

Faculty of
Mathematics and
Computer Science

Network Steganography

01731

Introducing Myself

Positions:

- *Lecturer (Lehrbefugter/Privatdozent)*, Faculty of Mathematics & Computer Science, FernUniversität in Hagen, Germany
- Professor of Computer Networks and Information Security at Hochschule Worms, Germany
 - Scientific Director, Centre for Technology & Transfer (ZTT), HS Worms (previously several years as Scientific Co-director)
- Previously: Head of a research team on smart building security at Fraunhofer FKIE, Bonn, and Associate Researcher at a German-New Zealand research project of HS Augsburg, U Augsburg and U Waikato

Education:

- Habilitation (Dr. habil.) in CS (2020), University of Hagen, Germany
- Ph.D. (Dr. rer. nat.) in CS (2013), University of Hagen, Germany
- M.Sc. in CS (2011), Univ. Appl. Sc. Augsburg, Germany (enrolled in parallel at University of Hagen) and Dipl.-Inf.(FH) (2009), Univ. Appl. Sc. Kempten, Germany.




Primary research interests:

- Network Information Hiding/Covert Channels
- IoT/Smart Home/Smart Building Security
- Operating Systems (+Security) / Linux & BSD, author of some German Linux books
- Methodology of Information Security (IWSMR) & Scientometrics

Overview of this Course

1. Introduction to **steganography** and **covert channels**
2. Introduction to local covert channels
3. Introduction to generic countermeasures (not network-specific)
4. Fundamental network information hiding techniques
5. Getting the big picture: **hiding patterns**
6. Staying under the radar: sophisticated hiding methods
7. Selected countermeasures
8. Replicating experiments for scientific advancement
9. OMG! I found a new hiding method. How to get famous?!?
a.k.a. How to describe a new hiding method in a paper?
10. My smart fridge does strange things ...
a.k.a. Steganography in the Internet of Things (IoT)
11. Overall conclusion



Partial overlap with class
01730 "Introduction to
Information Hiding".

NETWORK INFORMATION HIDING

CH. 1: INTRODUCTION

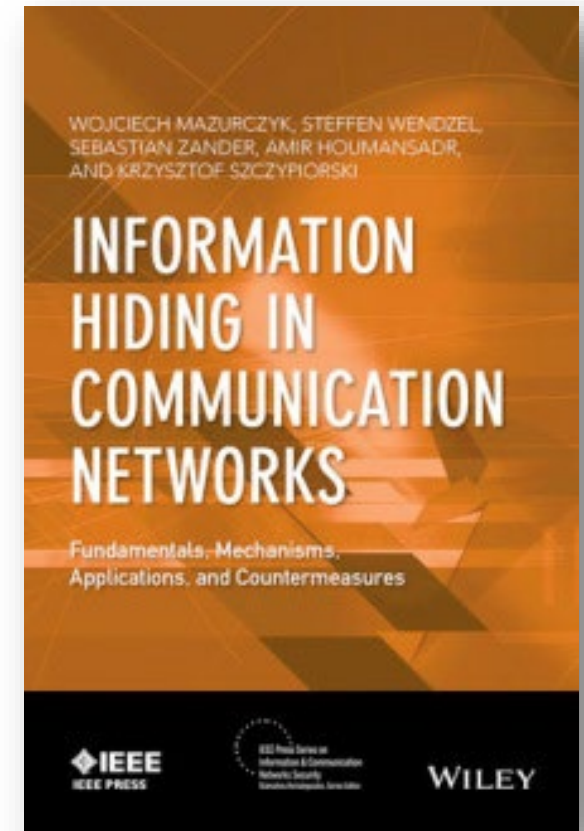
Prof. Dr. Steffen Wendzel

<https://www.wendzel.de>

Book Recommendation

Several content of this lecture is based on our book on Information Hiding in Communication Networks (Wiley-IEEE, 2016).

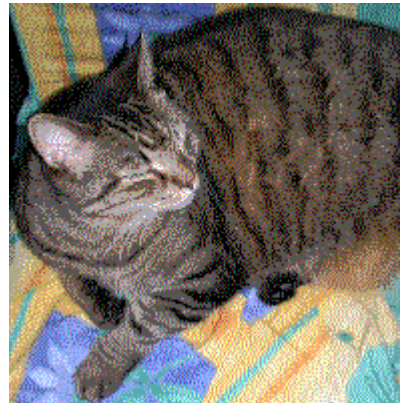
- This book is optional and not required for this class. It should be **freely downloadable via IEEEXplore if you are an IEEE member** (or: if your university is a member).
- Community agreed on common understanding of many terms to find a good basis for this book.
- Based on several years of research of the authors.
- Please note: the topics traffic obfuscation and network flow watermarking are not covered in this class.



Information Hiding: What is it?

Only a brief introduction as the fundamentals of information hiding are covered by the other part of this module.

What is „Information Hiding“? Two different examples:



All figures taken from Wikipedia articles on ‚Steganography‘ and ‚Watermarking‘

Information Hiding: What is it?

