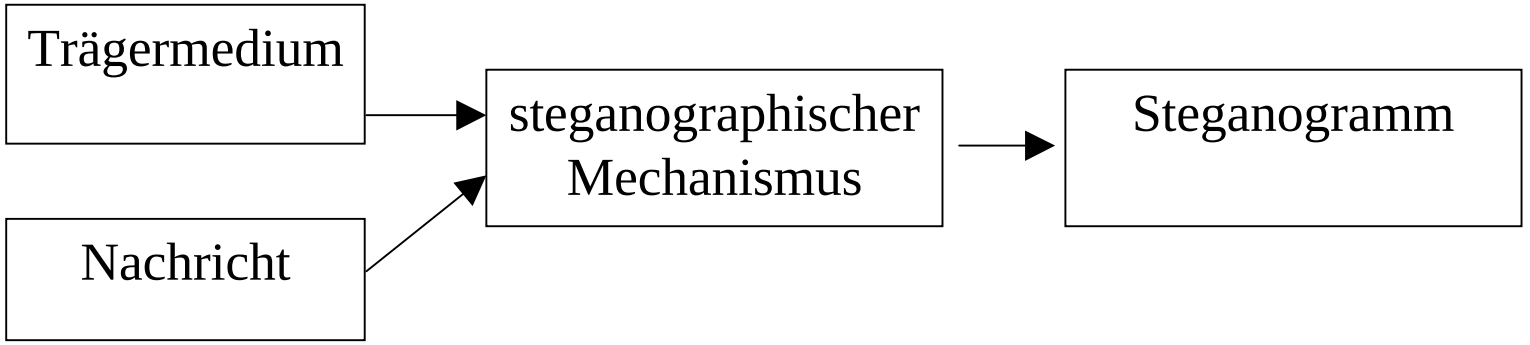
- Die Nachrichten sind unsichtbar, d.h. es sind keinerlei Informationen zu sehen.

Semagramm

- Die langen und kurzen Grashalme neben der Brücke stellen die Nachricht dar.
- Nur wer weiß, was und wo er suchen muss, wird schnell fündig.

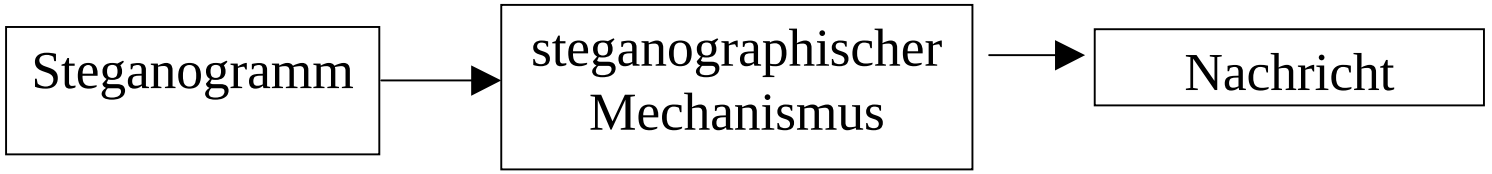
Steganogramm(1)

- Einbetten einer Nachricht in ein Trägermedium.



Steganogramm(2)

