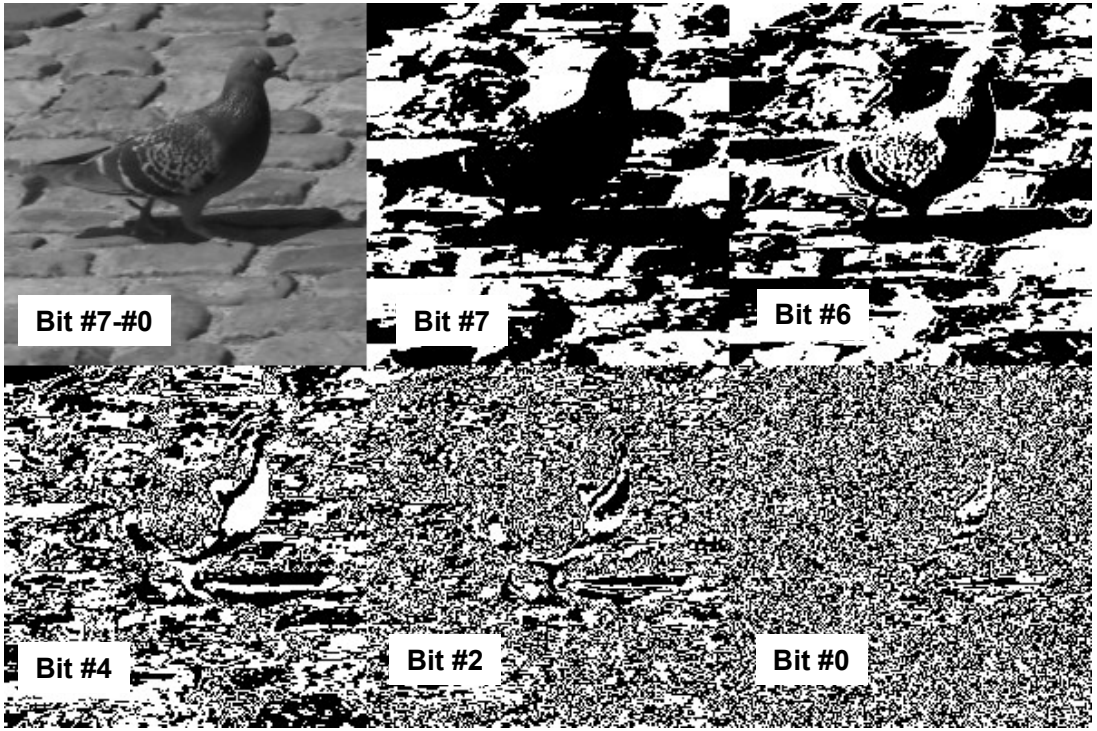
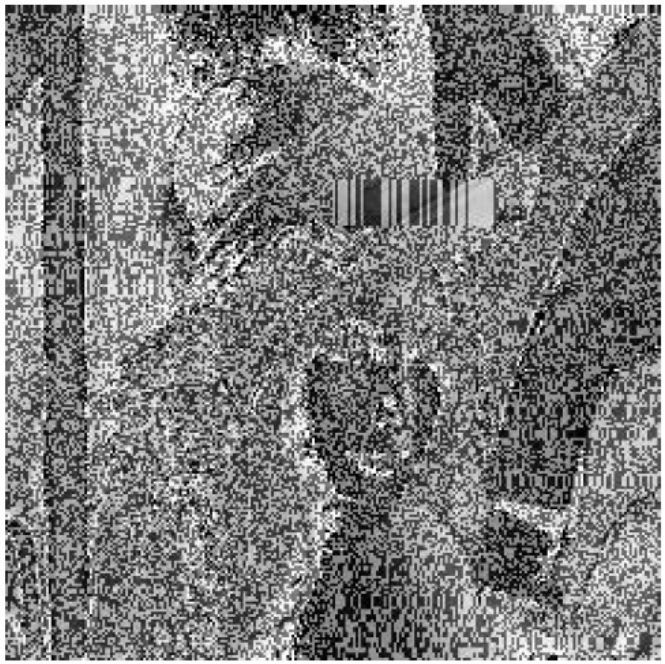
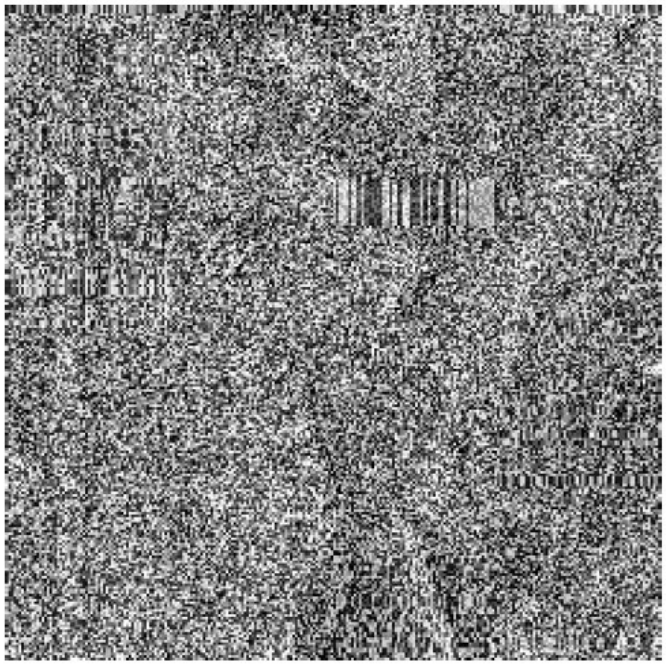
- Bitebenen Pixel
  - Je nach Wertigkeit eines Bits sind diese unterschiedliche relevant für die Darstellung eines Bildes
  - Je niedriger der Wert, desto mehr ähnelt die Bitebene Rauschen





