Face encryption in surveillance videos

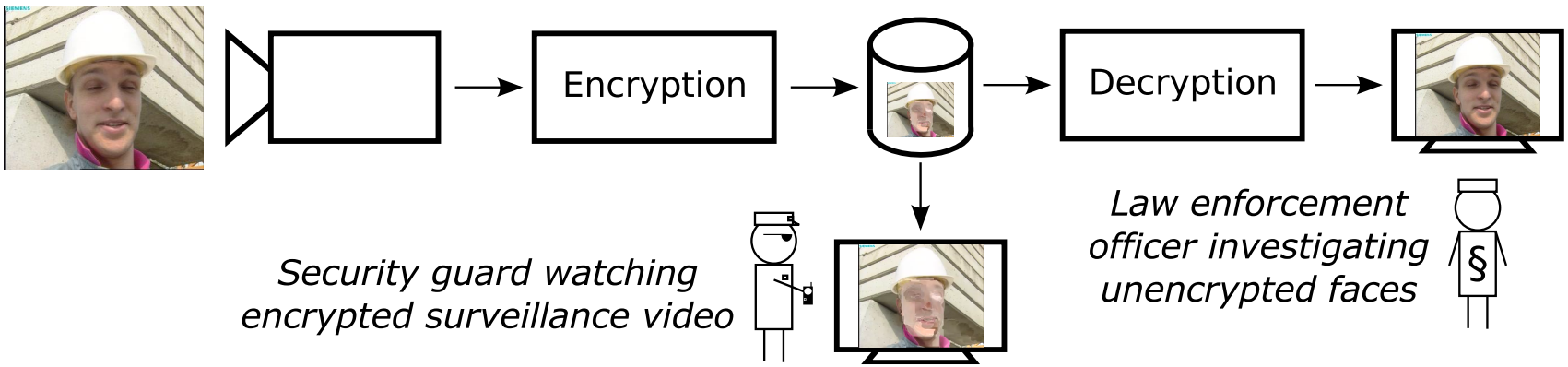
Andreas Unterweger

Salzburg University of Applied Sciences

May 30, 2017

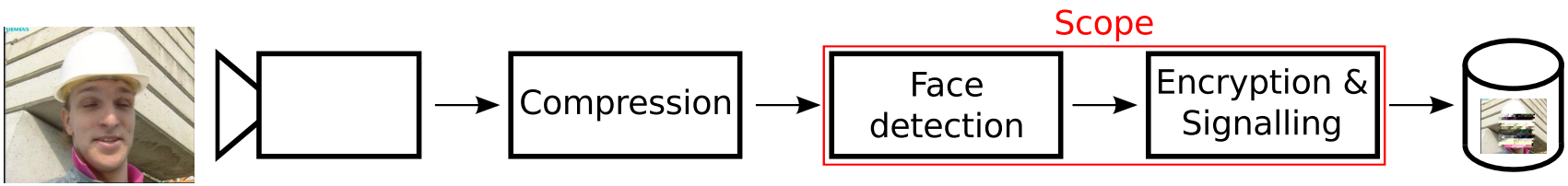
Context: Project overview

- Scenario
  - Surveillance cameras capture people → privacy is an issue
  - Solution: Encryption for privacy preservation
  - Quasi all existing approaches focus on in-compression encryption
  - Issue: In-camera compression process cannot be intercepted
- Project PrivSurv: Development of post-compression encryption approaches for JPEG, JPEG 2000 and JPEG XR, H.264 and SVC



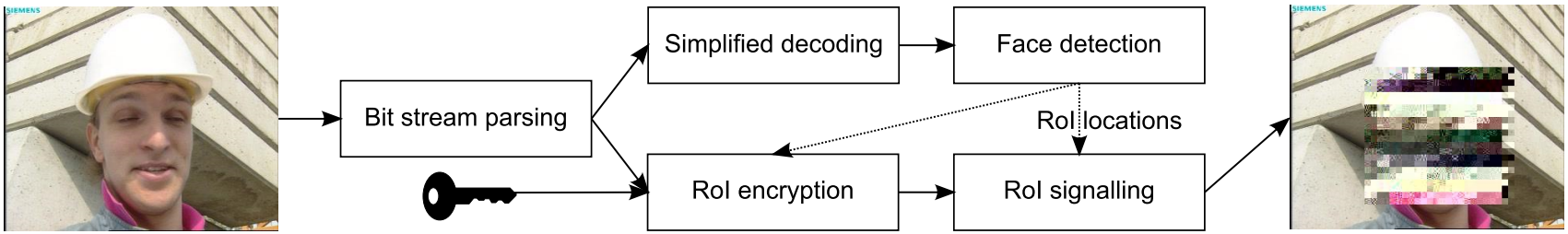
Overview

- Typical environment
  - Cameras deliver (Motion) JPEG
  - No possibility to encrypt in-camera
  - Need for fast and cheap post-processing
- Proposed approach and implementation
  - Encryption of (Motion) JPEG streams
  - Framework for real-time processing
  - Evaluation of performance and security

