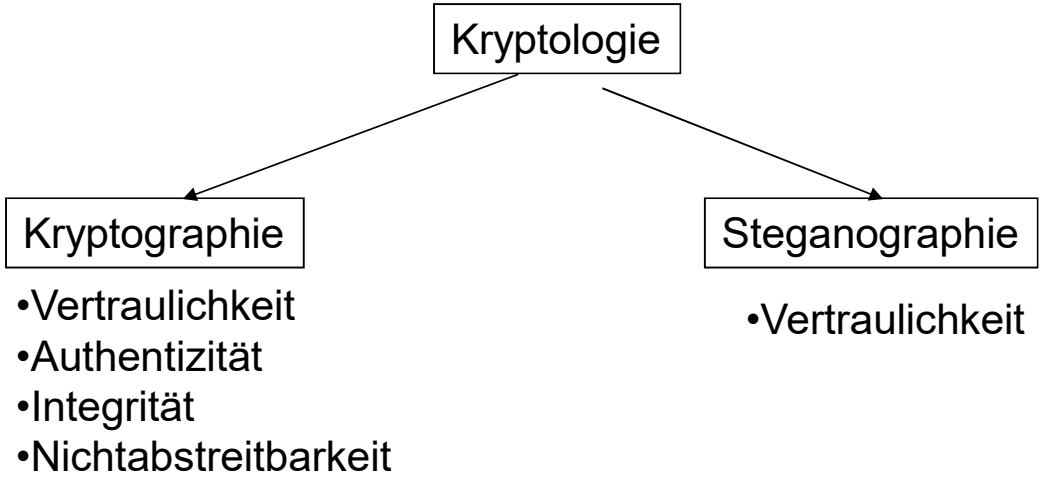
Steganographie

Steganographie

- "verdecktes Schreiben“
- Verbergen der geheimen Kommunikation

- ZIEL: geheime Nachrichten in harmlosen Nachrichten verbergen, so daß ein Angreifer nicht erkennt, daß eine zweite geheime Nachricht präsent ist

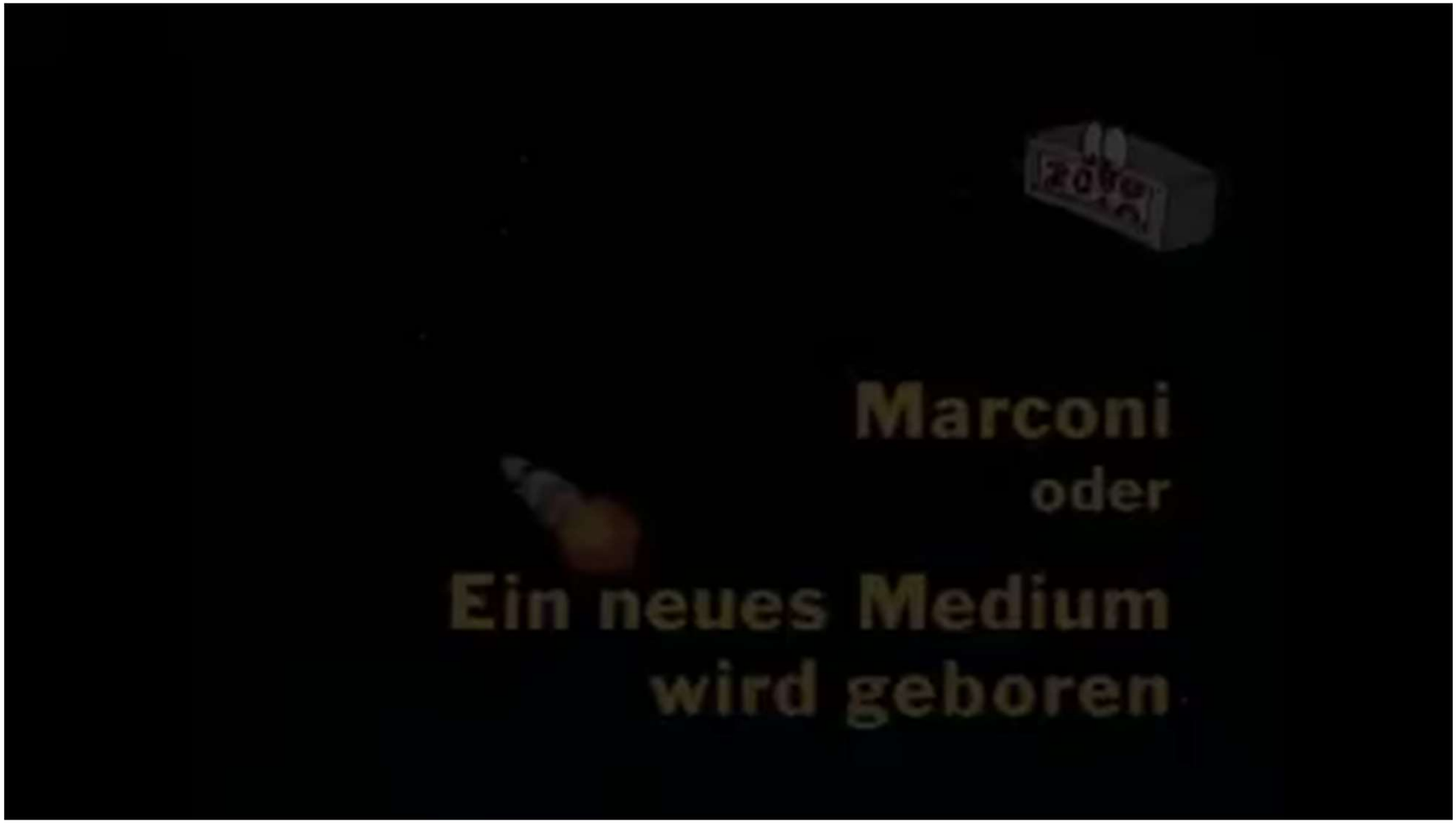


Steganographie/ Definition

- Hiding a secret message within a larger one in such a way that others can not discern the presence or contents of the hidden message. For example, a message might be hidden within an image by *changing the least significant bits to be the message bits.*

  – Chaffing and Winnowing: Confidentiality without Encryption, Ronald L. Rivest, MIT Lab for Computer Science, 1998-03-22

- Historisches Beispiel



- Ave Maria Kode
- 1508, Trithemius, *Polygraphiae libri sex (1. Buch über Kryptologie), Steganographia um 1500*

A impendat omnibus
B conferat cunctis
C donet uniuersis
D largiatur credentibus
E concedat nobis
F condonet christianis
G tribuat fidelibus
H distribuat petentibus
I retribuat expetentibus
K contribuat orantibus
L indulgeat exorantibus
M exhibeat postulantibus
N præstet expostulantibus
O offerat quærentibus
P deferat christicolis
Q ostendat inquirentibus
R reuelet requirentibus
S manifestet exquirentibus
T insinuet optantibus
V aspiret exoptantibus
X restituat præoptantibus
Y reddat expectantibus
Z administret sperantibus
W faueat desiderantibus

A ij

A Maiestas summi
B Bonitas magni
C Dulcedo maximi
D Charitas supremi
E Sapientia excelsi
F Potestas optimi
G Miseratio clarissimi
H Benignitas sanctissimi
I Mansuetudo potentissimi
K Excellentia sapientissimi
L Pietas fortissimi
M Suauitas mitissimi
N Claritas altissimi
O Clementia robustissimi
P Misericordia omnipotentis
Q Dulcitudo cunctipotentis
R Celsitudo sempiterni
S Deitas gloriosissimi
T Immensitas ineffabilis
V Virtus inuisibilis
X Fortitudo immortalis
Y Dilectio inaccessibilis
Z Munificentia eminentissimi
W Perfectio clementissimi

- Al-Kaida „kick ass“ und „sexy tanja“

„ Die 141 Dateien, die Maksud L. bei seiner Festnahme am 16. Mai 2011 in Berlin dabei hatte, sollten nie entdeckt werden. Sie waren auf einer Speicherkarte durch ein Passwort geschützt und mit spezieller Software quasi unsichtbar gemacht.“

