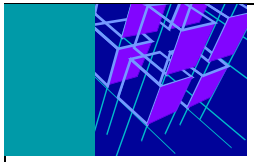
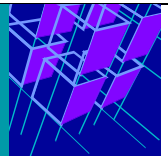


Das Internet der Zukunft
Sicherheit in Medienströmen

Prof. Dr.-Ing **Ralf Steinmetz**

TU Darmstadt, FB Elektrotechnik & Informationstechnik (Zweitmitglied FB Informatik)
KOM - Industrielle Prozeß- und Systemkommunikation,
Merckstr. 25, D-64283 Darmstadt, Ralf.Steinmetz@KOM.tu-darmstadt.de

GMD - Forschungszentrum Informationstechnik GmbH
IPSI - Institut für Integrierte Publikations- und Informationssysteme
Dolivostr. 15, D-64293 Darmstadt, Ralf.Steinmetz@darmstadt.gmd.de



1. Trends

System: Moore's Gesetzmäßigkeit erweitert

$$C(n) = C_0(2^{n/k})$$

	angewendet auf z.B.	Verdopplung alle k=
Endsystem	Prozessorgeschwindigkeit	1,5 Jahre
	Primärspeichergröße	1,2 Jahre
	Sekundärspeichergröße	1,1 Jahre
Kommunikation	Zahl der Internet-Hosts (mind.)	1 Jahr
	Größe des Webs (Seiten)	10 Monate
	Menge der Webdaten (bit)	6 Monate
	Internet-Datenverkehr (US Backbone)	5 Monate

Anwendungen:

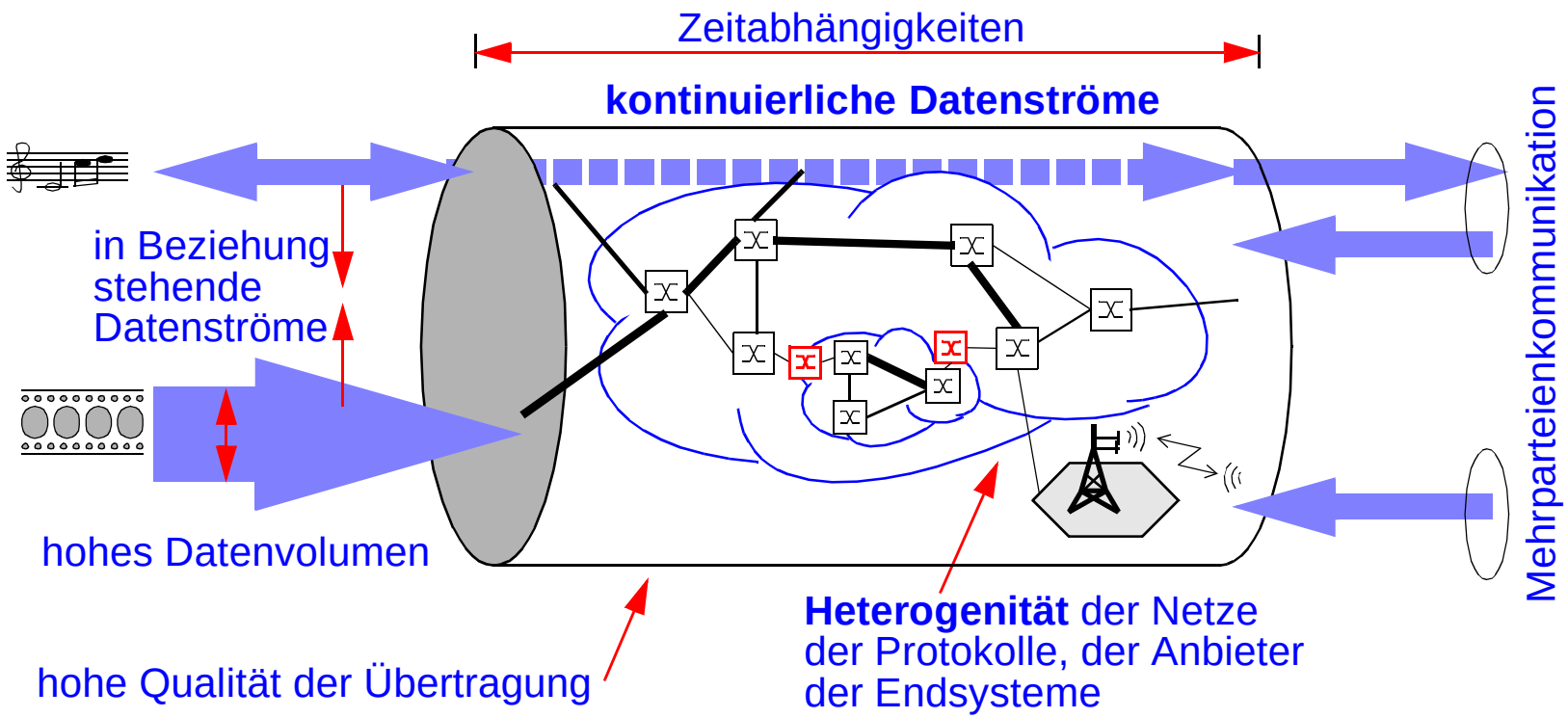
- Informationen, Transaktionen, ...
- elektronische Post, ...
- IP-Telefonie, "world wide wait", ...