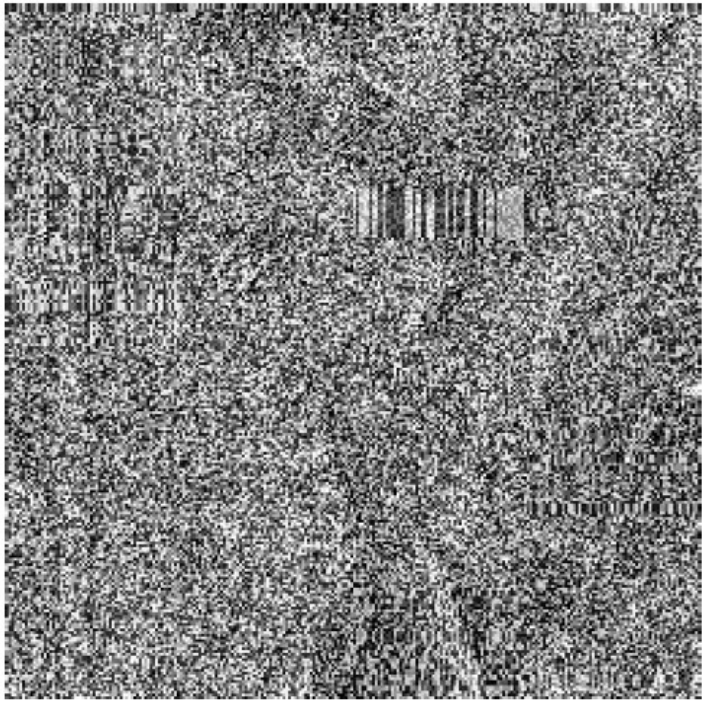
Ebene 8

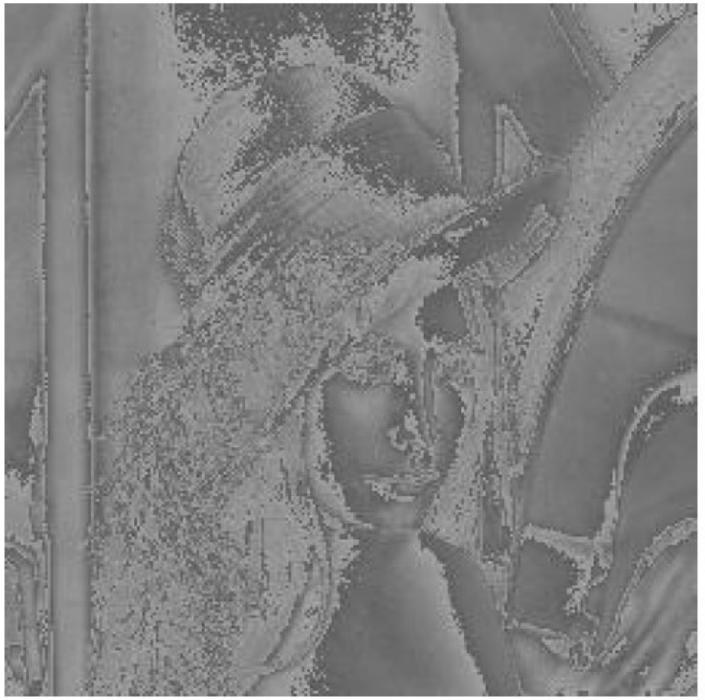


Ebenen 8+7

Verschlüsslung:
Modifikation von Bitebenen, beginnend mit dem MSB, 8 Bit Darstellung

Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments
Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl
http://www.cosy.sbg.ac.at/~uhl/norsig_slides.pdf





Ebenen 8+7

Replacement Attack:
Durchgehend verschlüsselte Bitebenen auf “0” setzen

Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments
Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl
http://www.cosy.sbg.ac.at/~uhl/norsig_slides.pdf

Original MSB

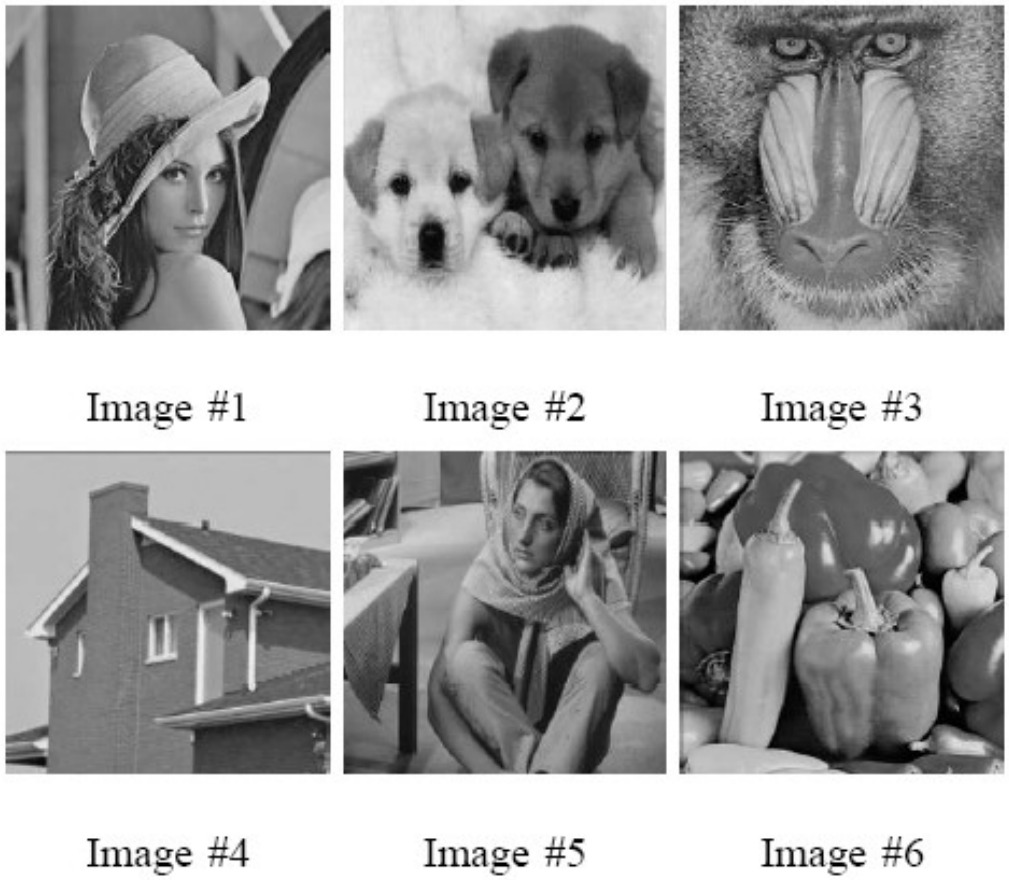
Rekonstruiertes MSB

Reconstruction Attack:

- Großteil eines Bildes besteht aus weichen Übergängen von Grauwerten
- MSBs in diesen Bereichen bleiben gleich
- Suchfenster errechnet Bereiche für gleiche Bitwerte von MSBs inklusive Kantenerkennung

Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments
Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl, http://www.cosy.sbg.ac.at/~uhl/norsig_slides.pdf

Angriffe auf Permutationen unter Kenntnis von n Testbildern, vorgestellt von Li, Li, Chen, Zhang and Bourbakis

