IT-Security: Theory and Practice

Steganography and Watermarking

January 8, 2002

Sven Wohlgemuth
wohlgemuth@iig.uni-freiburg.de

Lecture Homepage:
http://www.informatik.uni-freiburg.de/~softech/teaching/ws01/itsec

Example: Steganography

George obtains oranges daily yet eights' are rubbish!

Example: Steganography

George obtains oranges daily yet eights' are rubbish!

Example: Steganography

George obtains oranges daily yet eights' are rubbish!

↓

Good year!

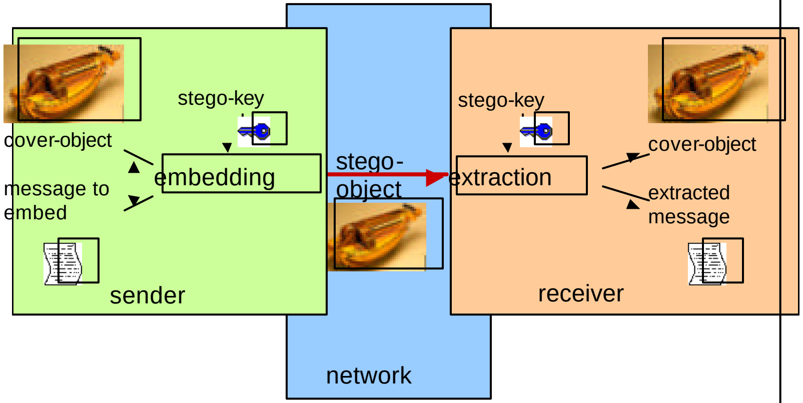
eorge btains ranges...	cover-object
George obtains oranges...	stego-object
Good year!	embedded message

Steganography: Introduction

- (Greek) "covered writing"
- Security through obscurity
- Invisible ink
- Very small holes above or below letters
- Hiding messages in music scores
- Tattoo on the scalp
- Computerized embedding in media data (e.g. for copyright)

Steganography permits an unobservable (and therefore confidential) communication

Structure of a Steganographic System



cover-object

message to embed

stego-key

embedding

sender

stego-object

network

stego-key

extraction

cover-object

extracted message

receiver

Properties

- Message will be embedded in a cover-object (carrier)
- Modification of the cover-object is hardly perceptible
- Modifications aren't verifiable by measuring methods
- Nobody is able to show the embedding message without the key (secret) in spite of knowing the algorithm (Kerckhoffs' Principle)
- symmetric and asymmetric schemes

Technological view: Steganography is not the encryption of data

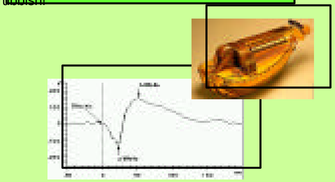
Cryptography: plain text ⇒ f ⇒ cipher text

Steganography: cover ⇒ g ⇒ cover*

Steganography ⇔ Cryptography

Stego-data are inconspicuous. Steganography will **not be detected**.

George obtains oranges yet eights' are rubbish!



Encrypted messages are conspicuous. They will be detected as ciphertext or silly data.

```
hIwDIwFpbAtjdf0BA/9KBX2jS17O5SRQsu2PF
caBqUXlQdyt1Fri/Wsg+eXoYsxnJI1Cn2JD7vjI
F2GH8GEr/vGQk8SQVCMyXzfPkgW0tr6RJX
AEIFF9rjnDB3kOmmVc1adrTQnLrqiC/l5r/xUs
ezowgZl82T/QVk59YsuChd+Ce8vqI/kICeqmv
w9J2amre3uxpWlOqCEQNzZyHx8HeYPf29k
Xu+uk1gekZZVdELmLD/Wa/xBKFTNUBrl+16
ewoQBxQ8+3cTXSIGPTqdzDSasgQG17Z1sr
/Lhu0qzcm64GYY0OukeiCPvhHJQuXZn2UW
```

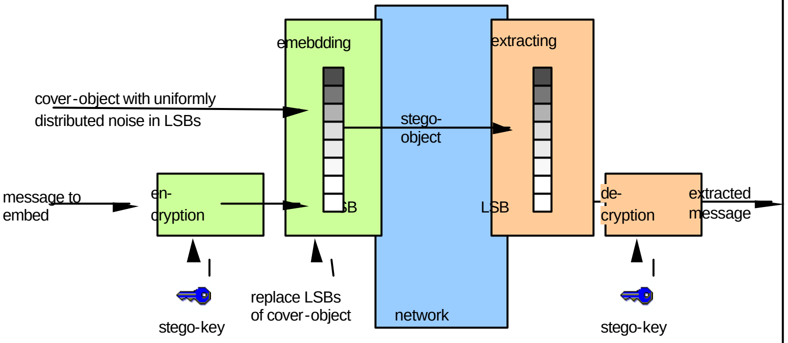
Question: Key/Algorithm?

