Post-Compression Multimedia Security

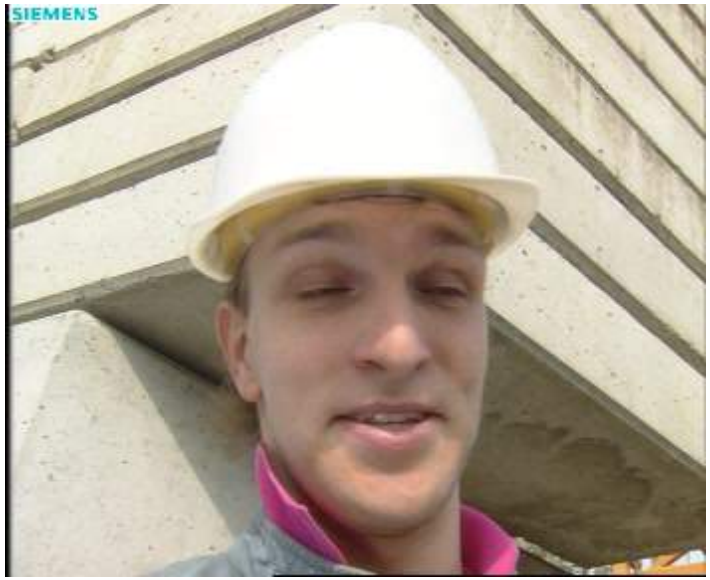
Dissertationsverteidigung

Andreas Unterweger

20. Februar 2015

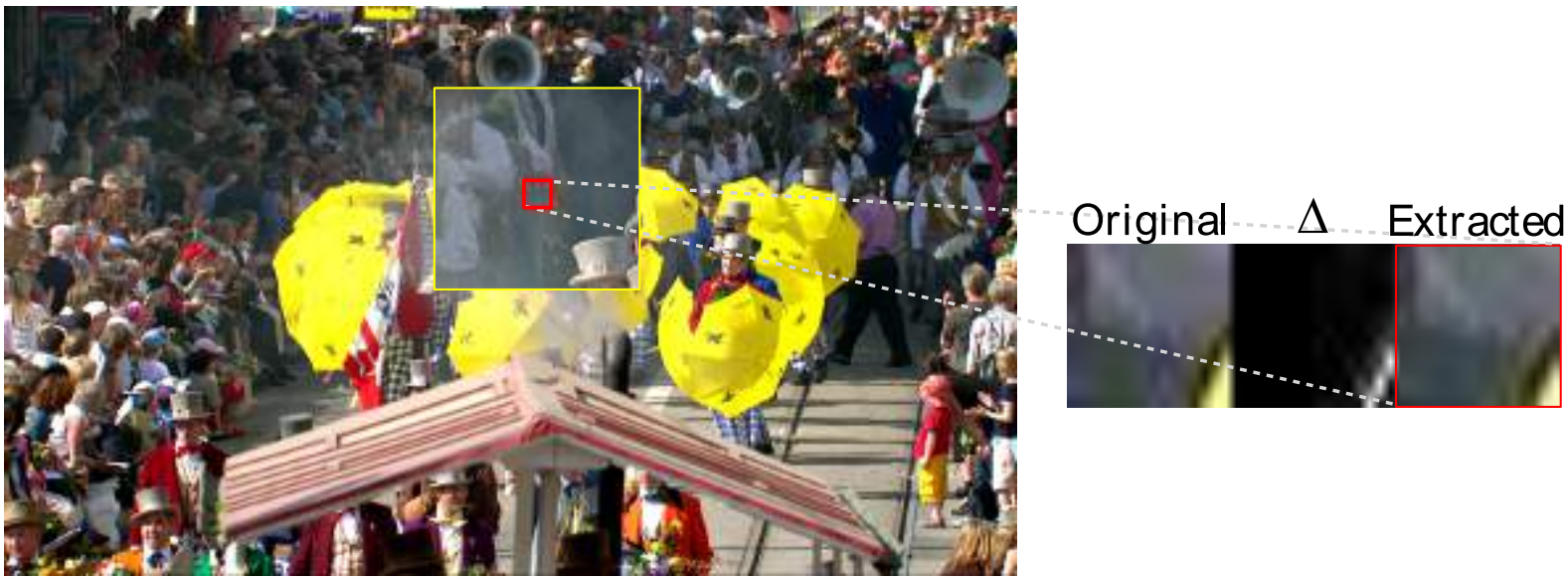
Begriffserläuterung „Multimedia Security“

- **Region of Interest Encryption**
- Watermarking
- Transparent Encryption



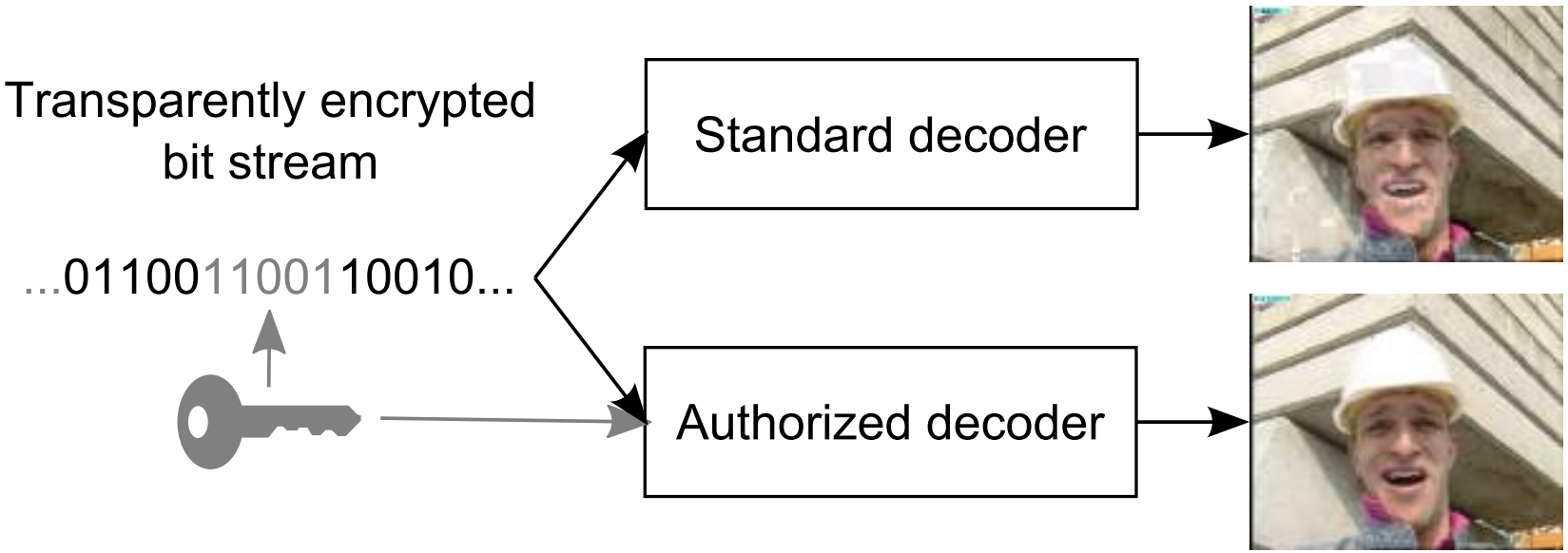
Begriffserläuterung „Multimedia Security“