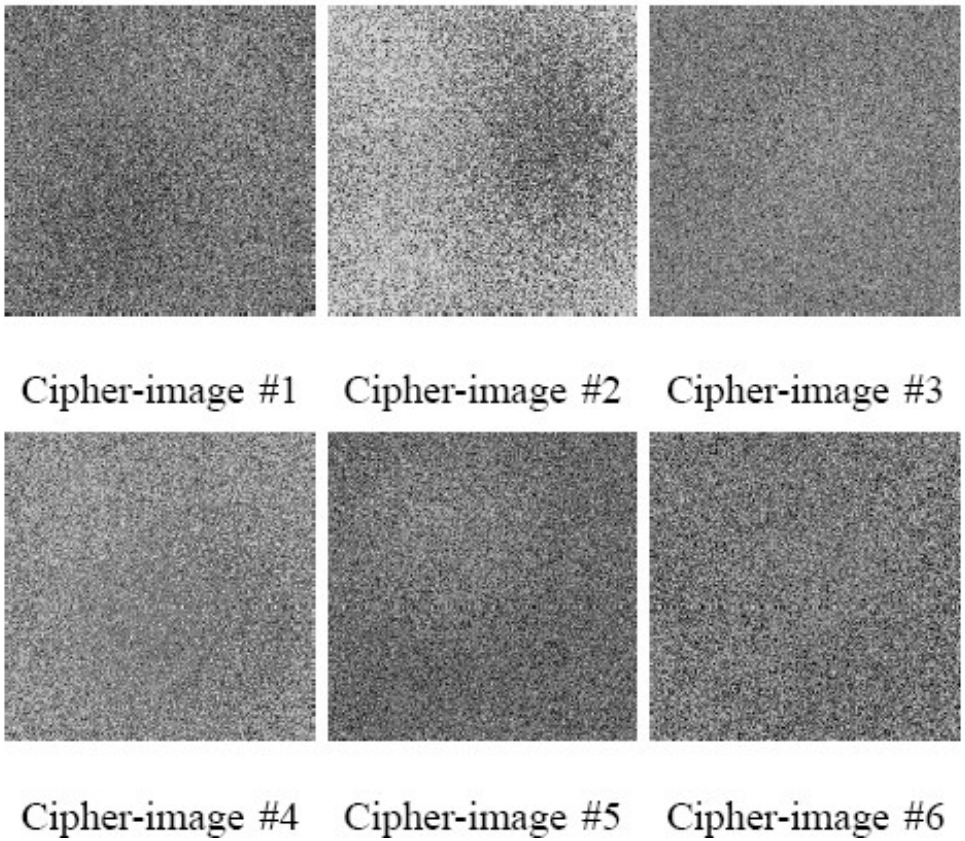


Quelle: A General Cryptanalysis of Permutation-Only Multimedia Encryption Algorithms

Shujun Li, Chengqing Li, Guanrong Chen, Fellow, IEEE, Dan Zhang and Nikolaos G. Bourbakis Fellow, IEEE

Alle Bilder werden mit dem selben Schlüssel permutiert, bei n Bildern kennt der Angreifer das Original.

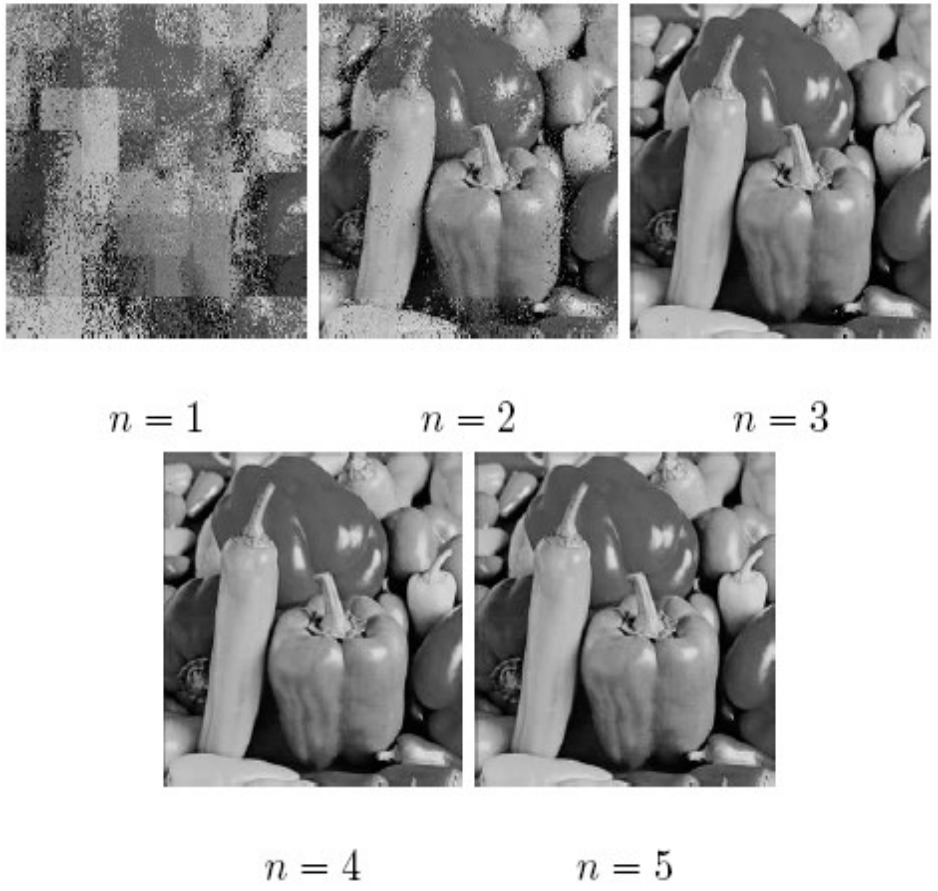
Kann er die Permutation richtig erraten, um ein weiteres Bild, vom der er nicht das Original kennt, zu rekonstruieren?



Je mehr Originale und ihr Chiffrat bekannt sind, desto besser kann das Bild rekonstruiert werden.

Hier die Ergebnisse für 1 bis 5 bekannte Originale.

