Kryptographie und Informationstheorie

WS 2002/03

Steganographie

Prof. Dr. Richard Eier
Institut für Computertechnik
TU Wien

Michaela Schuster

- Übermittlung geheimer Nachrichten
- Entwicklung der Steganographie
  - Linguistische und Technische Steganographie
- Steganographie heute
  - Digitale Steganographie
  - Anwendung
  - Unterschiede Stego-Nachricht / digitale Wasserzeichen
- Stegosystem
  - Modell eines Stegoystems
  - Anforderung
  - Wahl des Covers
  - Beispiel Bildformat
- Einbettung einer Nachricht
  - Manipulation im Bildraum
  - Manipulation im Frequenzraum
- Attacken visuell - statistisch
- Weitere Anwendungsbereiche
  - Beispiel für Audiocover

Geheime Nachricht

Steganographie

stegano = verdeckt
graphein = schreiben

Die Nachricht wird verborgen, nicht verschlüsselt

Scheinbar existiert gar keine Nachricht

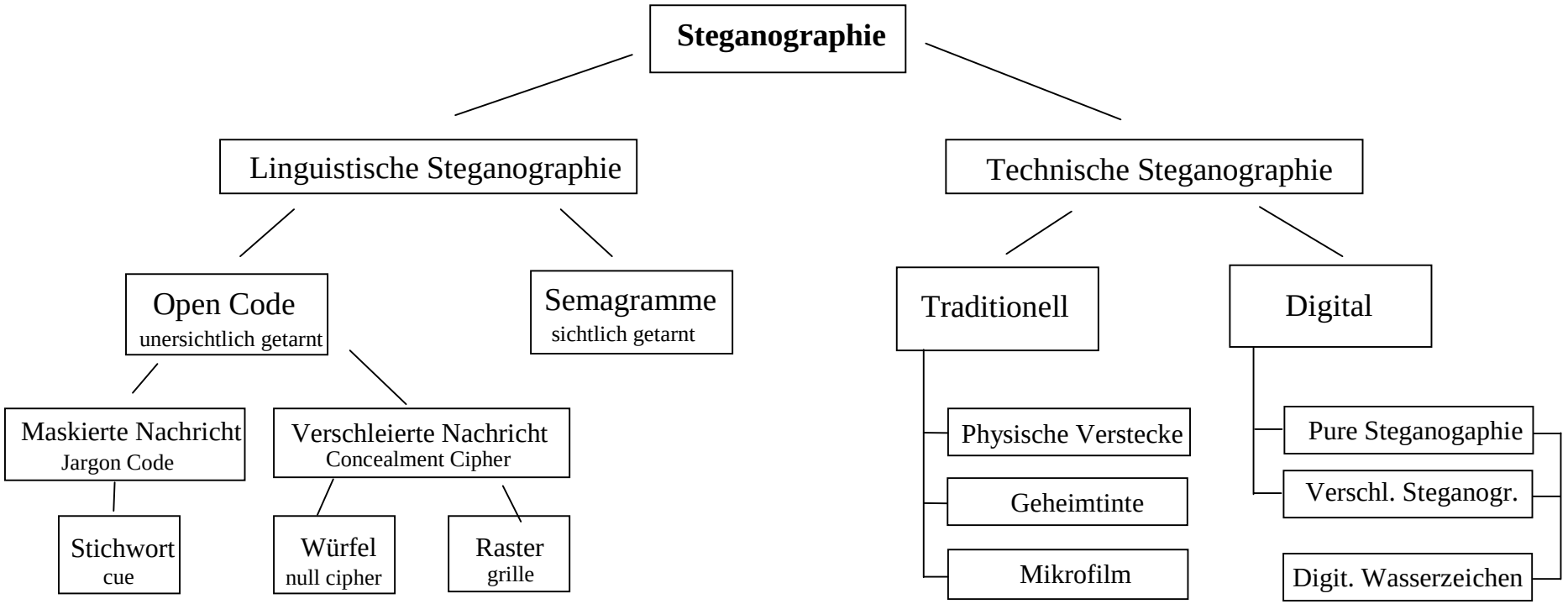
Kryptographie

krypte = geheim
graphein = schreiben

Die Nachricht wird verschlüsselt, nicht verborgen

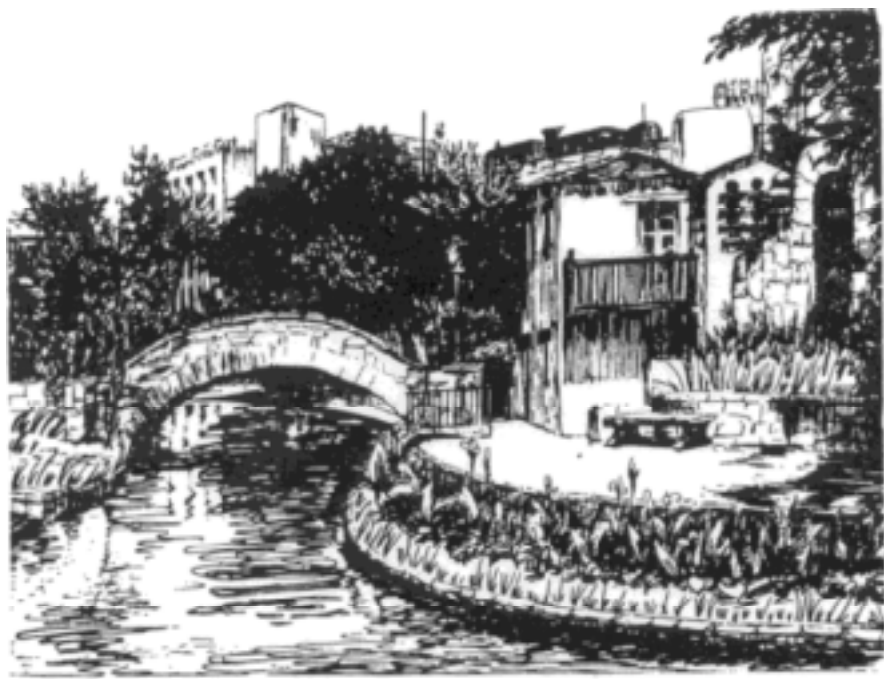
Die Nachricht existiert, kann aber nicht gelesen werden

Verschlüsseln & Verbergen
=> Doppelte Sicherheit


Steganographie
Linguistische Steganographie
Technische Steganographie
Open Code
unersichtlich getarnt
Semagramme
sichtlich getarnt
Traditionell
Digital
Maskierte Nachricht
Jargon Code
Verschleierte Nachricht
Concealment Cipher
Physische Verstecke
Geheimtinte
Mikrofilm
Pure Steganogaphie
Verschl. Steganogr.
Digit. Wasserzeichen
Stichwort
cue
Würfel
null cipher
Raster
grille

Semagramme - Die Nachricht ist zwar offen, aber getarnt, und so nur für den Eingeweihten erkennbar.

Zeichnung eines herbstliches Blattes - eigentlich eine Landkarte - die dunklen Flecken sind Artilleriestellungen



Im Vordergrund Grashalme verschiedener Länge (kurz, lang) = Morsezeichen

Open Code - unersichtlich getarnte Nachricht

Maskierte Nachricht -
mit nicht allgemein bekannten Codewörtern

Jargon code Zigarren=Kriegschiffe, Schnee=Heroin, Nachrichten in Notenschrift

Stichwort Ostwind, Regen = Kriegsbeginn Japan/USA

Verschleierte Nachricht

Prinzip: das beste Versteck ist die Menge

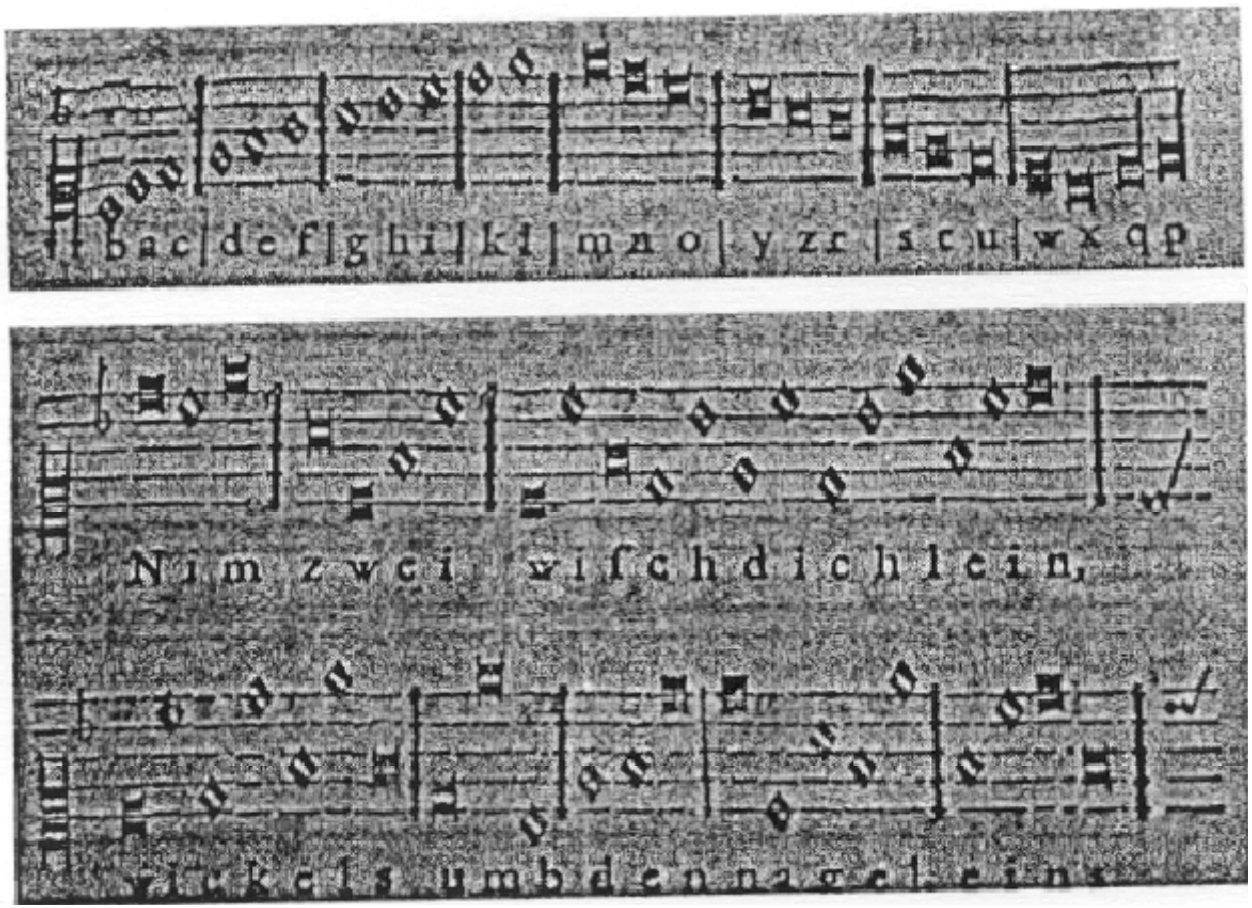
Würfel Bestimmte Buchstabe eines unverfänglichen Textes ergeben die Nachricht,

z.B. jeder 3.Buchstabe nach einem Satzzeichen.