Die Zeit, Ausgabe 12/2012

Aus Anklageschrift des FBI von 2010

III. MEANS AND METHODS OF THE CONSPIRACY

A. SECRET COMMUNICATIONS

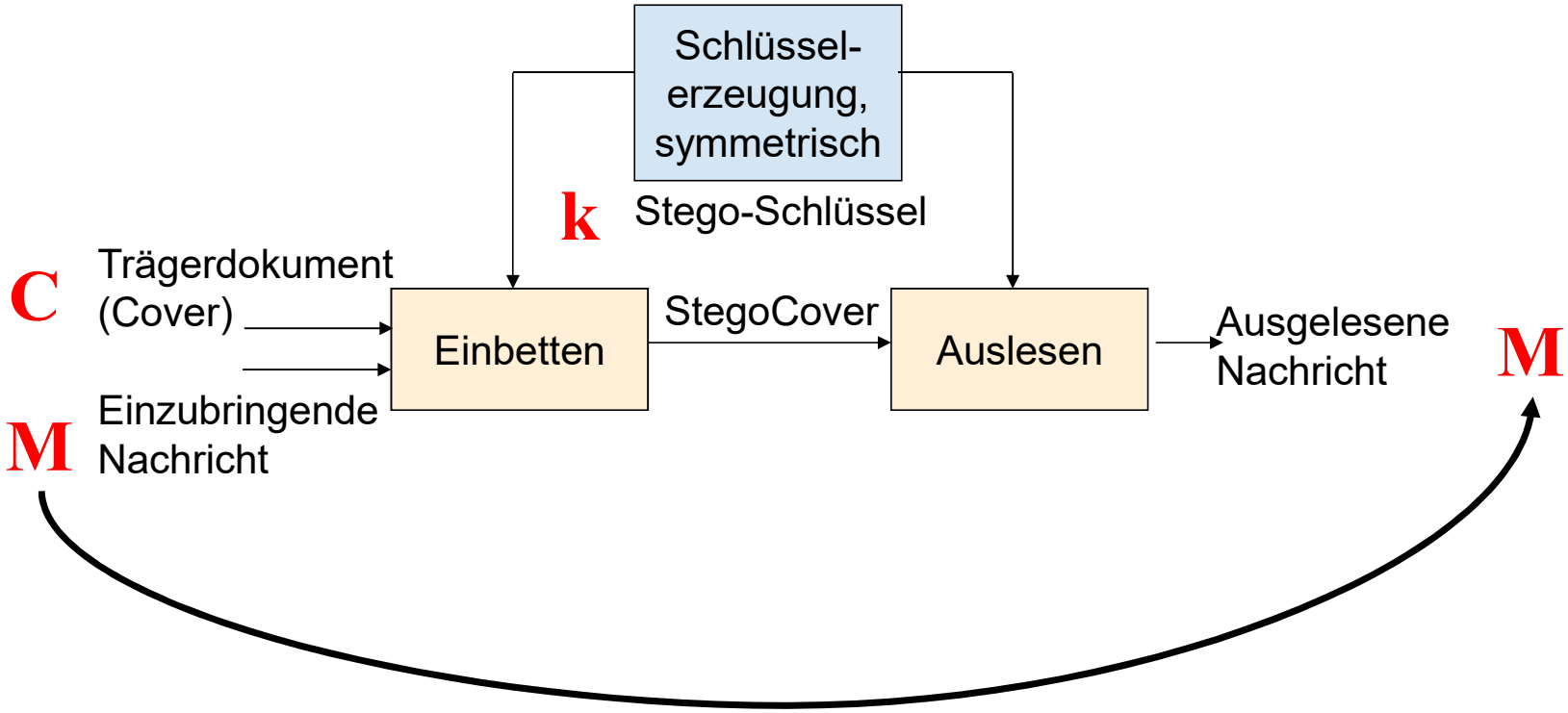
20. To further the aims of the conspiracy, Moscow Center has arranged for the defendants clandestinely to communicate with the Russian Federation. In particular, the conspirators have used, among others, the secret communications methods described below – steganography and radiograms.

1. STEGANOGRAPHY

21. Steganography is the process of secreting data in an image. Moscow Center uses steganographic software that is not commercially available. The software package permits the SVR clandestinely to insert encrypted data in images that are located on publicly-available websites without the data being visible. The encrypted data can be removed from the image, and then decrypted, using SVR-provided software. Similarly, SVR-provided software can be used to encrypt data, and then clandestinely to embed the data in images on publicly-available websites.

22. As is set forth below, certain of the Illegals have communicated with Moscow Center by means of steganography. In each of the three judicially-authorized residential searches referenced above (the 2006 Boston Search, the 2006 Seattle Search, and the 2005 New Jersey Search), law-enforcement agents observed and forensically copied a set of computer disks ("Password-Protected Disks"). Based on subsequent investigation as described below, I believe that the Password-Protected Disks contain a steganography program employed by the SVR and the Illegals.

http://www.justice.gov/opa/documents/062810complaint2.pdf


Schlüssel-
erzeugung,
symmetrisch
k
Stego-Schlüssel
C
Trägerdokument
(Cover)
M
Einzubringende
Nachricht
Einbetten
StegoCover
Auslesen
Ausgelesene
Nachricht
M

Beispiel

Gen 1:1 Am Anfang schuf Gott Himmel und Erde.
Gen 1:2 Und die Erde war wüst und leer, und es war finster auf der Tiefe; und der Geist Gottes schwebte auf dem Wasser.
Gen 1:3 Und Gott sprach: Es werde Licht! und es ward Licht.
Gen 1:4 Und Gott sah, dass das Licht gut war. Da schied Gott das Licht von der Finsternis
Gen 1:5 und nannte das Licht Tag und die Finsternis Nacht. Da ward aus Abend und Morgen der erste Tag.
Gen 1:6 Und Gott sprach: Es werde eine Feste zwischen den Wassern, und die sei ein Unterschied zwischen den Wassern.
Gen 1:7 Da machte Gott die Feste und schied das Wasser unter der Feste von dem Wasser über der Feste. Und es geschah also.
Gen 1:8 Und Gott nannte die Feste Himmel. Da ward aus Abend und Morgen der andere Tag.
Gen 1:9 Und Gott sprach: Es sammle sich das Wasser unter dem Himmel an besondere Örter, dass man das Trockene sehe. Und es geschah also.
Gen 1:10 Und Gott nannte das Trockene Erde, und die Sammlung der Wasser nannte er Meer. Und Gott sah, dass es gut war.
Gen 1:11 Und Gott sprach: Es lasse die Erde aufgehen Gras und Kraut, das sich besame, und fruchtbare Bäume, da ein jeglicher nach seiner Art Frucht trage und habe seinen eigenen Samen bei sich selbst auf Erden. Und es geschah also.
Gen 1:12 Und die Erde ließ aufgehen Gras und Kraut, das sich besamte, ein jegliches nach seiner Art, und Bäume, die da Frucht trugen und ihren eigenen Samen bei sich selbst hatten, ein jeglicher nach seiner Art. Und Gott sah, dass es gut war.
Gen 1:13 Da ward aus Abend und Morgen der dritte Tag.
Gen 1:14 Und Gott sprach: Es werden Lichter an der Feste des Himmels, die da scheiden Tag und Nacht und geben Zeichen, Zeiten, Tage und Jahre
Gen 1:15 und seien Lichter an der Feste des Himmels, dass sie scheinen auf Erden. Und es geschah also.
Gen 1:16 Und Gott machte zwei große Lichter: ein großes Licht, das den Tag regiere, und ein kleines Licht, das die Nacht regiere, dazu auch Sterne.
Gen 1:17 Und Gott setzte sie an die Feste des Himmels, dass sie schienen auf die Erde
Gen 1:18 und den Tag und die Nacht regierten und schieden Licht und Finsternis. Und Gott sah, dass es gut war.
Gen 1:19 Da ward aus Abend und Morgen der vierte Tag.
Gen 1:20 Und Gott sprach: Es errege sich das Wasser mit webenden und lebendigen Tieren, und Gevögel fliege auf Erden unter der Feste des Himmels.
Gen 1:21 Und Gott schuf große Walfische und allerlei Getier, das da lebt und webt, davon das Wasser sich erregte, ein jegliches nach seiner Art, und allerlei gefiedertes Gevögel, ein jegliches nach seiner Art. Und Gott sah, dass es gut war.
Gen 1:22 Und Gott segnete sie und sprach: Seid fruchtbar und mehret euch und erfüllet das Wasser im Meer; und das Gefieder mehre sich auf Erden.
Gen 1:23 Da ward aus Abend und Morgen der fünfte Tag.
Gen 1:24 Und Gott sprach: Die Erde bringe hervor lebendige Tiere, ein jegliches nach seiner Art: Vieh, Gewürm und Tiere auf Erden, ein jegliches nach seiner Art. Und es geschah also.
Gen 1:25 Und Gott machte die Tiere auf Erden, ein jegliches nach seiner Art, und das Vieh nach seiner Art, und allerlei Gewürm auf Erden nach seiner Art. Und Gott sah, dass es gut war.
Gen 1:26 Und Gott sprach: Lasset uns Menschen machen, ein Bild, das uns gleich sei, die da herrschen über die Fische im Meer und über die Vögel unter dem Himmel und über das Vieh und über die ganze Erde und über alles Gewürm, das auf Erden kriecht.
Gen 1:27 Und Gott schuf den Menschen ihm zum Bilde, zum Bilde Gottes schuf er ihn; und schuf sie einen Mann und ein Weib.
Gen 1:28 Und Gott segnete sie und sprach zu ihnen: Seid fruchtbar und mehret euch und füllet die Erde und machet sie euch untertan und herrschet über die Fische im Meer und über die Vögel unter dem Himmel und über alles Getier, das auf Erden kriecht.
Gen 1:29 Und Gott sprach: Sehet da, ich habe euch gegeben allerlei Kraut, das sich besamt, auf der ganzen Erde und allerlei fruchtbare Bäume, die sich besamen, zu eurer Speise,
Gen 1:30 und allem Getier auf Erden und allen Vögeln unter dem Himmel und allem Gewürm, das da lebt auf Erden, dass sie allerlei grünes Kraut essen. Und es geschah also.
Gen 1:31 Und Gott sah alles an, was er gemacht hatte; und siehe da, es war sehr gut. Da ward aus Abend und Morgen der sechste Tag.
Gen 2:1 Also ward vollendet Himmel und Erde mit ihrem ganzen Heer.
Gen 2:2 Und also vollendete Gott am siebenten Tage seine Werke, die er machte, und ruhte am siebenten Tage von allen seinen Werken, die er machte.
Gen 2:3 Und Gott segnete den siebenten Tag und heiligte ihn, darum dass er an demselben geruht hatte von allen seinen Werken, die Gott schuf und machte.