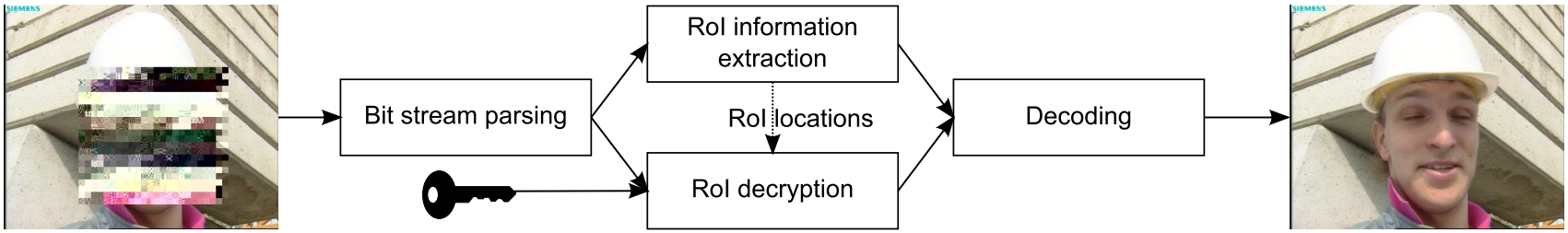


Framework overview

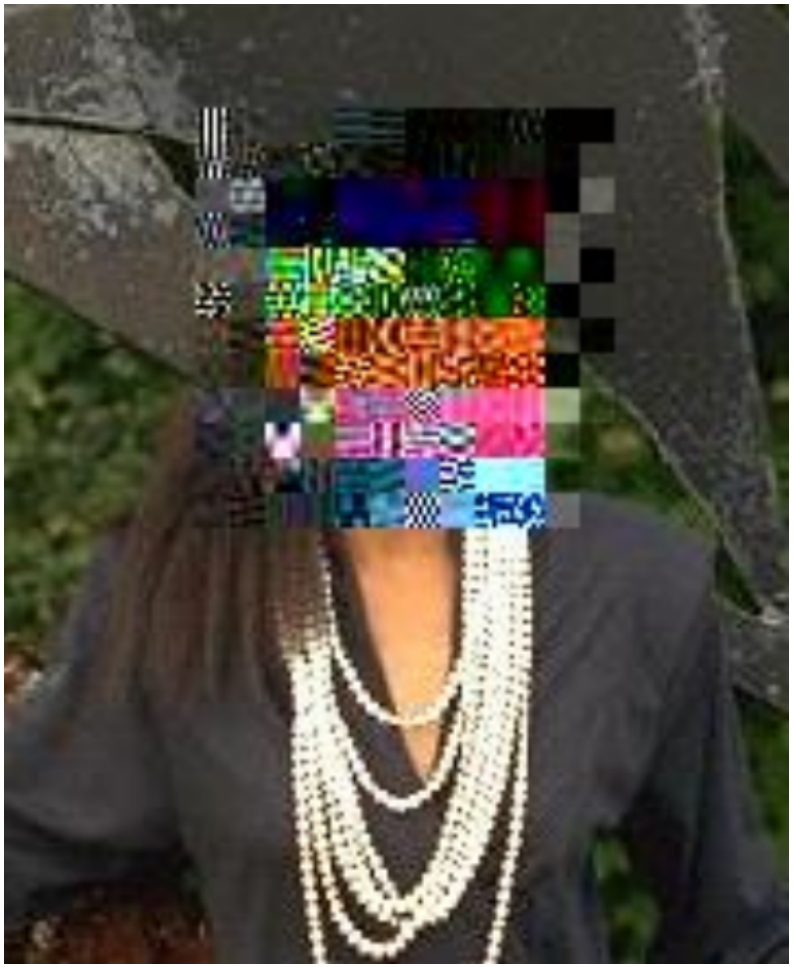
- Encryption side



- Decryption side

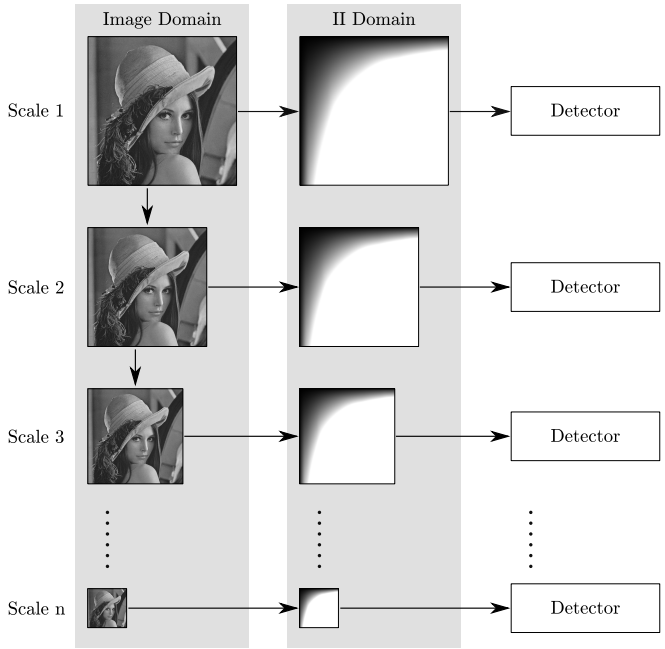


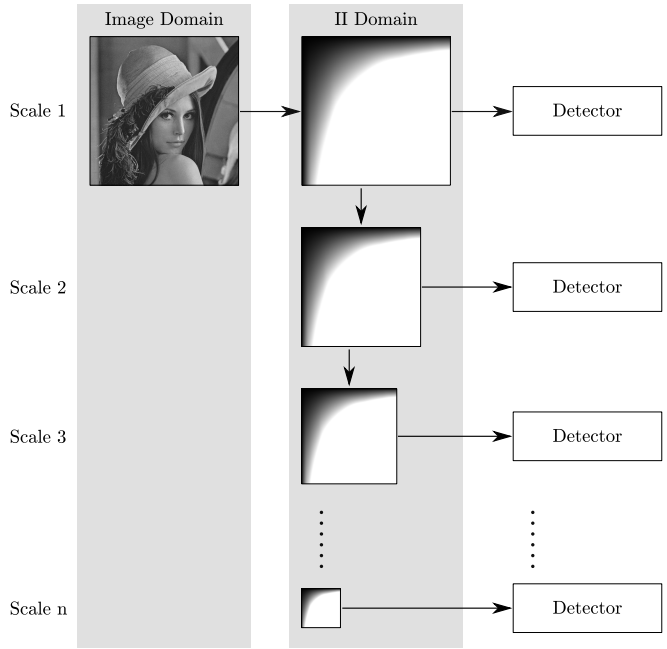
Encryption examples (large)