- Region of Interest Encryption
- **Watermarking**
- Transparent Encryption



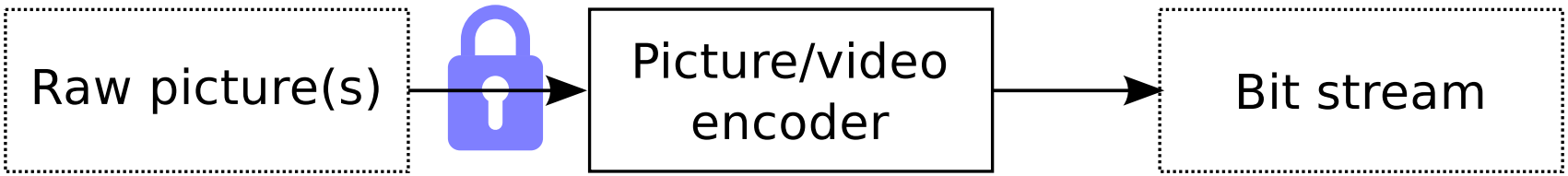
Begriffserläuterung „Multimedia Security“

- Region of Interest Encryption
- Watermarking
- **Transparent Encryption**



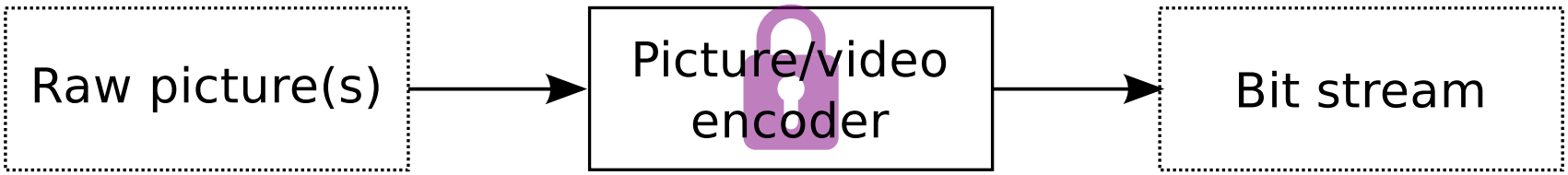
Begriffserläuterung „Post-Compression“

- **Pre-Compression**
- In-Compression
- Post-Compression



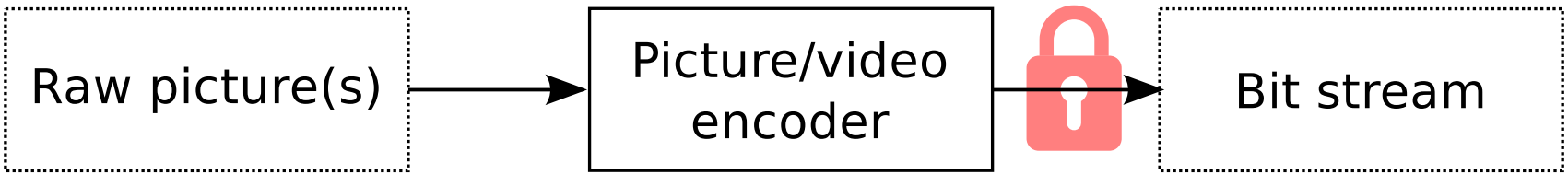
Begriffserläuterung „Post-Compression“

- Pre-Compression
- **In-Compression**
- Post-Compression



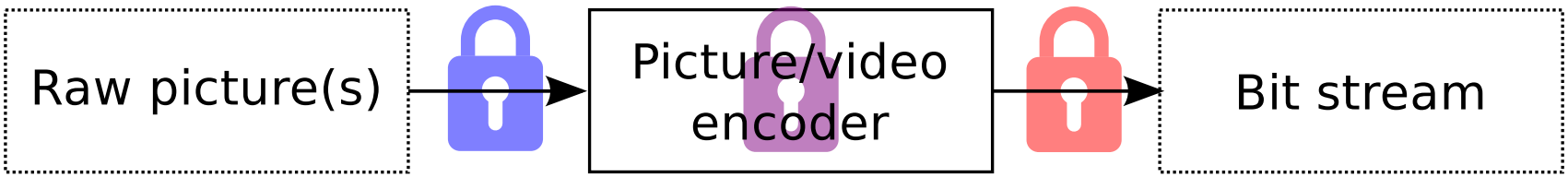
Begriffserläuterung „Post-Compression“

- Pre-Compression
- In-Compression
- **Post-Compression**



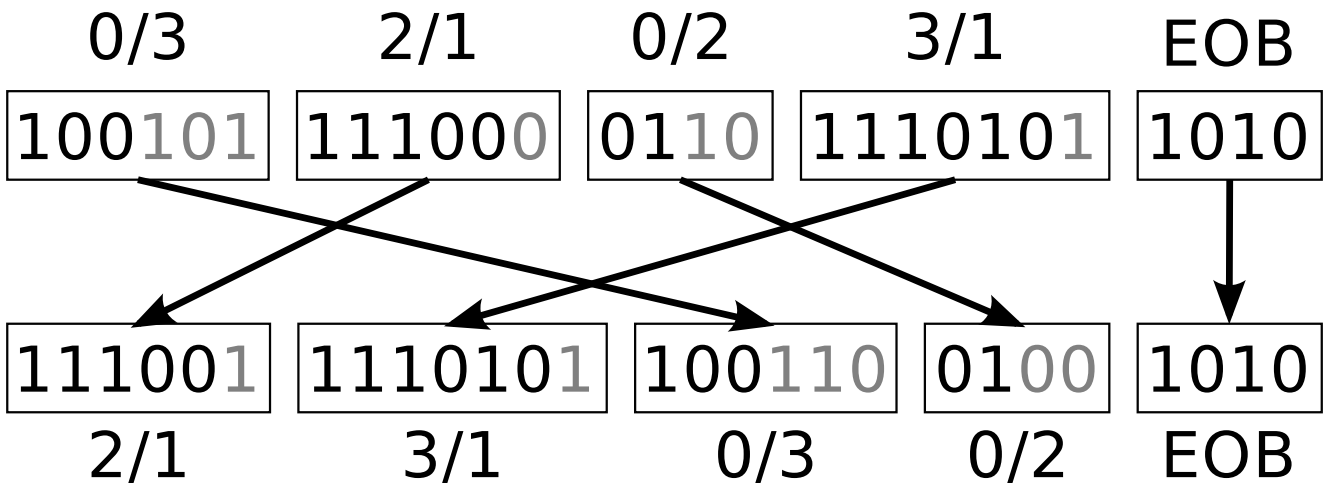
Problemstellung

- In der Literatur: Großteils Pre- und In-compression-Ansätze
  - Einfacher zu implementieren
  - Schneller (bei unkomprimierten Eingabedaten)
