

WIRTSCHAFTSINFORMATIK

Seminar: Web Security

Principles of Steganography



Quellenverzeichnis

- Information hiding techniques for steganography and digital watermarking, Chapter 2 (P. 17 – 41)
- Steganographie – Eine andere Art von Verschlüsselung, Alexandra Weikert,
<http://www.fitug.de/bildung/kongress/stegano.html>
- Steganographie, Baur, Gaertner, Mlinar
<http://rhlx01.fht-esslingen.de/projects/krypto/stega/stega.html>
- Sag's durch die Blume, Marit Koehntopp,
<http://www.koehntopp.de/marit/publikationen/steganographie/index.html>
- Steganographie, Oliver Müller,
<http://www-linux-magazin.de/ausgabe/1997/08/Krypto/krypto2.html>
- Internet – Technologie und Anwendungen, Kapitel 10,
<http://home.t-online.de/home/hr.assmann/technics/Vorlesung%20Internet%20-%20Technologie%207.htm>



Gliederung

- Geschichtliches
- Allgemeines
- Reine Stenographie
- Secret Key Stenographie
- Public Key Stenographie
- Sicherheit von Stenographie-Systemen
- Verstecken von Informationen in „noisy data“



Gliederung 2

- Adaptive vs. Nicht-adaptive Algorithmen
 - Laplace Filter
 - Benutzen von „Cover-Models“
- Aktive und Hinterhältige Attackierer
 - Aktive Attackierer: Robuste Stenographie
 - Supraliminale Kanäle
 - Hinterhältige Attackierer: Sichere Stenographie
- Versteckte Informationen im geschriebenen Text
- Weitere Beispiele
- Fazit



Geschichtliches

- Erste Formen schon seit antikem Griechenland
- Wachstafel
- Tätowierter Kopf
- Unsichtbare Tinte
- Microdots
- Rechnergestützte Steganographie



Allgemeines

- Steganographie = griech: stegano (geheim), grapheim (schreiben)
- Kryptographie = offensichtliches Verschlüsseln
- Steganographie = Informationen versteckt übertragen
 - Kommunikation auf eine Art und Weise, die die Existenz einer Kommunikation verbirgt
 - nicht unlesbar für Dritte übermitteln, sondern das Vorhandensein einer Nachricht verbergen
- 2 Verfahren:
 - Bit-Orientiertes Verfahren (LSB)
 - Spread-Spectrum-Techniken