Fluchtweg für Sir John Trevanion

Raster Sender und Empfänger haben die gleichen Schablonen.
Die unverdächtige Nachricht muss so abgefasst sein, dass die Schablonen den wahren Text zeigen.

Beispiel für **Jargon Code** in Pseudonotenschrift



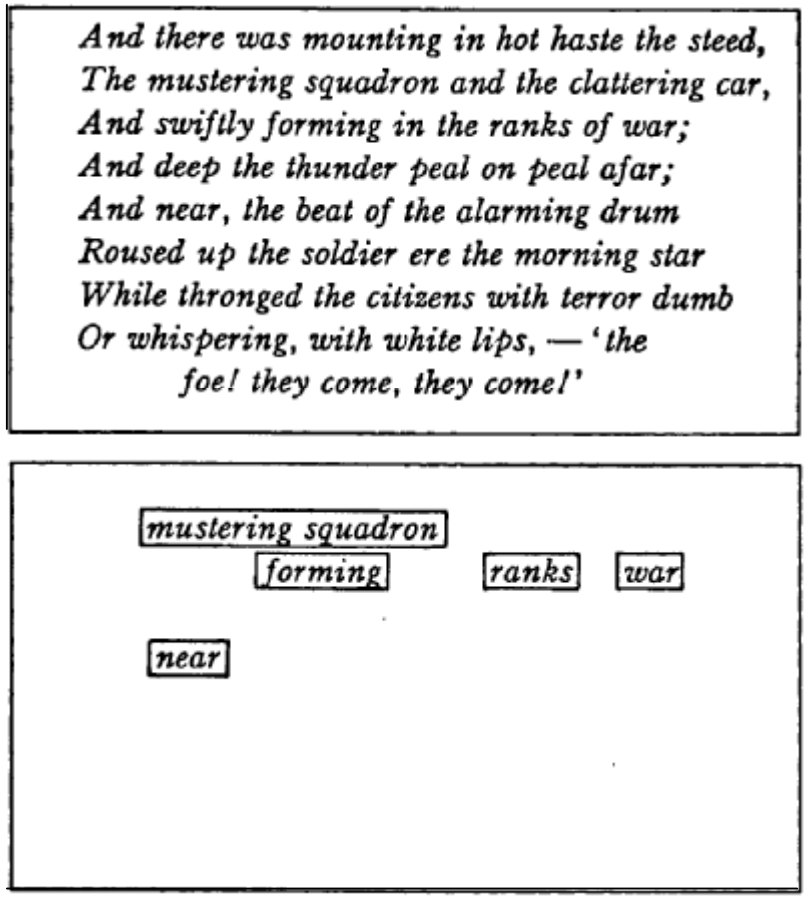
Beispiel für eine verschleierte Nachricht - **Würfeltechnik**
Jeder 3 Buchstabe nach einem Satzzeichen ergibt die Nachricht

Worthie Sir John:

Ho**p**e, th**a**t is ye beste comfort of ye afflicted, ca**n**not much, I f**e**ar me, he**l**p you now. Th**a**t I would say to you, is **t**his only: if **e**ver I may be able to requite that I do owe you, st**a**nd not upon asking me. `Ti**s** not much that I can do: bu**t** what I can do, be**e** ye verie sure I will. I k**n**owe that, if **d**ethe comes, if **o**rdinary men fear it, it **f**rights not you, ac**c**ounting it for a high honour, to **h**ave such a rewarde of your loyalty. Pr**a**y yet that you may be spared this soe bitter, cu**p**.
I f**e**ar not that you will grudge any sufferings; on**l**y if bie submissions you Can turn them away, ´ti**s** the part of a wise man. Te**l**l me, an **i**f you can, To **d**o for you anythinge that you wolde have done. Th**e** general goes back On Wednesday. Re**s**tinge your servant to command.
R.T.

Botschaft: „ **panel at east end of chapel slides“**
(Brett an Kapellen-Ostseite lose)

Beispiel für **Rastertechnik**: Sender und Empfänger haben die gleiche Schablone



Traditionell

Physische Verstecke
Geheimfächer
Doppelter Boden
etc.

Geheimtinte
War schon in der Antike bekannt (Plinius d.Ä), in der Renaissance weiterentwickelt und bis in die Zeit des kalten Krieges zusammen mit UV- Technik verwendet.

Mikrofilm
Wurde erstmals im preußisch-französischen Krieg mit Brieftauben eingesetzt, danach laufend verbessert.

Im 2. Weltkrieg Entwicklung der Microdots = Mikrofilme in Punktgröße.

Digitale Steganographie

Nicht erkennbare Einbettung von Nachrichten in digitale Inhalte
stehende / bewegte Bilder, Audio Daten, Multimedia

Reine Steganographie
Nur Stego-Schlüssel für
Einbetten und Auslesen

Verschlüsselte Steganographie-
Vor Einbetten und nach Auslesen
Krypto-Schlüssel anwenden
2 Schlüssel: Krypto + Stego-Schlüssel

Anwendung digitaler Steganographie

Umgehung der Krypto-Beschränkung

Beschränkungen des verschlüsselten Informationsaustausches privater Personen (USA, Frankreich, China)

Furcht vor:
- Terrororganisationen
  (11. Setember 2001)
- organisiertem Verbrechen
  (Rauschgift / Schlepperbanden)

Sicherung der Urheberrechte durch digitale Wasserzeichen

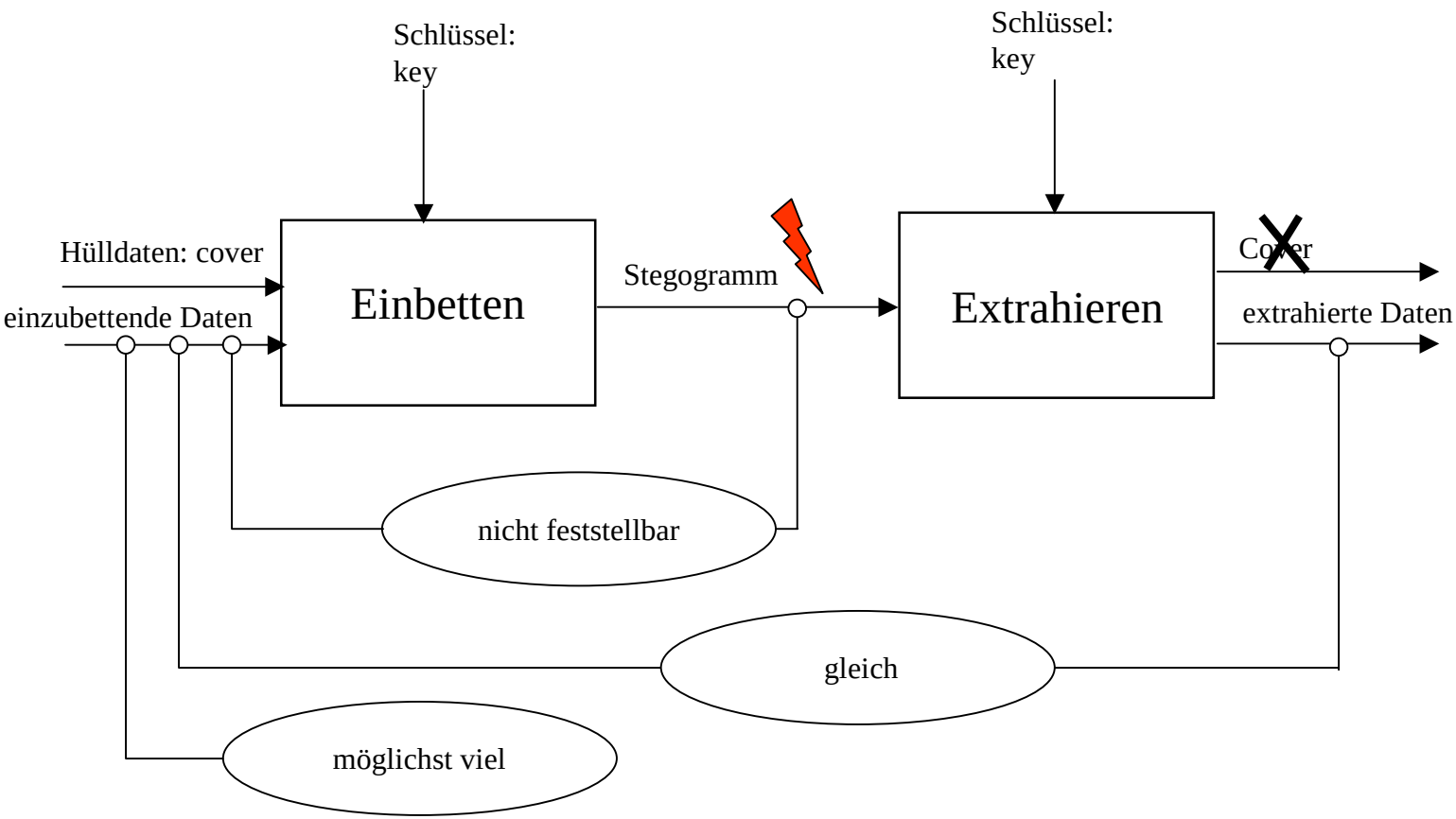
Wasserzeichen dienen der Beweis-Sicherung in einem Urheberrechts-Verfahren.

Derzeit ca.40 Steganographie-Tools verfügbar.

Unterschiede Stego-Nachricht / digitale Wasserzeichen

	Stego-Nachricht	digitale Wasserzeichen
Zweck	Nachrichten verdeckt übertragen	Urheberrechtschutz
Cover	Einwegverpackung	zu schützendes Gut
Umfang	groß (die Nachricht selbst)	klein (nur Copyright)
Nichtaufdeckbarkeit	existentiell wichtig	nur zum Schutz
Auslesen	nur der Empfänger	als Beweismittel (öffentlich)
Angriffsziel	Aufdecken der Kommunikation	Löschen / Ändern des WZ

