

Steganography



<https://iuk.one/1033-1032>

Clemens H. Cap
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of Rostock
Rostock, Germany
clemens.cap@uni-rostock.de

Version 2



Historical Cases of Steganography

Hair Steganography

- Tattoo a message onto the scalp of a slave
- Let hair grow over the message

Secret Ink Steganography

- Write message with lemon juice
- Let it dry - difficult to read
- Heat it near the fire - it turns black

A First Example

Cover Medium

Fishing freshwater bends and saltwater coasts reward anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyway.

Cover Medium with Hint to Hidden Information

Fishing freshwater bends and saltwater coasts reward anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyway.

Hidden Information

sendlawyersgunsandmoney

Mechanism: Message encoded in the third position of every word.

Steganography means:

Communicating partners have a better theory of noise than the steganalyst.

All media where there is room for randomness.

Examples:

- Text
- Images
- Video
- Audio
- Binaries
- Protocols and Behaviour

Textual Example

Normal Text

This is just a simple message consisting of some text.

Blank Modulation

This is just a simple message consisting of some text.

Blanks at position 2, 5 and 8.

Error Modulation

This is Just a siemple message consisting off sam text.

Typos at positions 3, 5, 8 and 9.

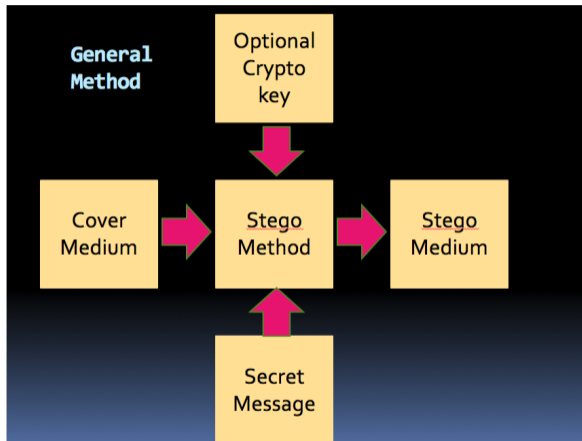


Fig. 1: General Steganographic Scheme

Image Steganography



Fig. 2: The image of the cat is hidden in the (noise of the) image of the tree.



Fig. 3: Showing only the most significant bit (MSB) of an image.

4-bit Extraction



Fig. 4: Showing only bit number 4 of an image.

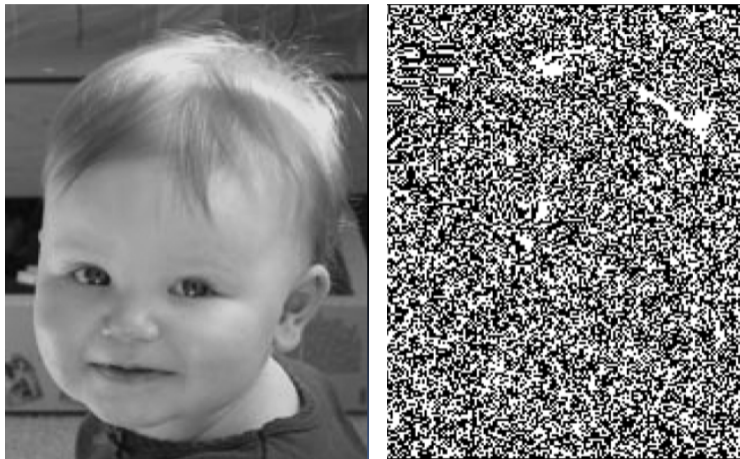


Fig. 5: Showing only the least significant bit (LSB) of an image.

General Strategy:

- Change the least significant bit(s) to the value of the secret.
- There is practically no effect on the human perception.
- Works with many media types (audio, video, image).

Question: Can this be detected?

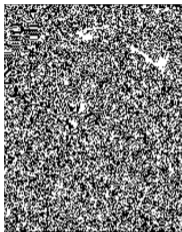


Fig. 6: Is this noise or does it contain a steganographic message?