Fundamental Taxonomy on Information Hiding by Petitcolas et al. [1]

Note: I will later show different taxonomies specific to Network Information Hiding

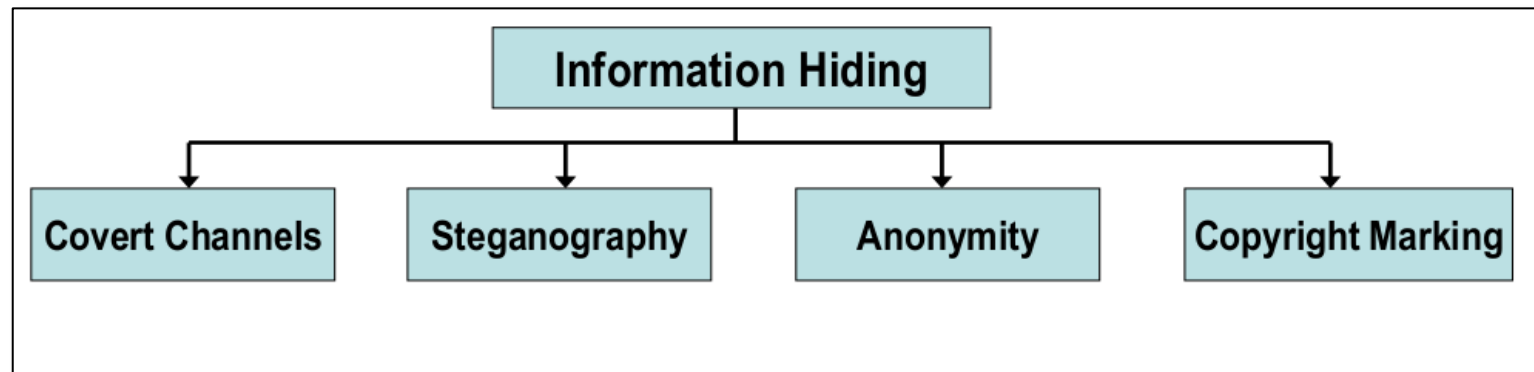


Fig.: [2] (but based on [1], where an extended taxonomy featuring linguistic/technical steganography and different types of copyright marking can be found).

[1] Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, 87(7), 1062-1078.

[2] Mazurczyk, W. et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016.

Information Hiding: What is it?

... it appeared in ancient Greece.

499 BC: **Histiaeus** (ruler of Miletus) tattooed a message on the head of one of his slaves to send a message to Aristagoras (his son-in-law) to instruct him to revolt against the Persians.

(Several more cases of Steganography in ancient Greece are known.)

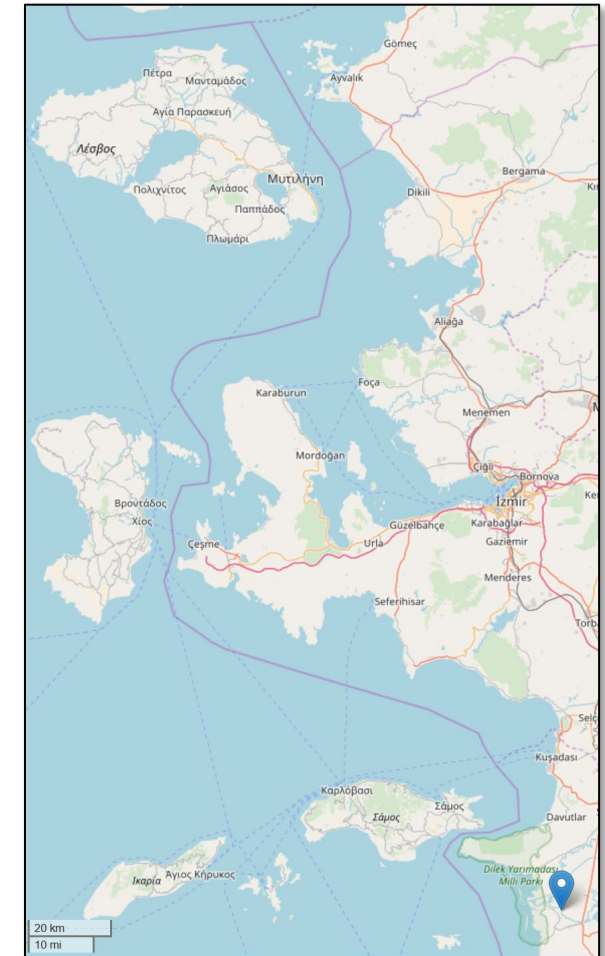


Image taken from Google Maps.

Information Hiding: What is it?

Another example:

1978 World Championship in chess between Viktor Korchnoi (CH/RU) and Anatoly Karpov (RU)

Officials „limited Karpov to consumption of only one type of yogurt (violet) at a fixed time during the game.“ [1]