Face detection

- Sped-up version of algorithm by Viola and Jones
  - Resizing in integral image domain $\rightarrow$ No (integral) recalculations
  - Up to 12% decrease in processing time without decrease in detection performance





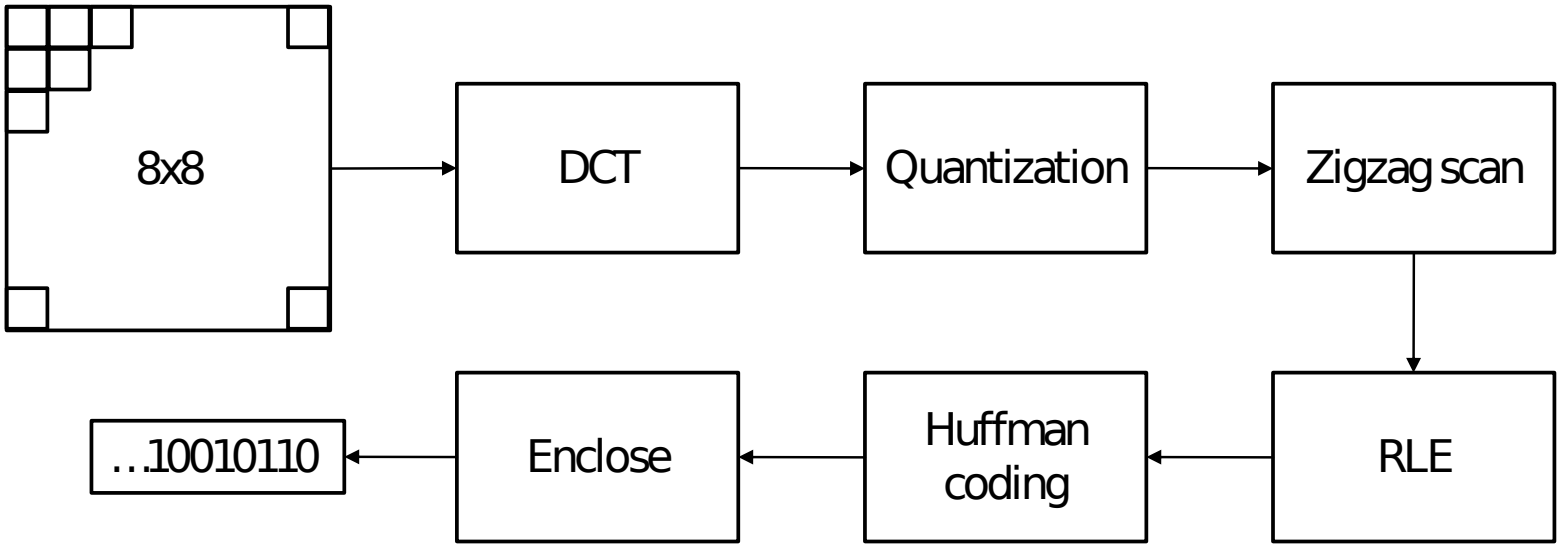
RoI signalling

- Signalling regions of interest
  - Coding of location and size of each region of interest (details omitted)
  - Block granularity (compare encryption approach)
  - Various JPEG-specific methods evaluated

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

JPEG overview

- Picture is split into blocks of size $8 \cdot 8$ (luma samples)
- Each block is processed separately



- Corresponding luma and chroma blocks form an iMCU
- JPEG files consist of multiple compressed iMCUs and headers