Can we detect, if an original media file has been tampered with?

Answer: Depends on the amount of hidden information.

If too much is embedded: Yes

Remaining issue: Use of cryptography.

Type of medium:

- Video: 3 dimensions of correlation
- Still: 2 dimension of correlation
- Audio: 1 dimension of correlation

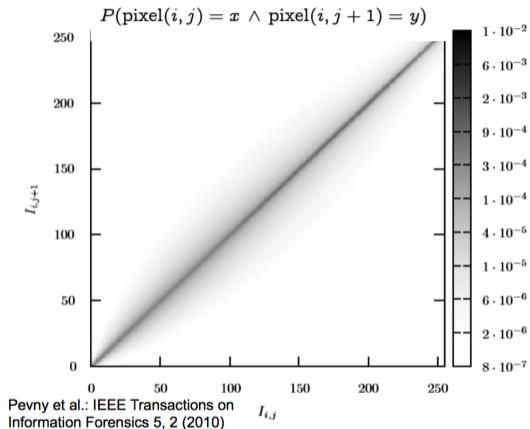


Fig. 7: Steganalysis in Images

Steganography in Audio Streams (1)

LSB Encoding:

- Adapt the LSB of the audio signal
- Produces 1 bit stego per 8 bit or 16 bit audio
- Approximately 10% of the data stream
- Typical audio stream is 44kbps
- Provides some 2-4 kbps stego channel

Echo encoding:

- Audio streams have an echo.
- Human ear is bad in detecting changes in echo.
- Modulate amplitude, decay rate and delay time of the echo.

Phase Coding:

- Break sound stream into short segments.
- Do an FFT and calculate phase of each segment.
- Set the phase of the first segment (this is the secret).
- Adjust the phase of the subsequent segments.
- Do this on several parts of the stream.

Steganography in Audio Streams (2)

Stereo Coding:

- Use subtle differences in left and right channel
- Change amplitude and phase in the channels
- Modulate the position of the speaker

Psychoacoustic Model Parameters:

- MP3 tampers with WAV for compression purposes.
- Utilize the same tampering strategy without using exact MP3 algorithm.

Direct Sequence Spread Spectrum (DSSS) Approach:

- Take high frequency random noise sequence
- Use it inverted or normal as additional noise signal
- Very robust against filtering and processing
- Adds some noise to the signal

Robustness against common processing:

- Resampling
- Recoding
- Compression
- De-noising

Degrading audio quality

Acoustical Steganalysis (1)

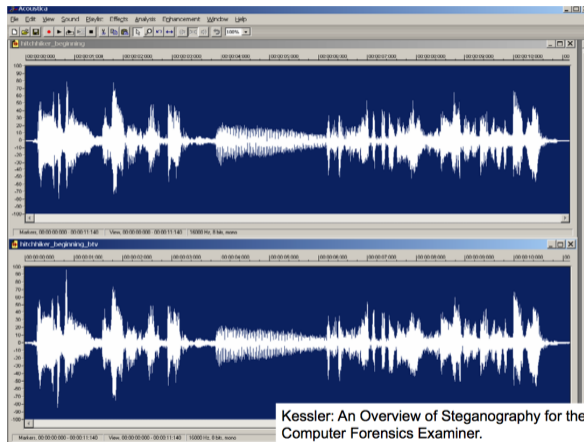


Fig. 8: Spectrogram of cover medium and of medium with hidden information

Acoustical Steganalysis (2)

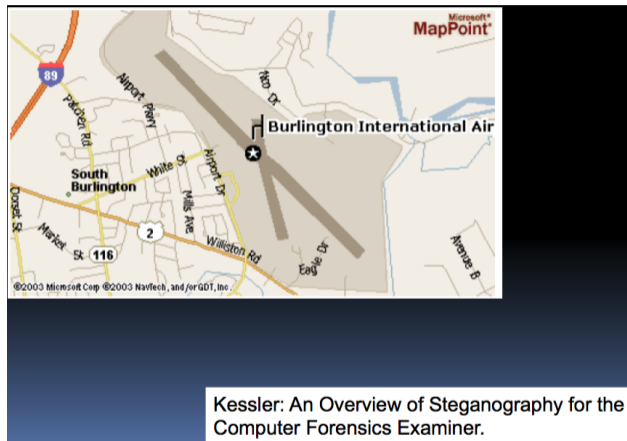


Fig. 9: Information hidden in the audio stream

Possibilities:

- Big variety, depending on what the text is.
- Usually sufficient to encode a serial number into the file.