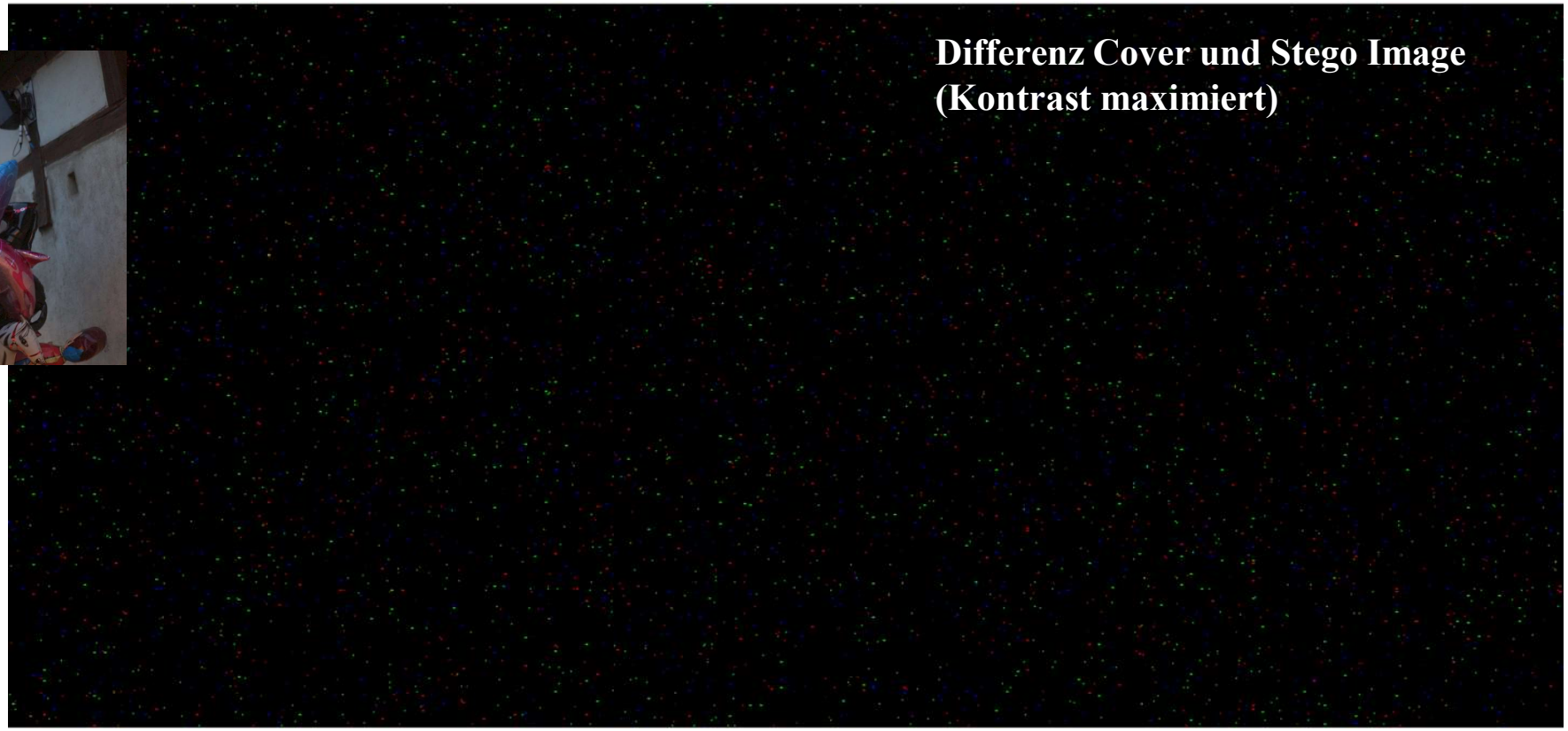
Nachricht

Beispiel

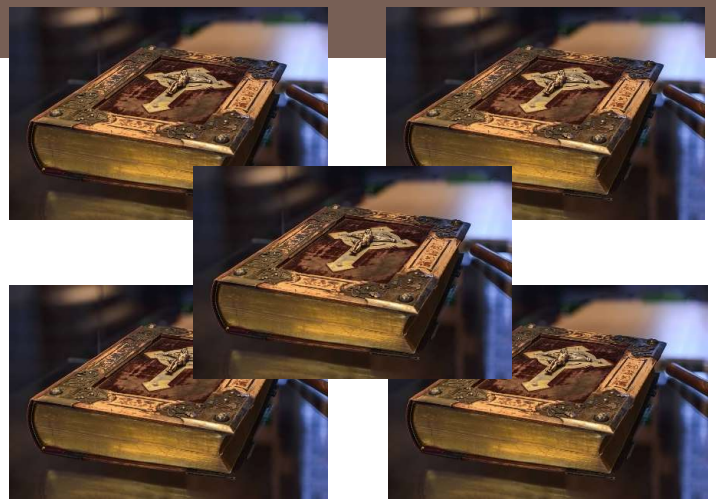
Eigenes Foto, Steinebach

Beispiel

Eigenes Foto, Steinebach



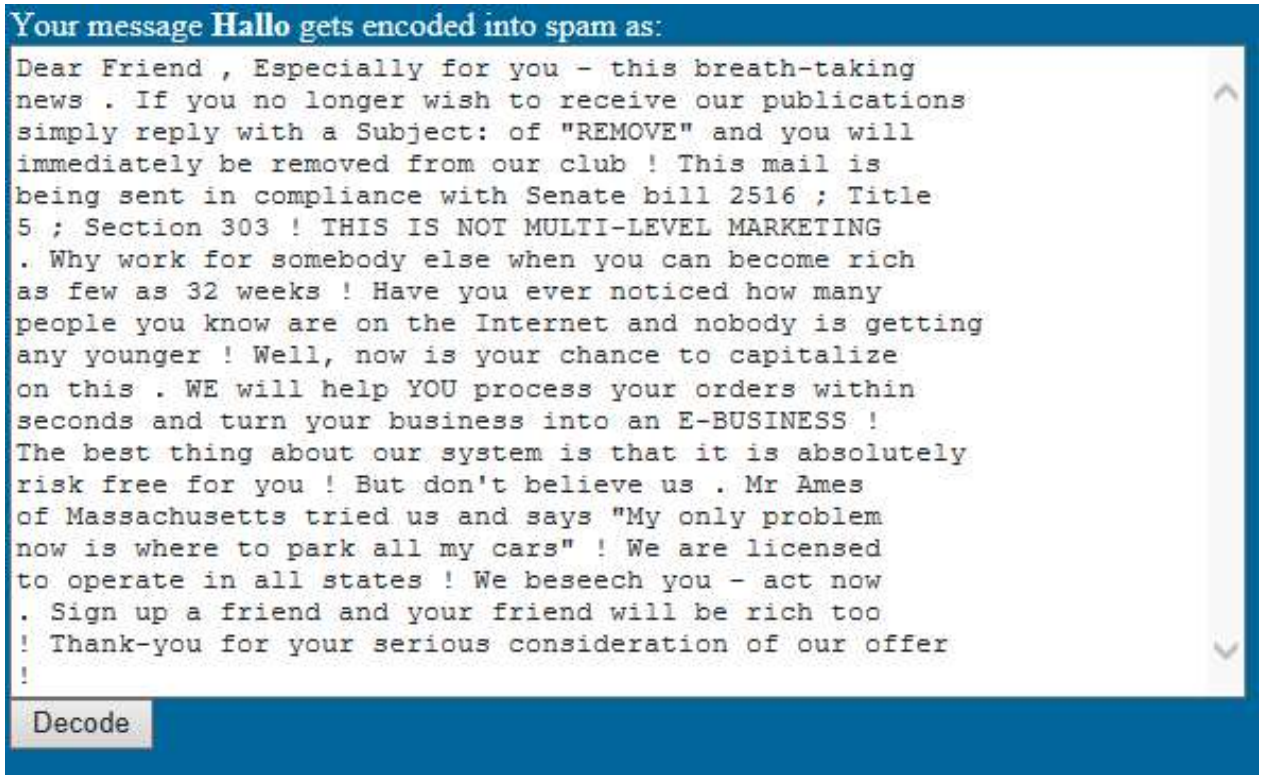
- Rechenbeispiel: Bild aus Digitalkamera
  - 5456 x 3632 Pixel, 3 Farbkanäle (24 Bit)
  - 59.448.576 Helligkeitswerte (8 Bit)
  - Davon jeweils das LSB: 7.431.072 Byte
  - Volltext Bibel in ASCII: 1.376.155 Byte