Encryption approach overview

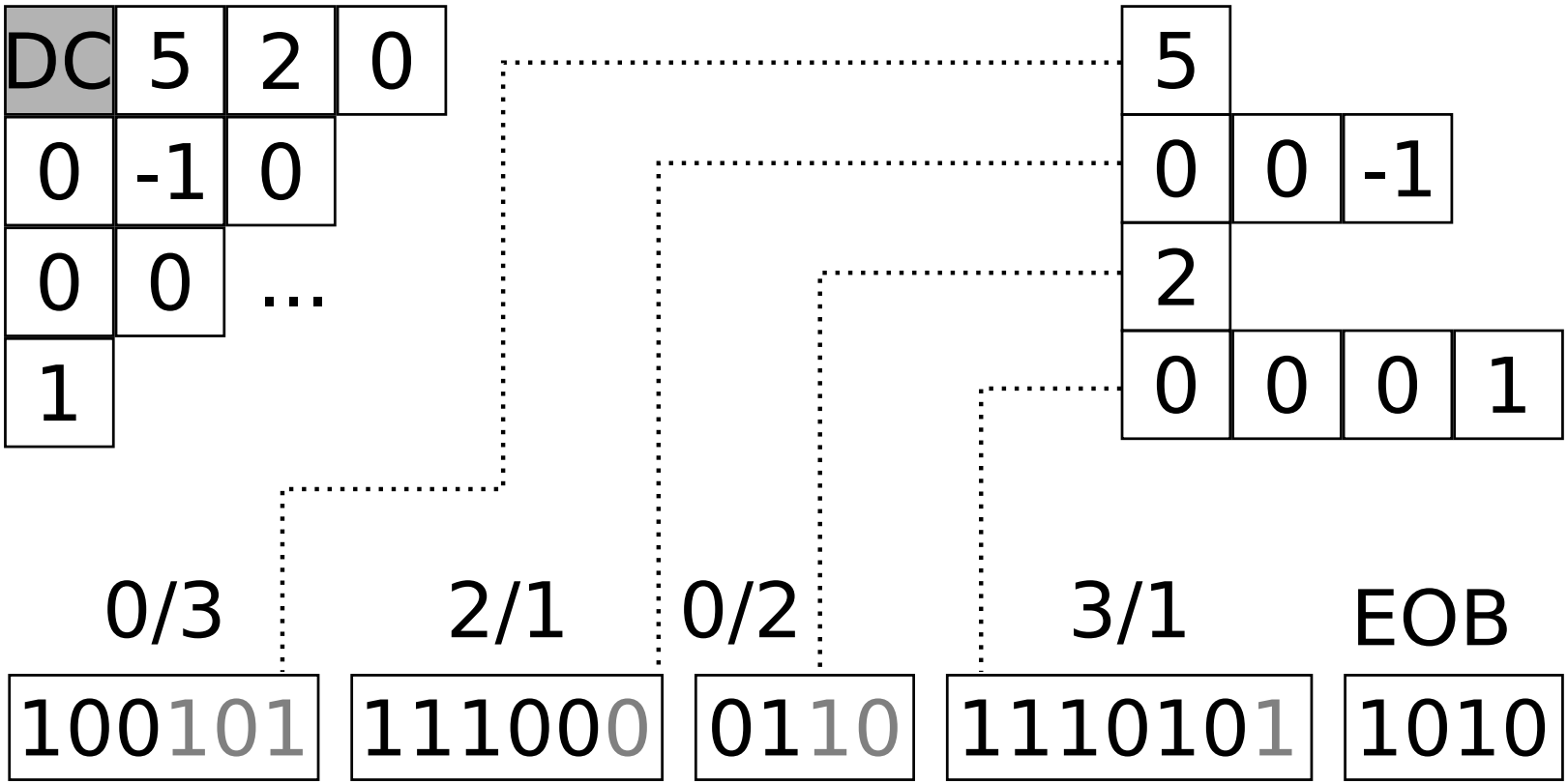
- Three operations per iMCU
  - Change order of run-length-value pairs (within each block)
  - Scramble value bits
  - Swap order of compatible blocks
- Practical considerations
  - PRNG required for reordering and scrambling $\rightarrow$ AES in OFB mode
  - iMCUs are spatially limited $\rightarrow$ support for selective encryption
  - DC coefficients are relatively easy to attack $\rightarrow$ encrypt them with a different key and algorithm (details omitted)