  - Transkodierungsproblematik
- In der Praxis: Komprimierte Daten
  - Überwachungskameraaufnahmen (JPEG, H.264 und SVC)
  - Blu-ray-Images (H.264)
  - Fernsehübertragungen (H.264 und bald H.265)



Ergebnisse: Region of Interest Encryption – JPEG I

- Längenerhaltende bitstrombasierte JPEG-Verschlüsselung[1]
  - Vertauschung von AC-Huffman-Codewörtern
  - Zusätzliche AC-Koeffizientenverschlüsselung (größerer Schlüsselraum)
  - Trivial auf Regions of Interest beschränkbar



[1] A. Unterweger and A. Uhl. Length-preserving Bit-stream-based JPEG Encryption. In *MM&Sec'12: Proceedings of the 14th ACM Multimedia and Security Workshop*, pages 85–89. ACM, Sept. 2012

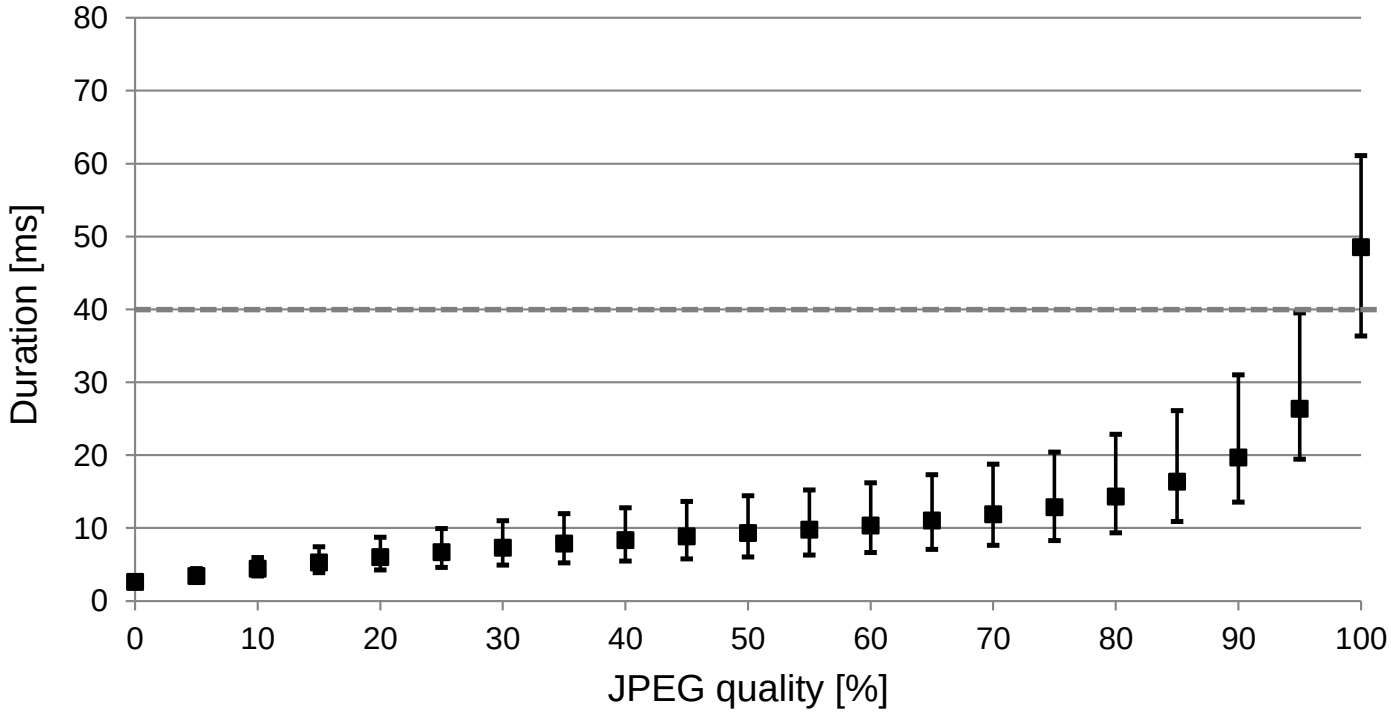
Ergebnisse: Region of Interest Encryption – JPEG I

- Längenerhaltende bitstrombasierte JPEG-Verschlüsselung[1]