Allgemeines 2

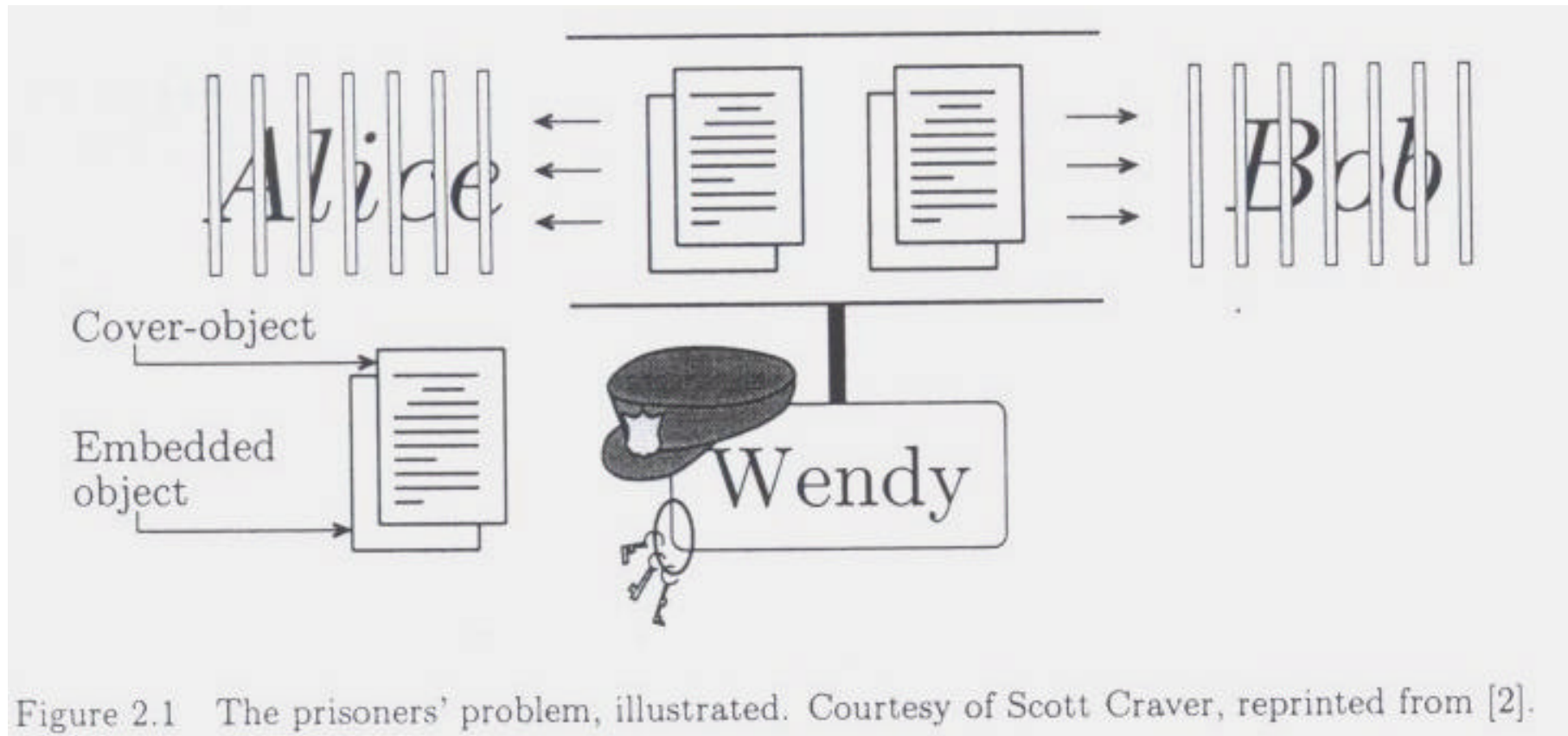
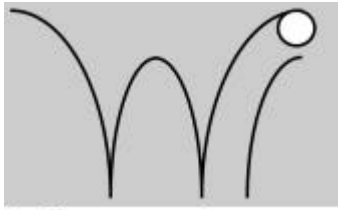


Figure 2.1 The prisoners' problem, illustrated. Courtesy of Scott Craver, reprinted from [2].