Approach part 1 – Run-length-value pair order change

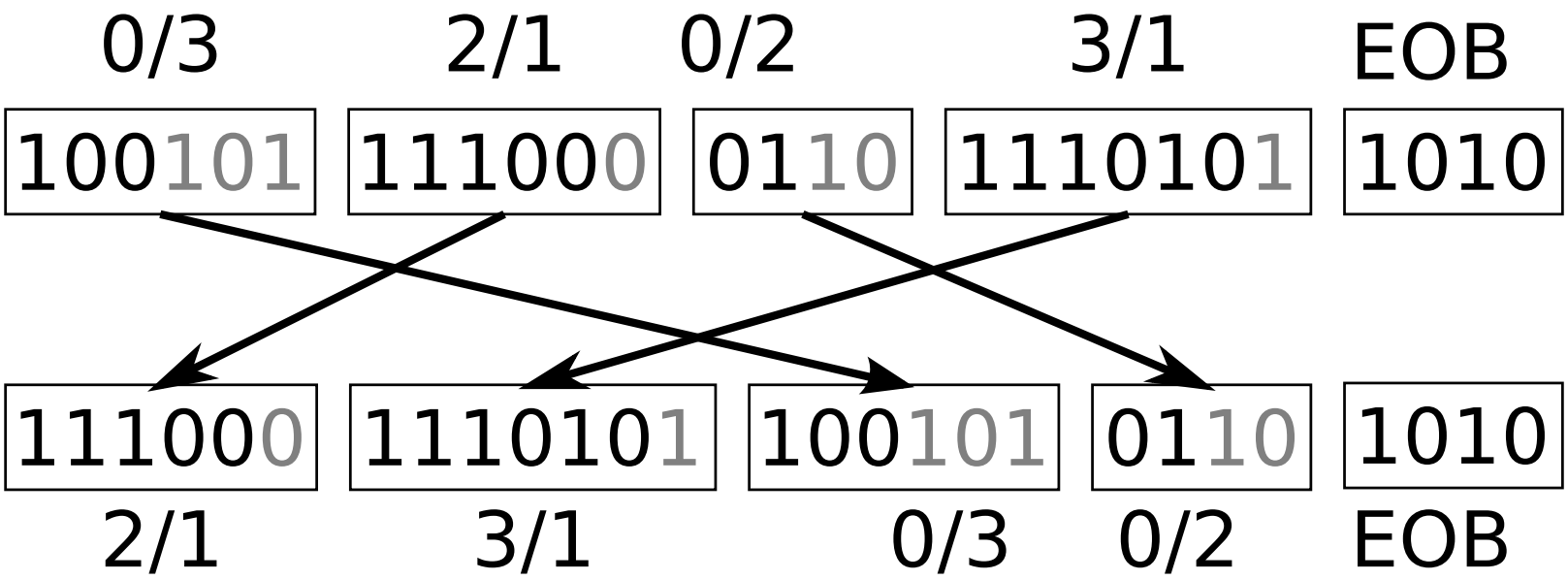
DC	5	2	0
0	-1	0	
0	0	...	
1			

5			
0	0	-1	
2			
0	0	0	1

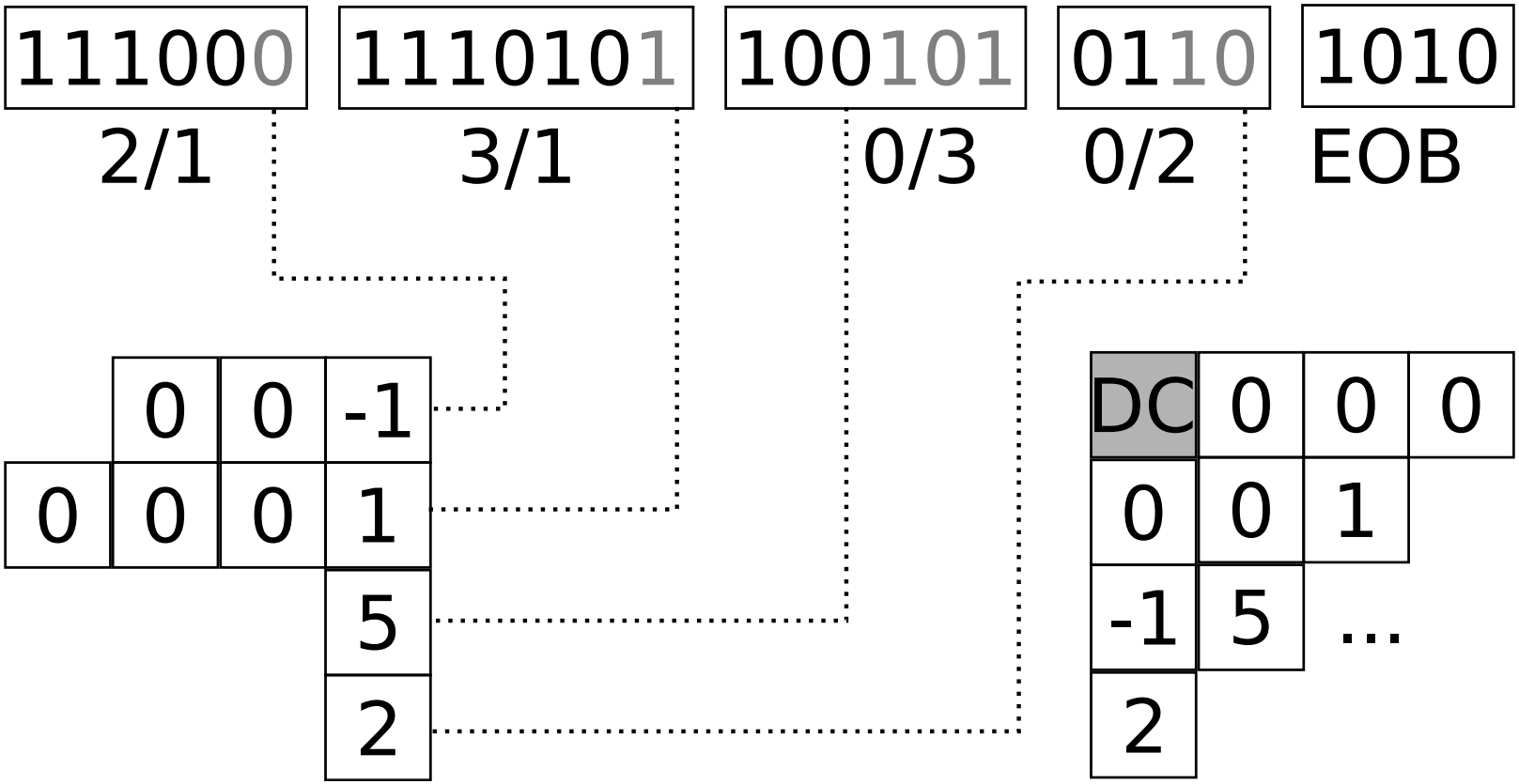
Approach part 1 – Run-length-value pair order change



Approach part 1 – Run-length-value pair order change



Approach part 1 – Run-length-value pair order change



Approach part 1 – Run-length-value pair order change

DC	5	2	0
0	-1	0	
0	0	...	
1			

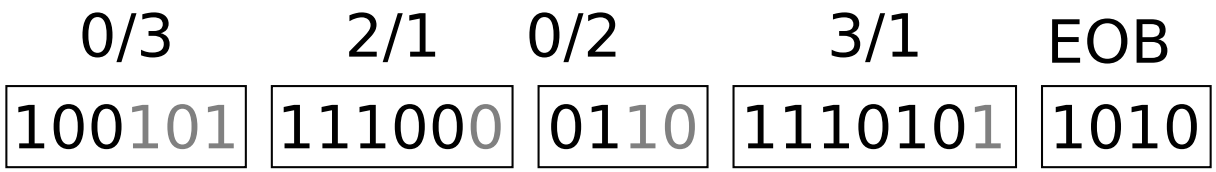
Before

DC	0	0	0
0	0	1	
-1	5	...	
2			

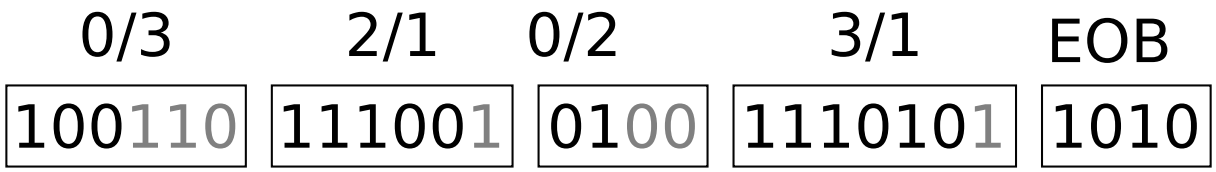
After

Approach part 2 – Value bit scrambling

AC coefficients (values in run-length-value pairs):