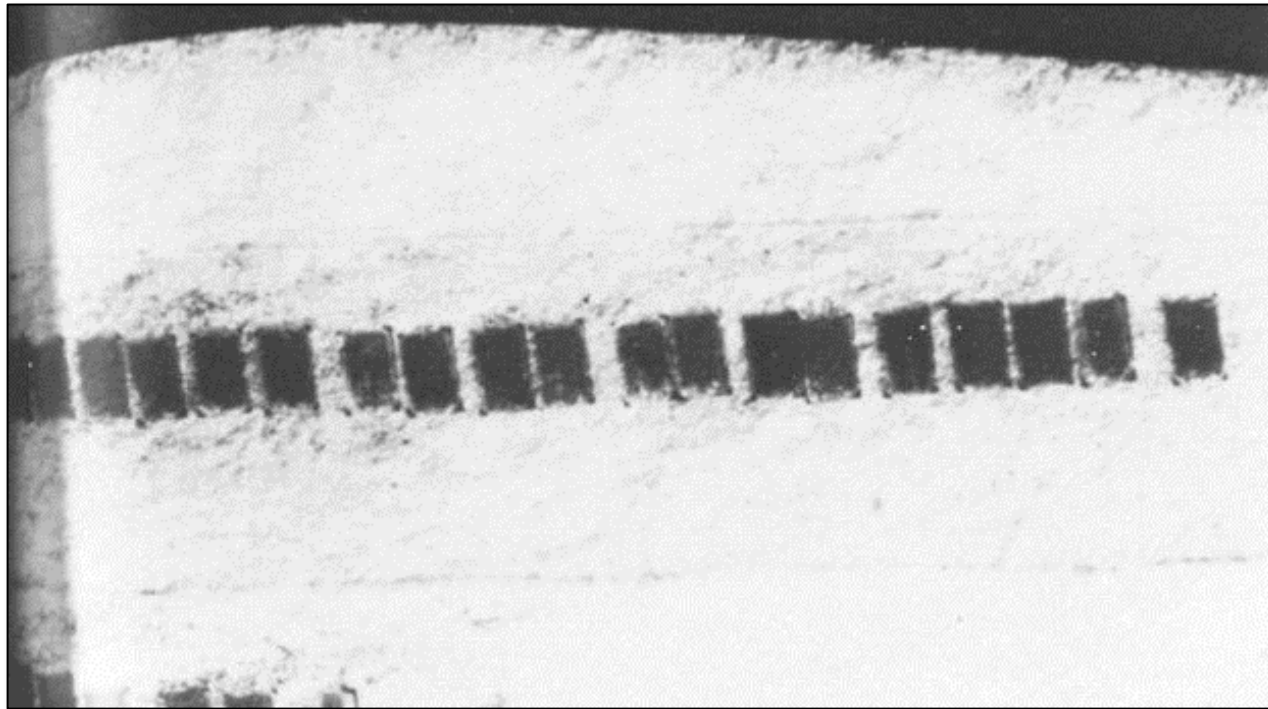


Fig.: private photo

[1] Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010.

Information Hiding: What is it?

Another example: Microdots; used during WW2, e.g. by German spies in Mexico.