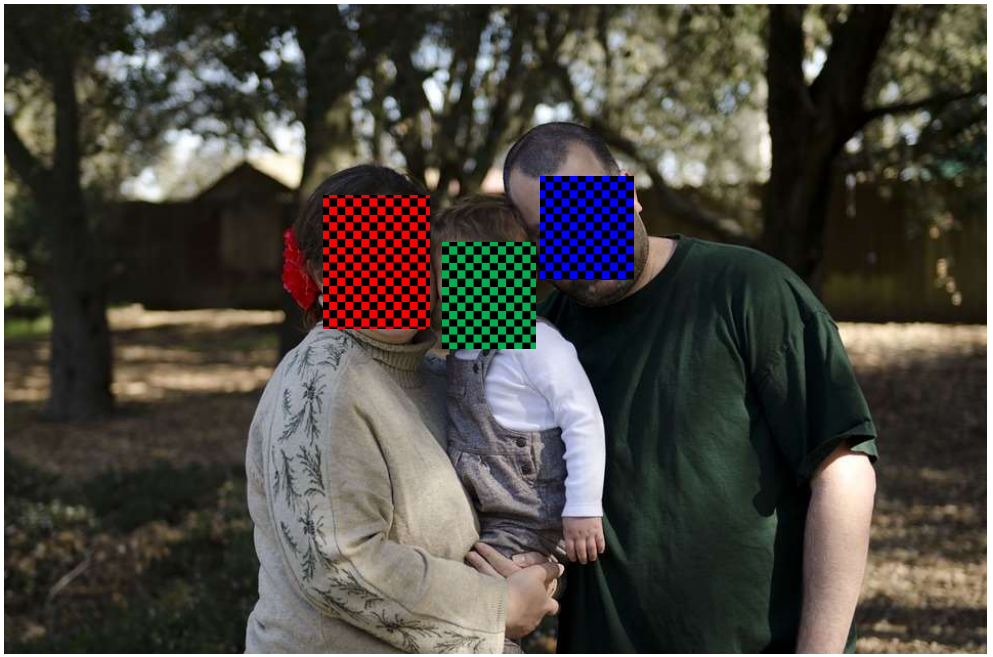
Die Umkehrung der Permutation kann immer präziser geschätzt werden.



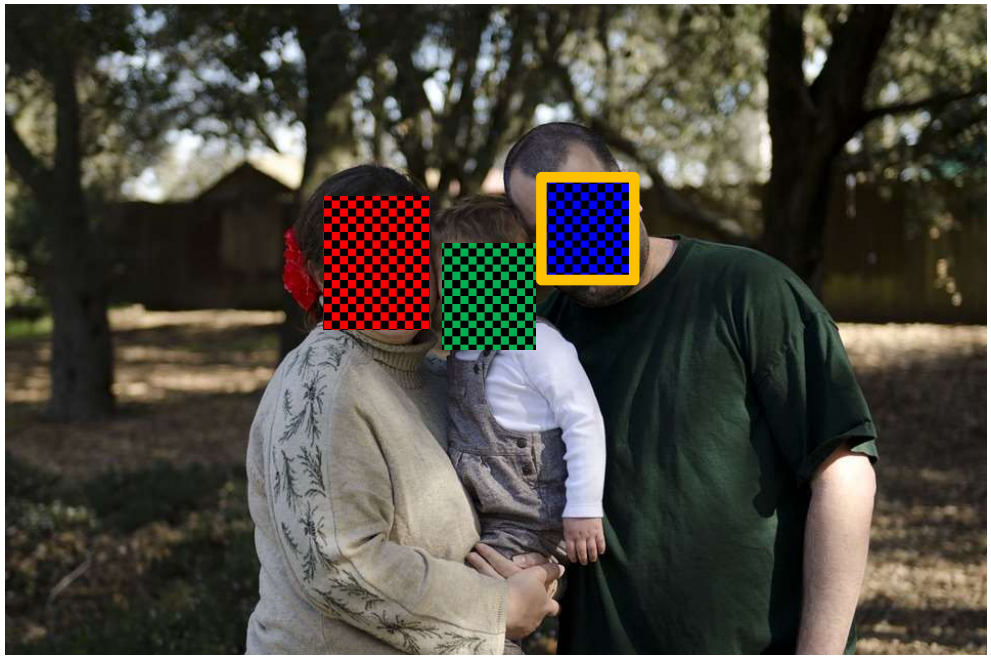
- Beispiel Bildauswertung
- Wer darf in einer Ermittlung auf gesammelte Private Bilder zugreifen?
- Wie kann die Privatspähre von Unschuldigen geschützt werden?
- Ansatz: Lokale Verschlüsselung und geeignete Protokolle

– Original (Beispielfoto CC0, Pixabay)

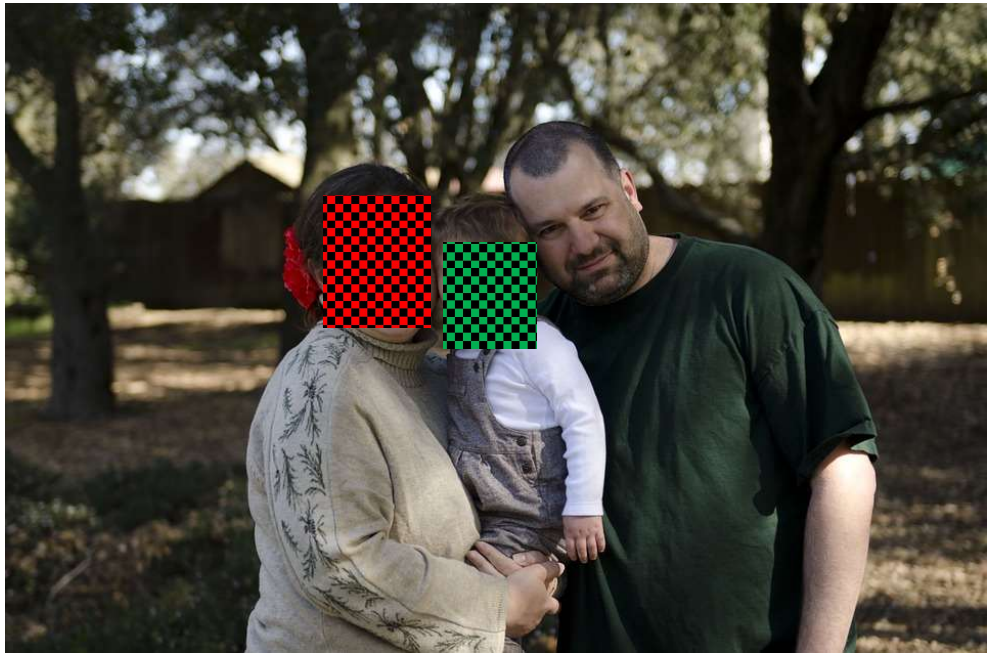
– Gesichtserkennung und lokale Verschlüsselung
  • Jedes Segment ist mit einem individuellen Schlüssel verschlüsselt



- Ein Ermittler möchte eine Person auf dem Bild identifzieren
- Dazu wählt er die entsprechende Person aus
- Ein Staatsanwalt erhält die Anfrage zur Demaskierung
- Er kann dem Ermittler den Schlüssel bereitstellen



- Ermittler kann den individuellen Bereich entschlüsseln
- Restliche Personen bleiben geschützt



Hybride Verschlüsselung

- Datenschutzgerechter Umgang mit Personenbildern
  - Bilder müssen mit Standardsoftware darstellbar sein.
  - Speicherkosten müssen akzeptabel sein
  - Verlustfreie Entschlüsselung muss möglich sein
  - Die Sicherheit gegen die Privatsphäre muss hoch sein.
- Entschlüsselung auf eine Ebene, auf der Personen erkannt werden können.