Examples:

- Shift lines, shift words.
- Different fonts or attributes.
- Spelling mistakes, punctuation, spacing.
- Old or new, american or british writing style.
- Semantic variations.
- Begin every enumeration with longest or shortest word.
- ...

Counter-specification behaviour

Eg: Fields which should be zero are not zero

Coice of means

Use different techniques for the same goal

Timing

Issue a request on full second or 500ms later

Sequence of doing things

Ftp download files in specific permutation

Modulate ressource usage in time

Make some request appear to be serviced slower

Steganography and Watermarking

Steganography: Covert communication

- Application: Hidden (covert) communication for information exfiltration.
- Goal 1: Efficiency: Embed a large hidden message.
- Goal 2: Stay secret: Cannot be detected by third party.

Watermarking: Want to encode copyright message or buyer id

- Application: Document marking, copyright, leak detection.
- Goal 1: Permanency: User cannot remove easily.
- Goal 2: Robustness: Remains readable during all possible typical transformations of the over medium.
- Non-goal: Does not always have to stay secret.

Chaffing and Winnowing: Authentication can emulate encryption

- There is information and noise.
- Information is singled out by authentication.

Steganography: Covert communication

- There is information and noise
- Information is hidden in the what otherwise may be considered noise or coincidence

Appendix

Contents of Appendix

Terms of Use



Citing This Document



List of Slides



List of Figures

Terms of Use (1)

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das **Zitatrecht** in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise **Par 60a UrhG** ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions <https://github.com/logos> to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status nicht oder nur mit unverhältnismäßig hohem Aufwand abzuklären ist. Ebenso kann den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen, obwohl deren Leistungen genutzt werden.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 ([Pressemitteilung](#), [Blog-Beitrag](#), [Urteilstext](#)). ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungs- und Anreizsystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepasste Vergütungs- und Anreizsysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz [hier](#) und [hier](#) oder [hier](#).

Citing This Document

If you use contents from this document or want to cite it, please do so in the following manner:

Clemens H. Cap: Steganography. Electronic document. <https://iuk.one/1033-1032> 24. 4. 2023.

Bibtex Information: <https://iuk.one/1033-1032.bib>

```
@misc{doc:1033-1032,  
  author      = {Clemens H. Cap},  
  title       = {Steganography},  
  year        = {2023},  
  month       = {4},  
  howpublished = {Electronic document},  
  url         = {https://iuk.one/1033-1032}  
}
```

Typographic Information:

Typeset on ?today?

This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2

This is pgf in version 3.1.5b




This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

Title Page	1
What is Steganography?	2
Historical Cases of Steganography	3
A First Example	4
Media Suitable for Steganography	5
Textual Example	6
Core Problems of Steganalysis	7
GeneralScheme	8
Image Steganography	9
MSB Extraction	10
4-bit Extraction	11
LSB Extraction	12
LSB Embedding	13
Steganalysis	14
Steganalysis	15
Steganalysis in Images	16

Steganography in Audio Streams (1)	17
Steganography in Audio Streams (2)	18
Problems of Audio Steganography	19
Acoustical Steganalysis (1)	20
Acoustical Steganalysis (2)	21
Textual Steganography	22
Binary Steganography	23
Protocols and Behaviour	24
Steganography and Watermarking	25
Steganography and Chaffing & Winnowing	26

Legend:

-  continuation slide
-  slide without title header
-  image slide