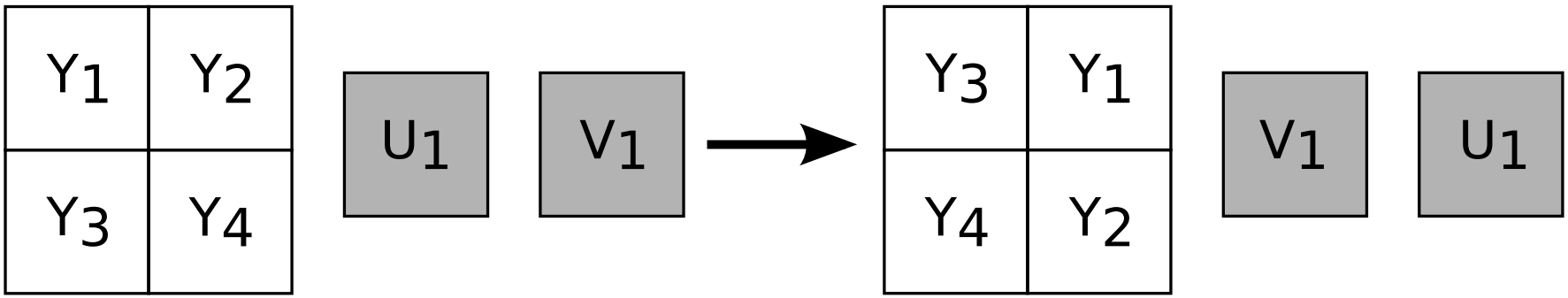
Before



After

DC differences are scrambled in a similar way (details omitted here)

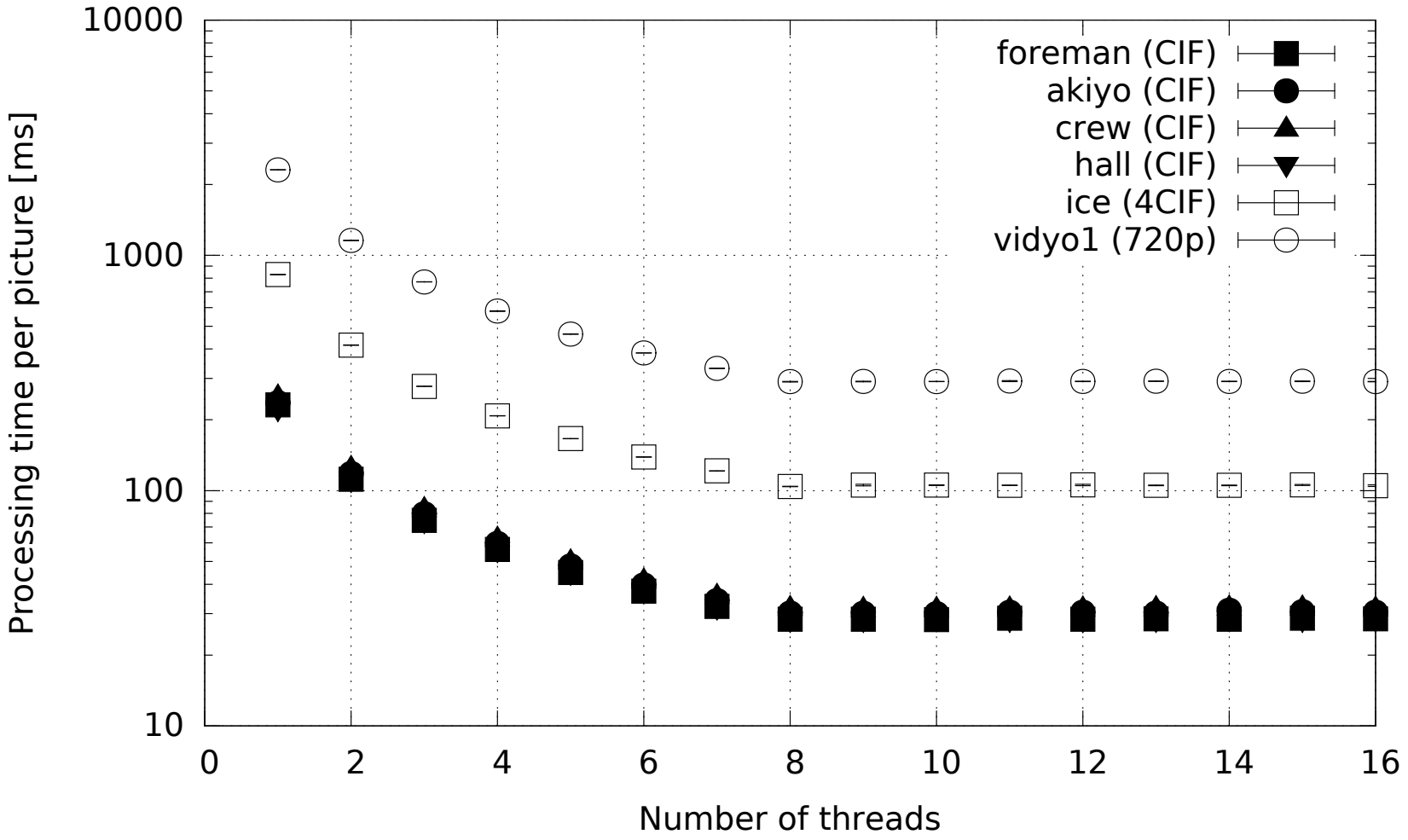
Approach part 3 – Intra-iMCU block swapping