Hybride Verschlüsselung

- Zwei Ansätze zur Verschlüsselung
- Vollständige Verschlüsselung
  - Standard-Verschlüsselung der ausgewählten Elementen
  - Z.B. Niedrige Koeffizienten von JPEG
  - Starke Teilsicherheit
  - Massive Erhöhung der Dateigröße

Origin coefficients	105	4	0
Bit-stream	00001101001	00000000100	00000000000
Encrypted bit-stream	10000111101	11101010110	11100011100
Encrypted coefficients	−963	−170	−228
Additional required Bits	3	5	16

Hybride Verschlüsselung

- Codefreundliche Verschlüsselung
- Anzahl der Bits wird nicht geändert
  - z.B. JPEG-Bit-Codierung für Koeffizientenwerte
- Schwache Teilsicherheit
- Keine Erhöhung der Dateigröße

Origin coefficients	105	4	0
Bit-stream	1101001	100	—
Encrypted bit-stream	1000011	111	—
Encrypted coefficients	67	7	0
Additional required Bits	0	0	0

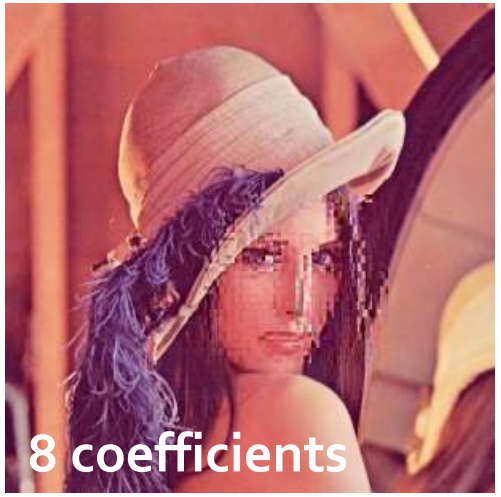
Hybride Verschlüsselung

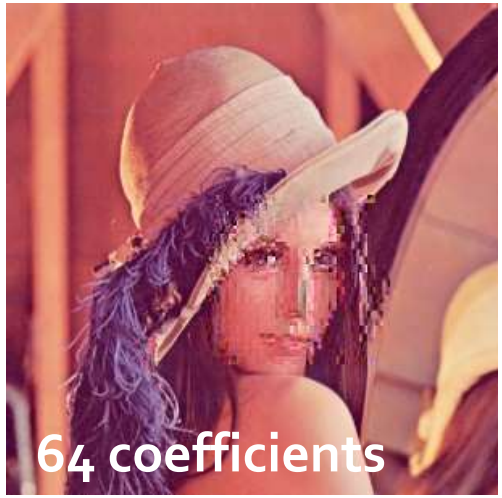
- Angriffe auf partielle Verschlüsselung
- Aufdecken der Identität möglich/ denkbar?

Beispiele

- Full encryption

- Code-friendly encryption





Hybrid Encryption

- Hybride Verschlüsselung
- Ziele
  - Replacement attack erschweren
  - Dateigrößen klein halten
- Strategie
  - Niedrige Frequenzen: Full encryption
  - Hohe Freuqenzen: Code-friendly encryption
- Wirkung
  - Zuwachs Dateigröße bei niedrigen Frequenzen überschaubar
  - Kanten bei hohen Frequenzen werden verwischt

Hybride Verschlüsselung:
N Koeffizienten Full Encryption
64-N Koeffizienten Code Friendly Encryption

Nach Replacement Attack

- Bildqualität nach replacement attack
- Jeweils mit 2 Koeffizienten full encryption

Nach Replacement Attack

Lokale partielle Verschlüsselung
von Gesichtern in JPEG-Bildern,
Richard Stein, Masterthesis TU Darmstadt

(a) Lena vollverschlüsselt
mit je 8 Koeffizienten pro Block

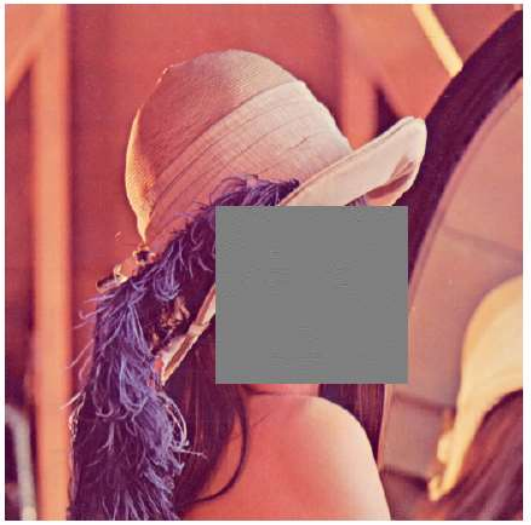
(b) Lena hybrid verschlüsselt
mit je 8 Koeffizienten pro Block

(c) Lena vollverschlüsselt
mit je 16 Koeffizienten pro Block

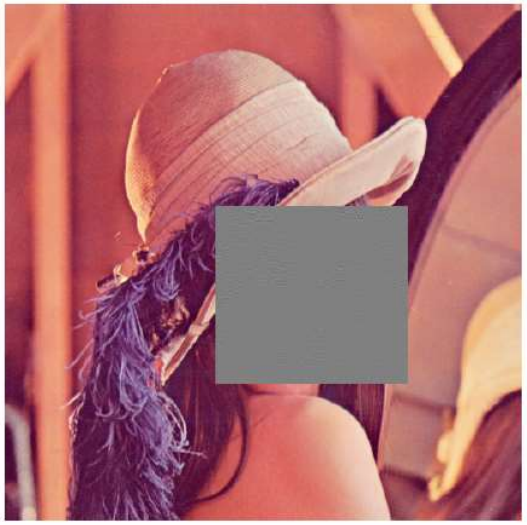
(d) Lena hybrid verschlüsselt
mit je 16 Koeffizienten pro Block

