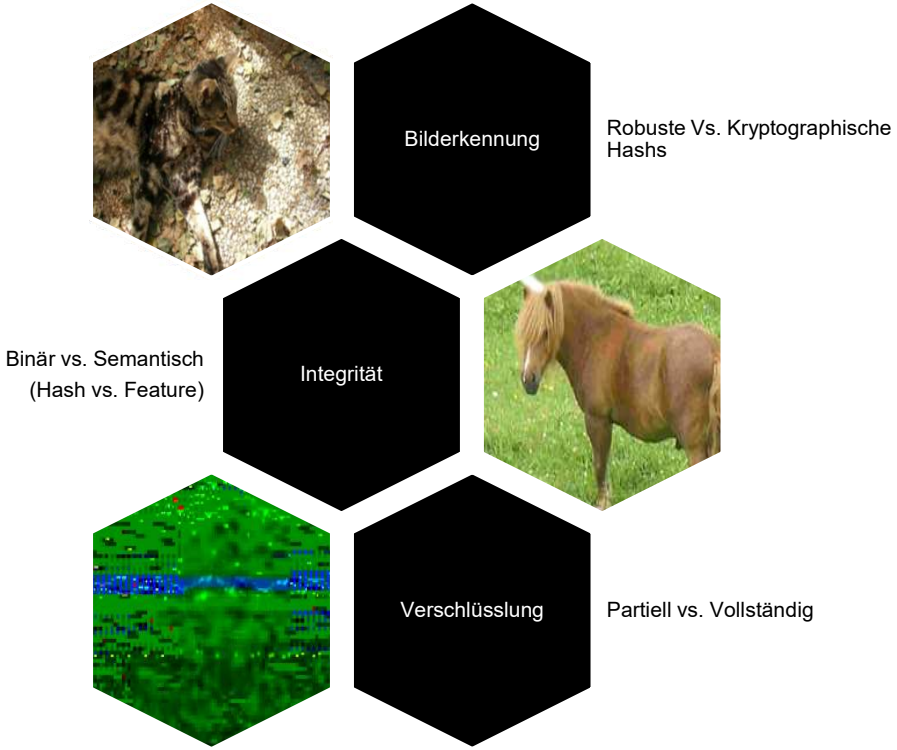
- Ist Kryptographie geeignet für Multimedia-Umgebungen?
  - Notwendige Rechenleistung für Video on Demand (VoD)
  - Übertragungskanäle für komprimiertes Audio und Video?
    - Wie reagiert eine Umgebung auf verschlüsselte Datenpakete?
  - Kryptographie endet beim Konsumenten ...

Herausforderungen Multimedia

- Kryptographie ist oft nur bedingt geeignet für Multimedia Anwendungen
- Beispiele



Partielle Verschlüsslung

- Verschlüsslung, angepasst an Anforderungen im Medienbereich
  - Video
  - Audio
  - Einzelbild
- Verschlüsslung von relevanten Teilen eines Medienstroms, wobei das Medium selbst abspielbar bleibt

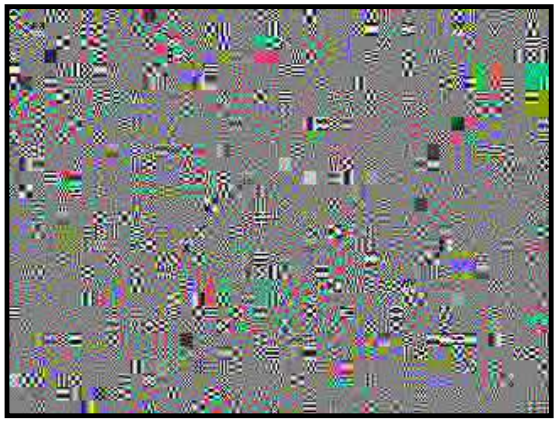
Partielle Verschlüsslung

- Es existieren zwei Anwendungsgebiete:
  - Partielle Verschlüsslung
    - Relevante Anteile werden unkenntlich gemacht
    - Schutz von Vertraulichkeit
    - Videokonferenzen
    - Telefonate über VoIP
  - Transparente Verschlüsslung
    - Qualitätsverminderung bei Wahrung relevanter Anteile
    - Schutz von Urheberrechten
    - Preview von Bildern, Audio, Video

Partielle Verschlüsslung

Original

Partielle Verschl.



Transparente Verschl.

Luminance 0
Luminance 0-5
Luminance und Chrominance 0-5

Partielle Verschlüsslung / Bild

Das Original

Partiell (Kopf)

Transparent (Scarring)

Missier, P. (1997). Technology for the copyright protection of digital images.