Modell eines Stegosystems



Anforderungen an ein Stegosystem

Robustheit gegen unwillkürliche nachrichtentechnische Verarbeitung

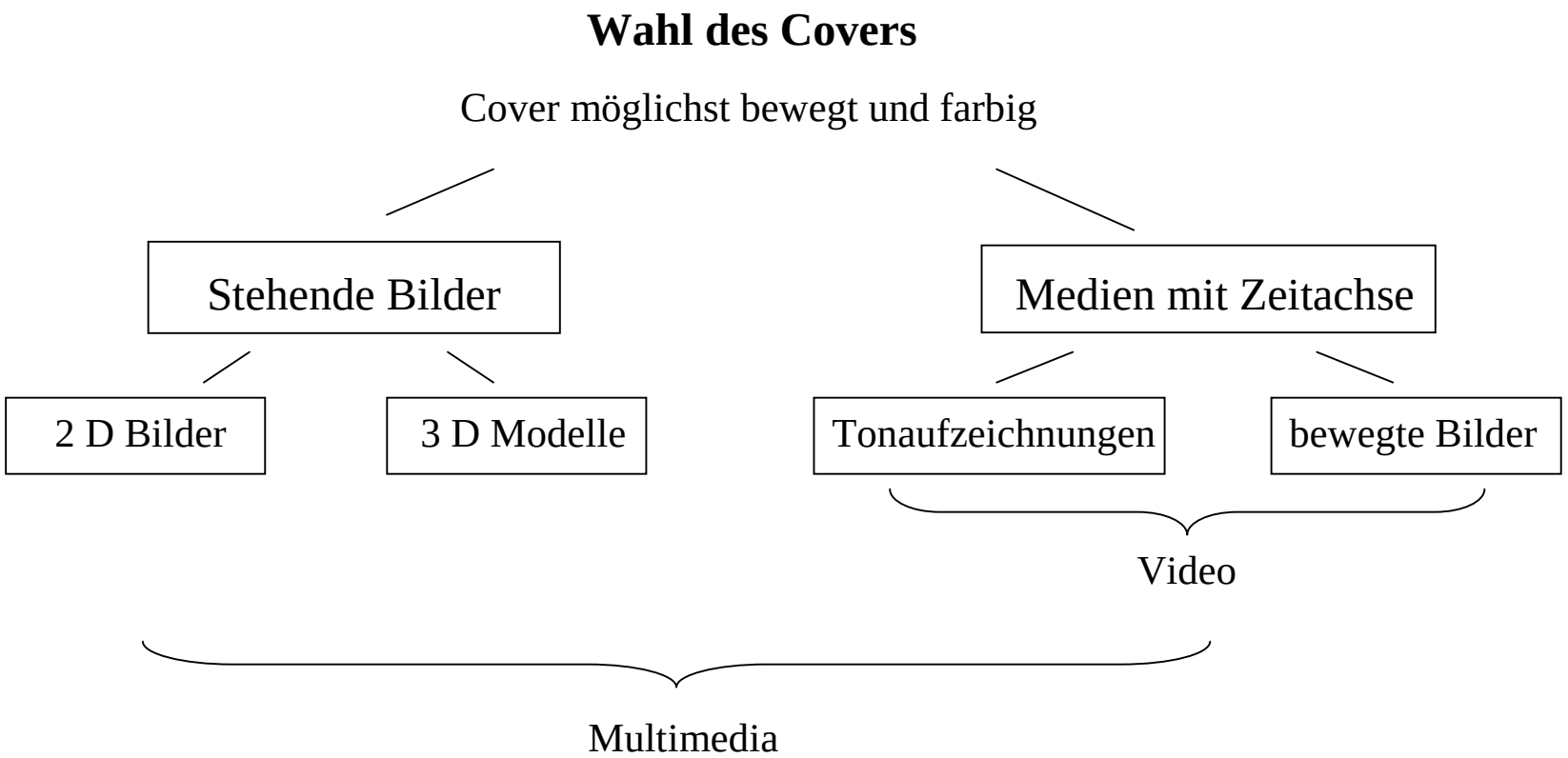
Sicherheit bezieht sich auf die Resistenz gegen gezielte Attacken

Nicht-Wahrnehmbarkeit mit menschlichen Sinnesorganen, visuell und auditiv

Nicht- Detektierbarkeit mit elektronischen Mitteln

Kapazität Die Menge der einzubettenden Daten ist begrenzt

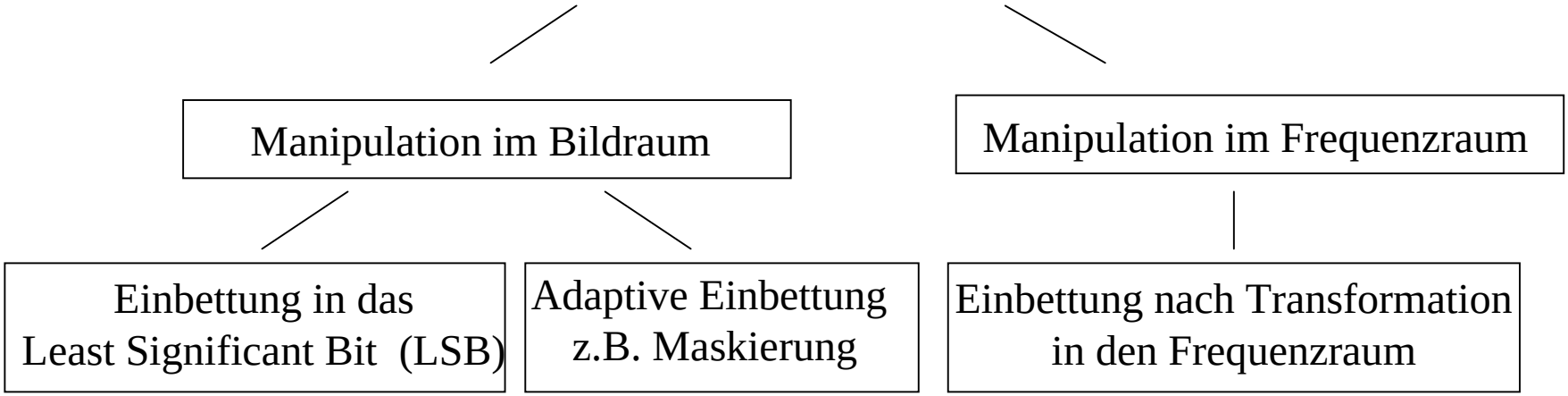
Die genannten Anforderungen an ein Stegosystem lassen sich nicht voll erfüllen, da sie sich teilweise widersprechen.


Wahl des Covers
Cover möglichst bewegt und farbig
Stehende Bilder
Medien mit Zeitachse
2 D Bilder
3 D Modelle
Tonaufzeichnungen
bewegte Bilder
Video
Multimedia

Beispiel Bildformat 640 x 480 Pixel

	Grauwert 8 bits/Pixel	Farbpalette 8 bits/Pixel	True Color 24 bits/Pixel 8 R+8 G+8 B
Kombinationen	2^8= 256	2^8= 256	2^24=16.777.216
Bytes / Pixel	1	1	3
Speicherbedarf Bytes / Bild	307.200	307.200	921.600
bits / Bild	2.457.600	2.457.600	7.372.800
LSB / Bild	307.200	307.200	921.600

Einbettung einer Nachricht
in stehende Bilder



Subsitutive Einbettungsverfahren: Veränderung vorhandener bits

Konstruktive Einbettungsverfahren: Hinzufügung von bits

Einbettung in das Least Significant Bit (LSB)

Die Einbettung der vertraulichen Nachricht erfolgt in die LSBs des Covers – möglichst als Rauschmuster codiert und über den Cover gespreizt.

24 bit Format mit RGB-Kanal => 3 LSBs / Pixel
Hohe Qualität – geringe Robustheit gegen Kompression – hohe Übertragungszeit.

8 bit Format verwendet Palette mit 256 Farben. Die 8 bit /Pixel repräsentieren nicht Farbwerte sondern sind Indizes, die auf Einträge der Farbpalette weisen. Palettenbilder sind bereits komprimiert und daher robust.

Stego-Tools: S-Tools, EzStego, StegoDos, Hide & Seek, White Noise Storm usw.

Beispiel für Einbettung in das LSB

Einbettung des Buchstaben „M“ in das LSB eines 24-bit Bildes (RGB)

Der Buchstabe M hat nach dem ASCII-Code den binären Wert 1001101 (= 77 dezimal). Der Buchstabe „M“ kann in das LSB von drei Pixel eingebracht werden.

Die Farbpunkte seien vor Einbettung:

Rot	Grün	Blau	
(00100111	11101001	11001000)	Pixel n
(00100111	11001000	11101001)	Pixel n+1
(11001001	00100111	11101001)	Pixel n+2

Nach Einbettung:

(00100111	11101000	11001000)	Pixel n
(00100111	11001001	11101000)	Pixel n+1
(11001001	00100110	11101001)	Pixel n+2

Drei der LSBs wurden geändert, im Grünkanal 2 und im Blaukanal 1. Sichtbarkeit ist nicht zu befürchten.

Einbettung einer Nachricht in LSB eines 24 bit Formats

Hidden Picture - Flugzeugträger

Foto: Associated Press

89 KB

Cover burg.bmp

1.135 KB

Stego-Tool: **S-Tools**

Kein visueller Unterschied zwischen Cover und Steganogramm

Cover

1.135 KB

Steganogramm

1.135 KB

Kein sichtbarer Unterschied auch bei stark vergrößertem Ausschnitt

Cover
1200%

Stegogramm
1200%

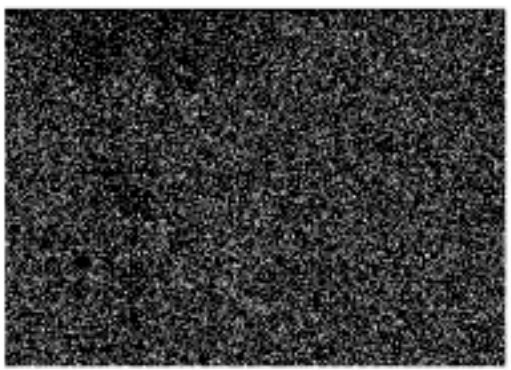
Differenz: Steganogramm minus Cover

Rotkanal

Grünkanal

Blaukanal

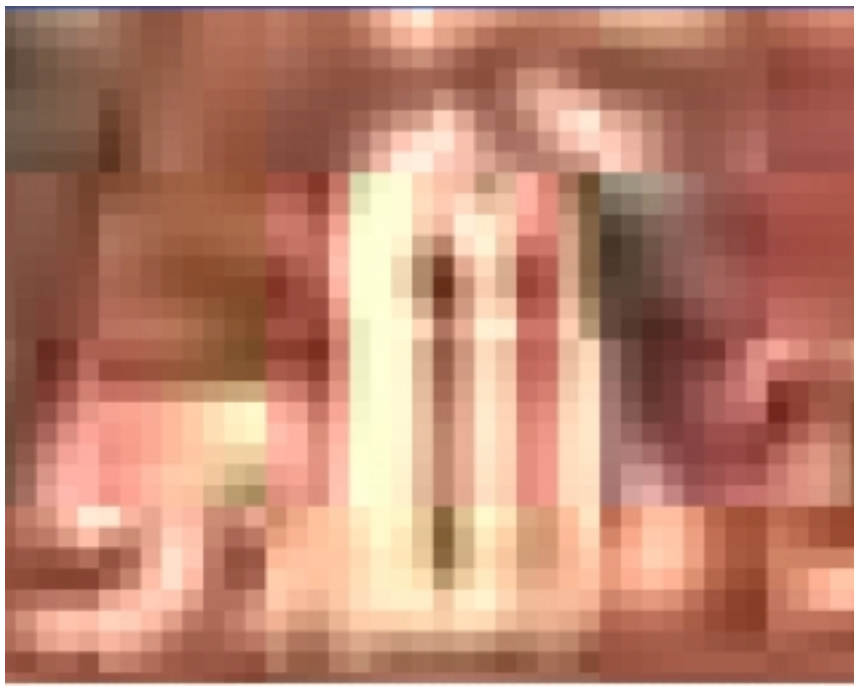
gesamt



S-Tools wandelt die Nachricht in Rauschen um und bettet sie in die Farbkanäle über den gesamten Bildbereich ein.

Nach JPEG-Kompression kann Nachricht nicht mehr ausgelesen werden !