NSA photo of microdots used by German spies, source: Wikipedia, author: unknown

Information Hiding: What is it?

Another Example: Printer Watermarking

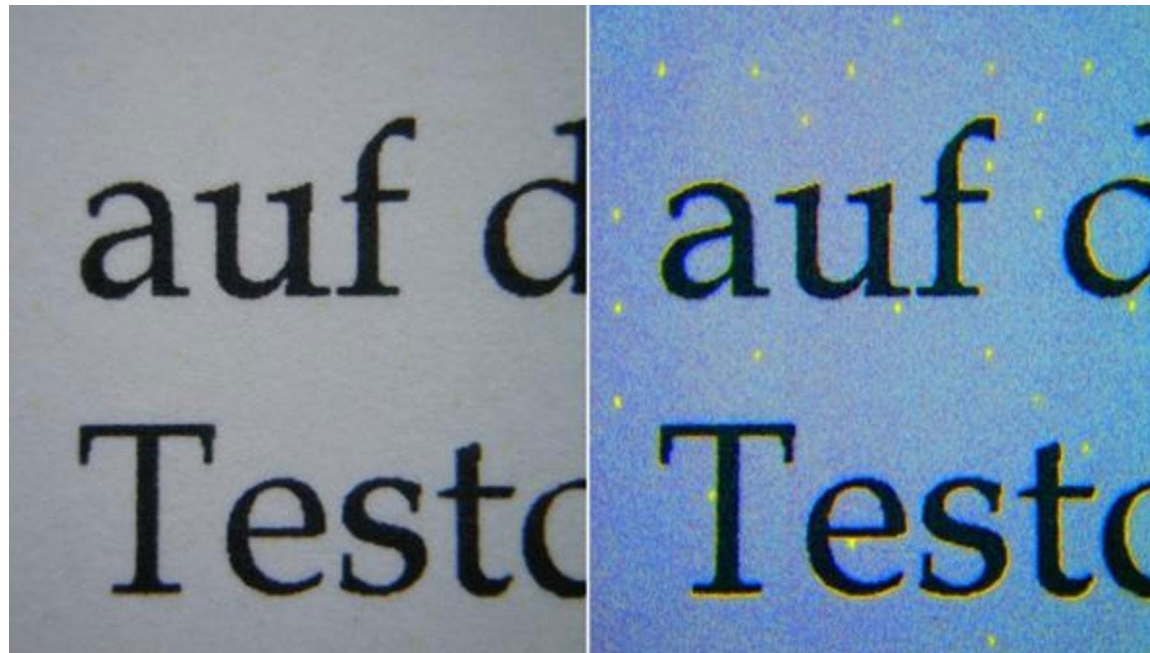
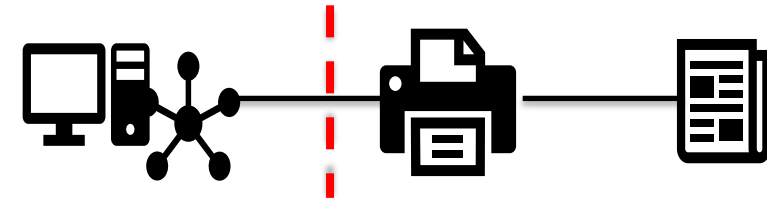
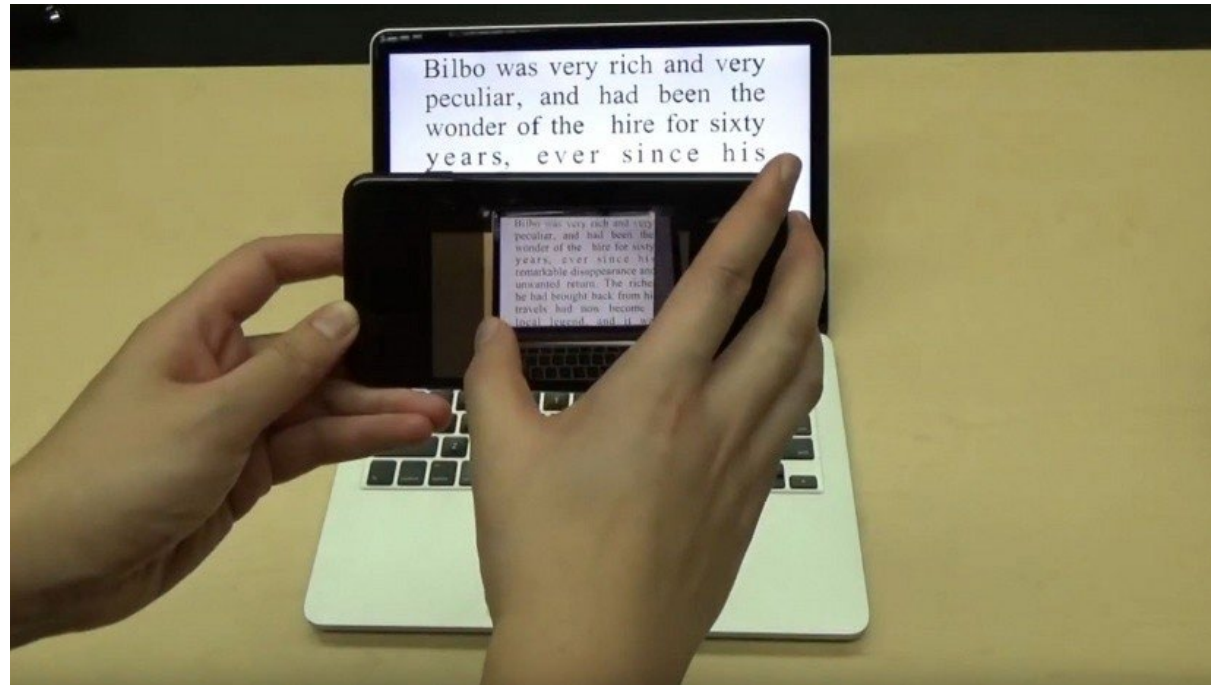