[1] A. Unterweger and A. Uhl. Length-preserving Bit-stream-based JPEG Encryption. In *MM&Sec'12: Proceedings of the 14th ACM Multimedia and Security Workshop*, pages 85–89. ACM, Sept. 2012

Ergebnisse: Region of Interest Encryption – JPEG II

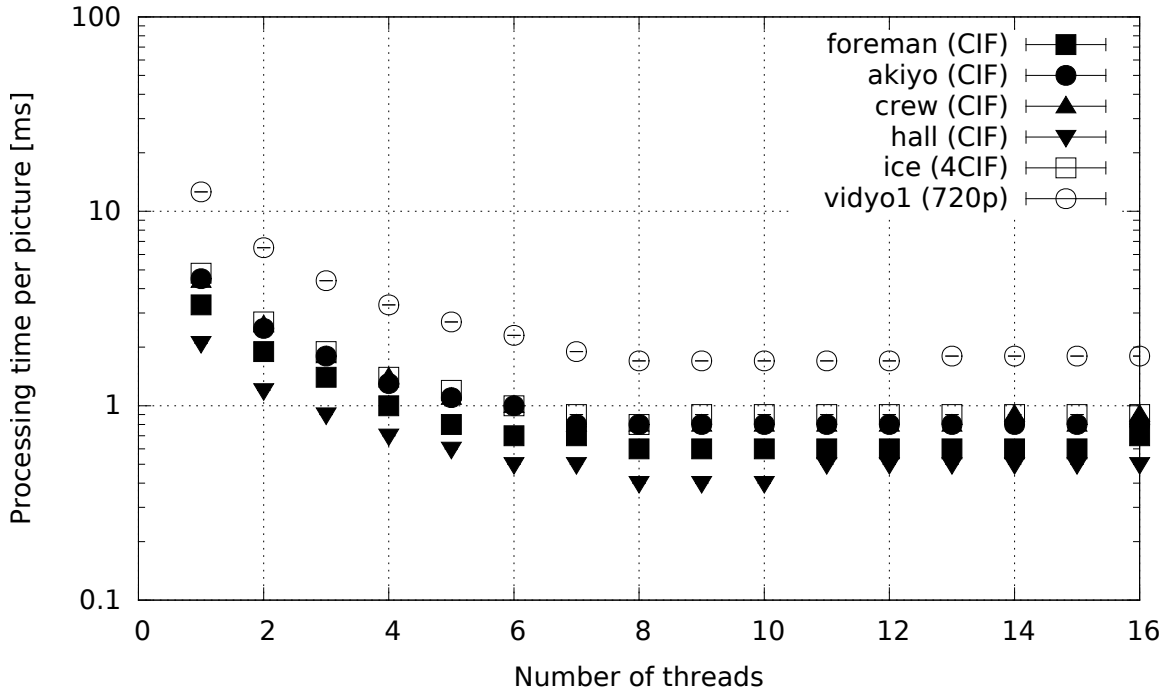
- Echtzeit-JPEG-Verschlüsselung[2]
  - C-Implementierung der bitstrombasierten JPEG-Verschlüsselung
  - Verschlüsselung in VGA-Auflösung in Echtzeit



[2] S. Auer, A. Bliem, D. Engel, A. Uhl, and A. Unterweger. Bitstream-Based JPEG Encryption in Real-time. *International Journal of Digital Crime and Forensics*, 5(3):1–14, 2013

Ergebnisse: Region of Interest Encryption – JPEG III

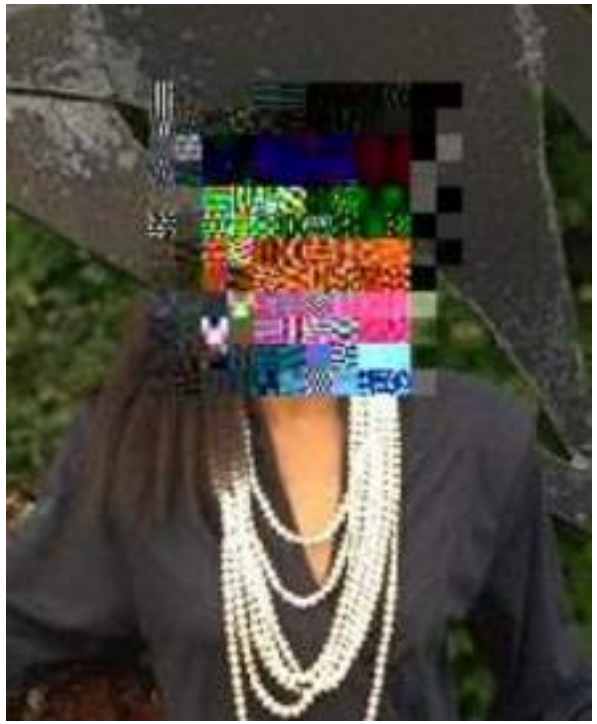
- Erweiterte JPEG-Verschlüsselung[3]
  - Erweiterung der C-Implementierung um DC-Koeffizienten-Verschl.
  - Korrektur an den Rändern der Region of Interest notwendig



[3] A. Unterweger, K. Van Ryckegem, D. Engel, and A. Uhl. Building a Post-Compression Region-of-Interest Encryption Framework for Existing Video Surveillance Systems – Challenges, obstacles and practical concerns. *Multimedia Systems*, 2015. submitted