CC0, Pixabay

Steganographie/ Beispiel

- Spam Mimic (www.spammimic.com)



- Spam Mimic (www.spammimic.com)

Steganographie/ Beispiel

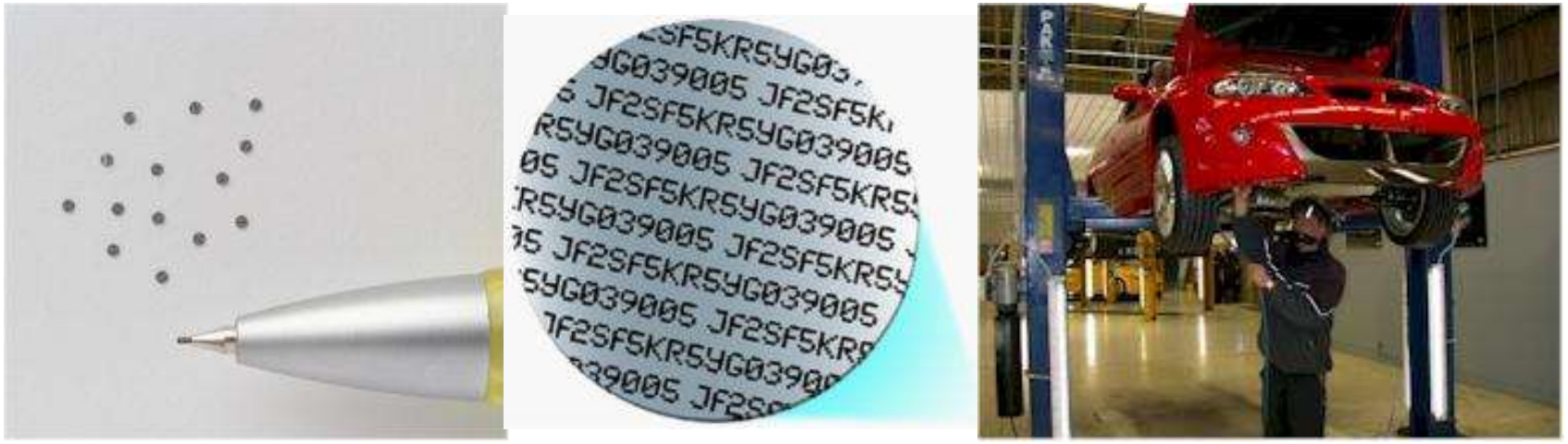
- Jeremiah Denton

Steganographie/ Beispiel

- Jeremiah Denton
- Morsecode T-O-R-T-U-R-E durch Zwinkern
- http://www.nytimes.com/2014/03/29/us/politics/jeremiah-a-denton-jr-war-hero-and-senator-dies-at-89.html?_r=0

Steganographie/ Microdot

- Übermitteln von Nachrichten mittels eines verkleinerten Textes in ansonsten unscheinbaren Nachrichten
- Größe entsprichten ca. 1 mm
- Einsatz im 2. Weltkrieg verbreitet
- Heute verwendet zur Markierung von z.B. Autoteilen

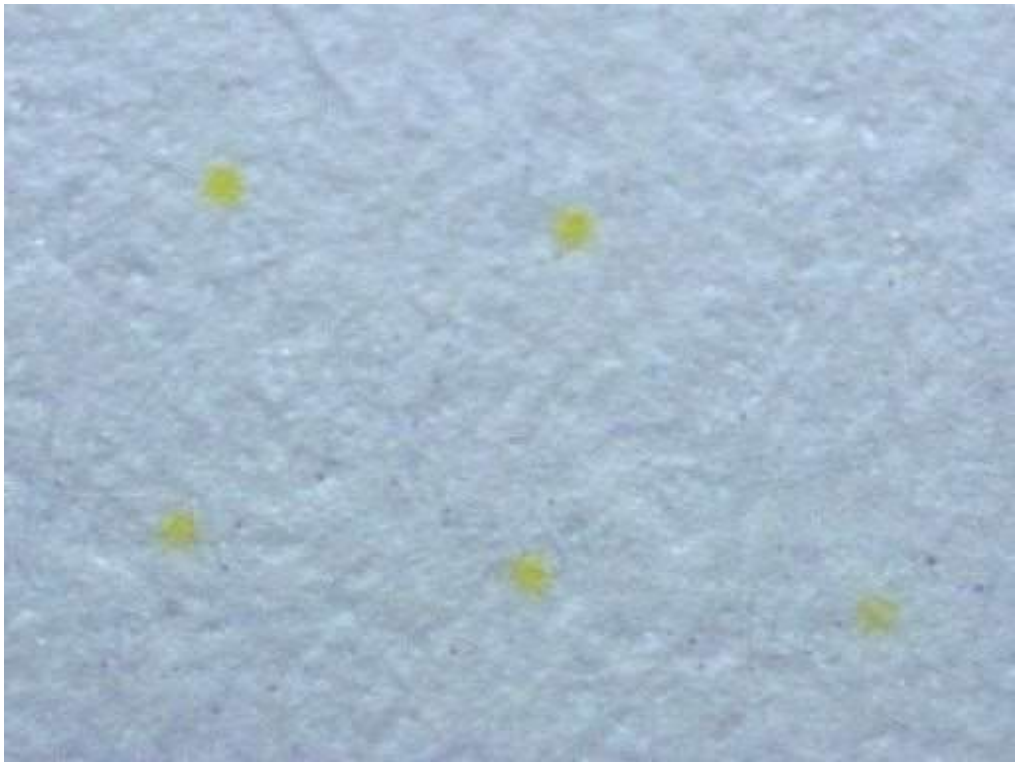


http://www.scienceinafrica.co.za/pics/11_2005

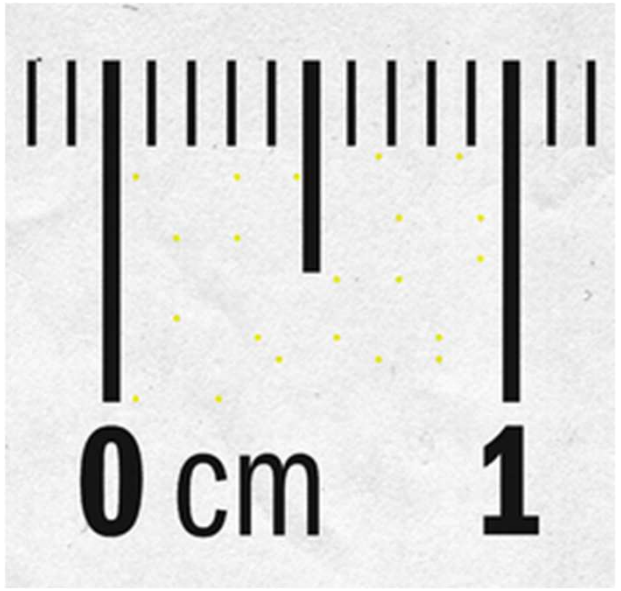
…und im Kino

MI3, Paramount Pictures

Steganographie/ Yellow Dots



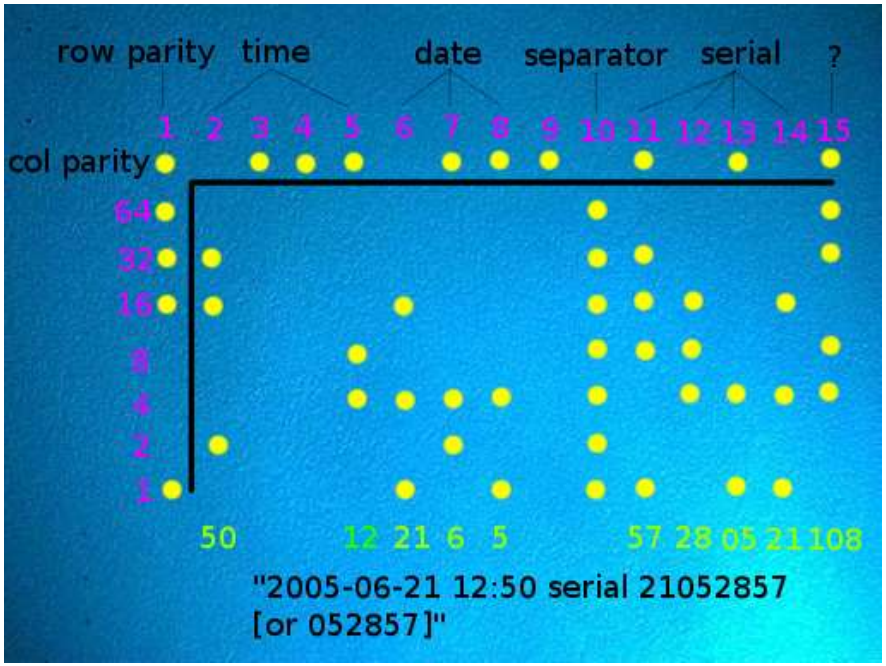
(c) EFForg (cc)