Fig. source/attribution: F. Heise/Wikipedia/BBC

Information Hiding: What is it?

Final example: *fontcode* (works with digital and printed documents)



Video: <https://youtu.be/dejrBf9jW24>

History of Information Hiding

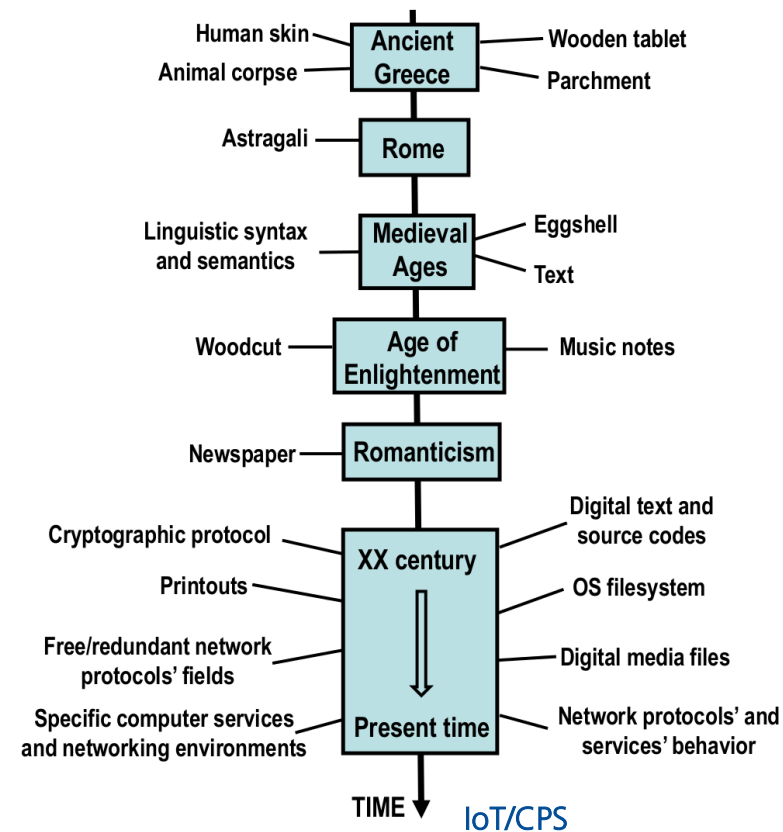


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

History of Information Hiding

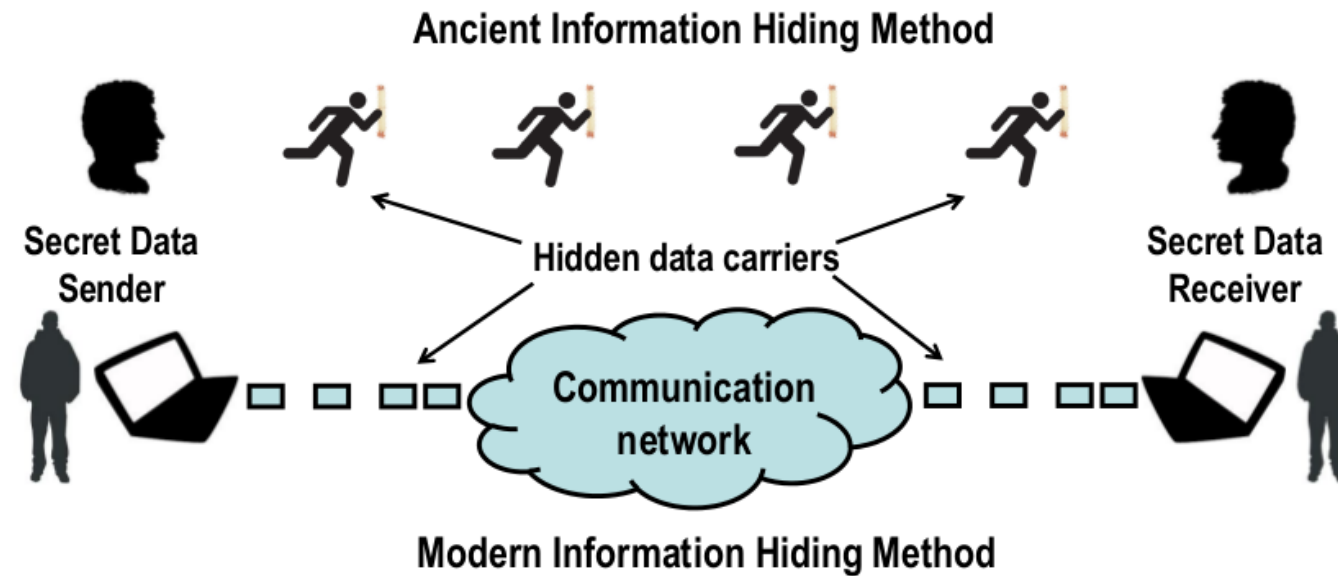


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Covert Data Storage and Transfer

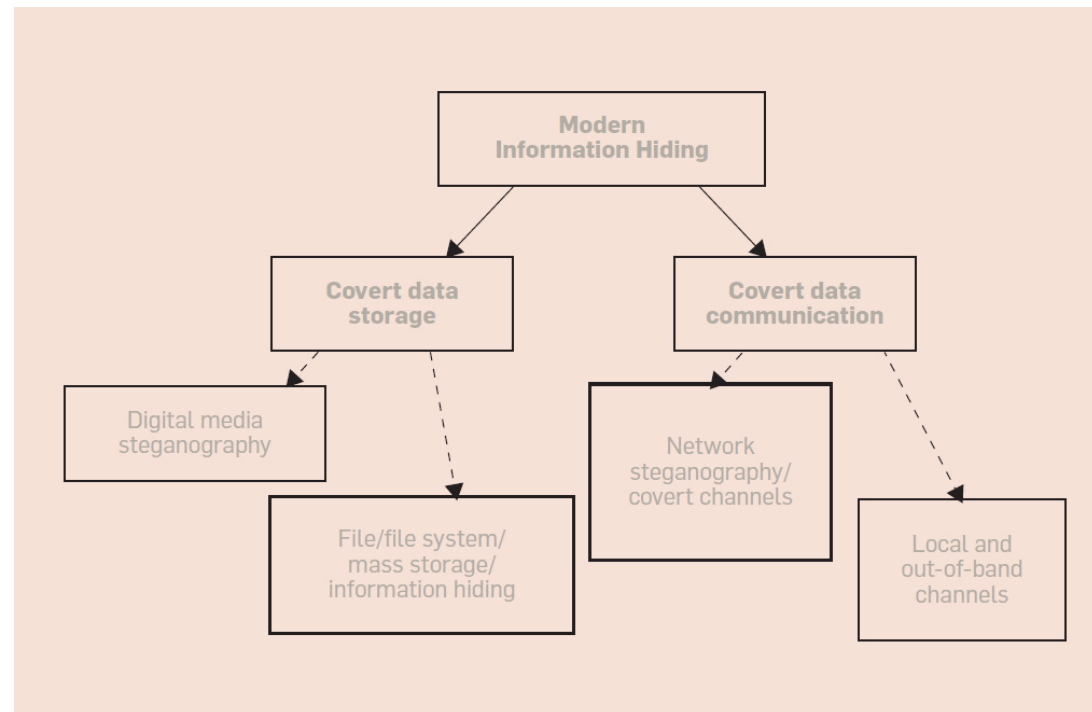


Fig.: W. Mazurczyk, S. Wendzel: [Information Hiding: Challenges for Forensic Experts](#), Comm. ACM, 2018.

Application of Hiding Techniques

What is the big difference between digital media and network carriers?

| Feature/Type of the carrier | Digital media | Network traffic |
|--|---|--|
| Method's capacity/ bandwidth | Limited by the type of the digital media and the size of a file | Limited by the type of the traffic and the length of a transmission |
| Hidden data embedding | Cannot exceed file capacity | Can be slow but continuous over longer period of time |
| Data hiding application | Covert storage | Covert communication |
| Nature | Permanent | Ephemeral |
| Clues for forensic analysis | Can be available for forensic experts after transmission | Often not available when transmission ends |
| Method's detectability | Easy only if an original file is available | Hard due to different forms of acceptable traffic and varying network conditions |
| Cost of applying data hiding | Decrease in digital media quality | Increased delays, raised packet loss level, reduced feature set of protocols and/or affected user transmission quality |
| Robustness (secret data resistance to modifications) | Typically cannot survive conversion to another format | Typically vulnerable to dynamically changing network conditions |

Fig.: W. Mazurczyk, S. Wendzel: [Information Hiding: Challenges for Forensic Experts](#), Comm. ACM, 2018.

Basic Mimicry System [1]