Ergebnisse: Region of Interest Encryption – JPEG III

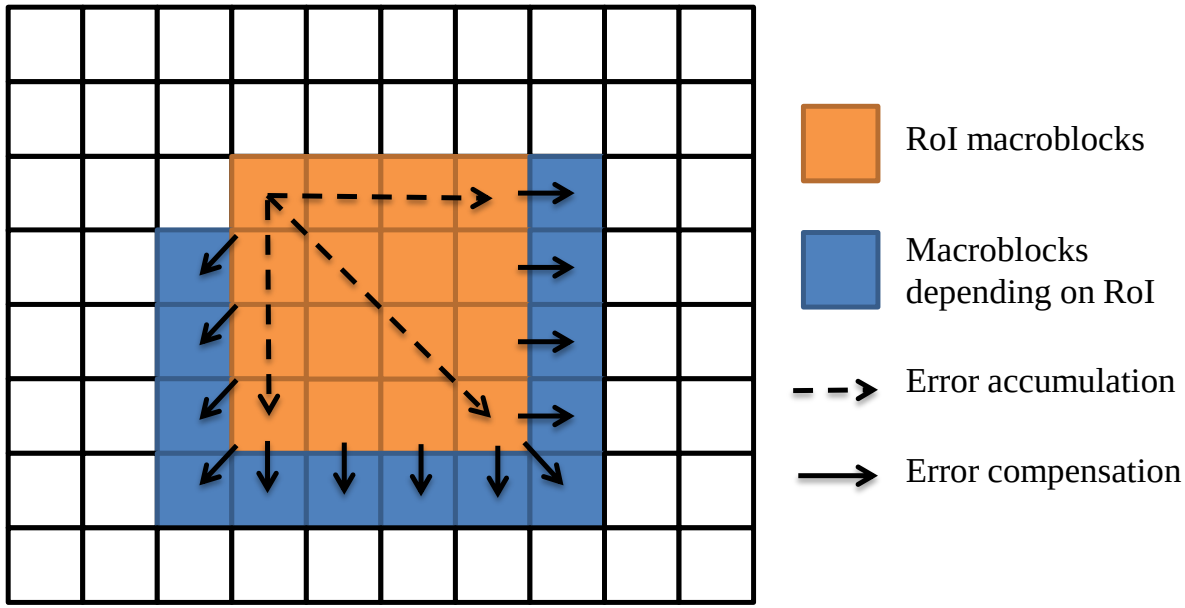
- Erweiterte JPEG-Verschlüsselung[3]



[3] A. Unterweger, K. Van Ryckegem, D. Engel, and A. Uhl. Building a Post-Compression Region-of-Interest Encryption Framework for Existing Video Surveillance Systems – Challenges, obstacles and practical concerns. *Multimedia Systems*, 2015. submitted

Ergebnisse: Region of Interest Encryption – H.264 I

- H.264-Verschlüsselung mit Drift-Minimierung[4]
  - (Teilw.) Driftkompensation an den Rändern der Regions of Interest
  - Erhöhung der Datenrate um max. 3% durch Kompensation
  - Reduktion der Verarbeitungszeit um 45% (vergl. zu Transkodierung)



[4] A. Unterweger, J. De Cock, and A. Uhl. Bit-Stream-Based Encryption for Regions of Interest in H.264 Videos With Drift Minimization. In *2015 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE, 2015. submitted

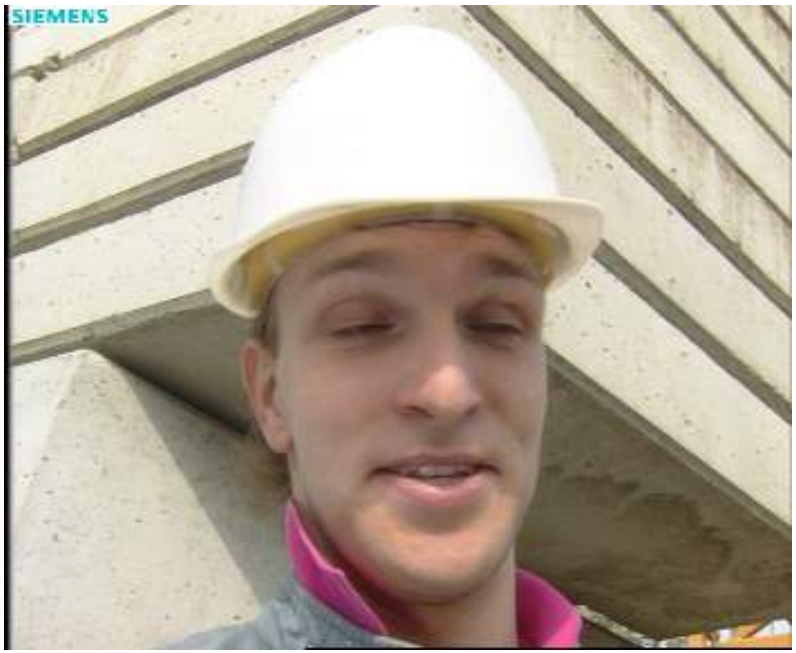
Ergebnisse: Region of Interest Encryption – H.264 I

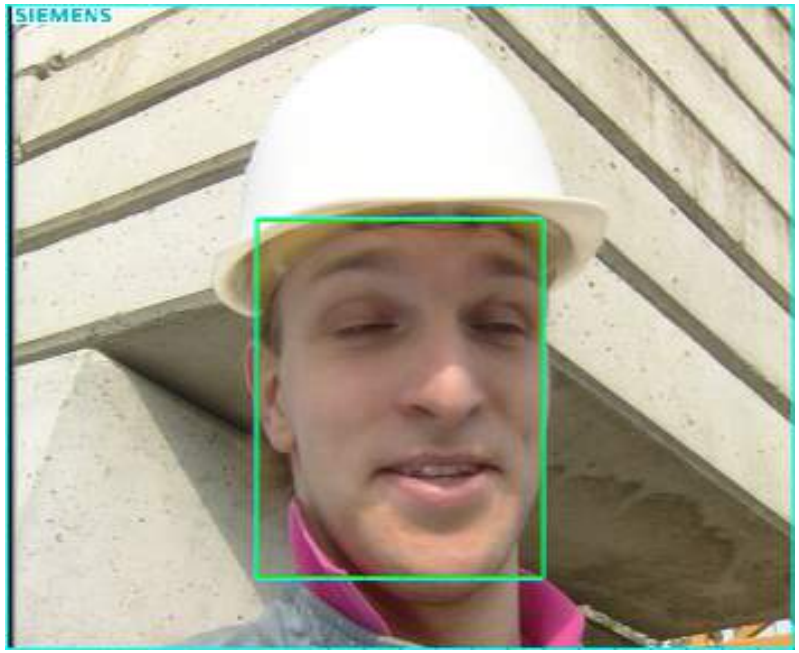
- H.264-Verschlüsselung mit Drift-Minimierung[4]

[4] A. Unterweger, J. De Cock, and A. Uhl. Bit-Stream-Based Encryption for Regions of Interest in H.264 Videos With Drift Minimization. In *2015 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE, 2015. submitted