(c) EFForg

Steganographie/ Yellow Dots

- Seriennummer und Datum werden vom Drucken kaum wahrnehmbar als Punktekode auf Ausdrucken versteckt
- Ziel: Lokalisieren von Bekennerschreiben, Fälschungen,…
- Druckerfirmen: Brother, Canon, Dell, Epson, HP, IBM, Konica Minolta, Kyocera, Lanier, Lexmark, Ricoh, Toshiba and Xerox (nach EFF)



(c) EFForg

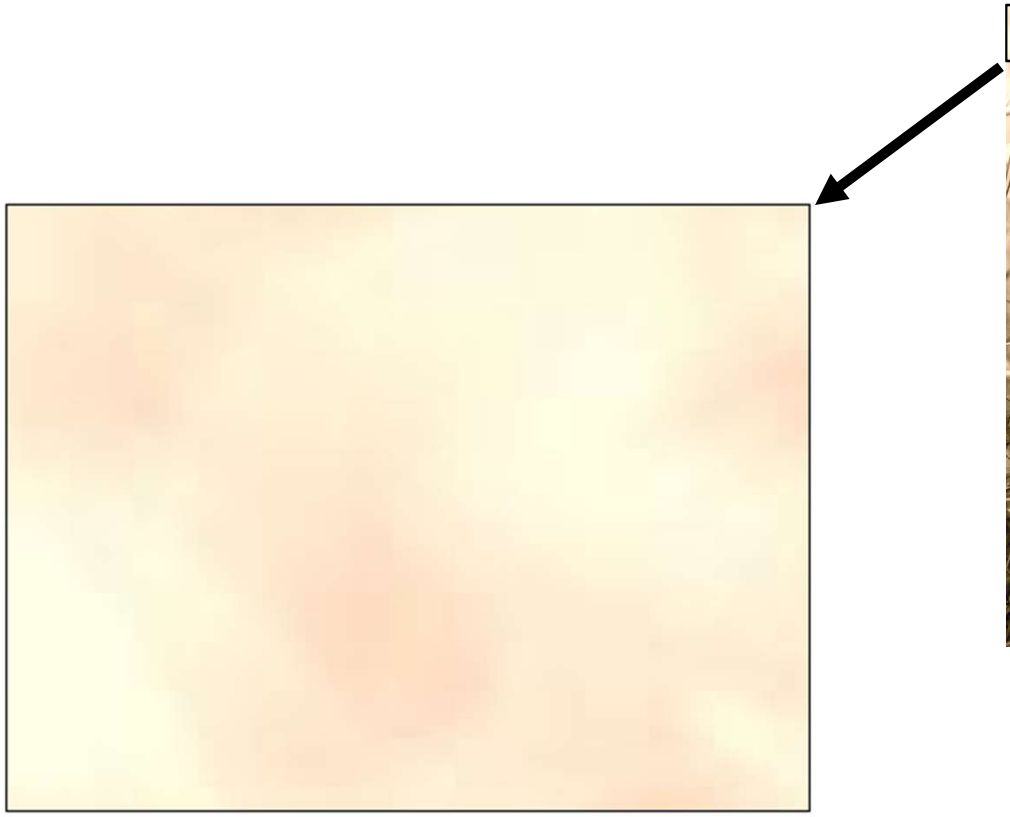
Bild als Folge von Lichtintensitäten:

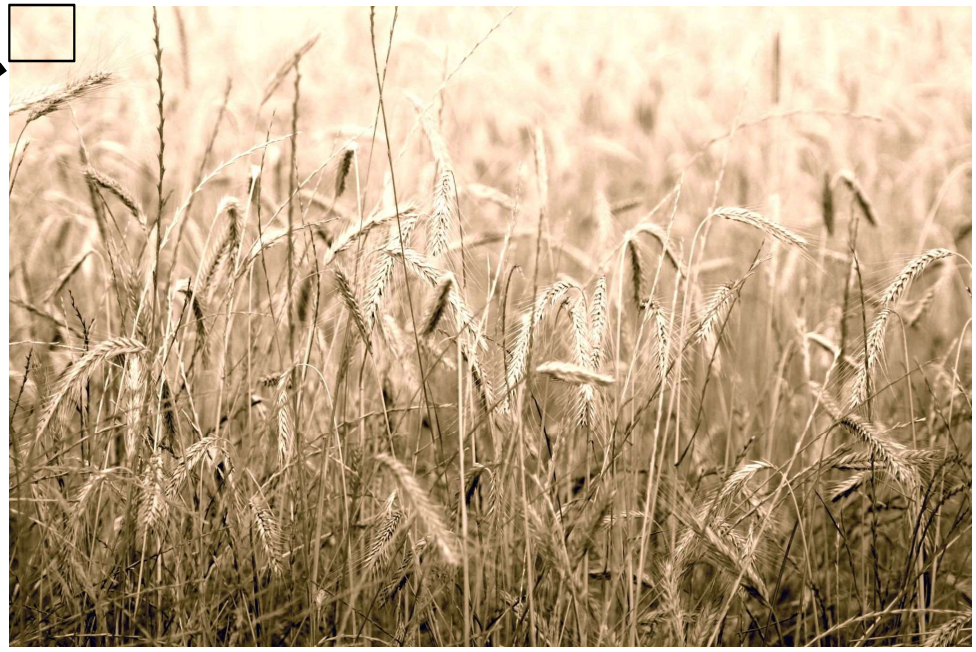
- z.B. 640*480 Pixel mit 256 Farben (8 Bit pro Pixel),
- Byte 213 (binär 11010101) als LSB:

132	134	137	141	121	101	74	38
10000100	10000110	10001001	10001101	01111001	01100101	01001010	00100110

133	135	136	141	120	101	74	39
1000010**1**	1000011**1**	1000100**0**	1000110**1**	0111100**0**	0110010**1**	0100101**0**	0010011**1**

LSB Steganographie



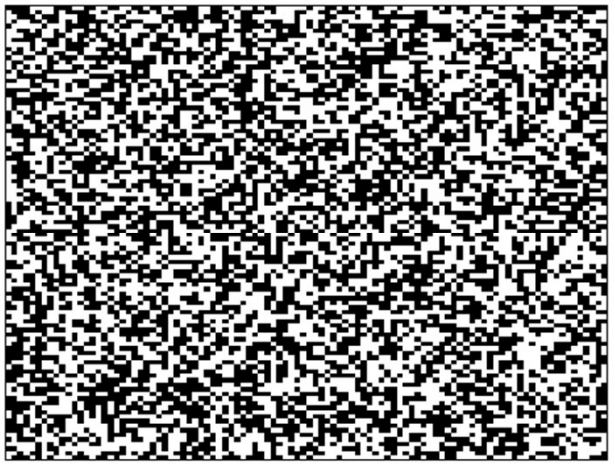


Eigenes Foto, Steinebach

Steganalyse

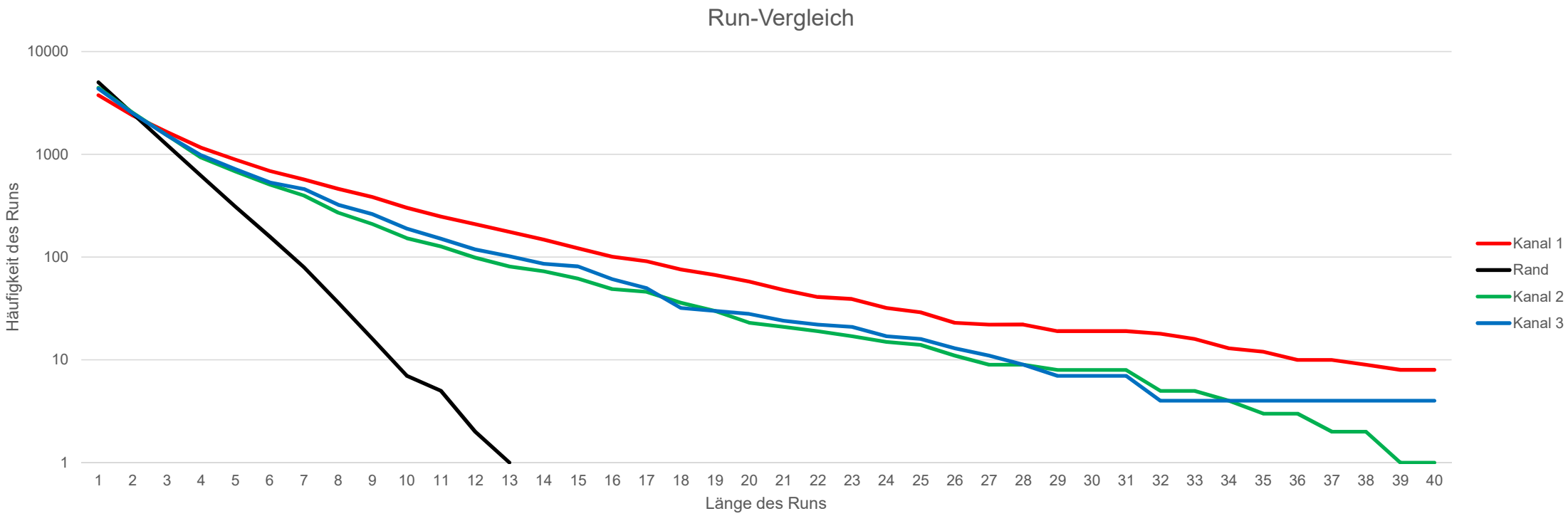
- LSB Ebenen erscheinen zufällig
- Im Vergleich zu echt zufälligen Sequenzen sind aber noch immer Bereiche zu erkennen