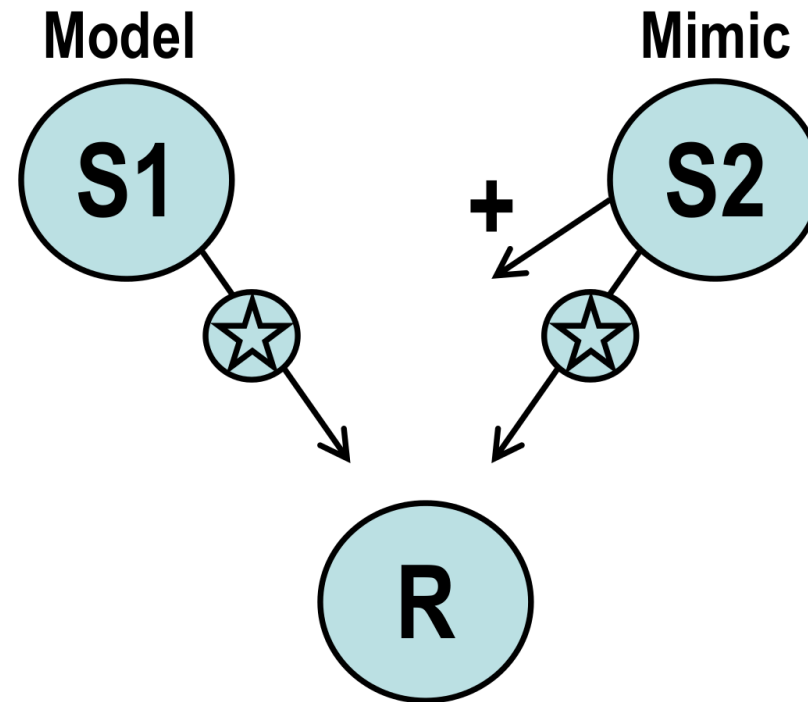


Fig.: [2]

[1] Vane-Wright, R. I.: A unified classification of mimetic resemblances, Biological Journal of the Linnean Society, 1976.

[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Terminology: Prisoner's Problem (Simmons, 1983)

- Covert Channel definition by Lampson [1]: *"...not intended for information transfer at all"*

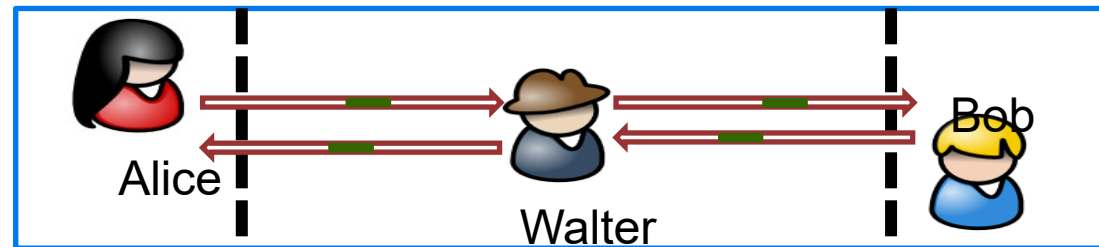
A covert channel without intention is a **side channel**

DoD defined it differently: CCs break a security policy (usually in MLS) [2]

- Steganography [3]:

"Steganography can be informally defined as the practice of undetectably communicating a **message (a.k.a. steganogram)** in a **cover object**."

- Prisoner's Problem by Simmons [4]:



[1] Lampson, B.W.: A Note on the Confinement Problem, Comm. ACM, 1973. |||

[2] DoD: Trusted Computer System Evaluation Criteria (TCSEC), Department of Defense, 1985. |||

[3] Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010. |||

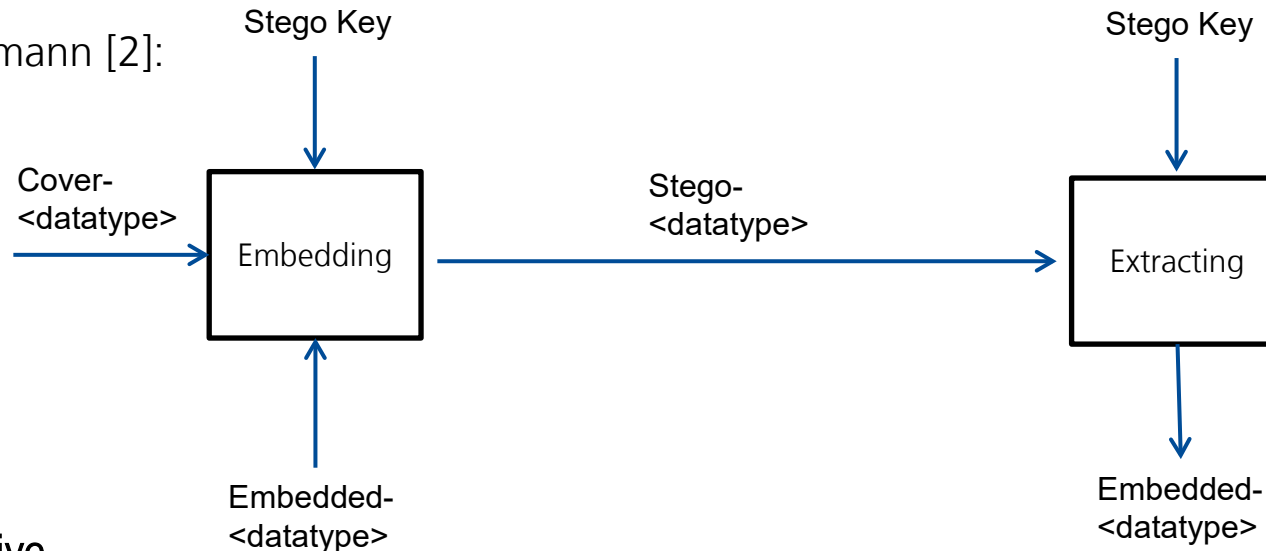
[4] Simmons, G. J.: The Prisoners' Problem and the Subliminal Channel, in Proc. Crypto'83 – Advances in Cryptology, 1984.

Terminology

- Remember [1]:

“Steganography can be informally defined as the practice of undetectably communicating a **message (a.k.a. steganogram)** in a **cover object**.”

- Terminology of Pfitzmann [2]:



- This process is **bijective**

[1] Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010.

[2] Pfitzmann, B.: Information Hiding Terminology, Proc. 1st Information Hiding Workshop, Springer, 1996.