Ergebnisse: Region of Interest Encryption – H.264 II

- Slice Groups zur Vermeidung von Drift[5]
  - Definition von Slice-Group-Grenzen rund um Regions of Interest
  - Vermeidung von örtlichem, nicht aber zeitlichem Drift
  - Erhöhung der Datenrate mit Qualität (ca. 5% bei mittlerer Qualität)

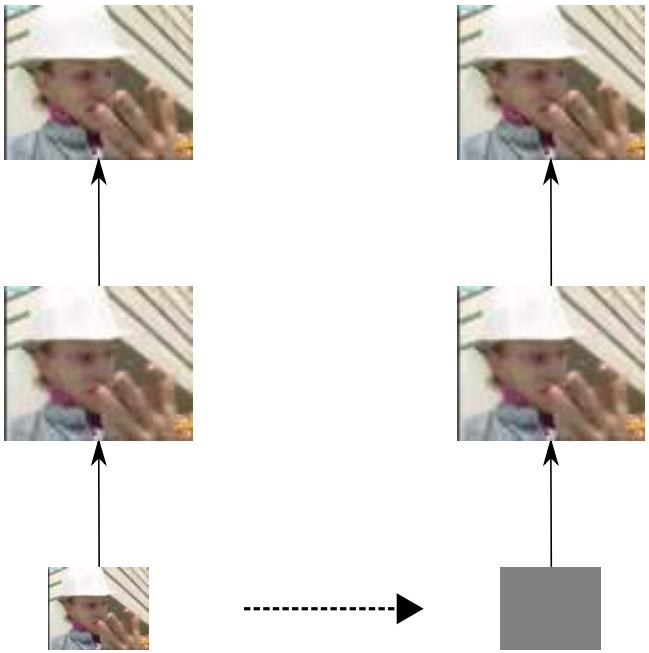


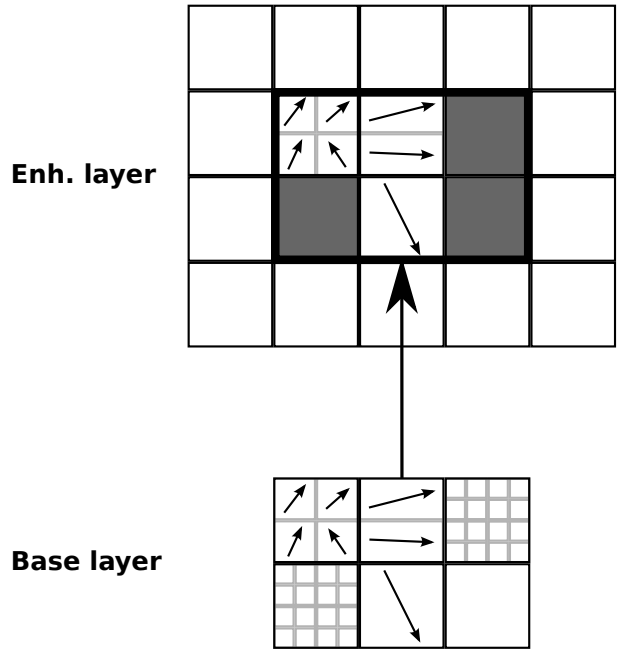


[5] A. Unterweger and A. Uhl. Slice groups for post-compression region of interest encryption in H.264/AVC and its scalable extension. *Signal Processing: Image Communication*, 2014. accepted

Ergebnisse: Region of Interest Encryption – SVC

- Slice Groups zur Vermeidung von Drift[6]
  - Keine Slice Groups im Base Layer erlaubt → Ersetzung durch grauen Layer (minimale Datenrate)
  - Zusätzliche Vermeidung von Inter-Layer-Drift durch Constrained ILP

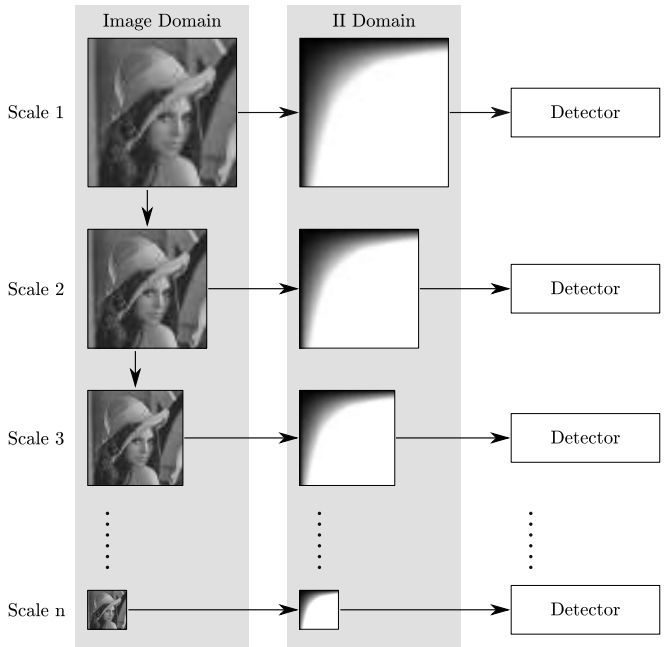


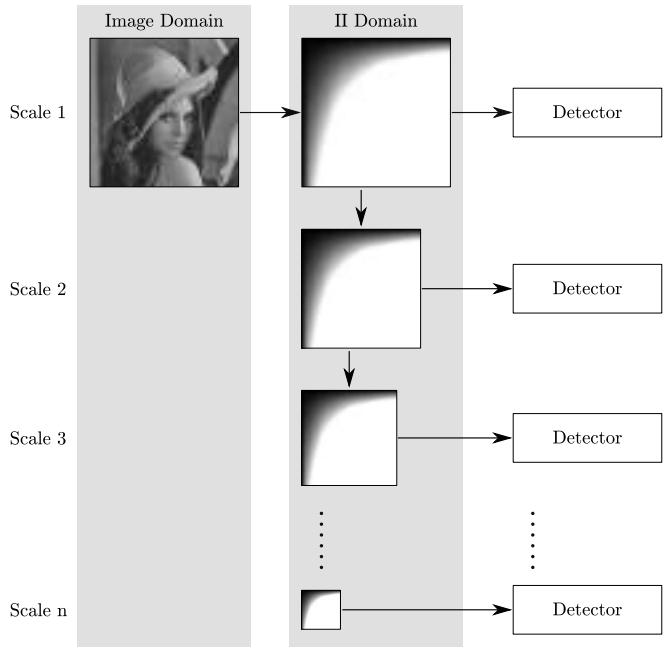


[6] A. Unterweger and A. Uhl. Slice Groups for Post-Compression Region of Interest Encryption in SVC. In *IH&MMSec'14: Proceedings of the 2014 ACM Information Hiding and Multimedia Security Workshop*, pages 15–22, Salzburg, Austria, June 2014. ACM