100x100 LSBs aus einem Bild



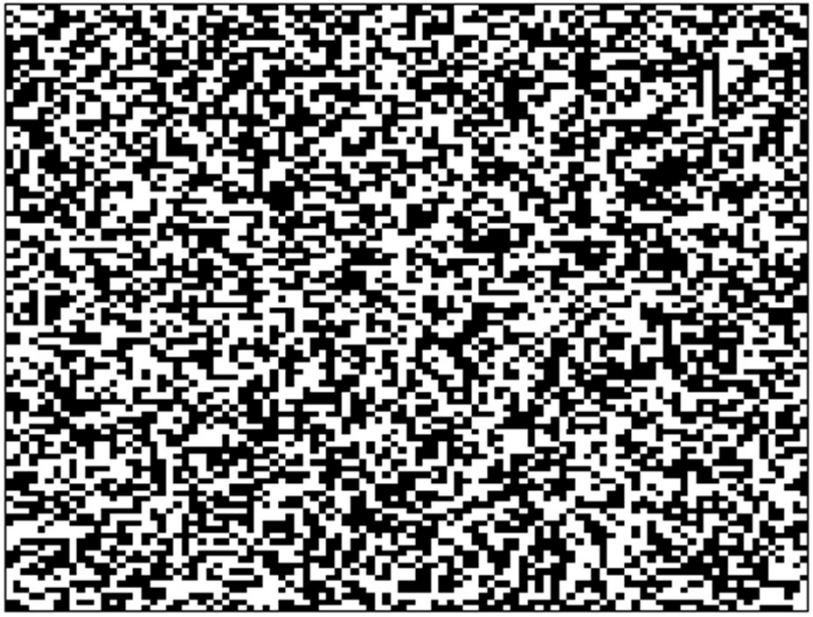
100x100 zufällige Bits

- Run=Sequenz von Bits mit gleichem Wert
  - Sequenz 000 = Run 0 der Länge 3

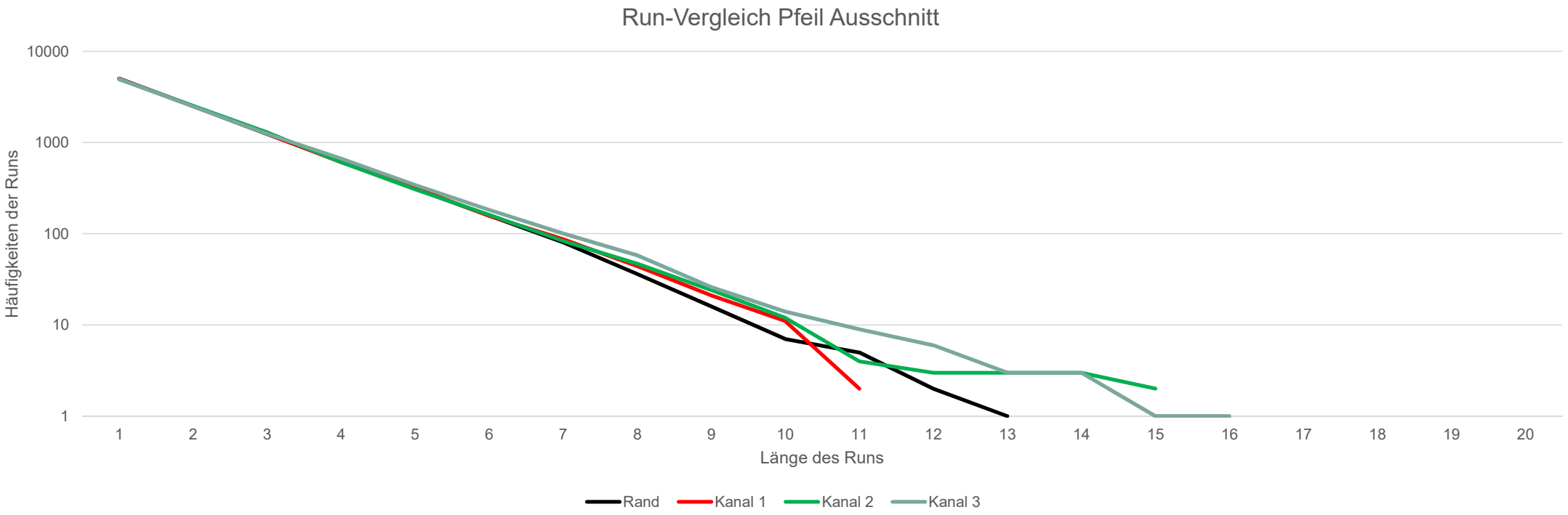


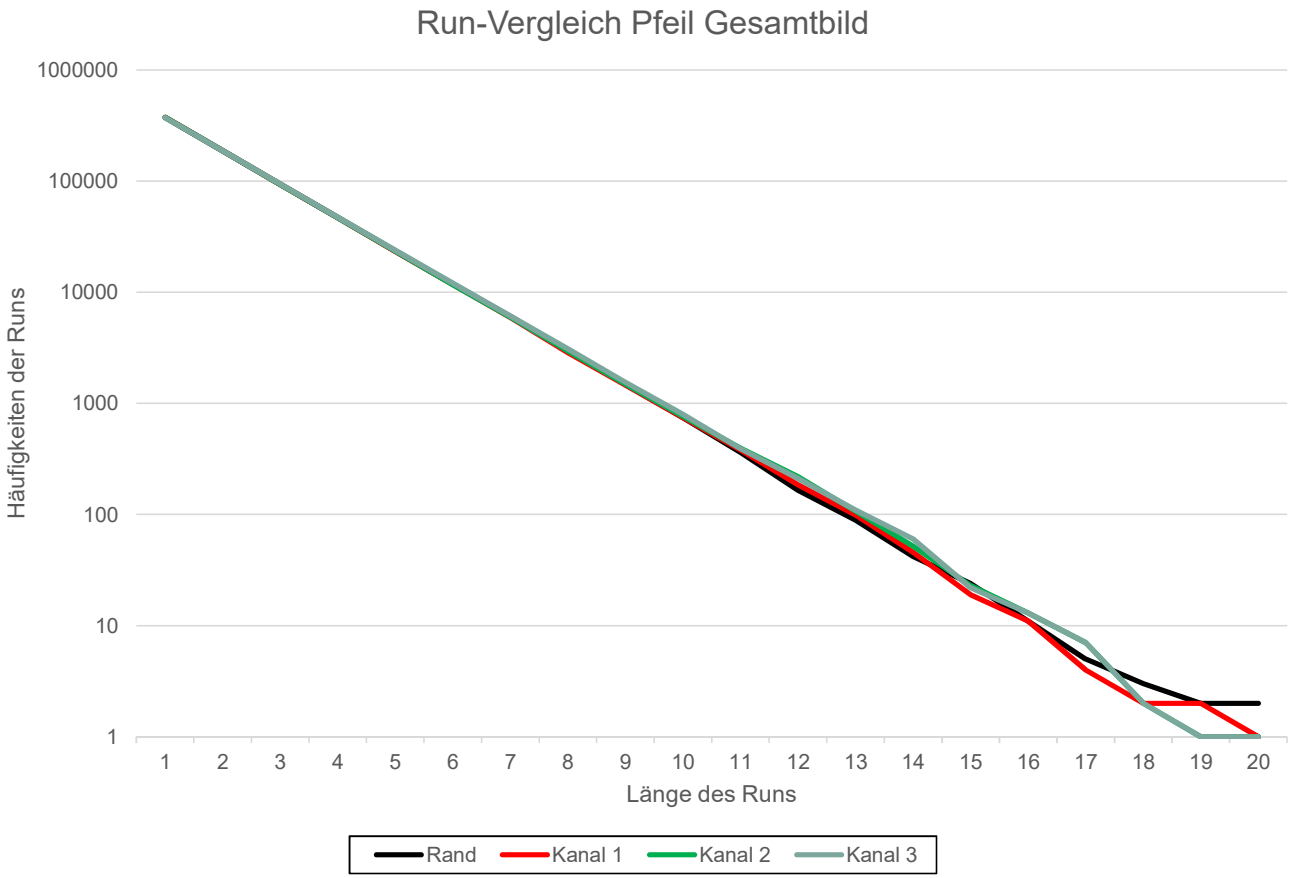
- Aber: Andere Bilder haben unterschiedliche Charakteristiken