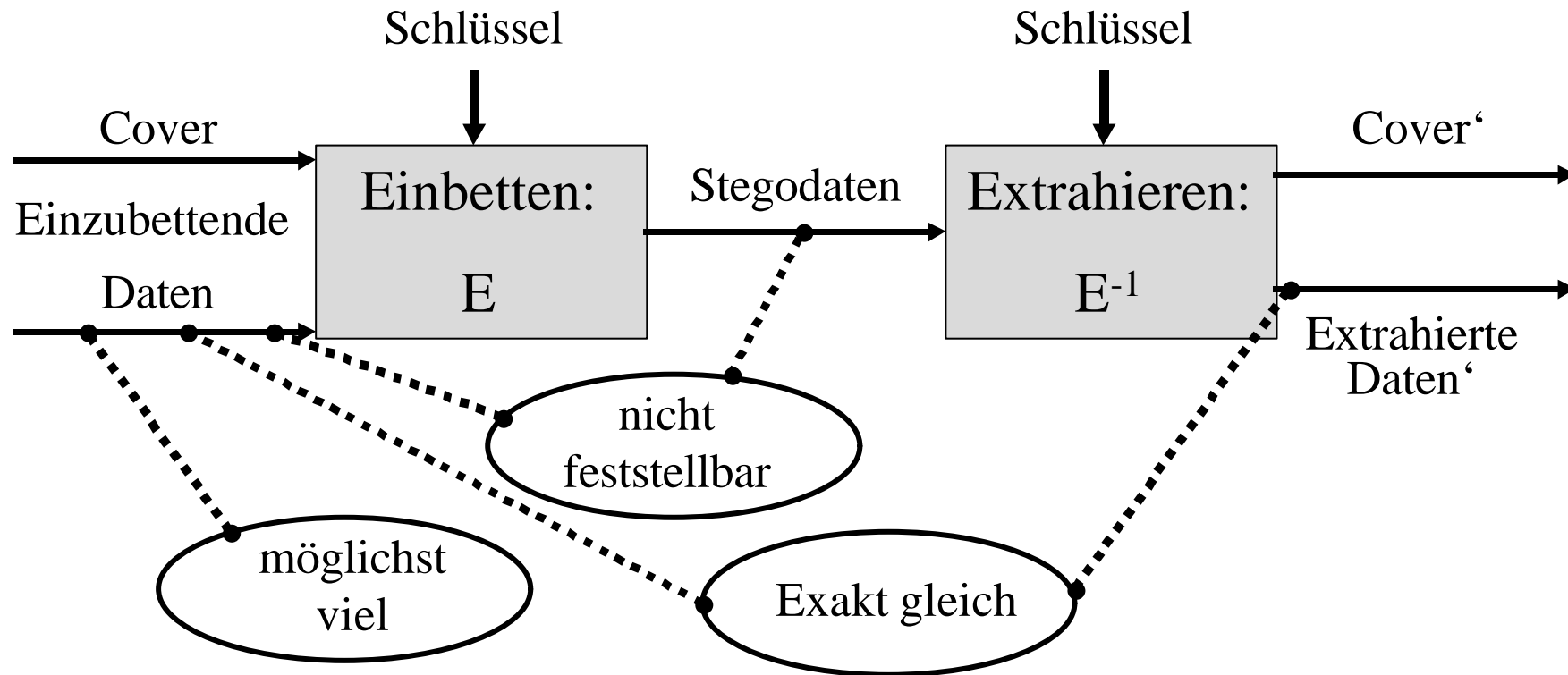


Reine Steganographie

- Steganographie *ohne* Schlüssel
- Geheime Nachricht wird in Cover eingebunden bzw. entbunden
- Algorithmus muss beiden Parteien bekannt sein
- Vor-Verschlüsselte Nachricht im Nachricht erhöht den Schutz (bei starken Steganographie-Systemen nicht notwendig)
- Authentizität nicht gegeben + plus weitere Gefahren!



Steganographie mit Keys (allg.)





Secret Key Steganographie

- Steganographie-System sollte auf einem „Stego-Key“ basieren.
- Nachricht wird mittels Stego-Key ins Cover eingebunden und kann auch nur damit wieder entschlüsselt werden.
- Austausch des Keys über sicheren Kanal notwendig
- Schlüssel auch über signifikante Bits mit Hash-Funktion generierbar (Session Key)



Public Key Steganographie

- Basiert auf 2-Schlüsselsystem
 - Private Key
 - Public Key (öffentlich zugänglich)
 - Beide Keys unabhängig; nicht voneinander ableitbar
- Encryption auch anwendbar auf Cover ohne Message
- Problem: Bei jedem Bild muss man versteckte Nachricht erwarten → Jeder muss Extrahierung anwenden (Inet-Newsgroup)