Ergebnisse: Region of Interest Encryption – Sonstiges I

- Beschleunigung der Objekterkennung nach Viola und Jones[7]
  - Verkleinerung in Integralbilddomäne → Keine Neuberechnungen
  - Bis zu 12% Zeitersparnis bei gleichen Erkennungsraten





[7] M. Gschwandtner, A. Uhl, and A. Unterweger. Speeding Up Object Detection – Fast Resizing in the Integral Image Domain. In *VISAPP 2014 – Proceedings of the 9th International Conference on Computer Vision Theory and Applications*, volume 1, pages 64–72, Lisbon, Portugal, January 2014. SciTePress

Ergebnisse: Region of Interest Encryption – Sonstiges II

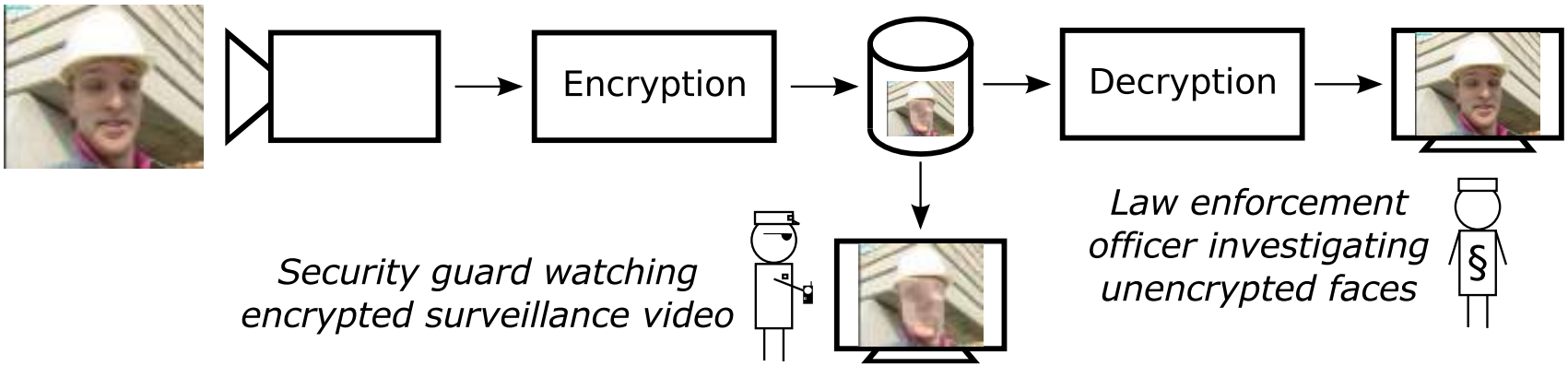
- Signalisierung von Regions of Interest[8]
  - Kodierung der Koordinaten und Größen von Regions of Interest
  - Verschiedene neue Arten der Signalisierung in JPEG-Dateien

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

[8] D. Engel, A. Uhl, and A. Unterweger. Region of Interest Signalling for Encrypted JPEG Images. In *IH&MMSec'13: Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security*, pages 165–174. ACM, June 2013

Ergebnisse: Region of Interest Encryption – Sonstiges III

- Framework für Überwachungssysteme[9]
  - Kombinierte (echtzeitfähige) JPEG-Verschlüsselung und Signalisierung
  - Modulare Implementierung mit Gesichtserkennung und Dekodierung
  - Erlaubt Erweiterung bestehender Überwachungssysteme



[9] A. Unterweger, K. Van Ryckegem, D. Engel, and A. Uhl. Building a Post-Compression Region-of-Interest Encryption Framework for Existing Video Surveillance Systems – Challenges, obstacles and practical concerns. *Multimedia Systems*, 2015. submitted

Ergebnisse: Region of Interest Encryption – Sonstiges III

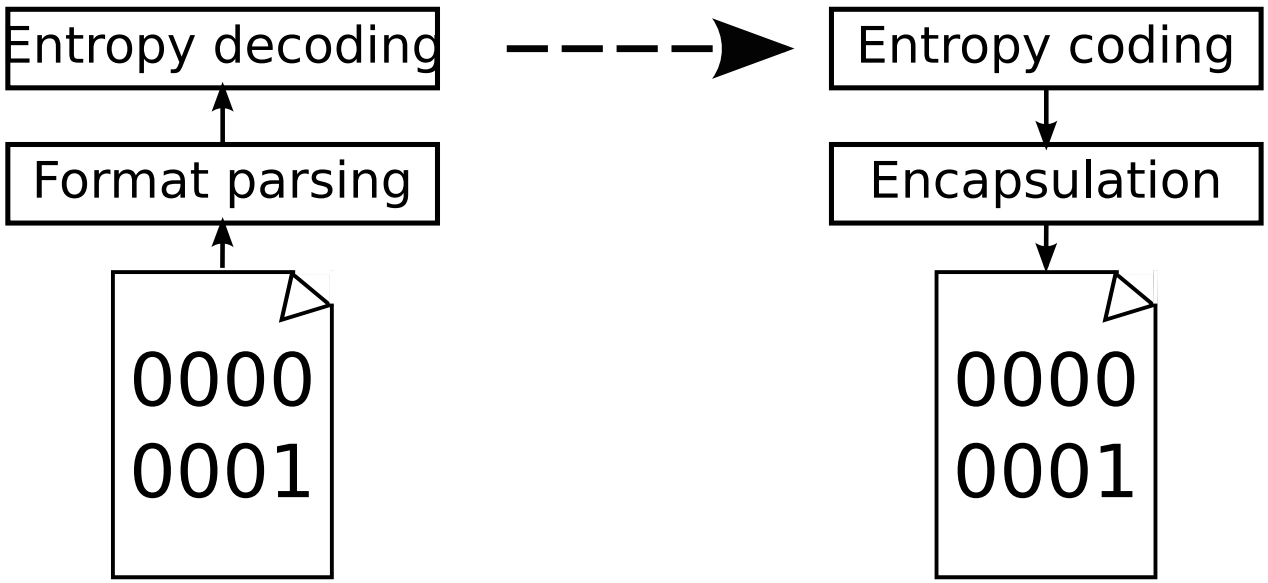
- Framework für Überwachungssysteme[9]
  - Gesichtserkennung kostet mehr als 99% der Verarbeitungszeit
  - Aktuelle Gesichtserkennungsalgorithmen nicht gut genug
  - Subjektive Auswertung verschiedener Verschlüsselungsmethoden
  - Personen können trotz Verschlüsselung erkennbar/zuordenbar sein