Partielle Verschlüsslung / Video

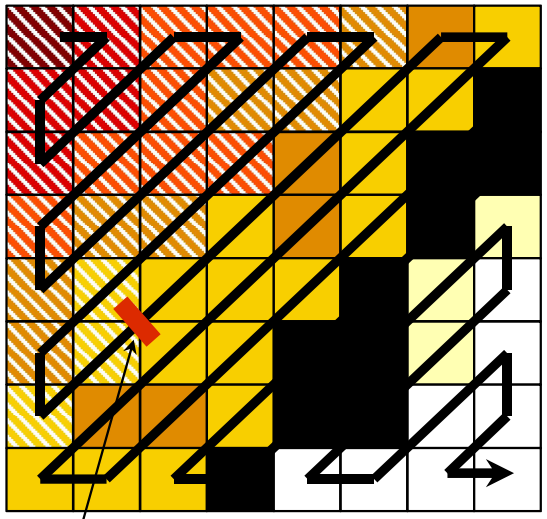
- Video Daten sind umfangreich
- In verschiedenen Anwendungen ist Echtzeit-Streaming notwendig
  - Aufwand für Verlüsslung sollte möglichst gering sein
- Vorteile der partiellen Verschlüsslung:
  - Leistung an schwächste Maschine im Gesamtsystem angepasst
  - Rechenleistungsfreisetzung
  - Applikation kann Gesamtstrom noch immer parsen und Synchronisation möglich
  - gezielter Schutz, transparente Verschlüsselung möglich
- Nachteile:
  - Zusatzinfos zur Lage und Umfang der verschl. Datenanteile
  - Veränderungen an Sende- und Empfangscodec
  - Redundanzen in Klartextanteilen lassen oft Rückschluss auf verschlüsselten Anteil zu

Partielle Verschlüsslung / Video

- Frage: Welche Daten verschlüsseln?

- Beispiel Videokonferenz:
  - Audiodaten zu Video
  - Schutz der Erkennbarkeit der Personen
  - Gesicht/Lippenbewegungen
  - Bildhintergrund, Rückschlüsse auf Situation
  - Textelemente
  - Angaben über Sender- und Empfänger (Anonymisierung)

- Permutation nach Kunkelmann
  - http://www.sigmm.org/archive/MMSec/mmsec98/workshop.pdf
- Auswahl der relevanten Bilddaten
  - Niedrige Frequenzen für partielle Verschlüsslung
  - Hohe Frequenzen für transparente Verschlüsslung
- Skalierbar durch Setzen eines Schwellwerts



Verschlüsselte Koeffizienten (schraffiert)

Unverschlüsselte Koeffizienten

Schwellenwert (Koeffizient n=23)

- Permutation von DCT-Koeffizienten
  - insgesamt 64 DCT-Koeffizienten werden permutiert
  - 64! oder 10^89
  - Nachteil: Entropiecodierung verschlechtert
  - 20-40% Vergrößerung der orginalcodierten Videos
  - nicht sicher gegen statistische Analysen, da DC-Koeffzient meist größter Wert (Aufteilung auf 2 andere)
  - Spezieller Video-Encoder und Video-Decoder nötig

Figure 6: *Coastguard*: Original (left), transparent encryption with 75% protected data (right).

- Beispiel für transparente Verschlüsselung
- http://www.sigmm.org/archive/MMSec/mmsec98/workshop.pdf

Mehr zum Thema:
T. Kunkelmann, U. Horn , Partial Video Encryption Based on Scalable Coding, 5th International Workshop on Systems, Signals and Image Processing (IWSSIP'98), Zagreb, Croatia, June 1998, ISBN 953-184-010-5

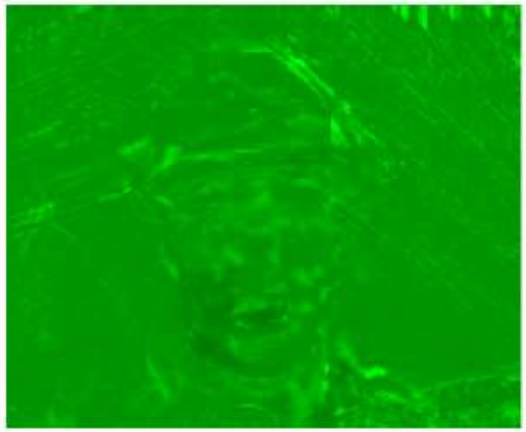
Partielle Verschlüsslung / Frühe Angriffe

- Recontruction attack
  - Erkennen von verschlüsselten Bereichen
  - Ersetzen von Crypto-Rauschen durch schwarze Flächen / Nullen
  - Beispiel: Angriff auf 50% partiell verschlüsseltes Video

http://www.sigmm.org/archive/MMSec/mmsec98/workshop.pdf

- " […] the image is degraded beyond acceptability for entertainment purposes. Since intra refreshes in P-VOPs are also encrypted, no blockwise revealations occur. It can be concluded that high motion sequences, where **bits corresponding to prediction errors coded as texture are unencrypted**, may reveal the nature of the motion and the video sequence […]. This revealation is not of acceptable quality for entertainment, but it may be informative if the encrypted video is just a peer-to-peer communication. […]

  Aus: Partial Encryption Of Video For Communication And Storage (2003) , Turan Yüksel



- Abhängigkeit Sicherheit und Medium:
  - Gleiches Verfahren bei weniger Bewegung und nierigerer Bitrate des Videos
  - Deutlich bessere Verschlüsselung bzw. höhere Unkenntlichkeit

Aus: Partial Encryption Of Video For Communication And Storage (2003) , Turan Yüksel