- Extrahierung einer Nachricht aus einem Steganogramm



Rechnergestützte Steganographie

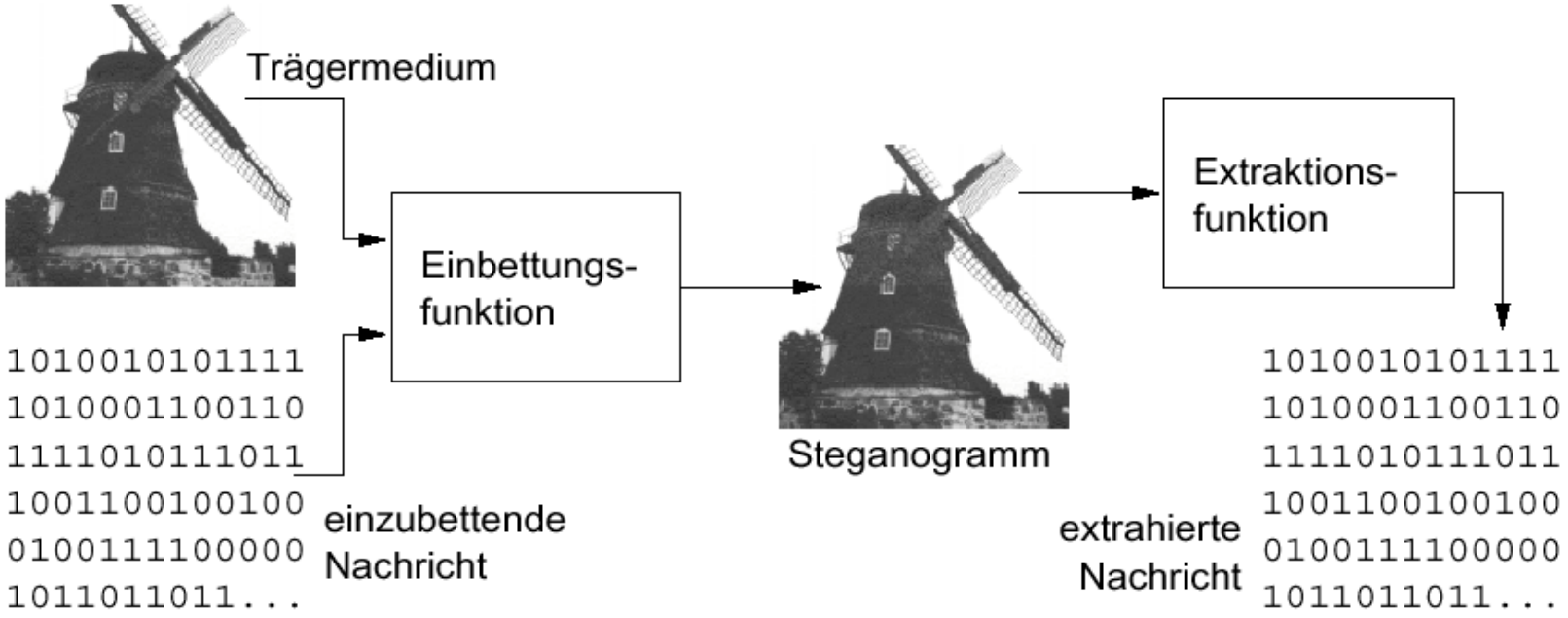
- Die Nachrichten werden innerhalb anderer, harmlos wirkender Daten versteckt.

  In digitale Bilder- oder Tondateien verpackt oder auch über das Hintergrundrauschen beim Telefonieren übertragen.
- Es werden als Trägermedium meist digitalisierte Bilder und andere Multimediadaten verwendet.

Dateien die sich für Steganographie eignen

- **Textdateien (**schlecht für die Steganographie)
- **Bilder** (eignen sich sehr gut)
- **Audio** (eignet sich auch sehr gut)

Funktionsweise rechnergestützter Steganographie(1)



Funktionsweise rechnergestützter Steganographie(2)

- Absender und Empfänger sollten den gleichen steganographischen Mechanismus verwenden.

- „Beim Extrahieren einer Nachricht aus dem Steganogramm ist es meist nicht möglich, das ursprüngliche Trägermedium zu rekonstruieren, da Teile der Daten beim Einbetten verloren gehen“