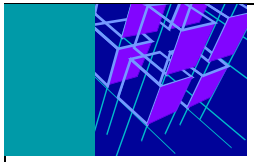
Eigenschaften:

- Internet: unvorhersehbare, oft schlechte Qualität der Datenübertragung
- "best effort Dienst"

d.h. "Wissen über Inhalte zur Kommunikation & Verarbeitung nutzen"

2. Anforderungen





3. Das Internet der Zukunft, diverse IETF Gruppen

Widersprüchliche oder koexistierende Ansätze?

Internet Integrated Services

- **Ratio**
  - begrenzte Betriebsmittel
  - harte Qualitätsanforderungen
- **Ansatz**
  - Betriebsmittelreservierung
  - pro Verbindung / Fluß
- **Methode**
  - verteiltes Steuerungsprotokoll Resource ReSerVation Protocol
  - Router identifizieren Flüsse
  - Scheduling
- **Dienste**
  - best effort service
  - controlled load service
  - guaranteed service
- **Skalierbarkeit für große Netze ?**
  - Paketklassifikation in Core-Router

Internet Differentiated Services

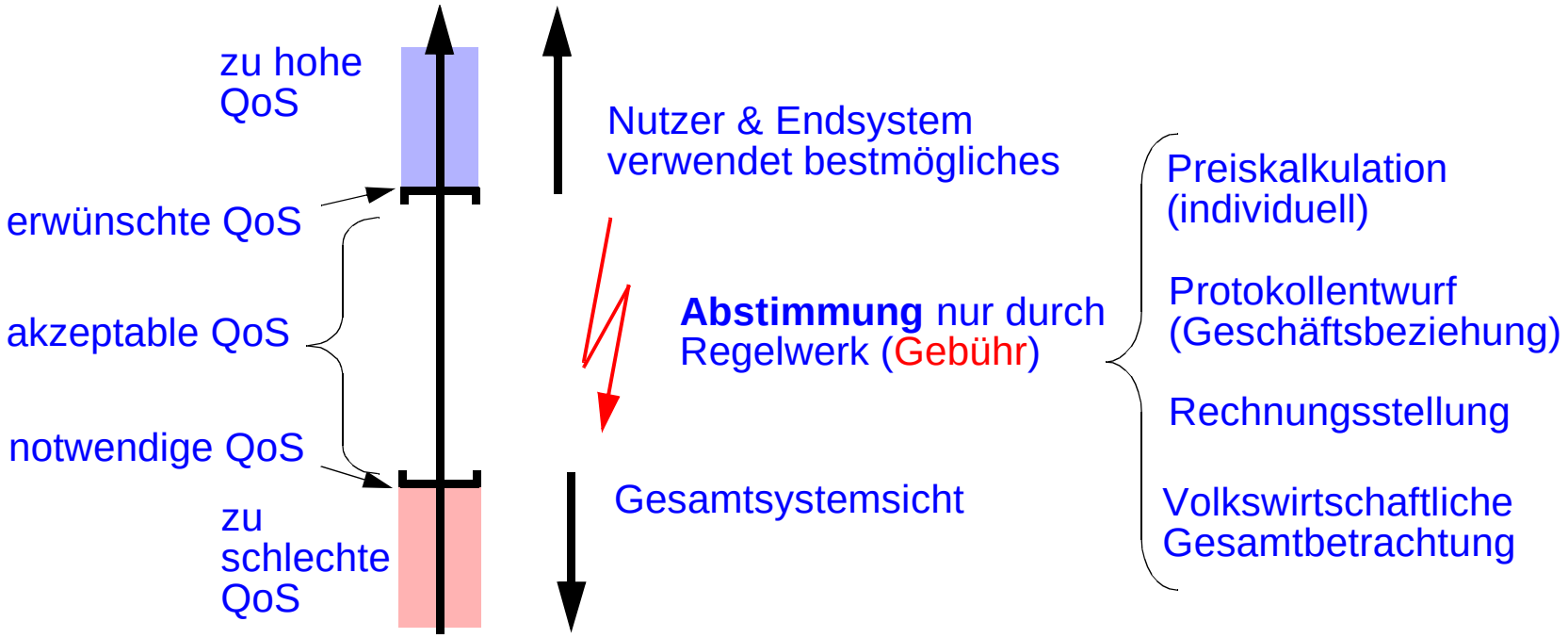
- **Ratio**
  - Überangebot von Betriebsmitteln
  - adaptive Datenströme
- **Ansatz:**
  - Aggregation von Flüssen
  - Reservierung für Aggregate
- **Methode**
  - statische Steuerung
  - Pakete mit Prioritäten markieren
  - Prioritätsklassen “loss” und “delay”
- **Dienste (Vorschläge)**
  - premium, expedited forwarding & assured (max. Pakete hoher Prio)
  - “Olympic”: (Gold 60%, Silber 30%, Bronze 10% Datenmenge)
- **keine harten Garantien**
  - Paketklassifikat. an Netzgrenzen