Steganographisches Key-Exchange Protokoll

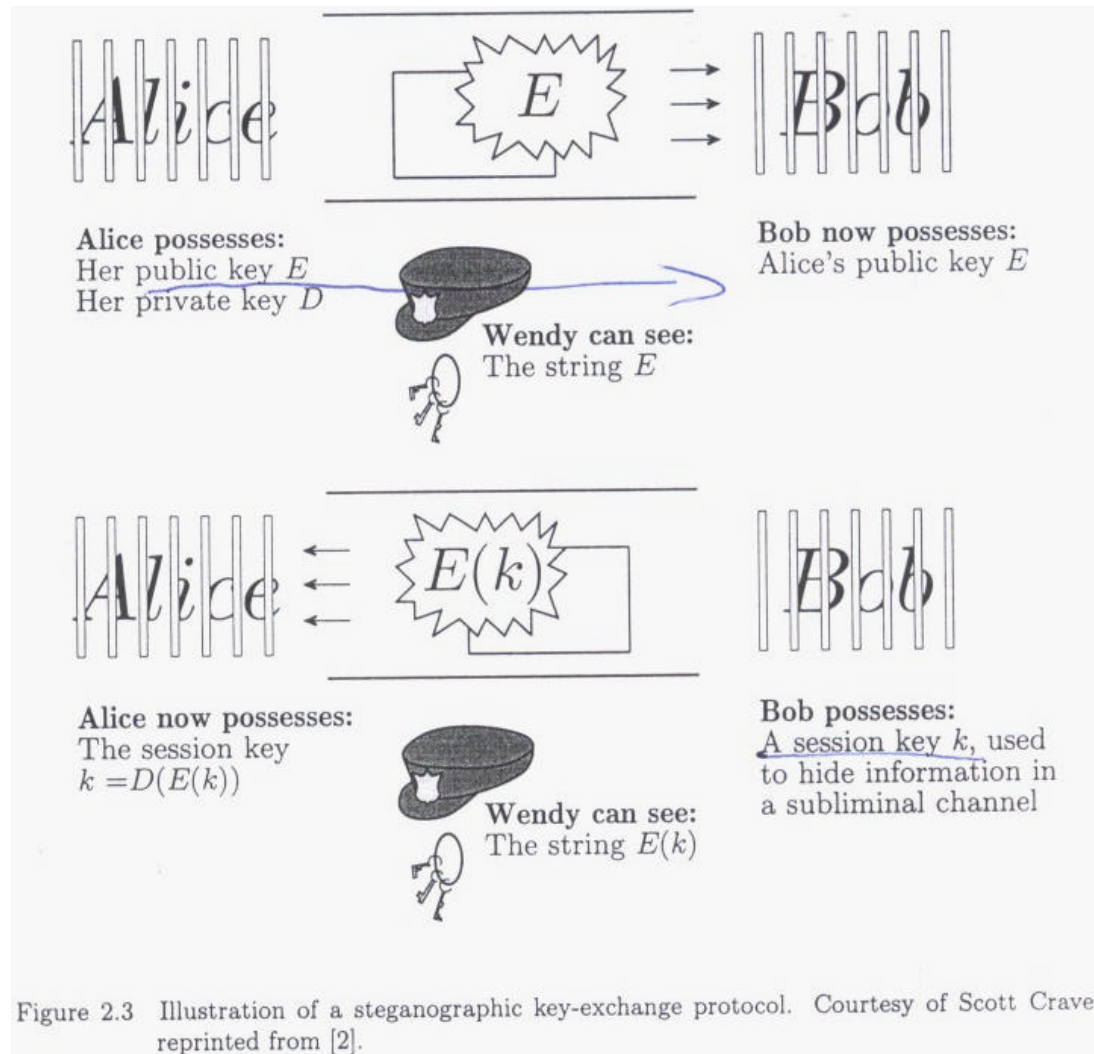


Figure 2.3 Illustration of a steganographic key-exchange protocol. Courtesy of Scott Craver, reprinted from [2].

Sicherheit von Steganographie-Systemen

- Das Knacken besteht aus „*Erkennen* – Extrahierung – Information unbrauchbar machen“
- Bereits „*Erkennen*“ macht das System unbrauchbar
- Annahme: Angreifer hat unendlich Computer-Power und wird verschiedenste Angriffsmethoden durchführen
- Wenn Angreifer die Existenz einer geheimen Nachricht nicht nachweisen kann ist das System per Definition sicher
- Theorem: Es existieren perfekte, sichere Steganographie-Systeme

Verstecken von Informationen in „noisy data“ (Rauschen)