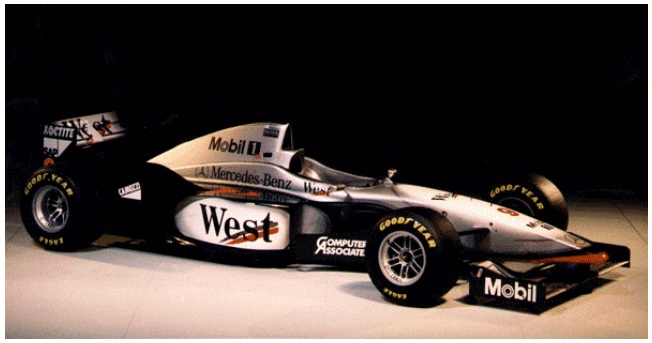
LSB-Methode

- Das LSB (Least Significant Bit) ist das Bit, das den Wert einer Zahl am wenigsten bestimmt. Hierfür wird das jeweils letzte Bit eines Byte der Trägerdaten überschrieben, da dieses den geringfügigsten Einfluss auf den Gesamtwert des Byte hat.

- Beispiel:
  Dezimal: 159 Dual: 1 0 0 1 1 1 1 [1]
  LSB

- Geringster Einfluß auf die Zahl
  Würden wir das LSB in unserem obigen Beispiel verändern (1 in 0) so würden wir den Wert 158 anstatt 159 erhalten.

Beispiel für rechnergestützte Steganographie (1)



Originalbild

Verstecktes Bild

Steganorgramm

Beispiel für rechnergestützte Steganographie (2)

- Abhängig von der Farbtiefe des dargestellten Bildes
- Zur Verfügung stehender Platz:

  1/8 der Trägergröße.

Beispiel für rechnergestützte Steganographie (3)

- Mit Änderung des zweitletzten Bits eines Trägerbytes: 1/4 des Trägermediums
- Steht im niederwertigsten Bit des Byte bereits das einzubettende Bit, so bleibt das Byte unverändert.
- Änderungsrate der letzten Bits von 50%.

Weitere Methoden

- **Schlüsselgesteuerte LSB-Methode**

  Die Reihenfolge der zu manipulierenden Trägerbytes wird unter Berücksichtigung eines Schlüssels festgelegt.

- **Paritätskodierung**

  Eine Anzahl von n Trägerbytes wird zu einem Block (K*odewort)* zusammengefasst und die Parität dieses Blocks, also die Quersumme, bestimmt.

- **Matrixkodierung**

  Im Gegensatz zur Paritätskodierung können bei der Matrixkodierung in jedem Block(Kodewort) gleich zwei Nachrichtenbits eingebettet werden, dadurch erhöht sich die Einbettungseffizienz.

- Durch eine Kombination verschiedener Methoden kann das Maß an Sicherheit weiter erhöht werden.

Vor- und Nachteile

- Vorteil der Steganographie ist, dass Mitleser gar nicht wissen, dass es sich um eine geheime Nachricht handelt.

- Nachteil der Steganographie ist, dass Mitleser die Nachricht auch leicht herausfinden können, wenn sie wissen wo sie suchen müssen.

Effizienz

- Komprimieren
- Verschlüsseln
- Steganographie

Angriffe auf Steganogramme

- Wer greift an?
  - Interesse am Wissen über eine Kommunikation
  - Verdacht einer Kommunikation
  - Zugriff auf die Masse von Dokumenten, die Steganogramme sein könnten.

Angriffe auf Steganogramme

- Ziele der steganographischen Angriffe:
  - Erhärtung des Verdachtes auf die Existenz einer eingebetteten Nachricht
  - Genau genommen nicht der Inhalt der Nachricht
- Ziel kryptoanalytischer Angriffe:
  - Kenntnisnahme der verschlüsselten Nachricht