Steganogramm
Qualität 0
1200%



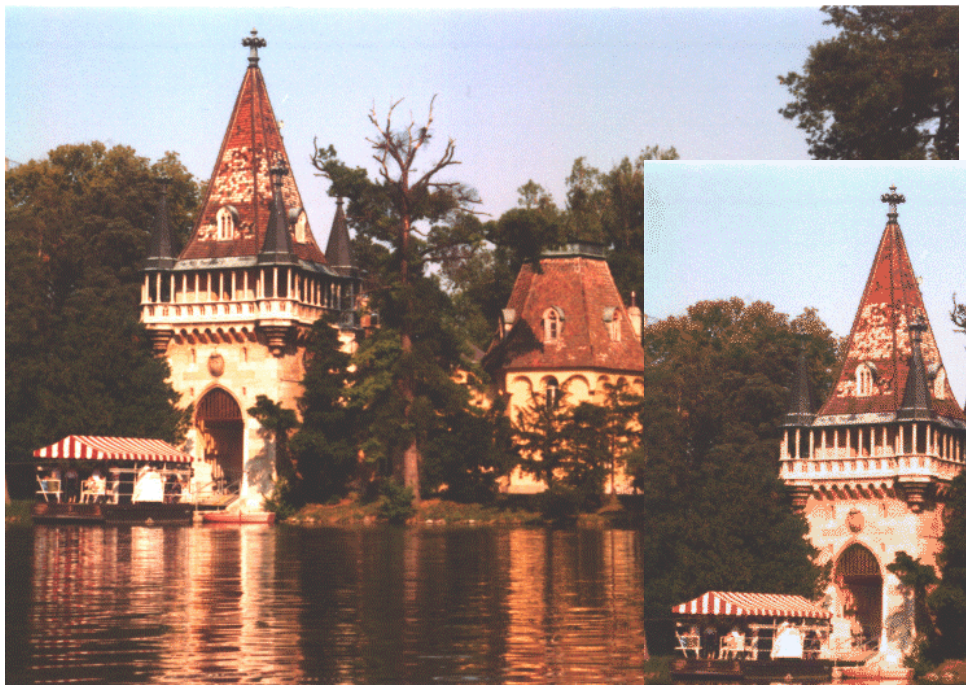
20 KB = Aufbau 8 sec

Steganogramm
Qualität 80
1200%

185 KB = Aufbau 67 sec

Einbettung einer Nachricht in LSB eines 8 bit Formats

Cover Burg.gif



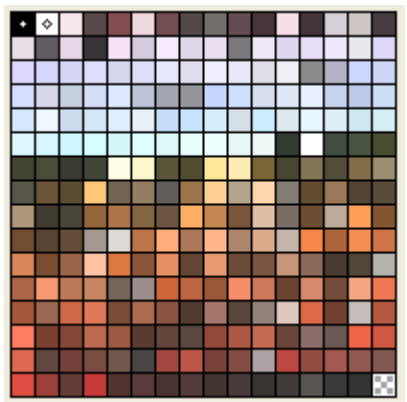
251 KB

Steganogramm
hiddenFlugzeugtr.gif

Stego-Tool: **S-Tools**

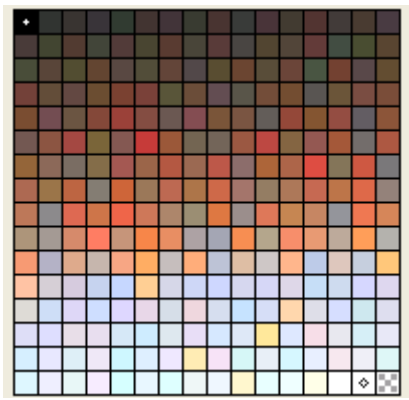
Farbpalette des 8 bit Formates

Cover
burg.gif



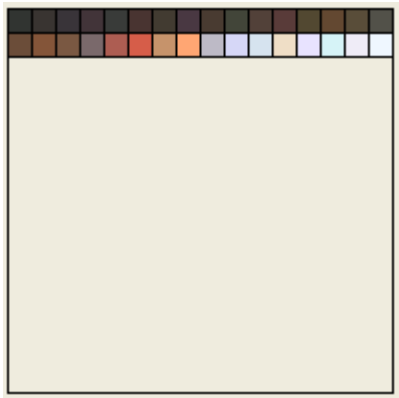
256 Farben unsortiert

Cover
burg.gif



256 Farben sortiert nach Helligkeit

Stegogramm
hiddenFlugzeugtr.gif



reduziert auf 32 Farben

Um in die LSB der Farbindizess einbetten zu können, wird die Farbpalette nach Helligkeit sortiert.

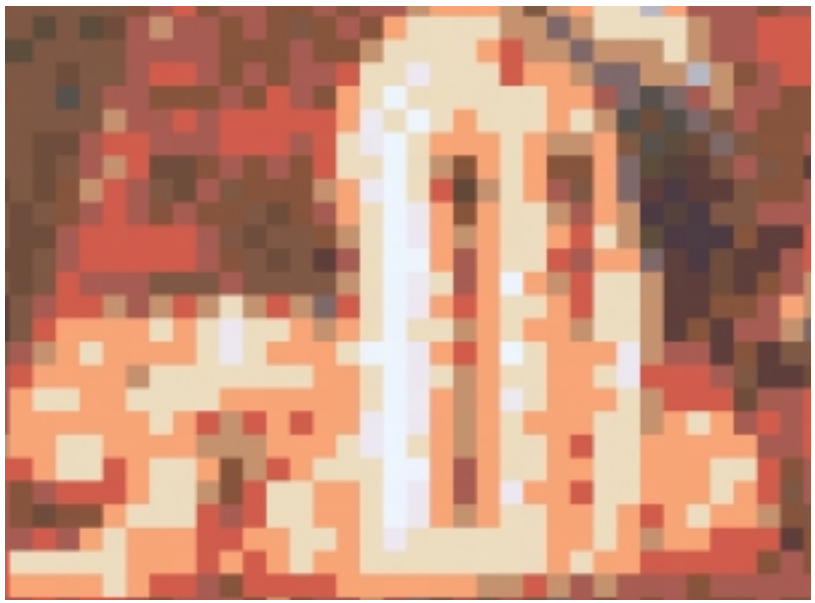
S-Tools reduziert die sortierte Farbpalette auf 256/8 = 32 Farben.

Die Vergrößerung des Bildausschnittes zeigt die Qualitätsabnahme bei Reduktion der Farbpalette von 256 auf 32 Farben - Sichtbarkeit kann nicht ausgeschlossen werden !

Cover Burg.gif
1600%

256 - Farbpalette

Steganogramm
1600 %



32 - Farbpalette

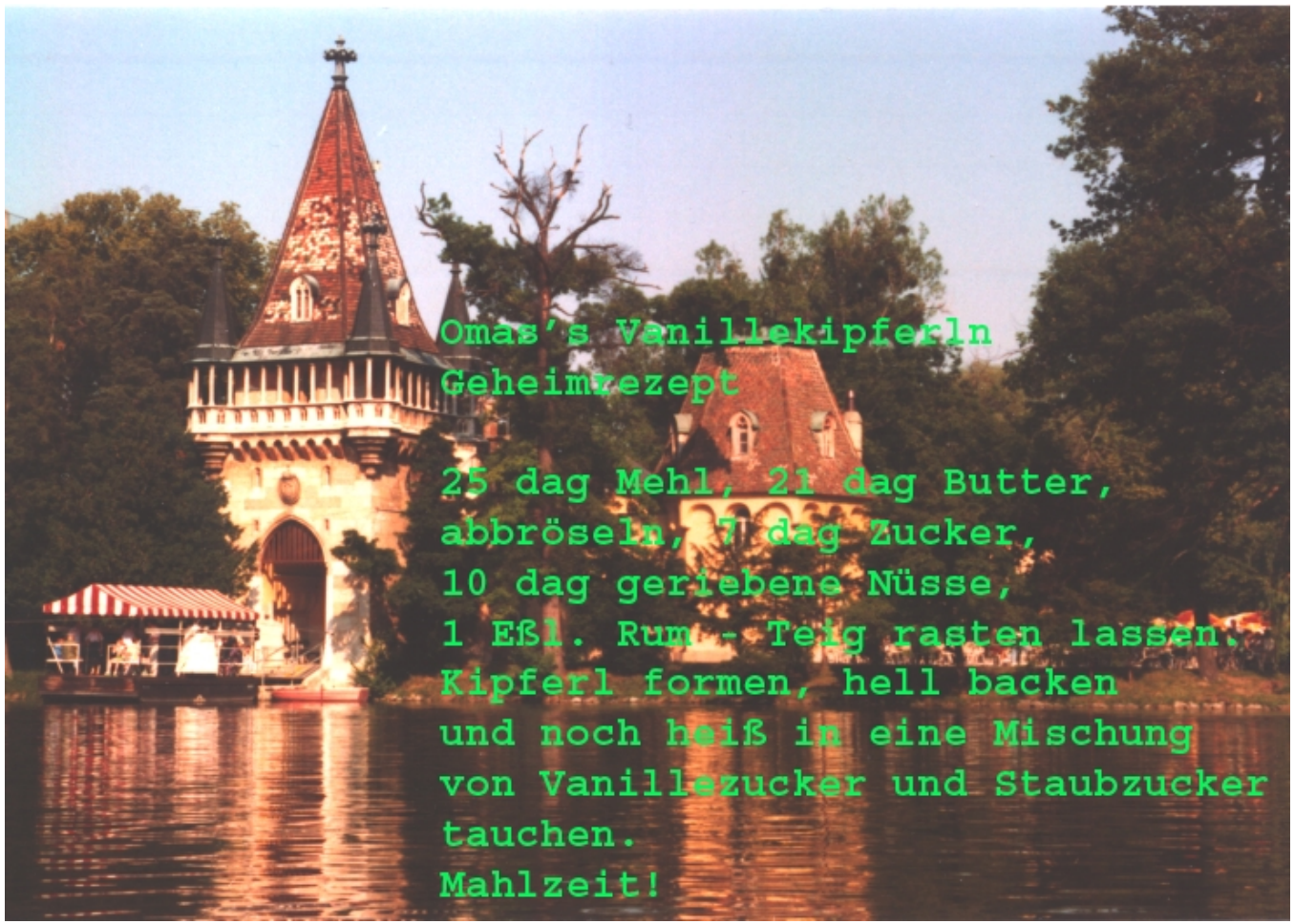
Einbettung durch Maskierung

Die Nachricht wird in höherwertige bits des Covers eingebettet und danach die Luminanz der Einbettung unter die Wahrnehmungsgrenze gesenkt.
Damit werden die eingebetteten Daten unsichtbar und robust.
Der Empfänger erhöht die Luminanz und macht die Nachricht sichtbar.