Nach Replacement Attack

- In den hohen Koeffizienten steckt so gut wie keine Bildinformation mehr

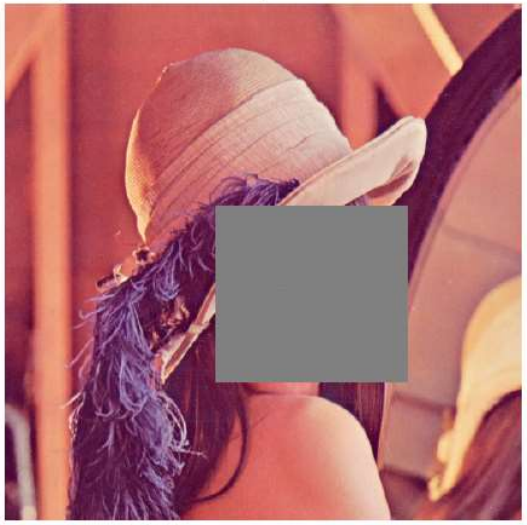


(e) Lena vollverschlüsselt mit je 32 Koeffizienten pro Block



(f) Lena hybrid verschlüsselt mit je 32 Koeffizienten pro Block

(g) Lena vollverschlüsselt mit je 48 Koeffizienten pro Block



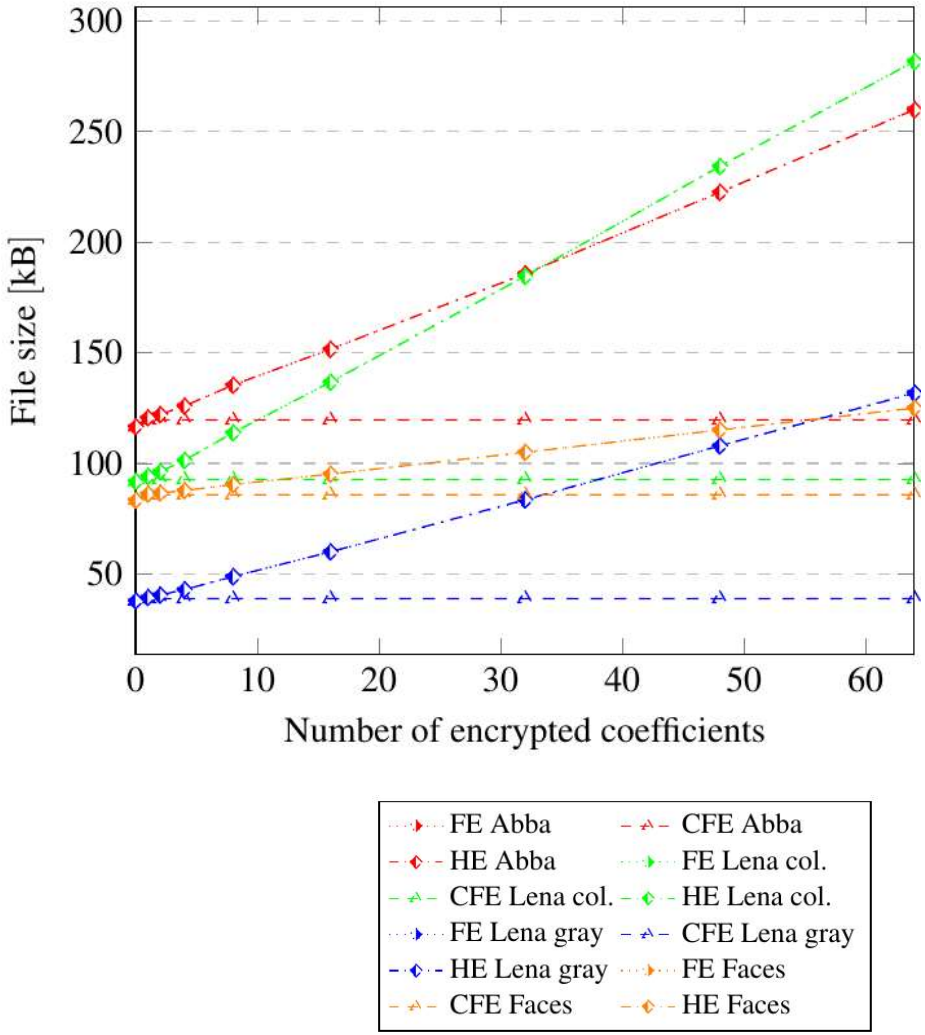
(h) Lena hybrid verschlüsselt mit je 48 Koeffizienten pro Block

Literatur

- Privacy Preserving Forensics for JPEG Images
  - https://doi.org/10.2352/ISSN.2470-1173.2018.07.MWSF-120
- Hybrid Image Encryption
  - https://doi.org/10.2352/ISSN.2470-1173.2018.07.MWSF-371

Dateigröße

- FE: Full Encryption
- HE: Hybrid Encryption
- CFE: Code-Friendly Encryption



Partielle Verschlüsslung / Audio

Welche Teile des MPEG Audio Frames lassen sich verschlüsseln?

- Header
  - Datenstrom wird falsch interpretiert, Datei nicht abspielbar,
  - mit Kenntnis des mp2-Formats kann Header durch Probieren ermittelt werden

- Audiodaten

  – Allokation, SFAI: Datenstrom wird falsch interpretiert, alle Bitfehler katastrophal

  – Abtastwerte: Datenstrom bleibt abspielbar, Auswirkungen auf Klang gut regelbar, Abtastwerte machen größten Teil der Datei aus (über 90%)

  – Skalenfaktoren: Datenstrom bleibt abspielbar, Auswirkungen gut regelbar, nur ca. 3% des Datenstroms bestehen aus Skalenfaktoren

jeder MP2-Skalenfaktor: 6 Bit Integer Wert (einige Dutzend pro Frame)

Auswirkungen auf Klangqualität bei Veränderung der MP2-Skalenfaktoren:

Parameter	Bit-Nummer	Auswirkungen
Bit Allokation	alle	katastrophal (nicht-abspielbar)
SFAI	alle	katastrophal (nicht-abspielbar)
Skalenfaktoren	5 (=MSB)	sehr störend
	4	sehr störend
	3	sehr störend
	2	störend
	1	wahrnehmbar, nicht störend
	0 (=LSB)	nicht wahrnehmbar
Abtastwerte	8-16 (=MSB)	sehr störend
	5-7	störend
	3,4	wahrnehmbar, nicht störend
	0-2 (=LSB)	nicht wahrnehmbar