4. Dienstgüte und Abrechnung

einige interessante Tatsachen

- Verbindungen oft nur von sehr kurzer Dauer und viele gleichzeitig
- nicht kooperative Anwendungen & Nutzer überschwemmen Netz
- Protokolle werden für individuellen Nutzen optimiert
  (mehr UDP Datenverkehr, unfaire TCP-Implementierung)
- in Ökonomie “Tragedy of commons” (jeder verwendet bestmögliches)
- eigentlich keine Gleichbehandlung aller Pakete erwünscht

Gleichgewicht ⇒ Gebühren (Kompensation, Wettbewerbsmechanismus)



5. “Internet 2” und “Next Generation Internet”

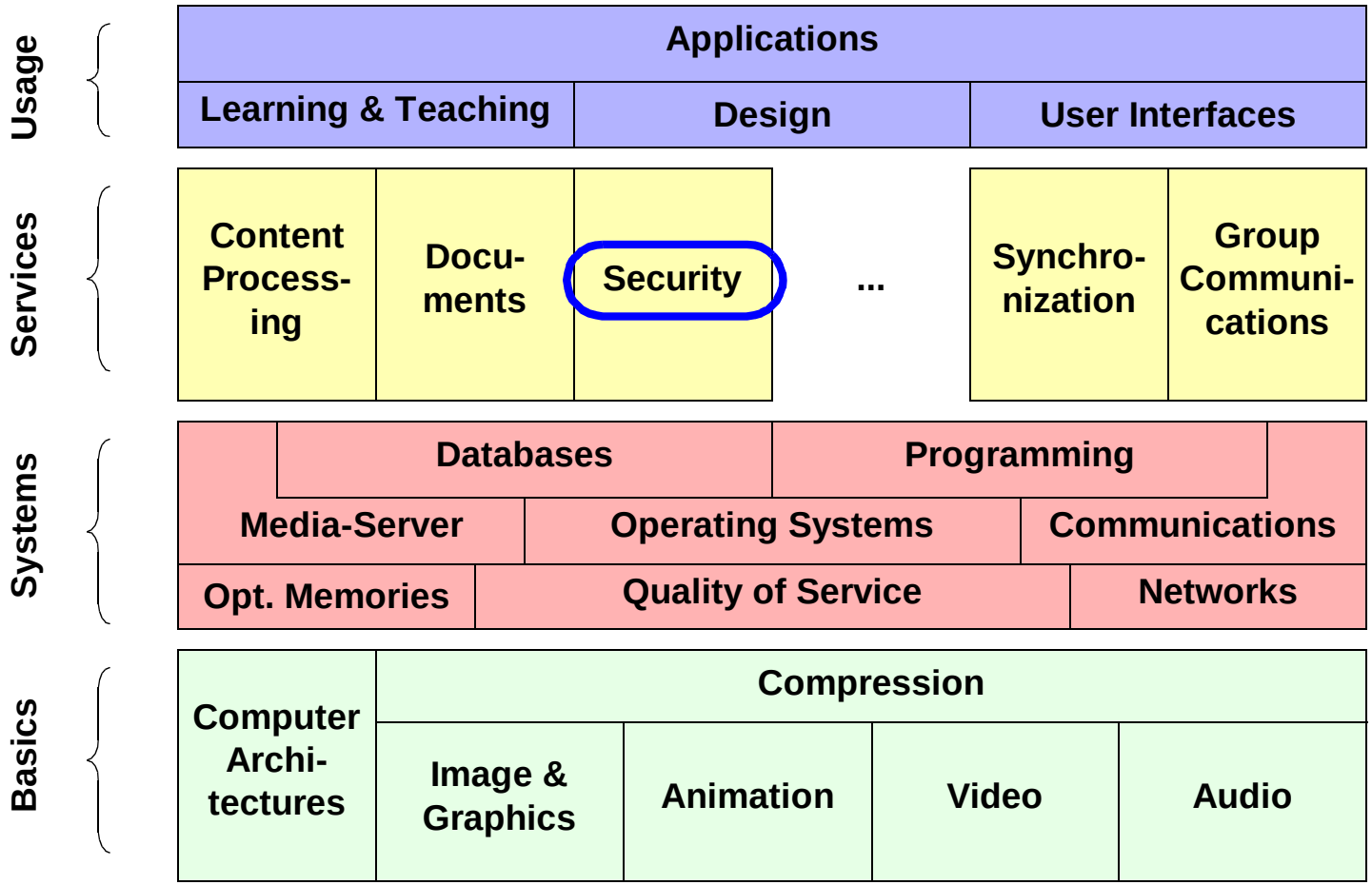
Internet 2

- **1996 Projekt zwischen 34 Univ. gestartet**
- **starke Industrieunterstützung**
  - $500Mio: Cisco Systems, 3Com, MCI ...
- **Infrastruktur für Wissenschaft und Lehre**
- **GigaPOPs mit Kapazitäten**
  - OC-12 (622 Mbps), OC-48 (2.5 Gbps), ..
- **Eigenschaften**
  - Dienstgütekonzepte integriert
  - als “proof of concept” angelegt
  - neuartige Anwendungen: was macht man mit der Bandbreite?