Vorteil: robuster als Einbettung im LSB

Nachteil: Funktioniert nur bei 8 bit Grauwertbilder und bei 24 bit Farbbildern

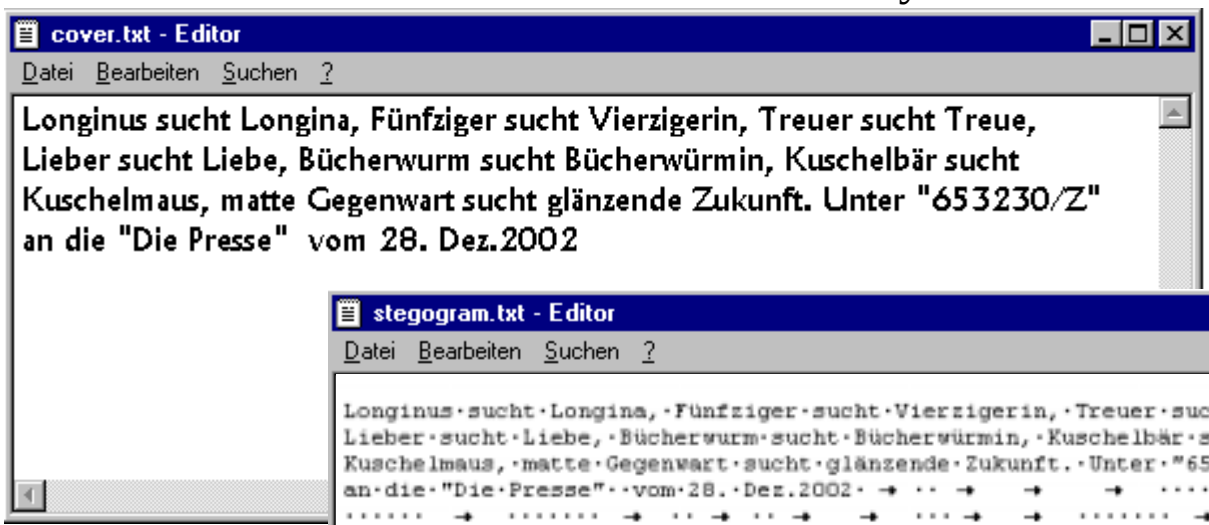
Einbettung eines Textes mit 100% Sichtbarkeit



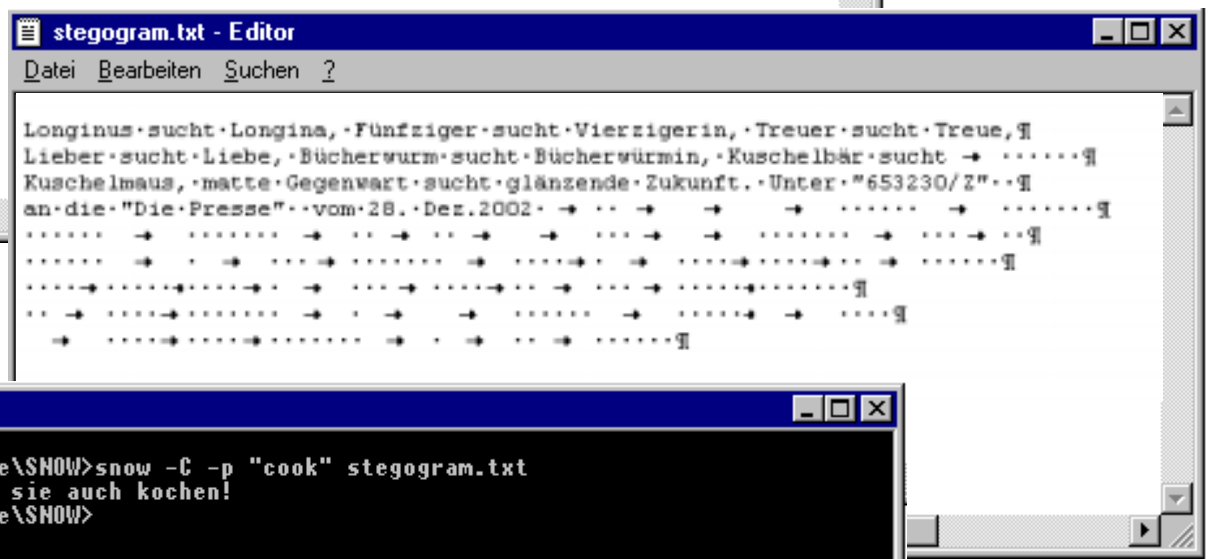
Maskierung des eingebrachten Textes durch Reduktion der Luminanz auf 2%

Konstruktive Einbettung einer Nachricht durch Hinzufügen von Tabulatoren und Leerzeichen

Cover 254 Bytes



Steganogram
496 Bytes



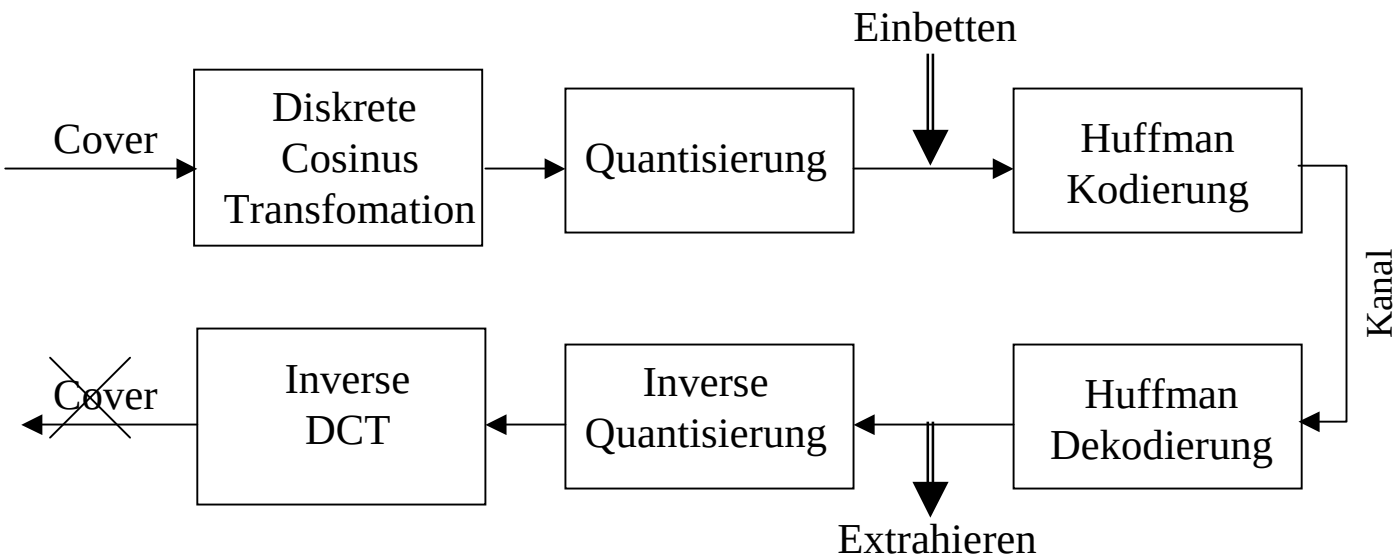
Stego-Tool: **Snow**

Einbettung nach Transformation

Der Cover wird mittels eines Transformationsalgorithmus (z.B. DCT)
in den Frequenzraum transformiert und verlustbehaftet quantisiert.
Danach wird die Nachricht in die LSB der Frequenzkoeffizienten eingebettet.
Die folgende Huffmancodierung ist verlustfrei.

Vorteil: Robust, visuell nicht erkennbar, hohe Kapazität
Nachteil: Einige Stego-Tools sind nicht gegen statistische Angriffe sicher

Stego-Tools: Jsteg, F3, F4, F5 usw.