[ISO MPEG-1]

→ MP2-Skalenfaktoren gut geeignet für partielle Verschlüsselung

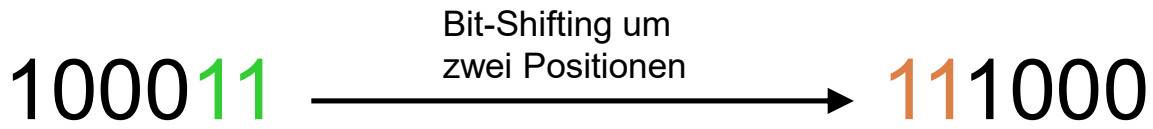
Nebenbedingung:

ein Skalenfaktor darf nicht den Wert 63 annehmen
(nach ISO MPEG Spezifikation verboten)

Gewählter Ansatz:

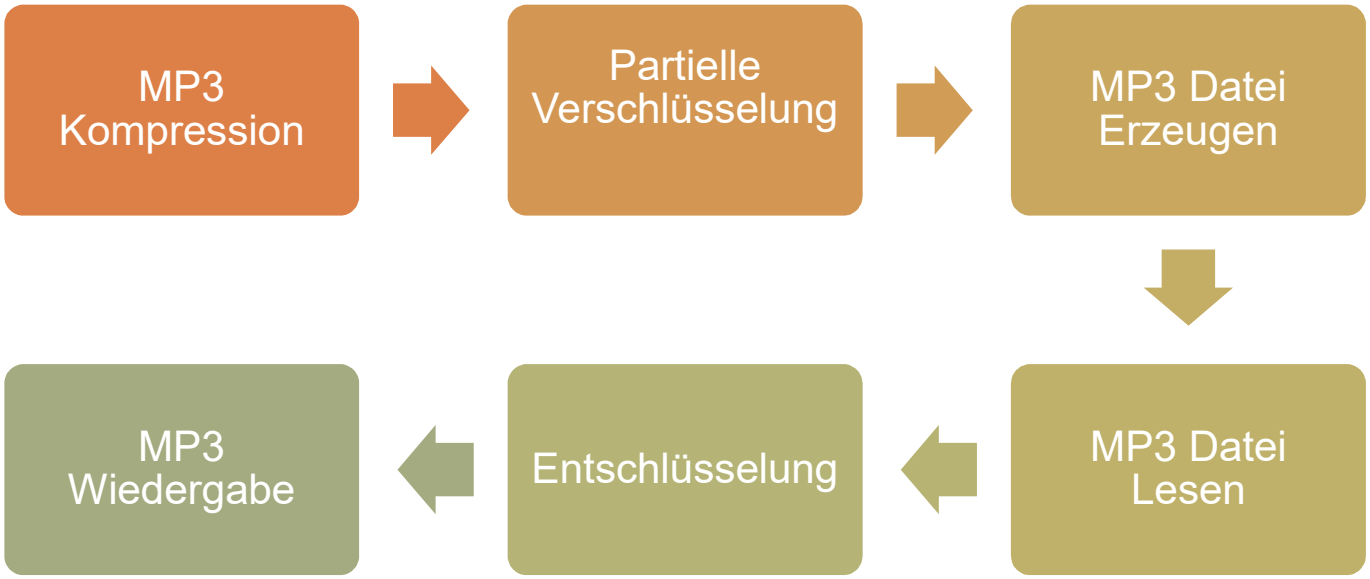
- pseudozufälliges Bitshifting der Skalenfaktoren

- je nach gewünschter Stärke werden nur die jeweils *n* niederwertigsten Bits eines Skalenfaktors verschlüsselt (*n* =1...6)



Partielle Verschlüsslung mp3

- Pragmatischer Ansatz:
  - Kombination mp3 codec und AES Verschlüsselung
  - Umgesetzt mit LAME und Krypto-Lib



Partielle Verschlüsslung mp3

- Ergebnisse
  - Verschlüsselung erzeugt kaum Overheadkosten

	Encoding	Decoding
Unmodified LAME	3.879 s / 0.336 s	0.384 s / 0.139 s
Modified LAME	3.872 s / 0.339 s	0.387 s / 0.138 s
SFC crypting	3.888 s / 0.332 s	0.394 s / 0.141 s
SF crypting	3.976 s / 0.350 s	0.504 s / 0.153 s

  - SF: Skalenfaktoren
  - SFC: SF Kompressionstabelle

  - AES auf unverschlüsselte Datei:
    - 0.557 s / 0.072 s Verschlüsselung
    - 0.538 s / 0.052 s Entschlüsselung

Steinebach, Martin & Berchtold, Waldemar. (2017). MP3 Partial Encryption for DRM. Electronic Imaging. 2017. 28-35. 10.2352/ISSN.2470-1173.2017.7.MWSF-322.

Paper Volltext: https://www.ingentaconnect.com/contentone/ist/ei/2017/00002017/00000007/art00006?crawler=true&mimetype=application/pdf

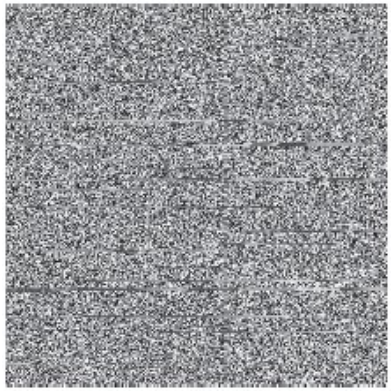
Robuste Verschlüsslung

- Verschlüsslung, die resistent gegenüber Operationen im verschlüsselten Zustand ist
- Motivation:
  - A will B ein Bild schicken
  - Dazu will A ein öffentliches Forum verwenden
  - Nur B soll das Bild lesen können
  - Die Bildfunktion im Forum passt Bilder automatisch an, z.B. über Skalierung
  - Das Forum erlaubt es nicht, verschlüsselte Daten als Anhang zu verwenden
- Kann ein Bild so verschlüsselt werden, dass
  - Das Format erhalten und es z.B. ein korrektes JPEG Bild bleibt
  - Das verschlüsselte Bild durch die Operationen im Forum nicht zerstört wird
- Naiver Ansatz:
  - JPEG Koeffizienten mit AES 256 verschlüsseln
  - Format: OK, Operationen: Fail…