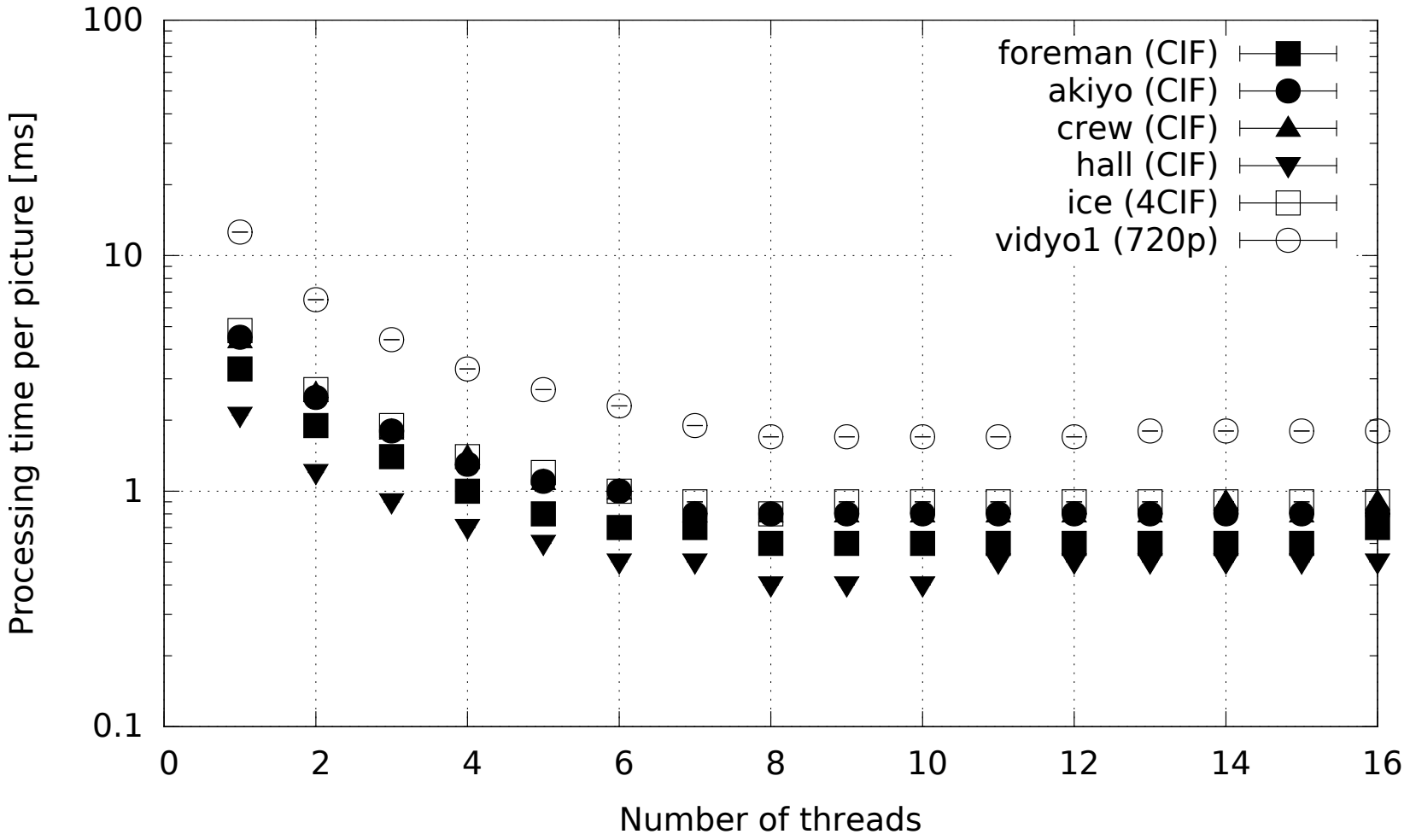
- Example: iMCU with 6 blocks (4 luma, 2 chroma)
- Luma and chroma blocks use different Huffman code words
- Block swapping between luma and chroma is not possible
- Inter-luma-block swapping is possible

Test sequences

Run time performance – encoding



Run time performance – decoding



Face detection performance

- Signalling overhead is negligible
- Face detection accounts for more than 99% of processing time
- Recall is too low compared to ground truth

→ Re-evaluation with algorithms by Sun et al. and (commercial) *KeyLemon* without improvements in detection performance