Beispiel für Einbettung einer Nachricht in den Frequenzraum

Cover burg.bmp

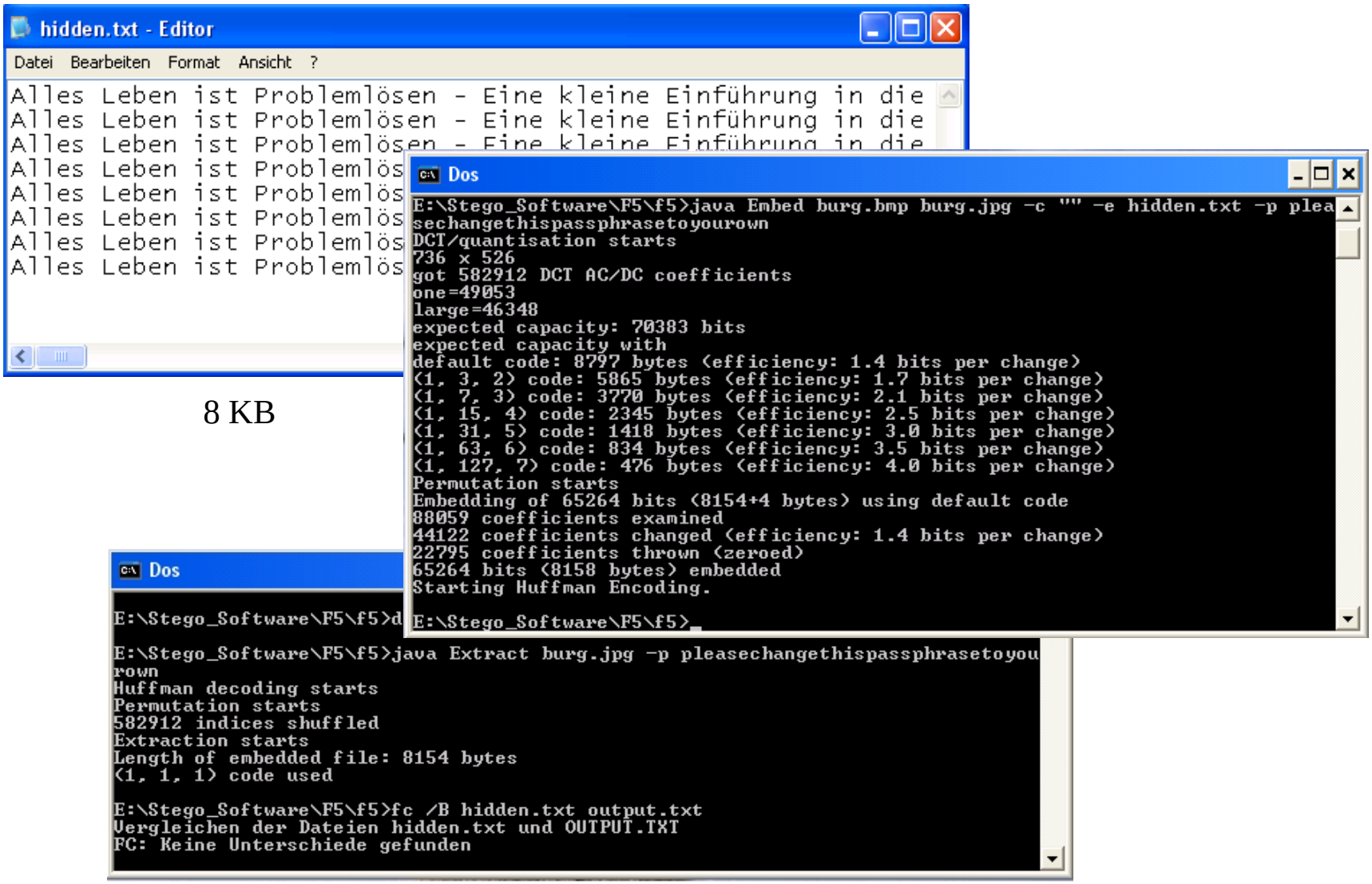
1.135 KB

Cover + hidden text
burg.jpg

65 KB

Stego-Tool: **F5**

Hiddentext mit Ein- und Ausleseprotokoll F5



Steganogramm - Attacken

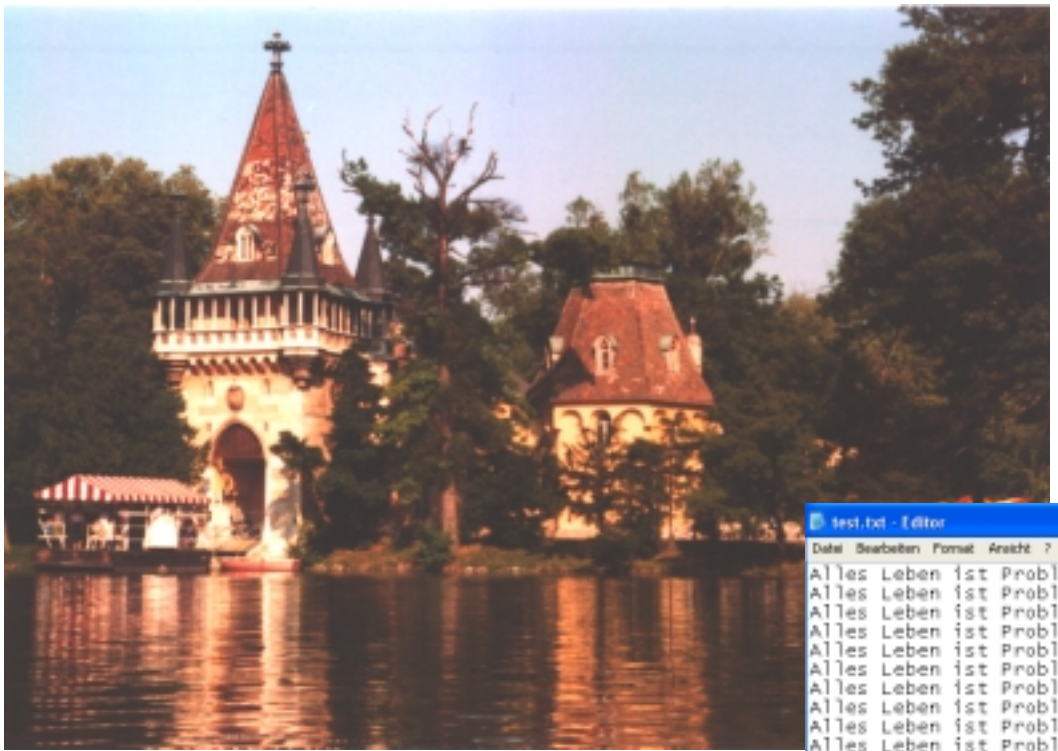
Zweck:
- Aufdeckung, ob eine versteckte Nachricht vorhanden ist.
- Kann diese Nachricht ausgelesen werden ?
- Eigener Sicherheitstest durch Nutzer.

Angriffsziel:
- Steganogramm
- Steganogramm + Cover

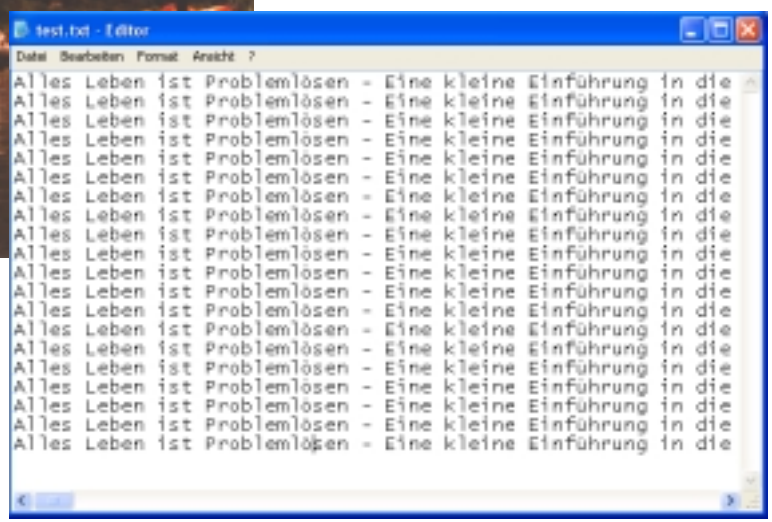
Methoden:
- visuell
- statistisch

Visuelle Attacke

Steganogramm

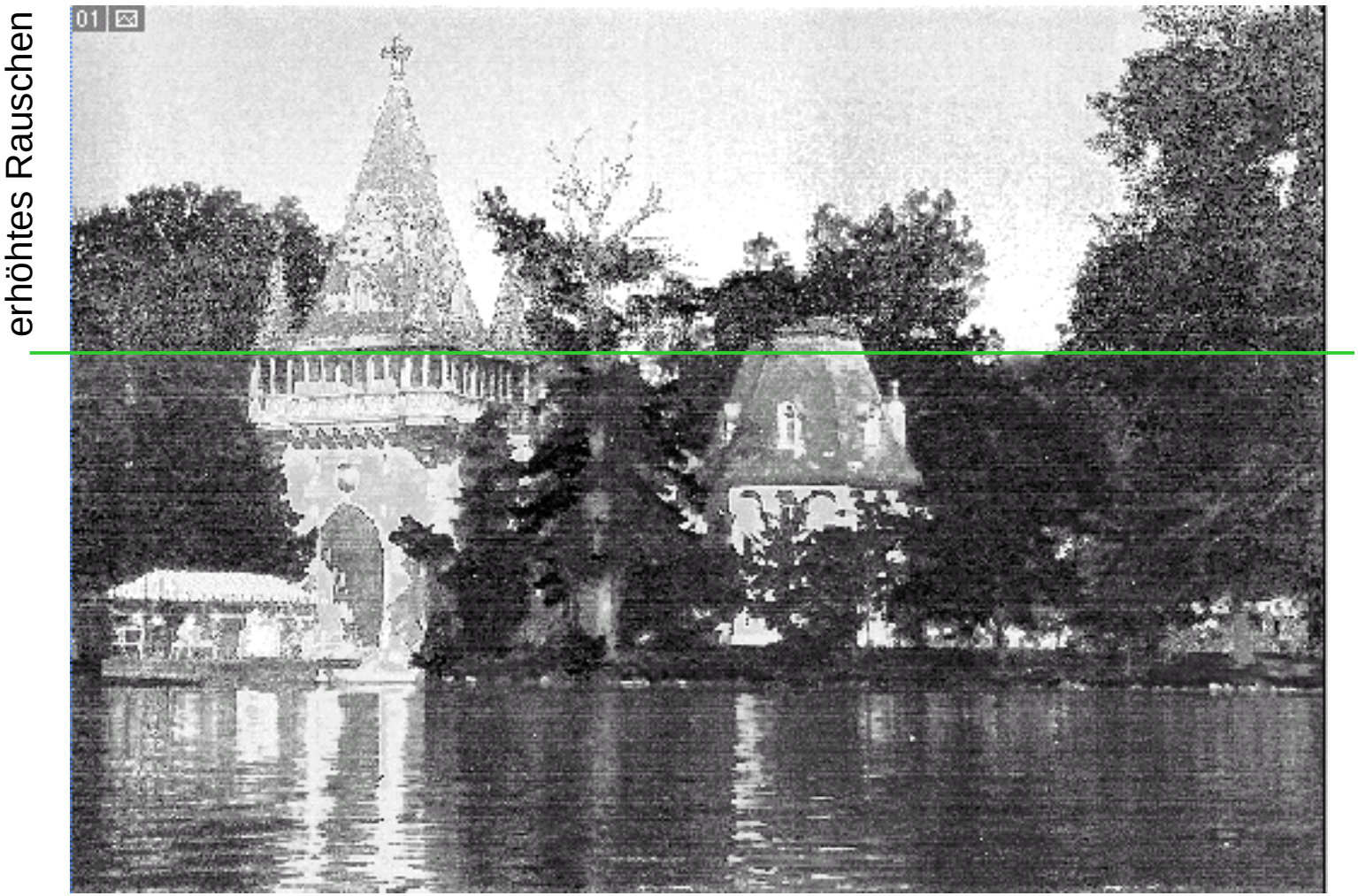


Hidden Text 20 KB



Stego-Tool: **White Noise Storm**

Stego-Attacke: Analyse mittels Manipulation im Grünkanal



Erhöhtes Rauschen im Steganogramm lässt eine eingebettete Nachricht vermuten.

Stego-Cover Attacke bestätigt die Vermutung einer verdeckten Nachricht

Rotkanal

Grünkanal

Blaukanal

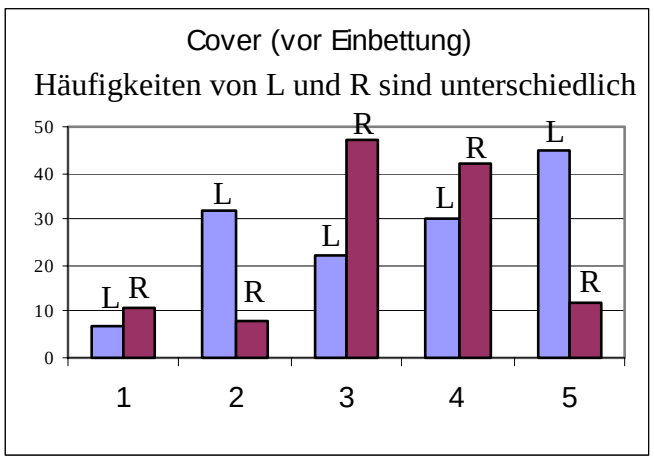
gesamt

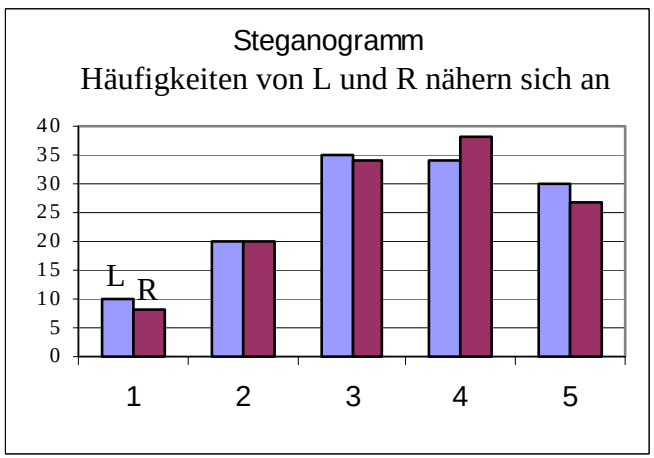
Mit White Noise Storm wird die Nachricht nicht über den Bildbereich gespreizt.

Statistische Attacke

Beispiel nach A. Westfeld für Einbettung der Nachricht in das LSB für eine Stichprobe von 5 Farbwerten.

	Cover (vor Einbettung) Häufigkeit der Farbwerte				**Steganogramm** Häufigkeit der Farbwerte		
	L	R	(L+R)/2		L	R	(L+R)/2
1	7	11	9,0		10	8	9,0
2	32	8	20,0		20	20	20,0
3	22	47	34,5		35	34	34,5
4	30	42	36,0		34	38	36,0
5	45	12	28,5		30	27	28,5
	CHITEST		0,000144		CHITEST		0,989264





L und R sind benachbarte Farbwerte, die sich nur im LSB unterscheiden.