Angriff über den „subjektiven Eindruck“

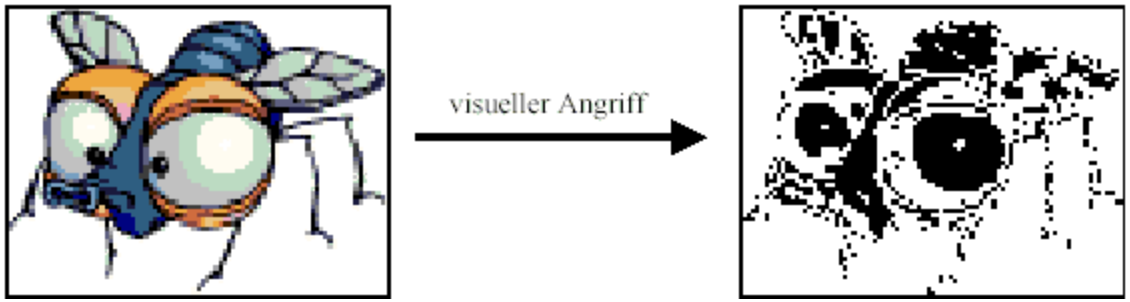
- Subtile, ungenaue Vorgehensweise
- hauptsächlich interessant für nicht rechnergestützte Steganographie
- z.B. in
  - handschriftlichen Texten
  - Zeichnungen und Bildern

Angriff über visuelle Verfahren

- Computerunterstützte Visualisierung bestimmter Bilddaten
- Gezielte Betrachtung der Daten, die für ein Steganogramm geeignet wären
  - Vor Allem der Least Significant Bits
- Die eigentliche Einschätzung über die Existenz eines Steganogrammes wird über den subjektiven, visuellen Eindruck ermöglicht.

Angriff über visuelle Verfahren

- Beispiel:
  - 8-Bit Bitmap
  - Analyse des letzten Bit pro Byte



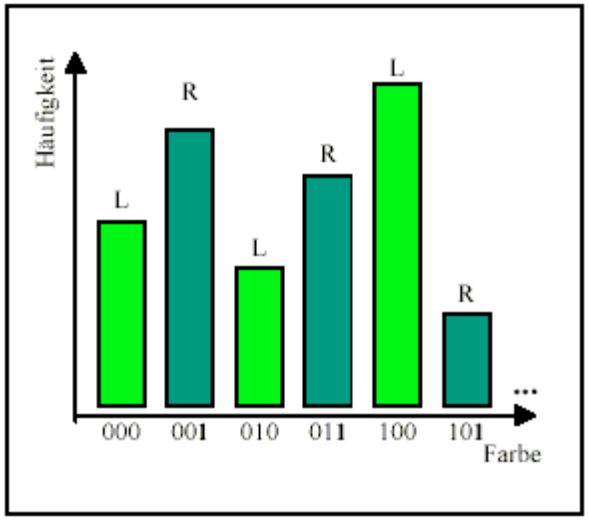
- Beobachtung:
  - Auch im letzten Bit sind viele Bildkonturen erkennbar

Angriff über visuelle Verfahren

- In einem Steganogramm sind die Konturen durch die veränderten Bits überschrieben.
- Außerdem hier sichtbar:
  - Ausnutzung von 2/3 der Trägerkapazität
  - Die Nachricht scheint aus regelmäßig wiederkehrenden Bitfolgen zu bestehen.

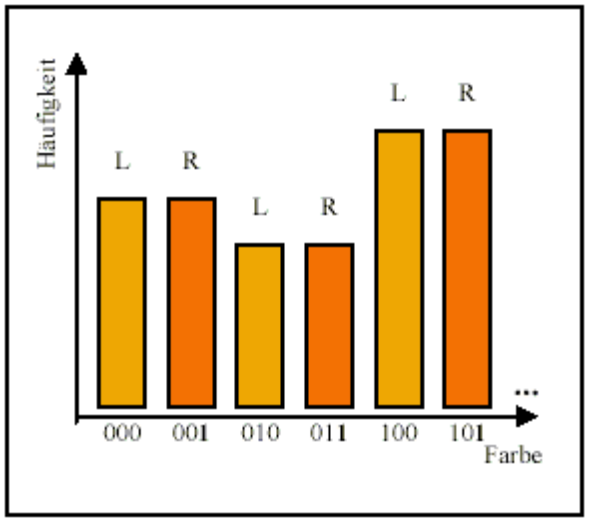
Statistischer Angriff

- Auswertung der Farbverteilung eines Bildes
  - Im Allgemeinen sind die Farben nicht gleichverteilt, bestimmte Farben kommen häufiger vor.
  - Daraus resultiert, dass die letzten Bits jedes Bytes auch nicht gleich häufig vorkommen