George obtains oranges daily yet eights' are rubbish!

- What is the key?
- What is the algorithm?

Embedding in LSB

most used method: embedding in **L**east **S**ignificant **B**it



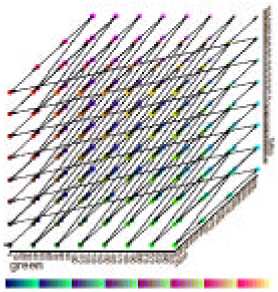
H. Federrath, G. Wicke: Vertrauliche Kommunikation mit Steganographie, PIK 3/97

Embedding in a GIF Image

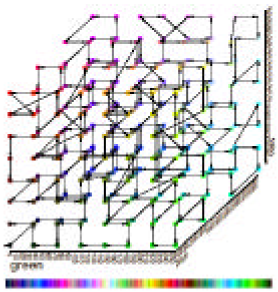
- GIF image = palette with 256 color
  + matrix of color indices (image)
- Every pixel is one entry in palette
- Palette remains unchanged
- Algorithm:
  1. Copying original palette
  2. Sorting copied palette
  3. Mapping original color indices to sorted color indices (bijective)
  4. Embedding steganographic value in LSB by replacing colors

Copying and Sorting Palette

Original



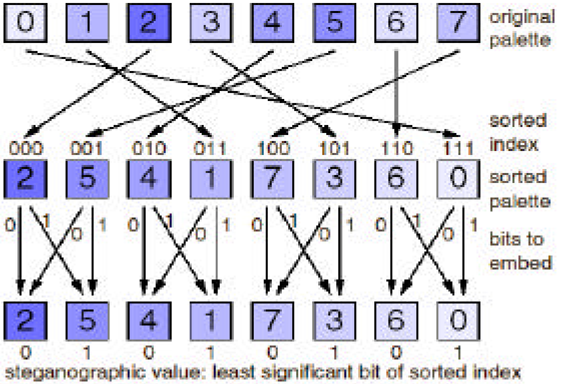
Sorted



- Every color is a point in the RGB grid
- Sorting color indizes by their distance

A. Westfeld, A. Pfitzmann: Attacks on Steganographic Systems, 1999

Embedding Steganographic Value

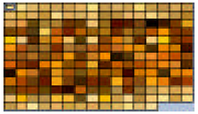


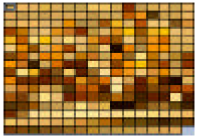
steganographic value: least significant bit of sorted index

A. Westfeld, A. Pfitzmann: Attacks on Steganographic Systems, 1999

Example: Embedding in a GIF Image

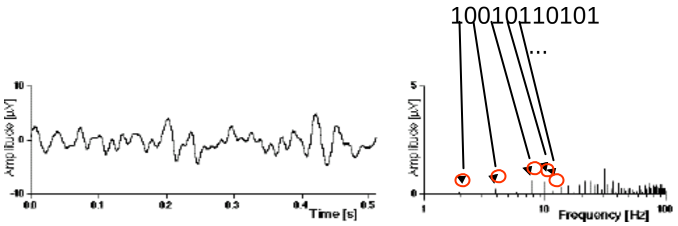
- GIF-Image, 25KB, 12KB text document embedded (S-Tools 4.0)





Embedding in Frequency Domain

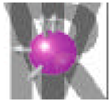
- Fast fourier transformation of a signal
- Coding message in certain frequencies (LSB of amplitude)
- Reverse transformation into time domain