100x100 LSBs aus Bild rechts



- Run=Sequenz von Bits mit gleichem Wert
  - Sequenz 000 = Run 0 der Länge 3

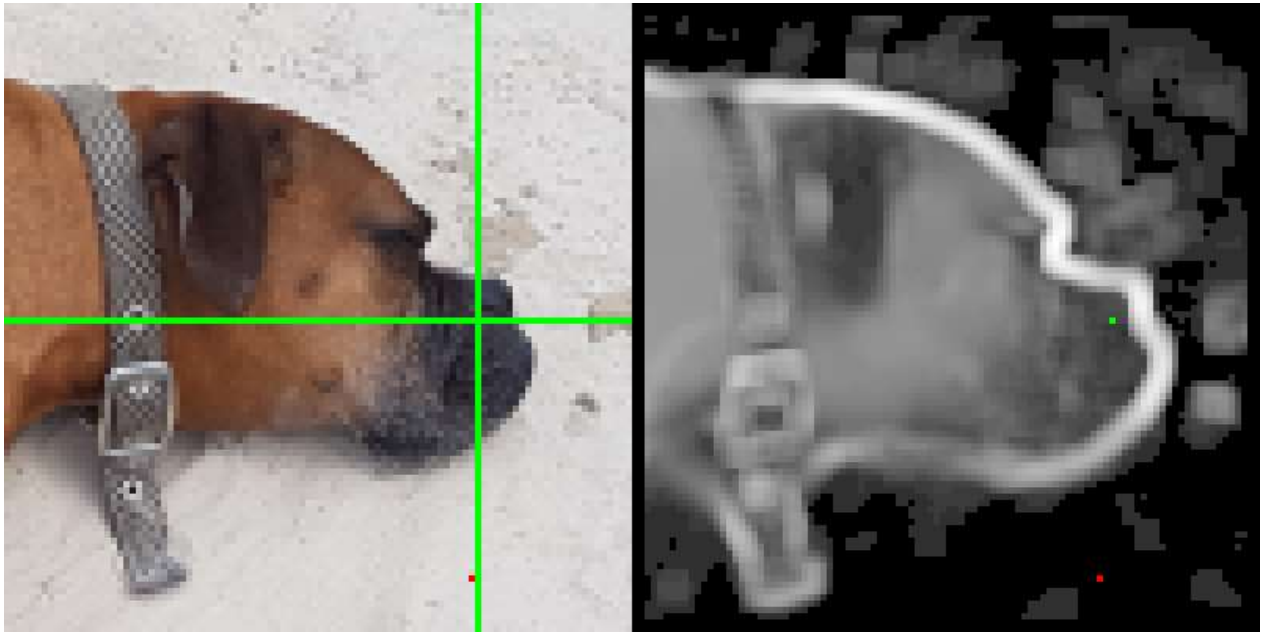





Eigenes Foto, Steinebach

Steganographie

- Gegenmaßnahmen gegen Entdeckung
  - Verstehen der Annahmen der Steganalyse
  - Entwickeln von Methoden, die diese Annahmen nicht befriedigen
- Beispiel:
  - Steganographie erzeugt Rauschen als LSB Muster
  - Steganalyse erkennt Rauschen
  - Verbesserte Steganographie vermeidet Rauschen
- Umsetzung
  - Lokale Masken, Eignung von Pixeln bewerten
  - Zufällige Auswahl von n Pixeln pro Bit
    - Statt nur ein Pixel pro Bit
  - Bitwert = Parität aller LSBs der Pixel
  - Änderung nur des am besten geeigneten Pixel
    - Grün: Veränderbares Pixel
    - Rot: Andere Pixel in der Gruppe

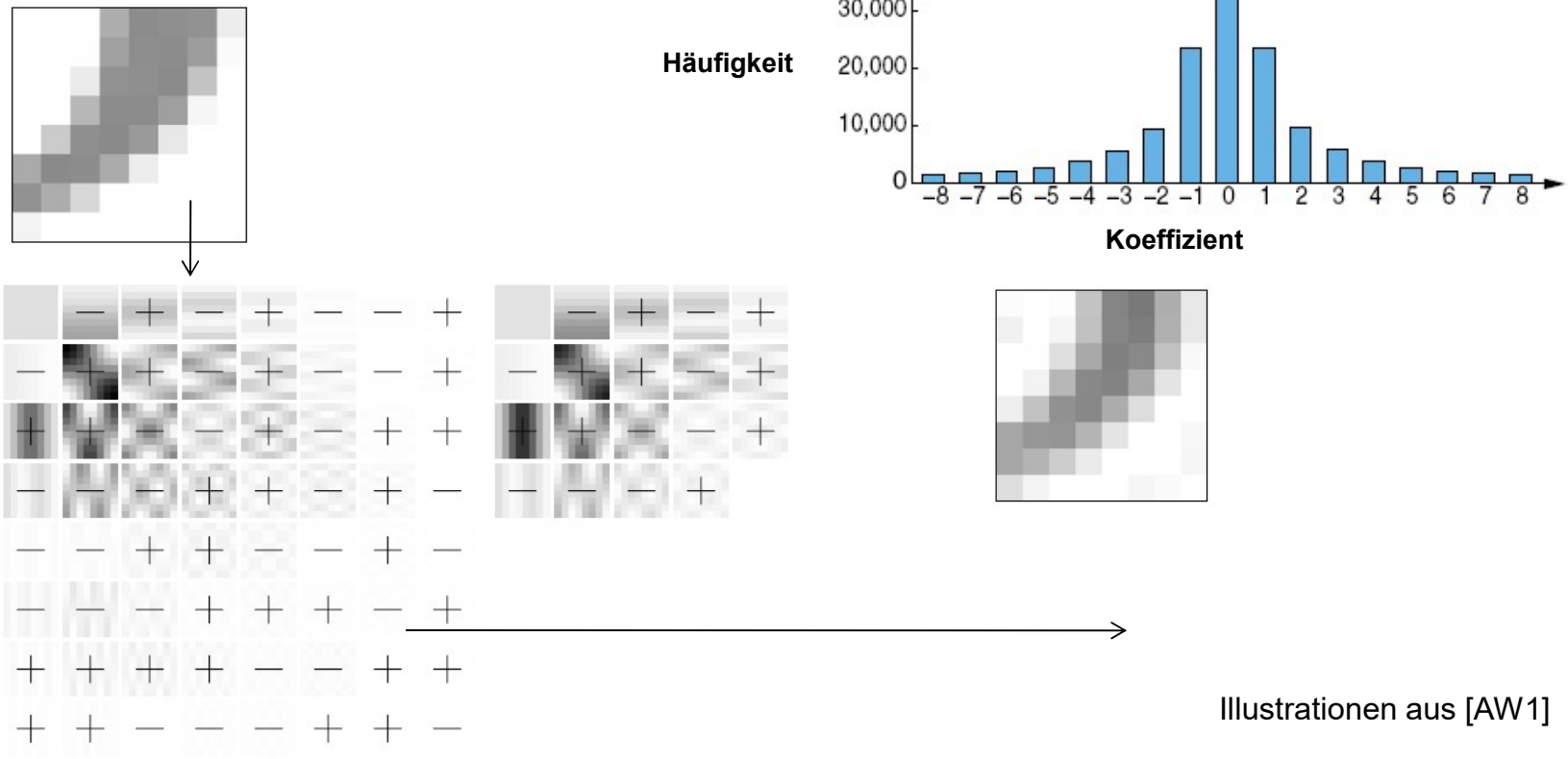


Steganographie

Steganographie/ F5

- Beispiel für steganografisches Verfahren
- F5 von Andreas Westfeld, TU Dresden
  - [AW1] http:// os.inf.tu-dresden.de/~westfeld/publikationen/f5.pdf
  - [AW2] http://os.inf.tu-dresden.de/papers_ps/westfeld.vis01.pdf
- “ F5 – ein steganographischer Algorithmus - Hohe Kapazität trotz verbesserter Angriffe“

- Trägersignal: JPEG-Bild
  - Wandlung
  - Statistik



Illustrationen aus [AW1]

- Einbetten in JPEG-Koeffizienten
  - LSB-Verfahren
  - Positive Koeffizienten werden erniedrigt, negative Koeffizienten werden erhöht
  - 0-Koeffizienten werden übersprungen

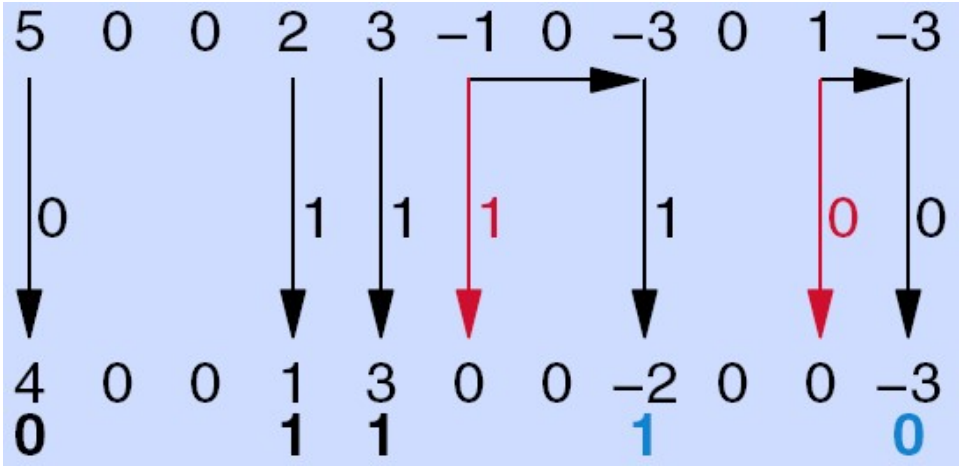


Illustration aus [AW1]