Next Generation Internet (NGI)

- **1996 als Regierungsinitiative begonnen**
- **Ziele (Clinton, 10.10.1996, Oak Ridge, Tenn.)**
  - “ 100 bis 1000 fach schneller als heutiges Internet, sicher genug, nutzbar für jeden Amerikaner, ...”
- **Nutzung in Medizin, Nationaler Sicherheit ,“Distance Education”**

6. Übersicht


Usage
Services
Systems
Basics
Applications
Learning & Teaching
Design
User Interfaces
Content Process-ing
Docu-ments
Security
...
Synchro-nization
Group Communi-cations
Databases
Programming
Media-Server
Operating Systems
Communications
Opt. Memories
Quality of Service
Networks
Computer Archi-tectures
Compression
Image & Graphics
Animation
Video
Audio

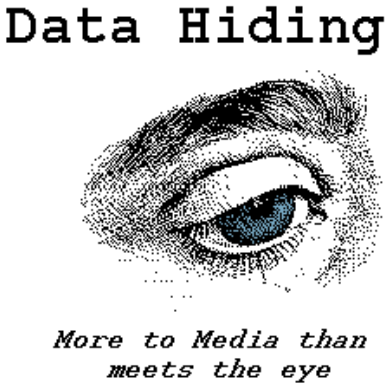
7. Motivation

Datenexplosion

- **digital Daten in mehreren Medien**

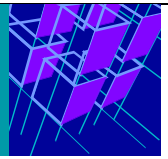
Auswirkungen im Anwendungskontext

- **im Web Bereitstellung von Information nur bei Urheberschutz**



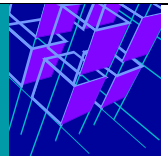
z.B. Urheberrecht

- **Schutz des geistigen Eigentums (auch digitale Daten, Programme, etc.) und der Art und Weise der Gestaltung vor**
  - unbefugte wirtschaftliche Verwertung des Werkes
  - Verletzung der ideellen Interessen am Werk
- **Rechte**
  - Urheberpersönlichkeitsrecht
  - Verwertungsrechte
  - (Vervielfältigungs-, Verbreitungs- und Senderechte)
  - sonstige Rechte
- **Grenzen des Urheberrechts: Allgemeininteresse**



7.1 Relevante Aspekte

• **Zugriffsschutz**	• Kontrolle des Systemzuganges und Zugriffsbeschränkungen	**Medien-Firewalls**
• **Authentizität**	• Nachweis der Identität des **Urhebers** • Verifizierung der Echtheit der Daten • Authentifizierung wird vorgenommen und damit die Authentizität bestätigt • “Spoofing”	**robuste Wasser-zeichen**
• **Vertraulichkeit**	• Verhindert, daß Unberechtigte Daten “lesen” bzw. darauf zugreifen können • “Man in the Middle”	**(partielle) Verschlüs-selung**
• **Integrität**	• Nachweis, daß die Daten unverändert vorliegen • “Replay”	**fragile Wasser-zeichen**
• **Nachweisbarkeit**	• Prüfung der **Authentizität** und **Inte-grität** der Daten (auch von berechtig-ten Dritten) • gewährleistet Verbindlichkeit der Kommunikation	**s.o.**



8. Vertraulichkeit - partielle Verschlüsselung

Kryptologie: **algorithmischen Methoden zur Sicherung oder Verheimlichung von Informationen**

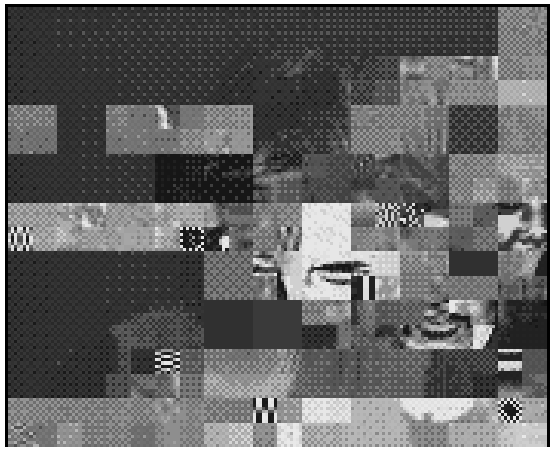
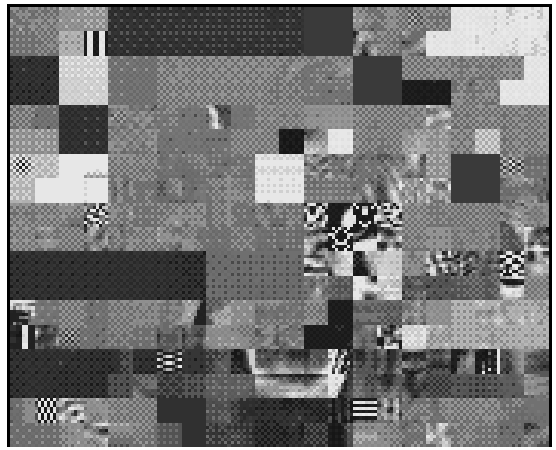
- ***Kryptographie*****: Entwicklung neuer Systeme zur Sicherung & Verheimlichung von Informationen**
- ***Kryptoanalyse*****: diese Systeme attackieren und brechen, um die Sicherheit zu beurteilen**