- Überall Rauschen (Telefon, Bilder, Musik)
- Nachrichten werden ins Least Significant Bit (LSB) geschrieben.
- 1 Byte = 8 Bit → geheime Nachricht darf max. 1/8 der Cover-Größe einnehmen
- $159 = 10011111$ *1* → 10011111 *0*
- Menschliches Auge / Ohr kann Änderung nicht wahrnehmen

Adaptive vs. Nicht-adaptive Algorithmen

- Die vorgestellten Methoden haben alle ein Merkmal:
Sie erstern signifikante Teile eines Covers mit der geh. Nachricht
- Problem: Statistische Eigenschaften werden dabei ohne Beachtung geändert!
- Erkennbar! Angreifer könnte das System knacken → Kapitel 4 für weitere Erläuterungen

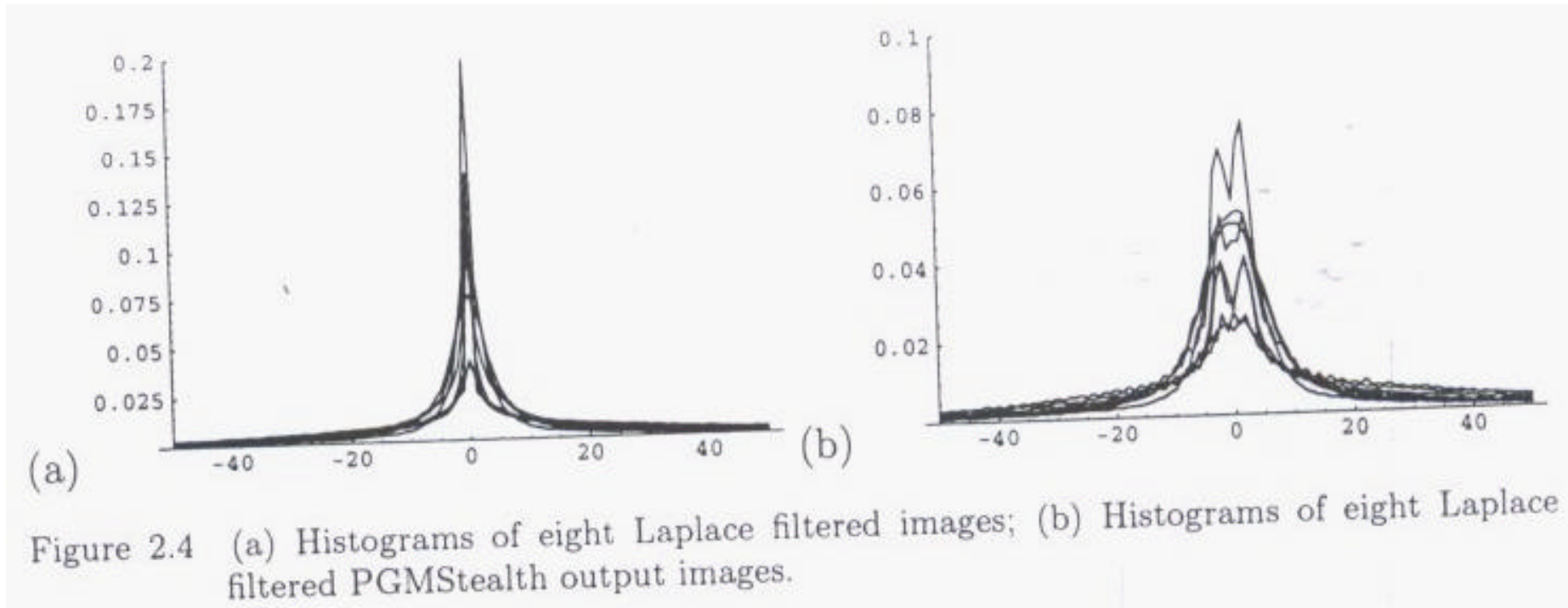


Laplace Filter

- Mittels dem diskreten Laplace Operator kann man die Existenz von versteckten Nachrichten von PGMStealth-generierten Bildern „nachweisen“
- Verfahren überprüft Nachbarpixel mit dem jetzigen. Der Unterschied sollte gegen Null gehen.