- Einbetten in JPEG-Koeffizienten
  - Permutation der Blöcke führt zur Verteilung der Nachricht über Bild hinweg
  - Schlüsselabhängig
  - Folge: Keine Häufungen der Änderungen am Anfang des Bildes

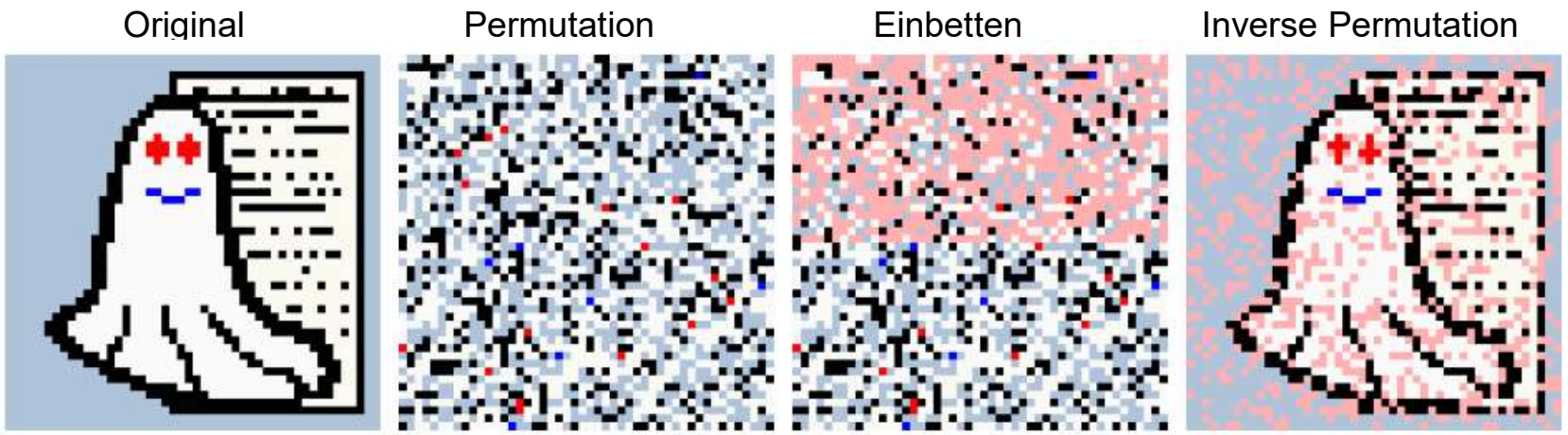


Illustration aus [AW1]

- Matrix-Kodierung der Nachricht
  - Einbetten mehrerer Bits mit minimalen Änderungen
  - Herkömliches Einbetten Sequenz “10”

Bit	0	1	0
Gruppe	-	-	-
Markiert	1	0	0

  - Matrix-Einbetten mit zwei Gruppen AB, ebenfalls “10”

Bit	0	1	0
Gruppe	A	B	AB
Markiert	0	1	1

Parity A: 0
Parity B: 1

Parity A: 1
Parity B: 0

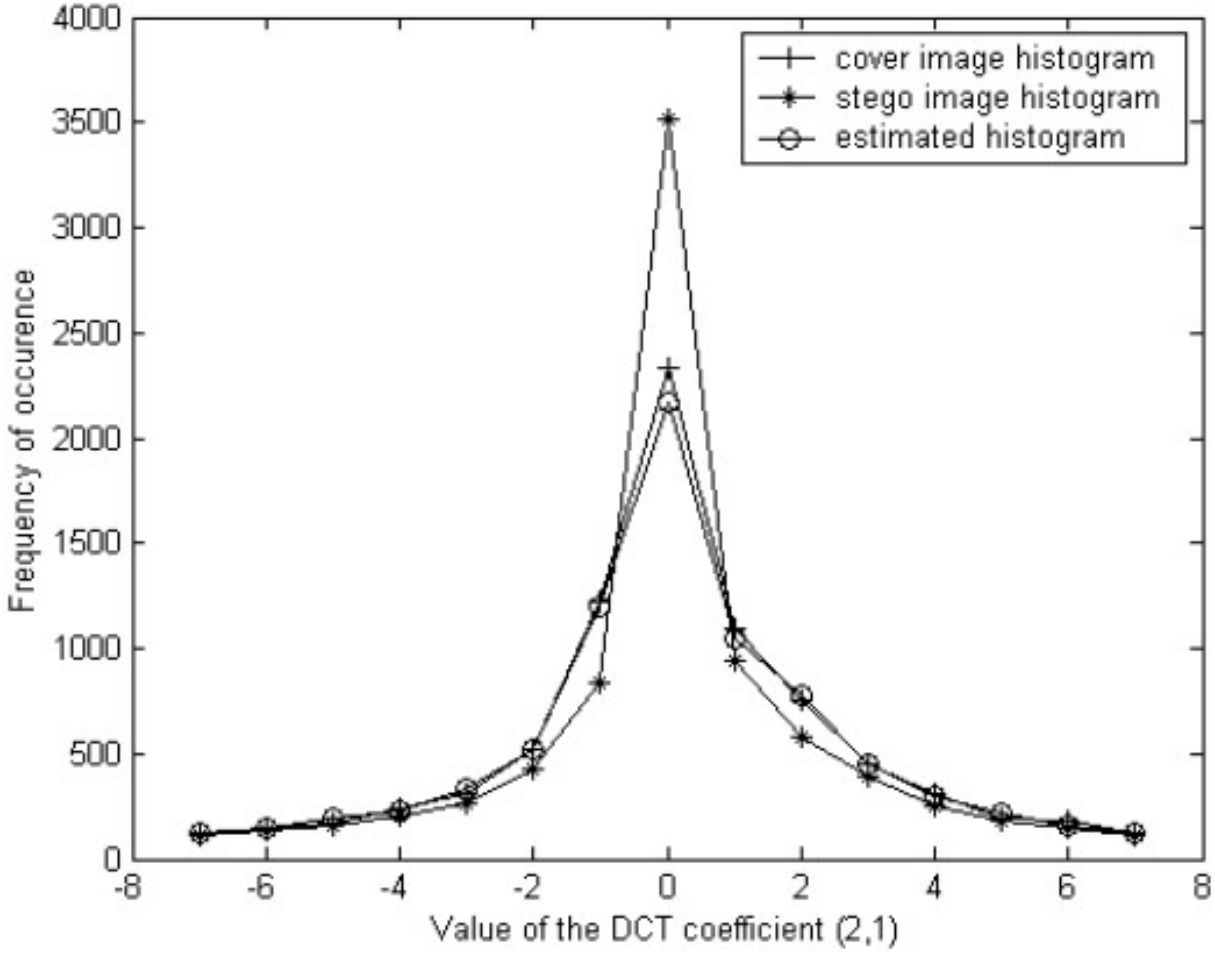
  - Veränderung von nur einem Bit

- Matrix-Kodierung der Nachricht
  - Tabelle der Effizienz aus [AW2]
  - Einbetten von k Bits durch Änderung eines von n=2^k-1 Bits
  - Effizienz = Durchschnittlich eingebettete Bits pro verändertes Bit

k	n	Änderungsdichte	Einbettungsrate	Einbettungseffizienz
1	1	50,00 %	100,00 %	2
2	3	25,00 %	66,67 %	2,67
3	7	12,50 %	42,86 %	3,43
4	15	6,25 %	26,67 %	4,27
5	31	3,12 %	16,13 %	5,16
6	63	1,56 %	9,52 %	6,09
7	127	0,78 %	5,51 %	7,06
8	255	0,39 %	3,14 %	8,03
9	511	0,20 %	1,76 %	9,02

- Erfolgreicher Angriff
  - Ziel bei Steganographie: Nachweis einer Nachricht
  - nicht Zerstören oder Auslesen der Nachricht
- Steganalysis of JPEG Images: Breaking the F5 Algorithm
  Jessica Fridrich, Miroslav Goljan, Dorin Hogea
  - http://www.ws.binghamton.edu/fridrich/Research/f5.pdf
- Prinzip: Erkennen von Unregelmäßigkeiten im Histogramm
  - Originalhistogramm möglichst gut abschätzen
    - Durch Errechnen des Histogramms von einer um vier Spalten verschobenen Kopie
  - Mit vorliegendem Histogramm vergleichen
  - Bei großen Unterschieden auf Einbettung schließen

- Grafik aus http://www.ws.binghamton.edu/fridrich/Research/f5.pdf



- Nachrichten, die die Kapazität ausnutzen, können verhältnismäßig gut erkannt werden
- Cover mit kurze Nachrichten (wenige Worte) sind nicht von einem Cover zu unterscheiden
- Eine Erweiterung des F5 Algorithmus erschwert/verhindert die Detektion deutlich
  - Einfach die Richtungen der Änderungen variieren, um Häufungen zur Null hin zu verhindern