Multimedia Daten - partielle Veschlüsselung

- wegen hoher Datenmenge, d.h. Aufwand
- wegen gewollter Darstellung in reduzierter Qualität

- **einfache Verfahren (wie Permutationsverfahren) sind angreifbar**
  - Zeilenpermutation (bzw. Pixelpermutation)
  - Zeilenverschiebung horizontal (auch analoges TV)
- **sichere Verfahren sind rechenintensiv**
  - Verschlüsselungsalgorithmen: DES, IDEA, RC4
  - Videodaten: Übertragung in Echtzeit
- **gezielter Zugriff auf Datenanteile**
  - Bild, Ton, Synchronisationsinformation, Metadaten
  - Charakteristische Daten für Klassifikation, Indexerstellung

8.1 Partielle Verschlüssellung bei H.261

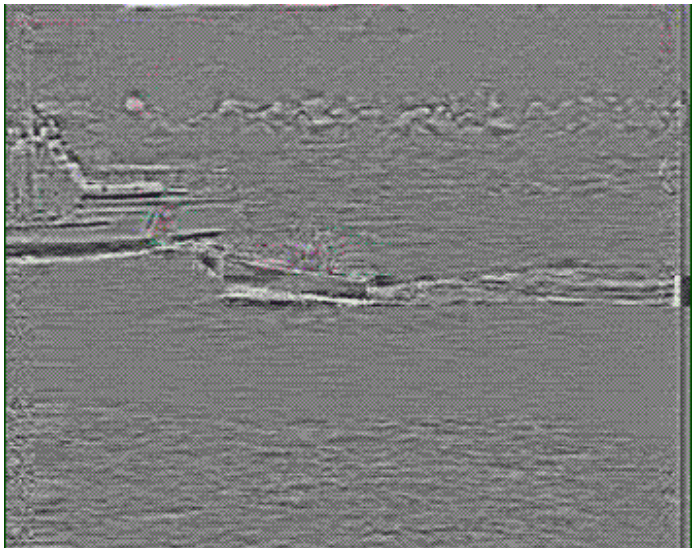
Regelmäßige Blöcke

- **Beispiel: einzelne Blöcke verschlüsseln**
- **Miss America in QCIF mit 1%, 5%, 10% verschlüsselten Daten**

8.2 Partielle Verschlüsselung bei MPEG-1 und -2

Verschlüsselung der Referenzblöcke (I-Frames)

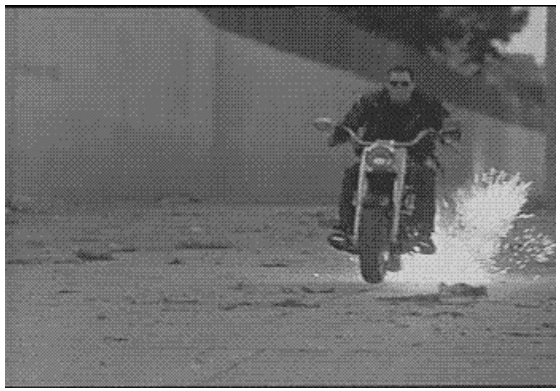
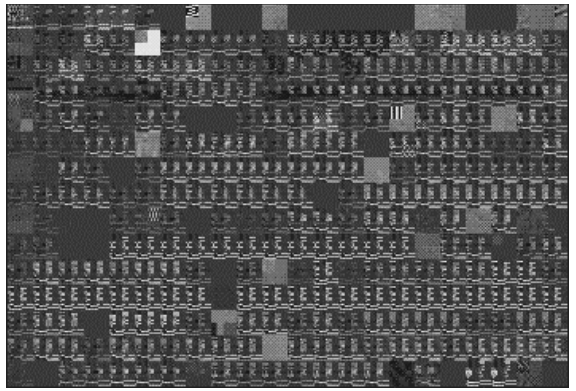
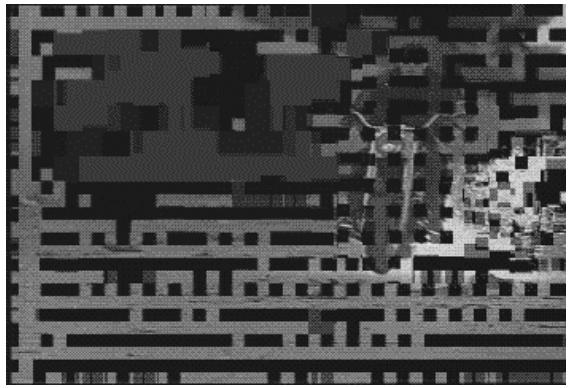
- **d.h. Referenzbilder sind entfernt**
- **P- und B- Bilder**
  - enthalten jedoch auch I-kodiert Makroklöcke
  - d.h. Problem
- **Beispiel:**
  - 25% von coastguard verschlüsselt