Cover-Object: Conditions

- Cover-object contains randomness
- Don't reuse cover-objects
- Destroy cover-object after use
- "Empty" cover-object mustn't be public (cover-stego attack)
- Cover-object has to be suitable:
  - scanned images, filmed videos, recorded music with a microphone
  - no vector graphic
  - no digital generated (audio) documents

good



bad

Comparison: Scanner / Steganography

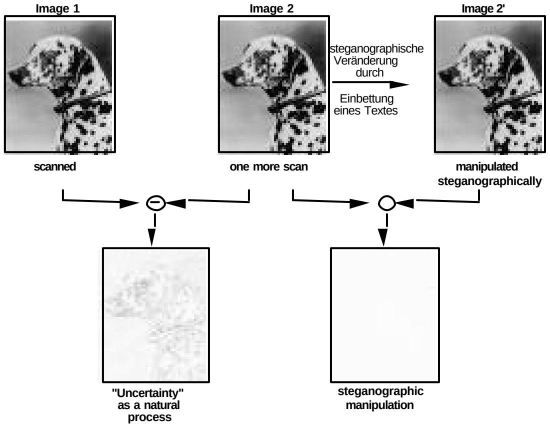


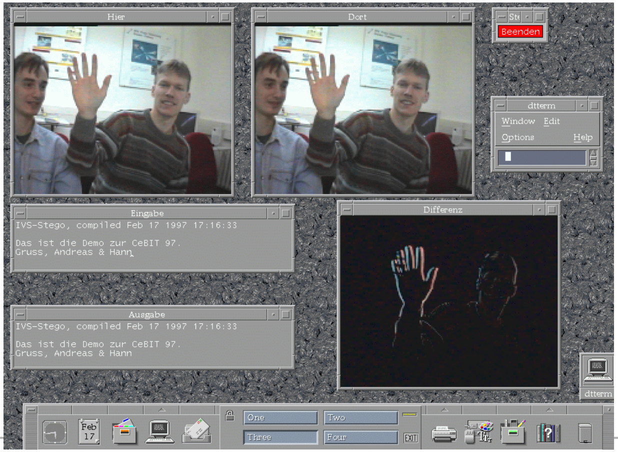
Image 1
Image 2
Image 2'
steganographische Veränderung durch Einbettung eines Textes
scanned
one more scan
manipulated steganographically
"Uncertainty" as a natural process
steganographic manipulation

H. Federrath , G. Wicke: Vertrauliche Kommunikation mit Steganographie, PIK 3 /97

Mix of Media

- Various tools for different media
  - Images (EzStego, Steganos, S-Tools, Jsteg, F5)
  - Video (F5)
  - Text (Texto, SpamMimix, WBStego99)
  - Audio (Steganos, S-Tools, MP3Stego)
- Mixing media or using same media
- Cover-object >> message to embed
- Capacities:
  - video stream: compressed telephone conversation (about 10 kbit/s)
  - scanned images: about 1% of image size

Steganography in Video Conference



Eingabe

```
IVS-Stego, compiled Feb 17 1997 17:16:33

Das ist die Demo zur CeBIT 97.
Gruss, Andreas & Hann
```

Ausgabe

```
IVS-Stego, compiled Feb 17 1997 17:16:33

Das ist die Demo zur CeBIT 97.
Gruss, Andreas & Hann
```

Demonstrator des Kollegs "Sicherheit in der Kommunikationstechnik" auf der CeBIT '97

Attacks: Objects and Types

- **Compromising steganographic tools has two stages:**
  - Identifying the embedded communication
  - Extracting the embedded message
- No formal proof of security up to now

Steganographic system	**Cryptographic system**
stego-only-attack	ciphertext-only-attack
cover-stego-attack	known-plaintext-attack

Quality of Steganographic Software

Available tools:

- often bad (public domain)

What distinguishes good steganographic tools?

- Algorithm is publicly known
- Parameterization by steganographic key
- Finding and making use of "natural uncertainty"(e.g. noise)

Regulation of Cryptography

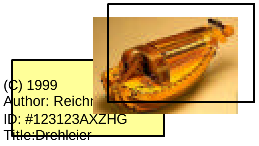
- Ban on strong cryptography planned (former minister of interior Kanther, 1997)
- Problem of control
- Has no effect if steganography is used
- Meanwhile government's opinion has changed
- Supporting of strong cryptography (e.g. gnupg)
- Preventing industrial espionage