Terminology

- Walter is referred to as a **warden**. He performs a so-called **steganalysis**.
- A warden can be [1]

Passive

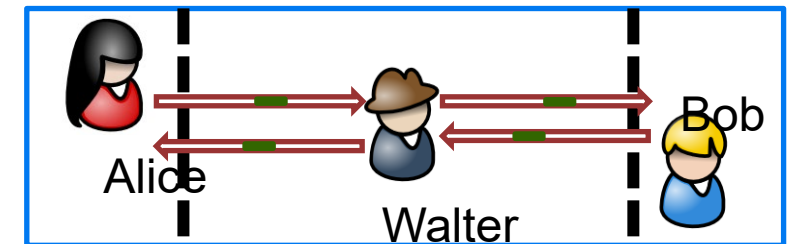
tries to detect the presence (and content) of a hidden message in a cover object and tries to determine who is involved in the steganographic communication

Active

modifies the cover object (e.g. removes or replaces steganogram)

Malicious

can introduce own messages to fool involved participants (e.g. message spoofing)



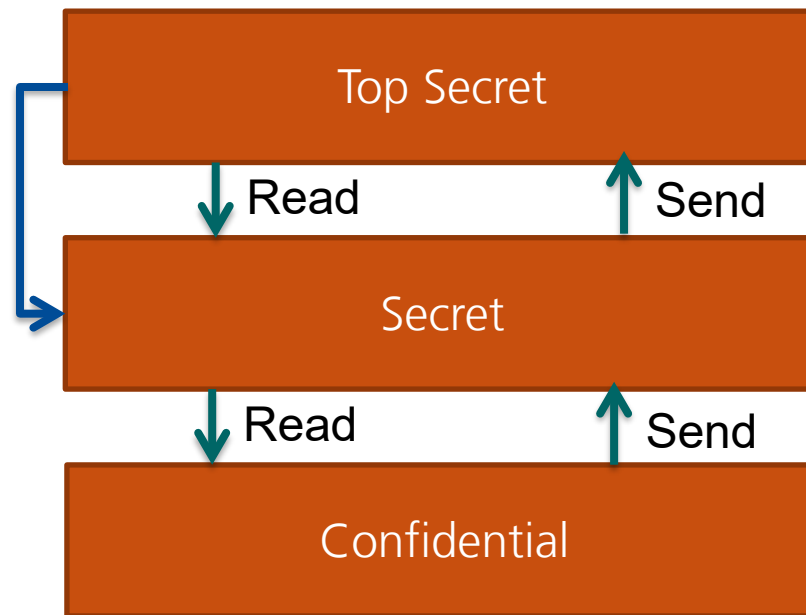
[1] Fisk, G., Fisk, M., Papadopoulos, C. and Neil, J., 2002, October. Eliminating steganography in Internet traffic with active wardens. In *International Workshop on Information Hiding* (pp. 18-35). Springer, Berlin, Heidelberg, 2002.

DoD Definition of Covert Channels in MLS Context

In classical papers, a covert channel either violates the NRU (no read-up) or the NWD (no write-down) rule of the Bell-LaPadula (BLP) Model.

Example:

Sending data
to „Secret“
level)



Reading data
from „Secret“
level

cf. DoD: Trusted Computer System Evaluation Criteria (TCSEC), Department of Defense, 1985 and works on the BLP.

Is it applied in practice?

Early cases:

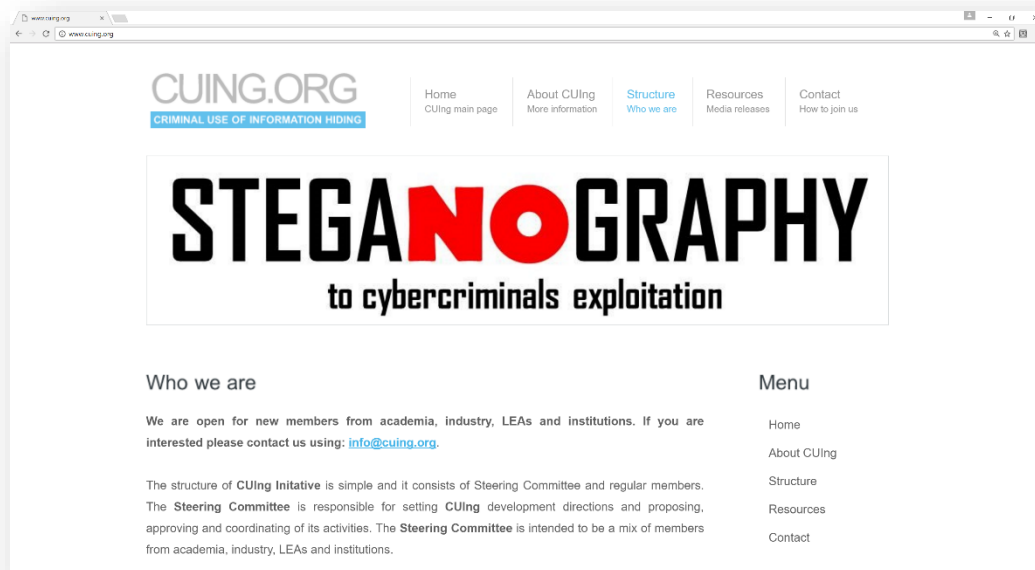
- **2002:** „Operation Twins“ culminated in the capture of criminals associated with the „Shadowz Brotherhood“ group, a world-wide Internet pedophile organization.
 - Digital image steganography was used to hide a pornographic file within another innocent-looking one.
- **2008:** Unknown person smuggled sensitive financial data out of U.S. Department of Justice using image steganography.
- **2010:** Russian spy ring leaked classified information via image steganography from USA to Moscow.
- **2013:** Linux Fokirtor malware hides traffic in SSH connections
- **Since 2014:** heavily increase in (Network) Information Hiding-capable malware, so-called **Stegomalware**

Sources:

Cases 1-3: Zielinska, E., Mazurczyk, W., Szczypiorski, K: Trends in steganography, Comm. ACM, 2014.