zusätzliche Verschlüsselung von intrakodierten Blöcken (P- und B-Frames)

- **z.B SEC-MPEG Methode**
- **Beispiel:**
  - 25% von coastguard verschlüsselt

8.3 Partielle Verschlüsselung bei JPEG

Permutation der DCT-Koeffizienten

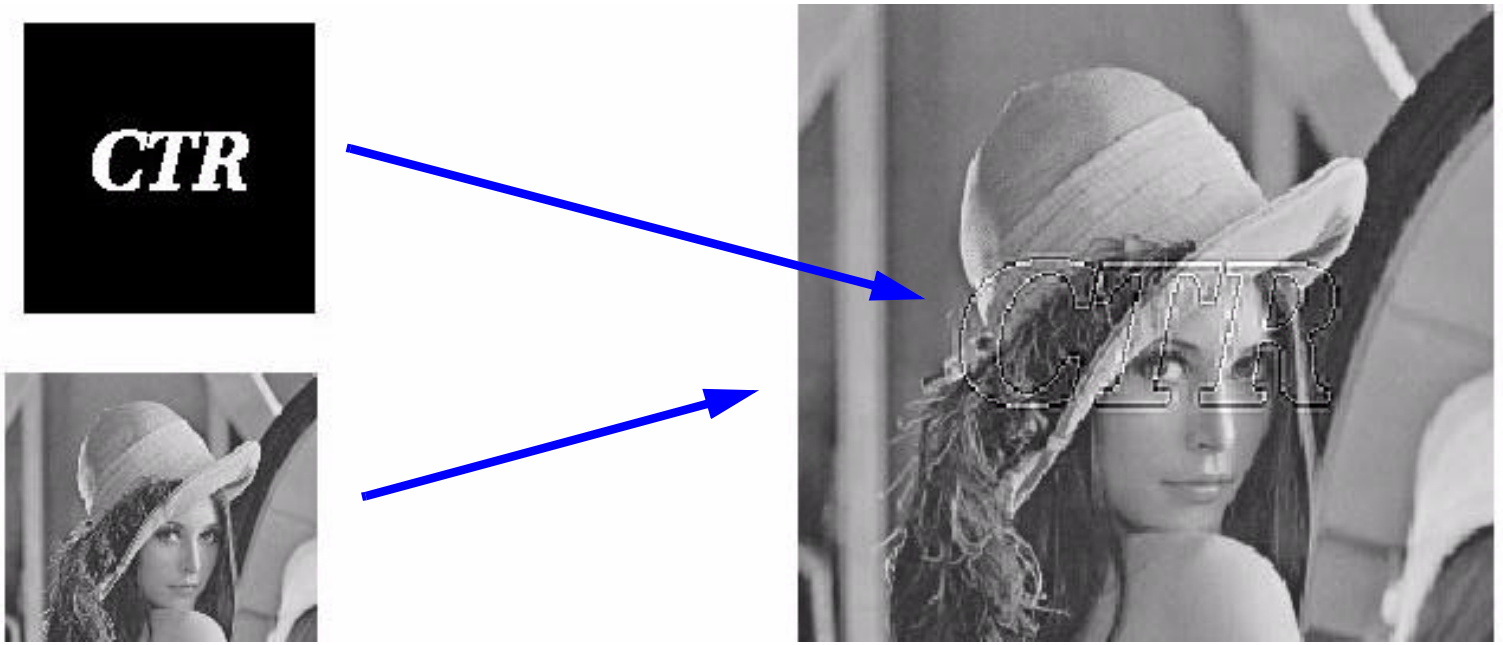
Vorteile

- **insgesamt 64 DCT-Koeffizienten werden permutiert**
- **64! , 10^{89} gegenüber DES 10^{16} 8**

Nachteile

- **Entropiecodierung verschlechtert**
- **20-40% Vergrößerung der orginalcodierten Videodaten**
- **nicht sicher gegen statistische Analysen, da DC-Koeffzient meist größter Wert**
  - mögliche Lösung: Aufteilung auf 2 andere Werte
- **spezieller Video-Encoder und Video-Decoder nötig**
- **einige Möglichkeiten der Skalierbarkeit gehen verloren**

9. Wasserzeichen

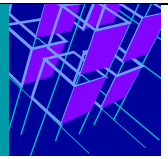


Verständnis

- **Markierung, Zeichen,**
- **oft das Verbergen von Informationen gemeint**

Varianten

- **sichtbare vs. unsichtbare**
- **robuste vs. zerbrechliche**
  - i.allg unsichtbare-robuste vs. unsichtbare-zerbrechliche



9.1 Anforderung: Nicht wahrnehmbar

d.h.