Protecting Digital Documents

- Digital data can be copied easily and without loss
- Fetching data can be protected by a password
- Spreading cannot be prevented
- Embedding copyright message in document
- Example: TV station's logo on TV channel
- Applications with watermarking functionality: looking for a watermark in documents (e.g. Adobe Photoshop)

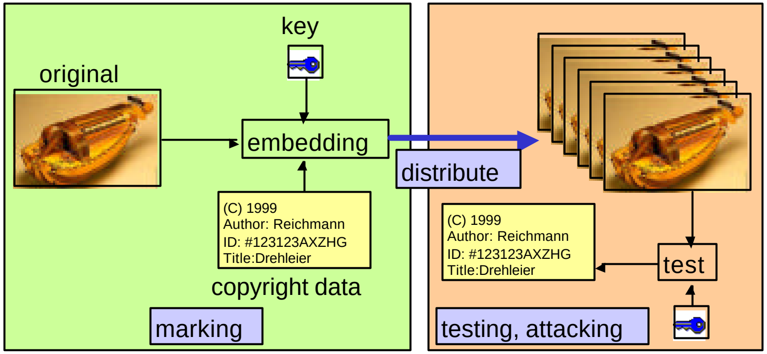
Watermarking

- Digital "watermark"
- Copyrighting digital documents
- Prosecuting copyright violaters
- Use: music, movies, images, ...
- Watermarks are impercetible or visible
- Additional property: Robustness



Watermarking

Embedding of copyright data, no reversible



key

original

embedding

distribute

(C) 1999
Author: Reichmann
ID: #123123AXZHG
Title:Drehleier

copyright data

marking

(C) 1999
Author: Reichmann
ID: #123123AXZHG
Title:Drehleier

test

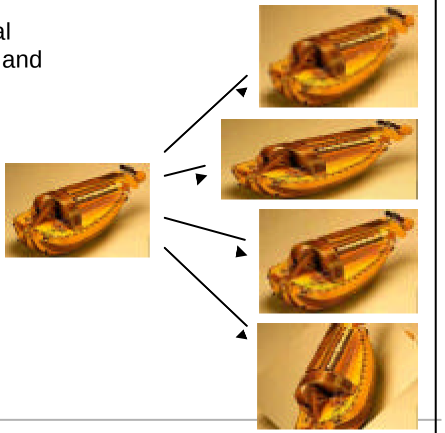
testing, attacking

Steganography ⇔ Watermarking

	Steganography	Watermarking
Object	• Unobservable, confidential communication	• Protecting authorship
Attack	• No modification of stego-object • Identifying communication • Extracting embedded message	• Massive modification of cover-object • Destroying/Changing embedded copyright data
Properties	• Embedding as much data as possible • No Precautions against destruction of cover-object • Not **verifiable** without stego-key	• Few data to embed • Data has to be embedded robust • Resistent to compression, etc. • Redundant embedding of copyright data • Embedded data is **inperceptible** • According to algorithm copyright data is not **verifiable** without key

Watermarking: Attacks

- Digital-to-analog-to-digital conversion (e.g. printing and scanning)
- Re-Sampling
- Compression
- Dithering
- Rotation (e.g. through 1 degree)
- Translation
- Cropping
- Scaling



Watermarking: Miscellaneous

- Similar algorithms to steganography
- Embedding in time and/or frequency domain
- Spread spectrum technology
- All known methods are easy to compromise
- In contrast to steganography very interesting and importing for economy (media corporation)

Further Information

- Steganography
  - Fabian A.P. Petitcolas, Ross J. Anderson and Markus G.Kuhn. Information Hiding – A Survey, *Proceedings of the I.E.E.E.*, 87(7):1062–1078, July 1999.
    http://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf
  - Andreas Westfeld: Visual and statistical attacks
    http://www.inf.tu-dresden.de/~aw4/
- Watermarking
  - Joachim Eggers: Digital Watermarking (Papers)
    http://www-nt.e-technik.uni-erlangen.de/~eggers/publications.html
  - André Adelsbach and Ahmad Sadeghi. Zero-Knowledge Watermark Detection and Proof of Ownership, *Information Hiding 2001*, LNCS 2137: 273–288, 2001.
- Portal and Tools
  - Uni GH Siegen: Steganographie
    http://www.uni-siegen.de/security/stegano.php
  - c't - Krypto-Kampagne - Steganographie
    http://www.heise.de/ct/pgpCA/stego.shtml