Case 4: Schneier, B.: Fokirtor, <https://www.schneier.com/blog/archives/2013/11/fokirtor.html>, Nov. 2013.

Is it applied in practice?



cf. W. Mazurczyk, S. Wendzel: *Information Hiding. Challenges for Forensic Experts*, Communications of the ACM, 2018.

Kabaj et al.: *The new Threats of Information Hiding: The Road Ahead*, IEEE IT Prof., Vol. 20(3), 2018 (Tab., r.).

Several more recent cases of stego-malware are covered in L. Caviglione, W. Mazurczyk: *Never Mind the Malware, Here's the Stego-malware*, IEEE Security & Privacy Magazine, Vol. 20(5), 2022.

| Malware/exploit kit | Information-hiding method | Purpose |
|---------------------|---|--|
| Vawtrak/Neverquest | Modification of the least significant bits of favicons | Hiding URL to download |
| Zbot | Appending data at the end of a JPG file | Hiding configuration data |
| Lurk/Stegoloader | Modification of the LSBs of BMP/PNG files | Hiding encrypted URL for malware components |
| AdGholas | Data hiding in images, text, and audio files | Hiding encrypted malicious JavaScript code |
| Android/Twitter.A | Impersonating a pornography player or an MMS app | Tricking users into installing malicious apps and spreading infection |
| Fakem RAT | Mimicking MSN and Yahoo! Messenger conversation traffic | Hiding command and control (C&C) traffic |
| Carbanak/Anunak | Abusing Google cloud-based services | Hiding C&C traffic |
| SpyNote Trojan | Impersonating Netflix app | Tricking users into installing malicious app to gain access to confidential data |
| TeslaCrypt | Data hidden in HTML comments tag of the HTTP 404 error message page | Embedding C&C commands |
| Cerber | Image steganography | Embedding malicious executable |
| SyncCrypt | Image steganography | Embedding core components of ransomware |
| Stegano/Astrum | Modifying the color space of the used PNG image | Hiding malicious code within banner ads |
| DNSChanger | Modification of the LSBs of PNG files | Hiding malware AES encryption key |
| Sundown | Hiding data in white PNG files | Exfiltrating user data and hiding exploit code delivered to victims |

Summary of use-cases.

- Stealthy command & control channels for botnets

- Covert data exfiltration

- Hiding confidential data

Some potential Scenarios

Advanced Persistent Threats (APT):
large-scale sophisticated data leakage, involving techniques such as 'spear phishing'

Malware: e.g. stealthy botnet C&C channels

Military/secret service: Industrial espionage, stealthy communication

Citizens: censorship circumvention

Journalists: freedom of speech -> expression of opinions in networks with censorship

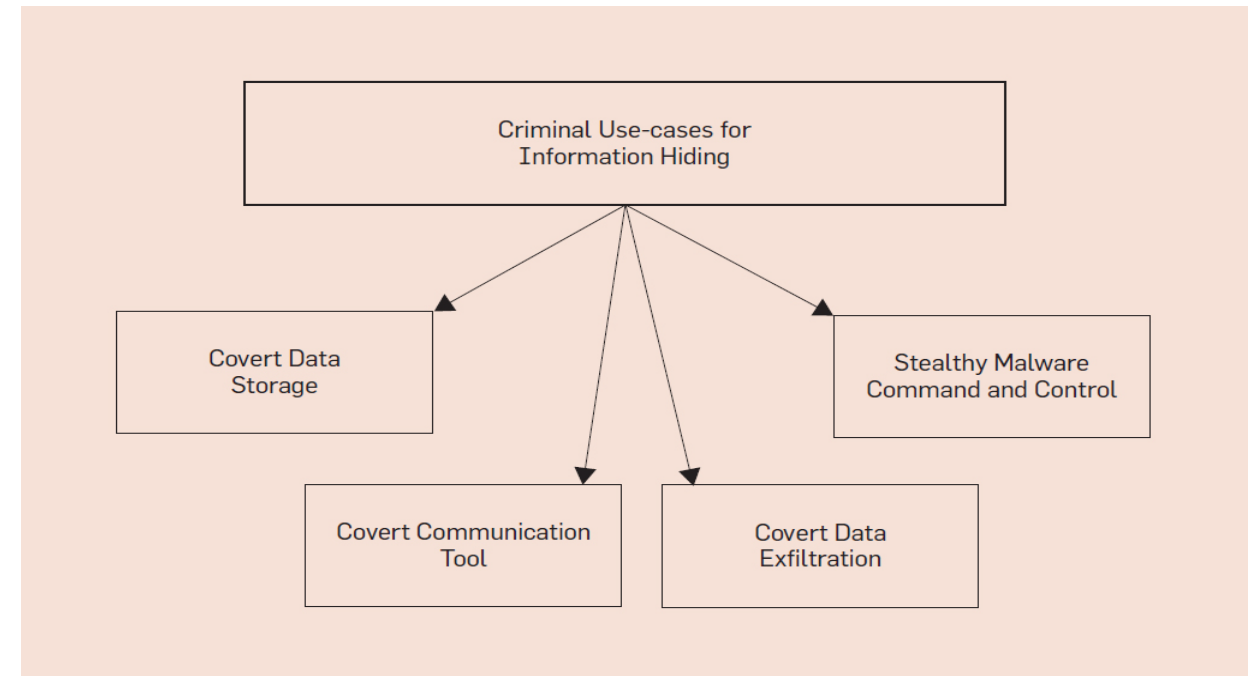


Fig.: W. Mazurczyk, S. Wendzel: Information Hiding: Challenges for Forensic Experts, Communications of the ACM, 2018. [\[link\]](#)