Laplace Filter





Benutzen von „Cover-Models“

- Modellierung der Cover-Charakteristika
- Einbindung eines adaptiven steganographie Algorithmus‘
- Einbau der geheimen Nachricht auf die Art, das sie vom „normalen Rauschen“ nicht zu unterscheiden
- Information dann in „highly noisy image regions“ wiederzufinden
- Schwer zu implementieren → Das exakte Modell des Covers muss bekannt sein.
- Verfahren durch „stärkeren“ Angreifer nachvollziehbar

Aktive und Hinterhältige Attackierer

- Attackierer / Eingreifer können Cover abfangen und ändern (eigentl. Parteien bemerken nichts)
- Aktiver A.: Kann nur kleinere Änderungen am Cover vornehmen: Objekt bleibt in Wahrnehmung und semantisch gleich.
- Hinterhältiger A.: Fälscht /erfindet Nachrichten oder protokolliert im Namen des Anderen

Aktive Attackierer: Robuste Steganographie

- Cover sind hochsensibel (smoothing, filtering usw...) → Attackierer könnte einfach Bild leicht ändern (auch egal wenn keine geh. Nachricht im Cover)
- Folge: Totaler Informationsverlust
- System ist robust, wenn Information ohne drastische Änderungen vorhanden bleibt.
- Trade-Off: Sicherheit vs. Robustheit
- Manche Systeme robust gegen Mapping-Komprimierungen (JPG-Format)
- Zwei Vorgehensweisen: (1) Mögl. Modifikationen beim Einbetten vorhersagen können
- (2) Versuch Modifikationen rückgängig zu machen



Supraliminale Kanäle

- = wenn in geh. Infos in Bildern so versteckt (signifikante Bits des Covers) sind, dass sie nur durch erkennbar-drastische Veränderungen am Bild zerstört werden
- Geeignet für Key-Exchange Protocol

Hinterhältige Attackierer: Sicherere Steganographie

- Authentizität des Absenders nicht nachweisbar!
- Anforderung an sicheren, steganographischen Algorithmus:
 - Nachrichten werden mittels Public/Secret-Key versteckt. Secret Key muss den Sender eindeutig identifizieren!
 - Nur der Halter des korrekten Schlüssel kann versteckte Nachricht entdecken, extrahieren und nachweisen. Niemand anders darf statistischen Beweis einer verst. Nachricht finden.
 - Versteckte Nachricht darf nicht computertechnisch entdeckt werden
 - Fehlerkorrektur sollte Korrektheit der Daten sicherstellen.
 - „Gewisses Maß an Redundanz der Daten“

Versteckte Informationen im geschriebenen Text

- Viele Ansätze = Viele davon nicht seriös (nutzlos)
- Liebe Kolleginnen! Wir genießen nun endlich unsere Ferien auf dieser Insel vor Spanien. Wetter gut, Unterkunft auch, ebenso das Essen. Toll! Gruß, M. K.
- Davon viele Varianten abgeleitet (Absatzbasiert, Kommasetzung, Grammatikfehler)
- Verstecken in „scheinbarer“ Nachricht



Weitere Beispiele

- Versteckte Nachrichten in Video-Streams (Video-Conferencing)
- Versteckte Nachrichten in ausführbaren Programmen
- Versteckte Kanäle in Betriebssystem (Systemauslastung, Positionierung des Schreibkopfes)
- Neg. Beispiel: Bin Laden in Porno-NewsGroups



Fazit

- Weltweite Lauschangriffe (Deutschland in den ersten Schritten)
- Daher prinzipiell unterstützenswert zur Sicherung der freien Meinungsäußerung
- Steganographie: Anwendungsfeld eher im Copyright- und Watermarking Bereich
- Für täglichen Komm.verkehr umständlich
- Möglichkeiten bei weitem nicht ausgeschöpft
- Einsatz guter Stego-Software nicht nachweisbar, daher nicht zu reglementieren