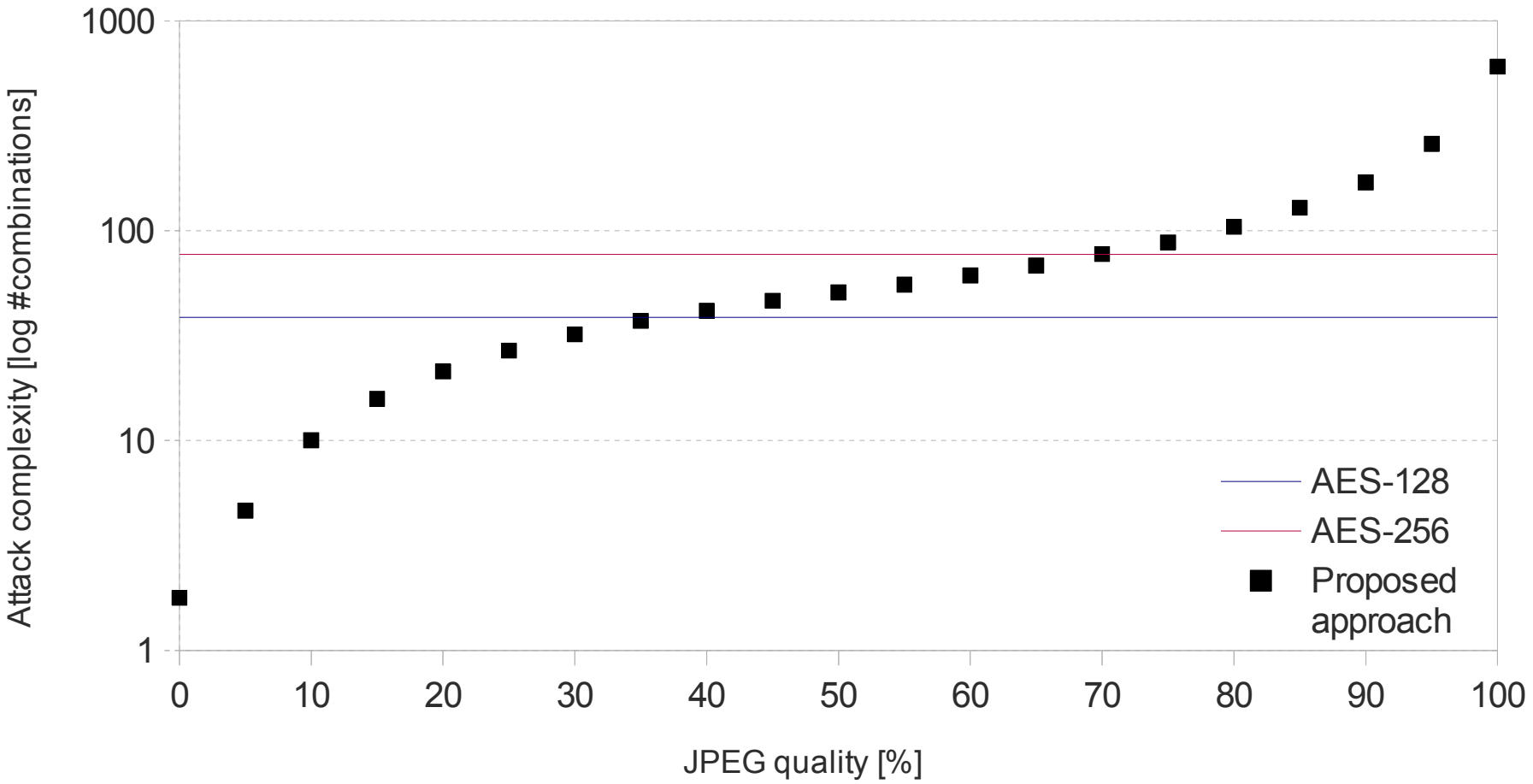
→ State-of-the-art face detection algorithms are not accurate enough

Sequence	**Signalling 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

Security assessment – theoretical considerations

- Analysis of attack complexity (re-reordering and descrambling)
- DC differences are not considered since they are easy to attack
- Tests with LIVE image data base and JPEG reference software
- Attack complexity increases with JPEG quality
- Typical picture: 75% JPEG quality; complexity $\approx 10^{87}$ ways/iMCU
- For comparison: AES-256 key space $\approx 10^{77}$
- Better bruteforce-search AES key than try to decode one iMCU
- Details omitted here

Typical attack complexity



Conclusion

- Encryption approach for (Motion) JPEG video streams
  - Bit-stream-based application (no recompression necessary)
  - All-in-one (including face detection and decryption)
  - Secure (attack complexity of AES-256)
- Prototypical implementation
  - Capable of real-time (CIF@25fps) encryption[1]
  - Face detection accounts for almost all of the processing time
  - Face detection performance is not sufficient yet

→ Future work: Use better and faster face detection algorithm

[1] approx. 4K@30fps without face detection (extrapol.)

References

- Andreas Unterweger, Kevin Van Ryckegem, Dominik Engel, and Andreas Uhl. Building a Post-Compression Region-of-Interest Encryption Framework for Existing Video Surveillance Systems – Challenges, obstacles and practical concerns. Multimedia Systems, 22(5):617-639, October 2016.
- Michael Gschwandtner, Andreas Uhl, and Andreas 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.
- Stefan Auer, Alexander Bliem, Dominik Engel, Andreas Uhl, and Andreas Unterweger. Bitstream-Based JPEG Encryption in Real-time. International Journal of Digital Crime and Forensics, 5(3):1-14, September 2013.
- Dominik Engel, Andreas Uhl, and Andreas Unterweger. Region of Interest Signalling for Encrypted JPEG Images. In IH&MMSec'13: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, pages 165-174. ACM, June 2013.
- Andreas Unterweger and Andreas Uhl. Length-preserving Bit-stream-based JPEG Encryption. In MM&Sec'12: Proceedings of the 14th ACM Multimedia and Security Workshop, pages 85-89, New York, New York, September 2012. ACM.

Thank you for your attention!

Questions?