Sequence	**Overhead [%]**	**Precision [%]**	**Recall [%]**
foreman (CIF)	0.137	50.3	82.4
akiyo (CIF)	0.242	53.2	99.5
crew (CIF)	0.353	33.2	53.3
hall (CIF)	0.102	62.3	28.3
ice (4CIF)	0.083	36.1	20.7
vidyo1 (720p)	0.163	18.0	70.6

[9] A. Unterweger, K. Van Ryckegem, D. Engel, and A. Uhl. Building a Post-Compression Region-of-Interest Encryption Framework for Existing Video Surveillance Systems – Challenges, obstacles and practical concerns. *Multimedia Systems*, 2015. submitted

Ergebnisse: Watermarking – H.264

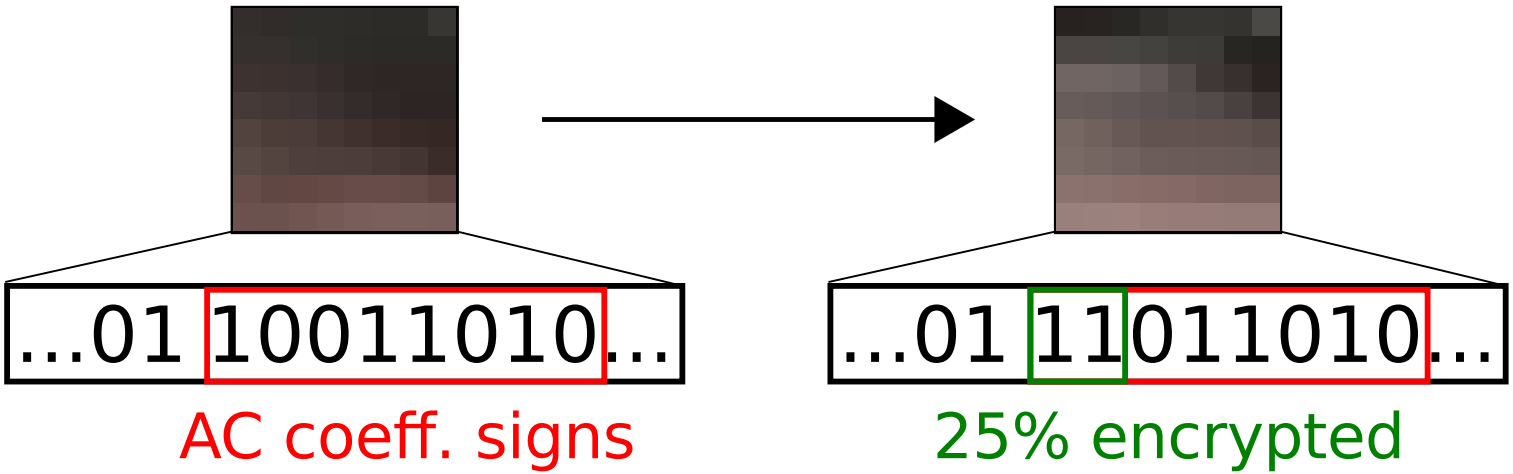
- Blu-ray-Watermarking[10]
  - Strukturerhaltendes Watermarking von MVD (CABAC)
  - Robust gegen Transkodierung, Skalierung und Cropping
  - Anwendung: Zuordnung von Leaks in der Blu-ray-Produktion



[10] J. De Cock, H. Hofbauer, T. Stütz, A. Uhl, and A. Unterweger. An Industry-Level Blu-ray Watermarking Framework. *Multimedia Tools and Applications*, 2014. accepted

Ergebnisse: Transparent Encryption – H.265

- H.265-Verschlüsselung[11]
  - Teilweise Verschlüsselung der AC-Koeffizientenvorzeichen
  - Stärke der Verschlüsselung durch Anteil regelbar
  - Vereinfachte Verarbeitung durch unkomprimierte Vorzeichen



[11] H. Hofbauer, A. Uhl, and A. Unterweger. Transparent Encryption for HEVC Using Bit-Stream-Based Selective Coefficient Sign Encryption. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1986–1990, Florence, Italy, May 2014. IEEE

Ergebnisse: Transparent Encryption – H.265

- H.265-Verschlüsselung[11]

[11] H. Hofbauer, A. Uhl, and A. Unterweger. Transparent Encryption for HEVC Using Bit-Stream-Based Selective Coefficient Sign Encryption. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1986–1990, Florence, Italy, May 2014. IEEE

Schlussfolgerung

- Vorteile von Post-compression Multimedia Security
  - Vermeidung der Transkodierungsproblematik (Zeitersparnis)
  - Einfacherer Erhalt notwendiger Dateneigenschaften
  - Einfachere Integration in bestehende (kompressionsbasierte) Systeme
- Nachteile von Post-compression Multimedia Security
  - Höhere Entwurfs- und Implementierungskomplexität
  - Vermeidung von Drift schwierig(er)
- Größtes offenes Problem: Zeitlicher Drift in H.264, SVC, H.265,...

Danke für Ihre Aufmerksamkeit!

Fragen?