Weitere Anwendungsbereiche der digitalen Steganographie

Video

Videokonferenzen

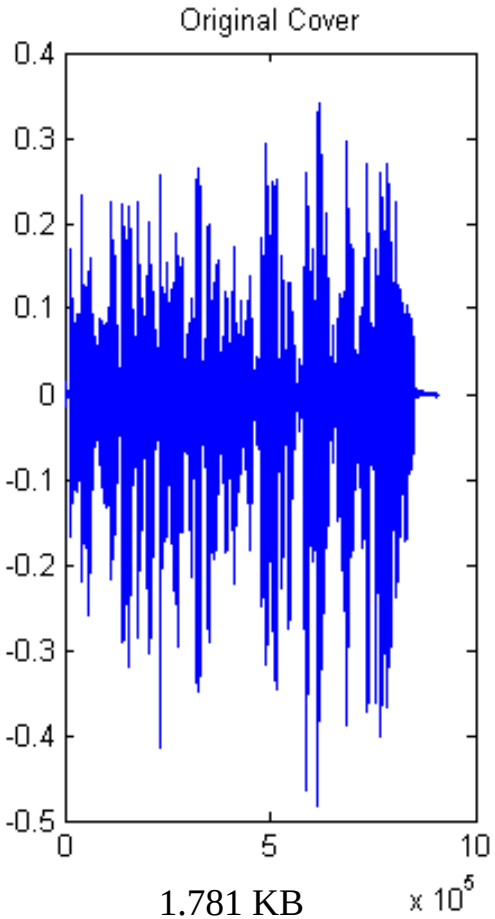
Audio

Telefonate

Protokolle (TCP/IP)

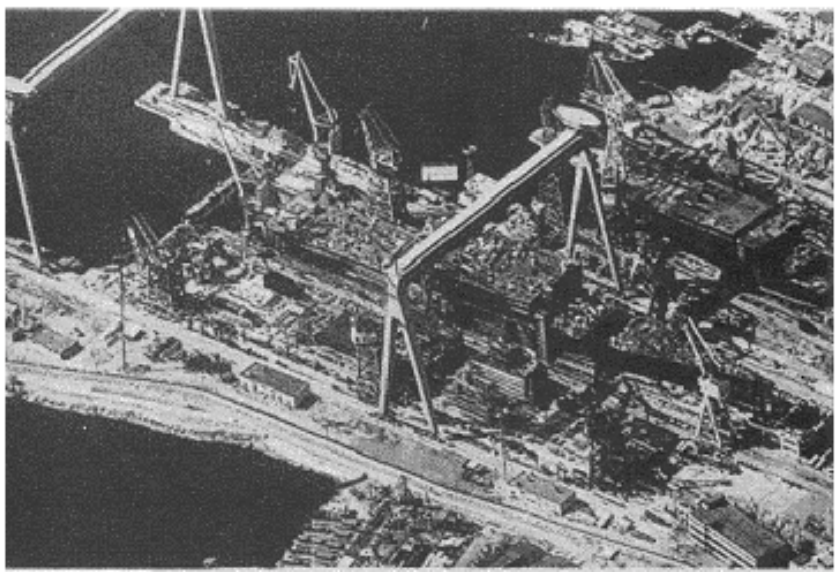
.....

Beispiel für Audiocover – svega.wav 44,1 kHz Abtastrate, 16 bit Abtastwert



1.781 KB

hidden picture



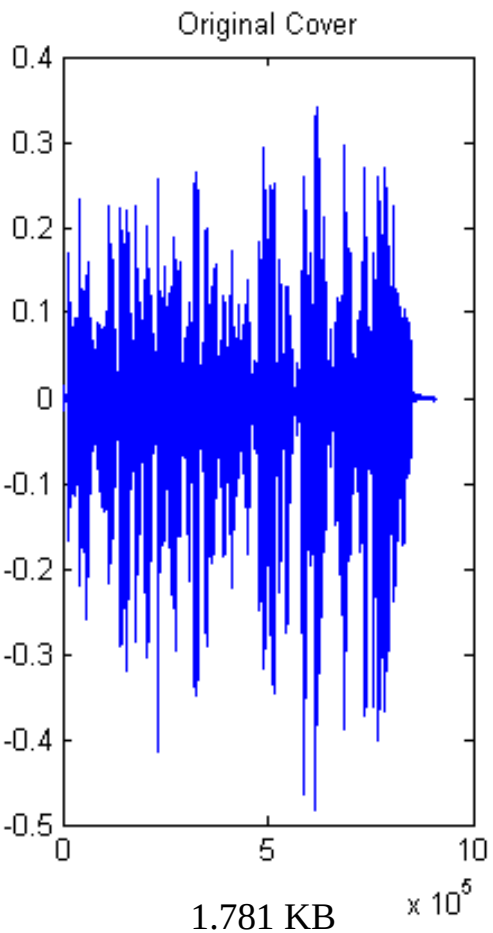
89 KB

Stego-Tool: **S-Tools** Einbettung der Nachricht in das LSB des 16 bit Abtastwertes.

Klangbild vor und nach Einbetten der Nachricht

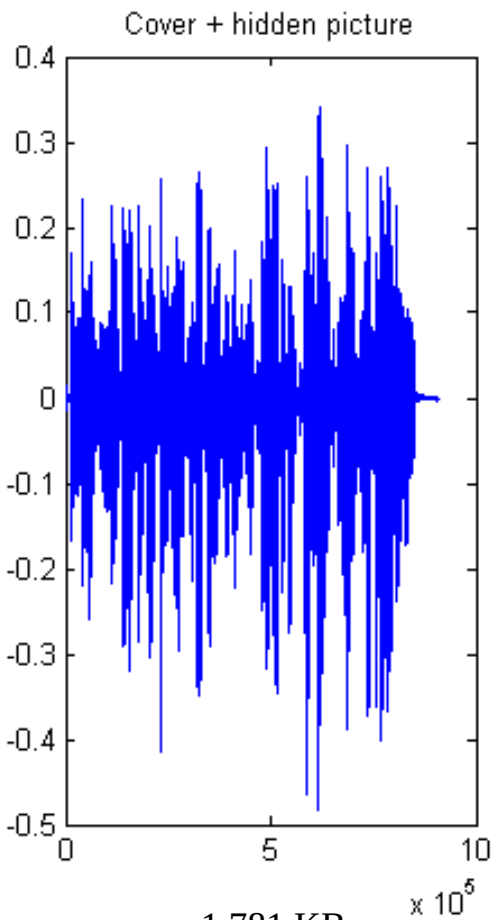
svega.wav

svega.wav



1.781 KB

hiddenflugzeugtr.wav

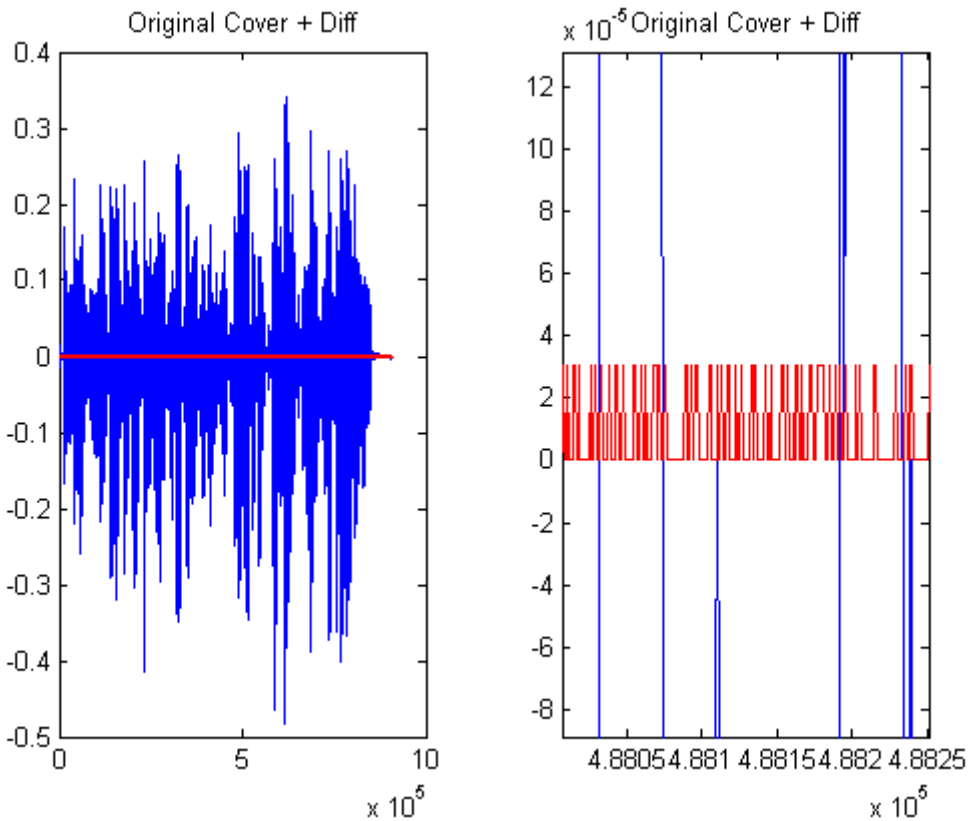


1.781 KB

hiddenflugzeugtr.wav

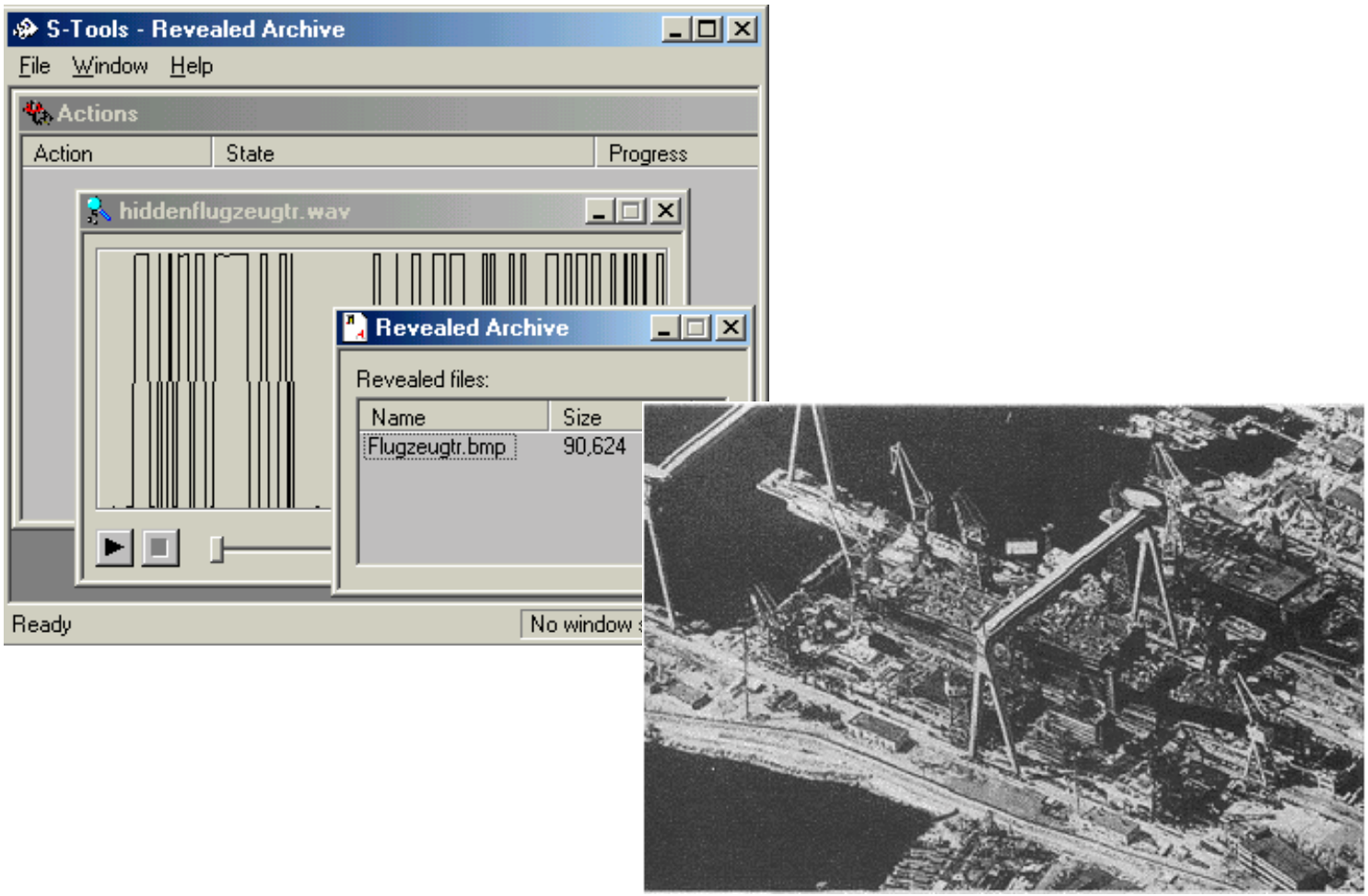
Sichtbarmachen der eingebetteten Nachricht