Statistischer Angriff

- In Nachrichten wird (insbesondere bei Kompression/Verschlüsselung) von einer Gleichverteilung von Einsen und Nullen ausgegangen.
- Bei der Einbettung wird die Verteilung ausgeglichen



Bewertung der Angriffsmöglichkeiten

- Ohne Intuition geht fast nichts
  - weil ein Verdacht auf ein Steganogramm vorliegen muss.
  - weil spezielle menschliche Fähigkeiten wie Konturerkennung nötig sind.
  - weil jedes Verfahren nur eine mehr oder minder genaue Wahrscheinlichkeit für die Existenz eines Steganogrammes ergibt.

Maßnahmen gegen Angriffe

- Wahl geeigneter Medien
  - hohe tatsächliche Farbtiefe
  - Fotos sind besser als Zeichnungen
  - evtl. spezielle Medien generieren
- Einbettung in die Bildkonturen
- Streuung (evtl. schlüsselgesteuert)
- Statistischer Ausgleich von eingebetteten Bits
- Kleine Nachricht in großem Trägermedium

Steganographie im BMP-Format

- Wegen fehlender Kompression gut geeignet
- Nebeneinanderliegende Farbwerte stehen immer für ähnliche Farben
- Die letzten 1-3 Bits pro Byte lassen sich ohne übermäßig auffällige Folgen manipulieren
- Trägerkapazität: etwa 1/8 bis 3/8 der Mediengröße je nach Farbtiefe
- Nachteil: Im Internet unübliches und damit auffälliges Format!

Steganographie im ASCII-Format

- Die Änderung von Bits führt zu auffälligen Veränderungen:

```
Überschreiben der niederwertigsten Bits
Ücdqrchsdiben!der!nidedsveruhgrudo Chst
```

- Nur unsichtbare Zeichen an bestimmten Stellen könnten unauffällig genutzt werden
  - z.B. Tabulatoren und Blank's am Zeilenende
- Linguistische Methoden
  - Anzahl der Buchstaben bis zum nächsten Blank
  - ausschließliche Auswertung der Großbuchstaben

Steganographie im WAV-Format

- Anstatt von Bildpunkten werden hier Samplewerte manipuliert
- Methoden:
  - LSB
  - Ersetzung von Abschnitten durch akustisch gleichwertige
  - Gezielte Einfügung von Echo-Daten
  - Ausnutzung spezieller Eigenschaften des menschlichen Gehörs, z.B. die kurze Taubheit nach lauten Passagen

Steganographie im GIF-Format

- GIF-Bilder sind Indexfarbenbilder => nebeneinander liegende Farbwerte stehen nicht notwendigerweise für ähnliche Farben

- Deshalb:
  - Vorherige Sortierung der Farbpalette
  - Alternativ Reduktion auf 128 Farben, von denen jede zweifach in der Palette vorkommt. (mit unterschiedlichem letzten Bit)

Steganographie im EXE-Format

- Im erweiterten Sinne verwenden Viren Steganographie
- Anstatt von Daten wird ausführbarer Code eingebettet.
- Häufig wird dieser Code am Ende des ursprünglichen Codes angefügt.
- Die normale Funktion der Programmdatei wird nicht notwendigerweise dabei verändert.

Abschließende Zusammenfassung

- Steganographie gibt es seit Jahrtausenden
- Insbesondere das Internet macht sie wieder aktuell.
- Analog zur Kryptographie haben sich mit verbesserten steganographischen Methoden auch die Angriffsmethoden verbessert.
- Die Eignung bestimmter Dateiformate für das Einbetten von Nachrichten variiert sehr stark.

Vielen Dank für die Aufmerksamkeit!

Noch Fragen?