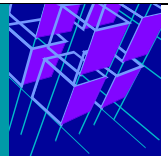
- **Informationen sollen Inhalt nicht stören**
- **Wasserzeichen ist nicht erkennbar, nicht hörbar**

Grund

- **zusätzliche Information direkt mit Inhalt “verwoben”**
- **z.B. Authentizität: Copyright**

Verfahren

- **Tests, Vergleiche zwischen**
  - Original ohne Wasserzeichen
  - Daten mit Wasserzeichen



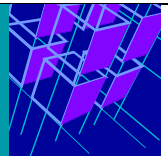
9.2 Anforderung: Reproduktion ohne Original

d.h.

- **Bei der Extraktion des Wasserzeichens ist Original nicht notwendig**

Grund

- **gespeicherte/übertragene Datenmenge ist begrenzt**
- **Verfahren sind dann schwerer angreifbar**



9.3 Anforderung: Hohe Datenmenge

d.h.

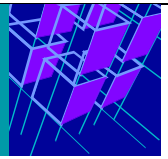
- **einzubringende Datenmenge bestimmt u.a. die Anwendungsmöglichkeiten**
- **dabei Datenrate der eigentlichen Daten nicht erhöhen**

Grund

- **z.B. Metadaten zu Szenenbeschreibung, etc. benötigen gewisse Datenmenge**

Erfahrungswerte

- **1-100 Bit pro Bild (bei robusten Wasserzeichen)**



9.4 Anforderung: Robustheit

(minimale ... stärkere) Veränderung des Datenmaterial darf nicht zum Verlust des Wasserzeichens führen

Notwendigkeit

- **Skalierung von Datenströmen**
- **Weiterverwertung von (zum Teil veränderten) Ausschnitten**

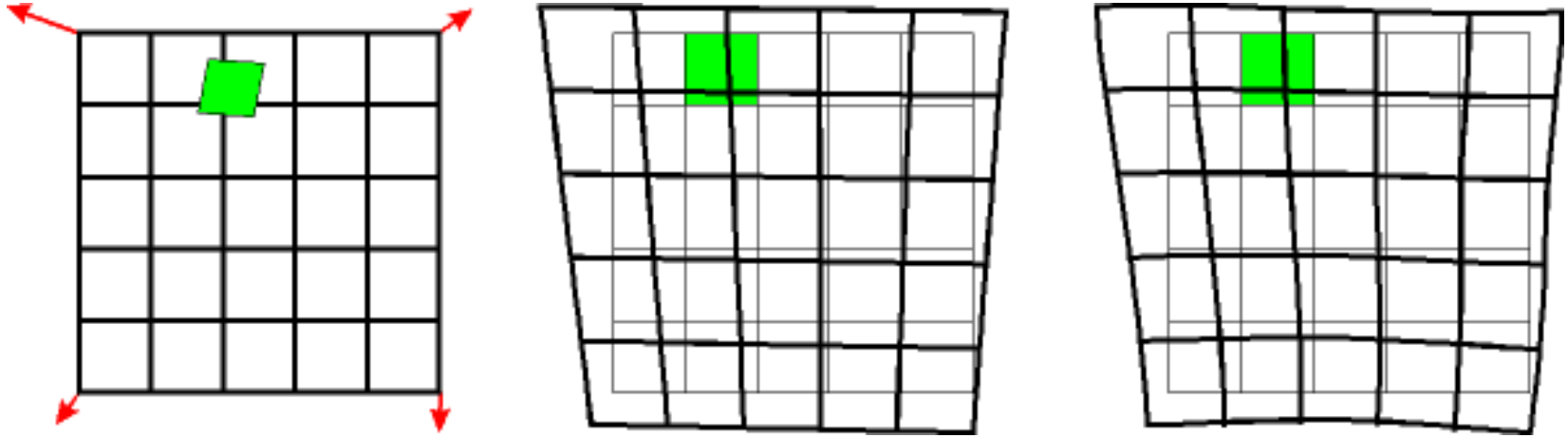
Ebenen der Robustheit

1. **digitale Kopie anfertigen**
2. **Ausdrucken - Einscannen**
3. **Ausschnitte und Objekte extrahieren**
4. **lineare Verzerrungen**
5. **Pixelmanipulation**
6. **Formatwechsel (Kodierungs-, Kompressionsformat)**
7. **nicht-lineare Verzerrungen**

Tests bezüglich Robustheit, zB.