Ausschnitt Vergrößerung



Eingebettete Nachricht ist bei 16 bit Abtastwerten nicht hörbar.

Extraktion der Nachricht



Beispiel für doppelte Steganographie

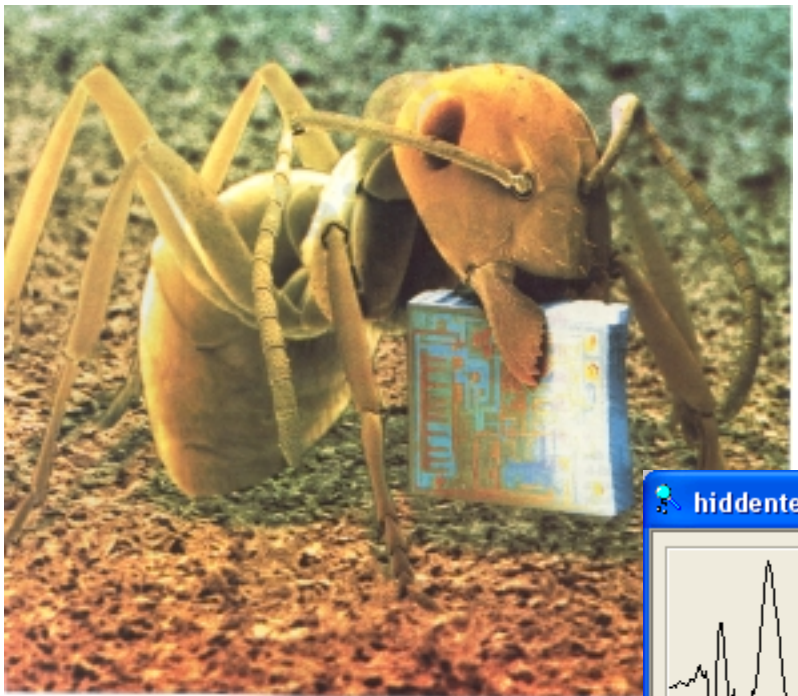
Steganogramm
hiddensound.bmp

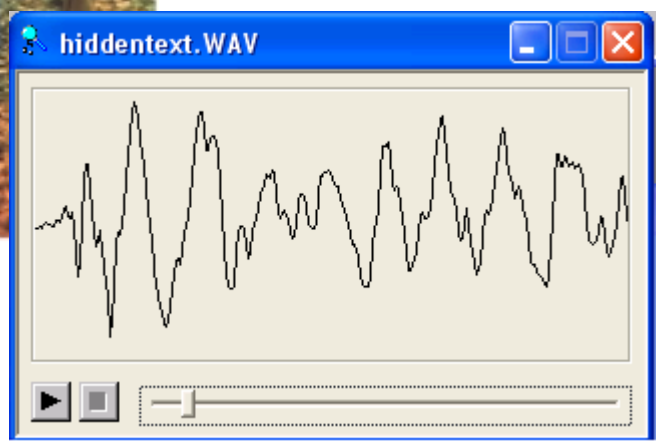
Foto: Contrast/Andrew Syred

3.822 KB

Stego-Tool: **S-Tools**

Auslesen der eingebetteten Nachricht, die wieder ein Steganogramm ist ….





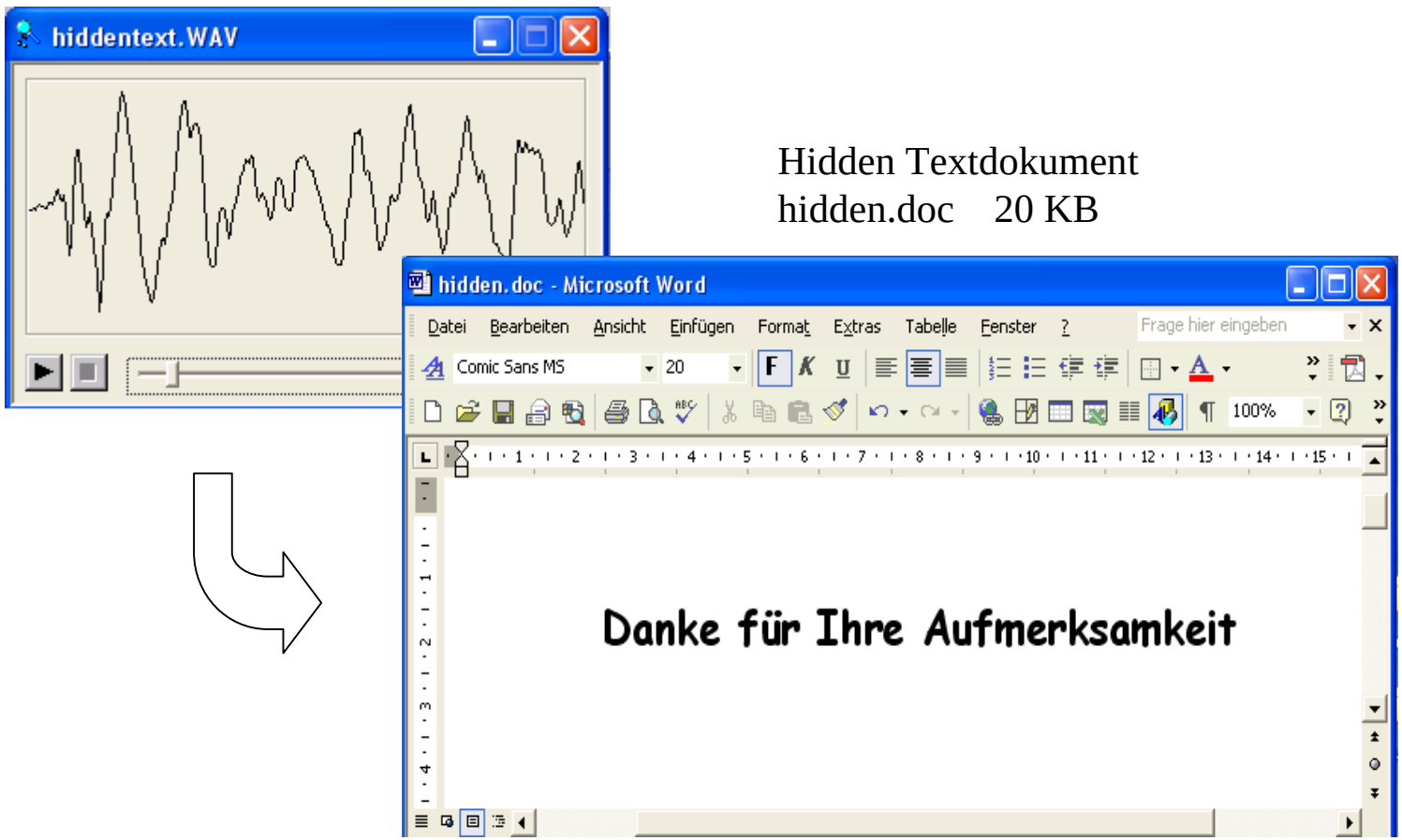
Steganogramm

hiddentext.wav

67 KB

Abtastrate 11.025 Hz
Abtastwert 8 bit

Auslesen der im Sound versteckten Nachricht



Hidden Textdokument
hidden.doc 20 KB

Jana Dittmann, *Digitale Wasserzeichen*, Springer Verlag, 2000.

F.L.Bauer, *Entzifferte Geheimnisse*, Springer Verlag, 3. Auflage, 2000.

Elke Franz und Andreas Pfiztmann, *Einführung in die Steganographie und Ableitung eines neuen Stegoparadigmas*, Informatik-Spektrum, 21: 183-193, Springer-Verlag, 1998.

Neil F. Johnson und. Suhil Jajodia, *Exploring Steganographiy: Seeing the Unseen*, IEEE, Computing Practices, 1998.

Neil F. Johnson, Zoran Duric, Sushil Jajodia, *Information Hiding*, Kluwer Academic Publishers, 2001.

Simon Singh, *Geheime Botschaften*, Deutscher Taschenbuch Verlag, 2001

Andreas Westfeld, *Unsichtbare Botschaften*, c‘t 2001, Heft 9, Heinz Heise Verlag, 2001.

Andreas Westfeld, *F5 – ein steganographischer Alogrithmus*, http://os.inf.tu-dresden.de/~westfeld/publikationen/westfeld.vis01.pdf, 2001.

Andreas Westfeld, *Attacks on Steganographic Systems*, Lecture Notes in Comp.Science 1768, herausgegeben von A.Pfitzmann, Information Hiding 1999, pp.61-76, Springer Verlag, 2000.

Fred B. Wrixon, *Codes, Chiffren & andere Geheimsprachen*, Könemann Verlagsgesellschaft, 2000.

Verwendete Stego-Tools :

S-Tools: ftp://ftp.ntua.gr/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip

Snow: http://www.darkside.com.au/snow/

White Noise Storm: ftp://ftp.funet.fi/pub/crypt/steganography/

F5: http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html

Weitere Tools findet man unter: http://www.heise.de/pgpCA/stego.shtml

Datenträger:

Flugzeugträger: Associated Press

burg.bmp, gif, jpg: Franzensburg in Laxenburg, eigenes Foto

ameise.bmp: Contrast / Andrew Syred

svega.wav: http://www.cl.cam.ac.uk/~fapp2/steganography/imp3stego

oldclock.wav: Heiner Küsters, *Bilddatenkomprimierung mit JPEG und MPEG*, Franzis Verlag