Robuste Verschlüsslung

- Transfer von Medien kann zu Übertragungsfehlern führen
- Bei gebräuchlichen Verschlüsslungsverfahren kann schon ein kleiner Fehler dazu führen, dass das Medium nicht mehr sinnvoll entschlüsselt werden kann
- Beispiel AES128 Verschlüsslung

Random Error
Bytewerte zufällig verändert



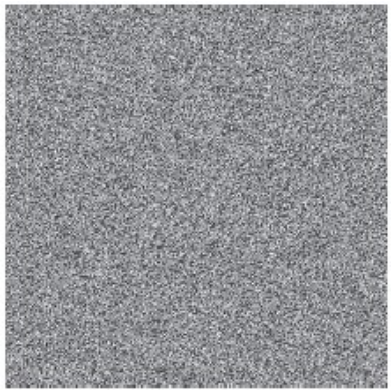
Random Buffer Error
Zufälliges Löschen oder Doppeln von Bytes

Hindawi Publishing Corporation EURASIP Journal on Information Security, Volume 2007, Article ID 48179, 16 pages
doi:10.1155/2007/48179
Transmission Error and Compression Robustness of 2D ChaoticMap Image Encryption Schemes
Michael Gschwandtner, Andreas Uhl, and Peter Wild

Robuste Verschlüsslung

- Alternative zur herkömmlichen Verschlüsslung: Chaotic Map (CM) Algorithmen
- Schlüsselabhängige Permutation von Pixeln in mehreren Iterationen
- Diffusion von Pixelwerte durch pseudozufällige Werte zum Schutz vor Known Plaintext Angriffen
- Beispiel: 2DCatMap

Random Error
Bytewerte zufällig verändert



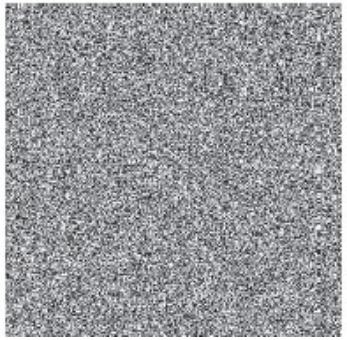
Random Buffer Error
Zufälliges Löschen oder Doppeln von Bytes

Hindawi Publishing Corporation EURASIP Journal on Information Security, Volume 2007, Article ID 48179, 16 pages
doi:10.1155/2007/48179
Transmission Error and Compression Robustness of 2D ChaoticMap Image Encryption Schemes
Michael Gschwandtner, Andreas Uhl, and Peter Wild

Robuste Verschlüsslung

- 2DCatMap Robustheit gegen JPEG
- Erforderlich: Abwägen zwischen Sicherheit und Robustheit

Robust bei Permuation



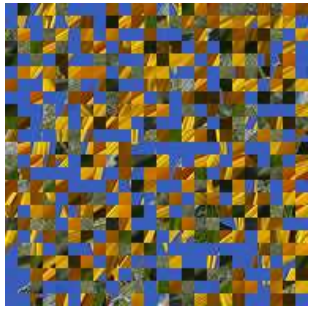
Diffusion zerstört die Robustheit

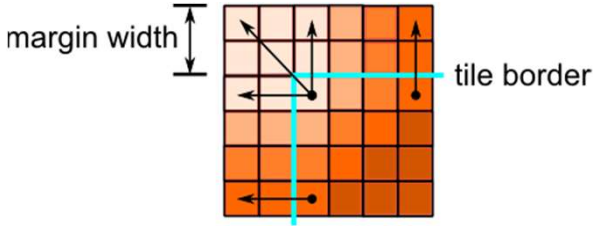
Hindawi Publishing Corporation EURASIP Journal on Information Security, Volume 2007, Article ID 48179, 16 pages
doi:10.1155/2007/48179
Transmission Error and Compression Robustness of 2D ChaoticMap Image Encryption Schemes
Michael Gschwandtner, Andreas Uhl, and Peter Wild

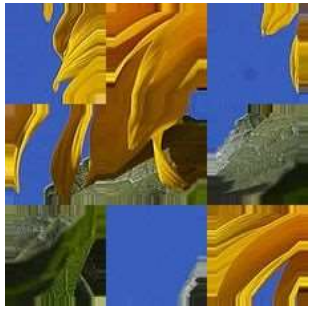
- Robustheit gegen
  - JPEG Kompression
  - Skalierung
- Ansätze
  - Permutation
  - Rauschmuster
  - Kombinationen aus beiden

Poller, Andreas, Martin Steinebach, and Huajian Liu. "Robust image obfuscation for privacy protection in web 2.0 applications." *Media Watermarking, Security, and Forensics 2012*. Vol. 8303. International Society for Optics and Photonics, 2012.

- Robuste Verschlüsslung durch Permutation von Kacheln
- Qualitätsverlust durch JPEG an Kanten
- Lösung: Übergänge an Kachelrändern

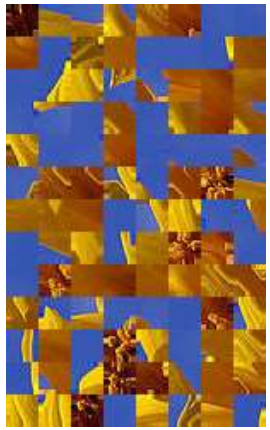






Kacheln als robuste Verschlüsslung

Original

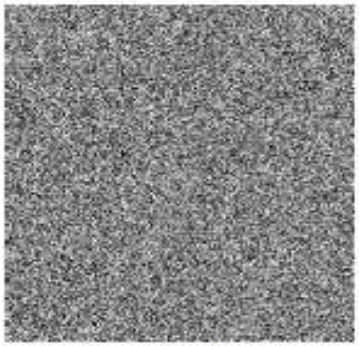


Obfuscated

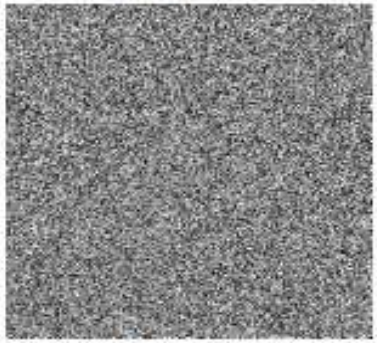
- Robuste Verschlüsselung durch Helligkeitsmuster

original

limited



pattern



obfuscated

de-obfuscated

obfuscated with 16x16 pattern

- Fehler bei Addition, Kompression und Subtraktion

Pixel P + Maske M = P‘
Kompression P‘ = P“
P“ – M <> P

254+30=284
284Mod256=28
Kompression (28)=30
30-30=0
Aus fast weißem Pixel wurde ein schwarzes Pixel.