- **UnZign und StirMark**

Angriff: StirMark



Verfahren

- **simuliert sogenannte resampling Prozesse**
- **zB. Ausdruck und erneutes Einscannen**
- **dabei werden**
  - kleine zufällig ausgewählte geometrische Operationen ausgeführt wie
    - Verzerren, Skalieren, Rotieren oder Resampling mit Nyquist Interpolationen

Angriff: Mosaikverfahren

Verfahren

- **Wasserzeichen bezieht sich auf ganzes Bild**
- **somit**
  - Aufteilung eines Bildes in viele einzelne Bilder (zerstört Wasserzeichen)
  - Zusammensetzung beim Anzeigen (Rekonstruktion des Originals)

9.5 Anforderung: Sicherheit

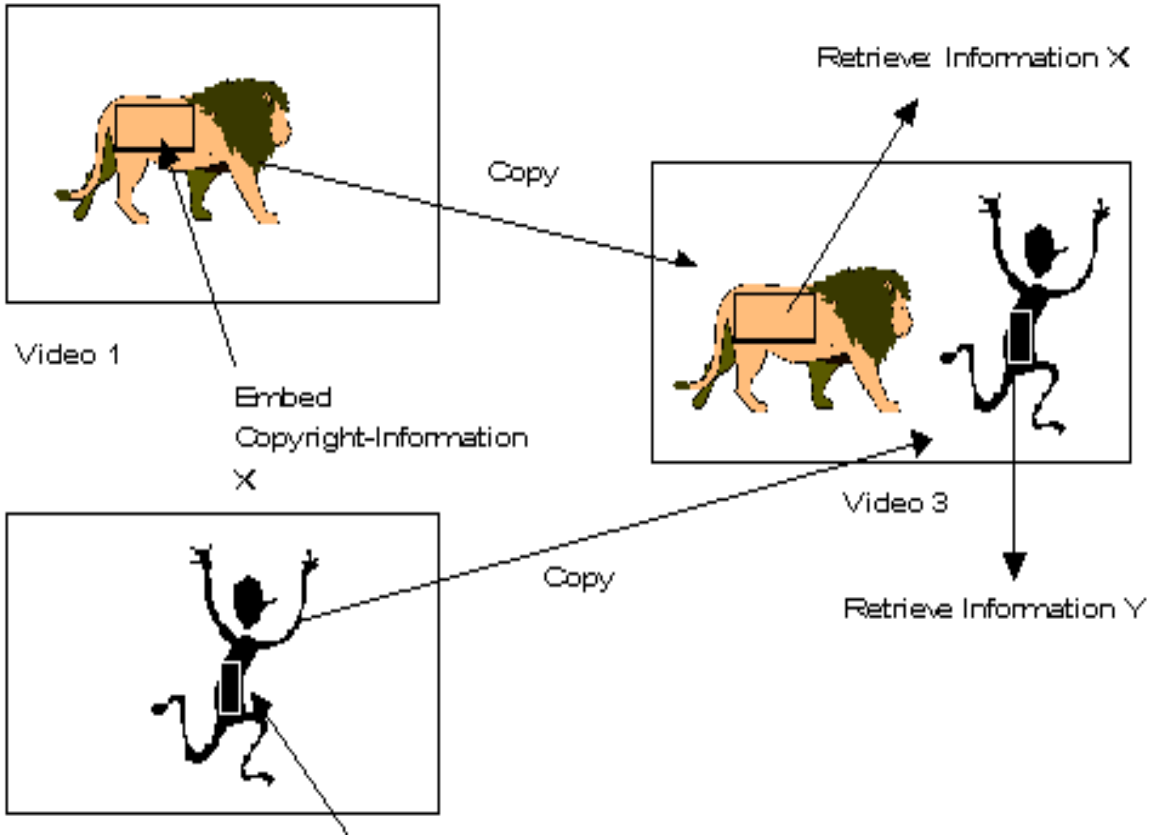
Wasserzeichen kann (mit vertretbarem Aufwand)

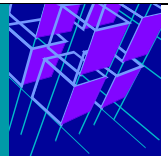
- **nicht entfernt, nicht verändert**
- **und je nach Anwendung: überhaupt nicht gelesen werden**

Grund

- **Wasserzeichen soll eindeutige Kennung sein**

Beispiel aus objektbasierter Kodierung (AVOs) in MPEG-4





9.6 Anforderung: Eindeutige Authentizität

d.h.

- **eindeutige Zuordnung: Wasserzeichen - Ursprung**
  - auch bei mehrmaligem Einbringen von Wasserzeichen

Problematik: "Rightful Ownership" am Beispiel

Jana	Orig			Jana's Wasserze-ichen			markiertes Bild von Jana	
	10	5	=	1	-1	=	11	4
	-2	0		-1	1		-3	1

Dieter	markiertes Bild von Jana			Dieter's Wasserze-ichen			Dieters vor-getäuschte Original	
	11	4	+	-2	0	=	9	4
	-3	1		0	0		-3	1

- **<u>beide</u> Wasserzeichen enthalten**
- **unklar wer <u>zuerst</u> Wasserzeichen eingebracht hat**
- **ungelöst, wenn Originaldaten nicht verfügbar sind**