Univ. Udine, December 2014

Security and Privacy Protection in Smart Camera Networks

ALPEN-ADRIA UNIVERSITÄT
KLAGENFURT | WIEN GRAZ

FAKULTÄT FÜR TECHNISCHE WISSENSCHAFTEN

Institut für Vernetzte und Eingebettete Systeme

Bernhard Rinner
http://bernhardrinner.com

Ubiquitous Cameras

- We are surrounded by billions of cameras in public, private and business spaces
- Various well-known domains
  - Transportation
  - Security
  - Entertainment
  - Mobile

- Cameras serve a purpose and provide some utility
  - Providing documentation/archiving
  - Increasing security
  - Enabling automation
  - Fostering social interaction

Challenges for Security and Privacy

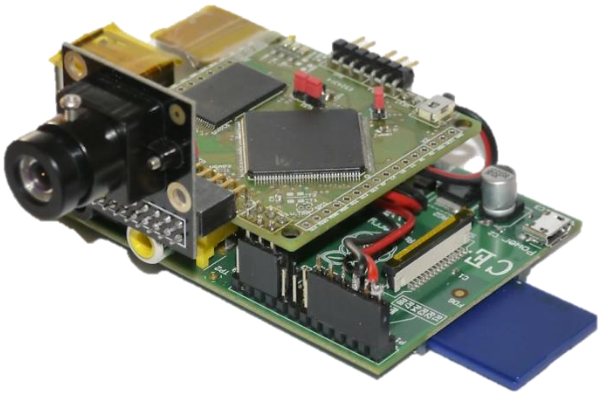
- Unlimited amount of image/video data
- Data can be directly analyzed by humans
- Huge camera/social networks deployed
- Automated analytics in operation

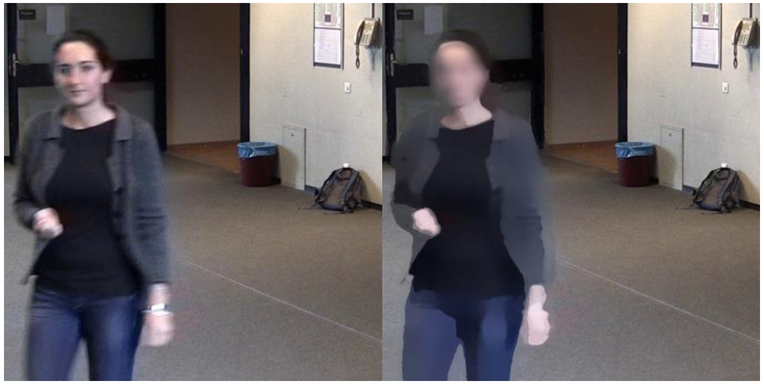
© zeit.de; ucf.edu

Security and privacy protection should be major concern !

Agenda

1. Basics of security und privacy protection in camera networks
   – Threads and challenges
   – Security requirements
2. Our approach
   – Security-enabled smart cameras
   – Privacy protection in videos





Security and Privacy Protection in Camera Networks

[Winkler, Rinner. Security and Privacy Protection in Visual Sensor Networks: A Survey. ACM Computing Surveys, 2014]

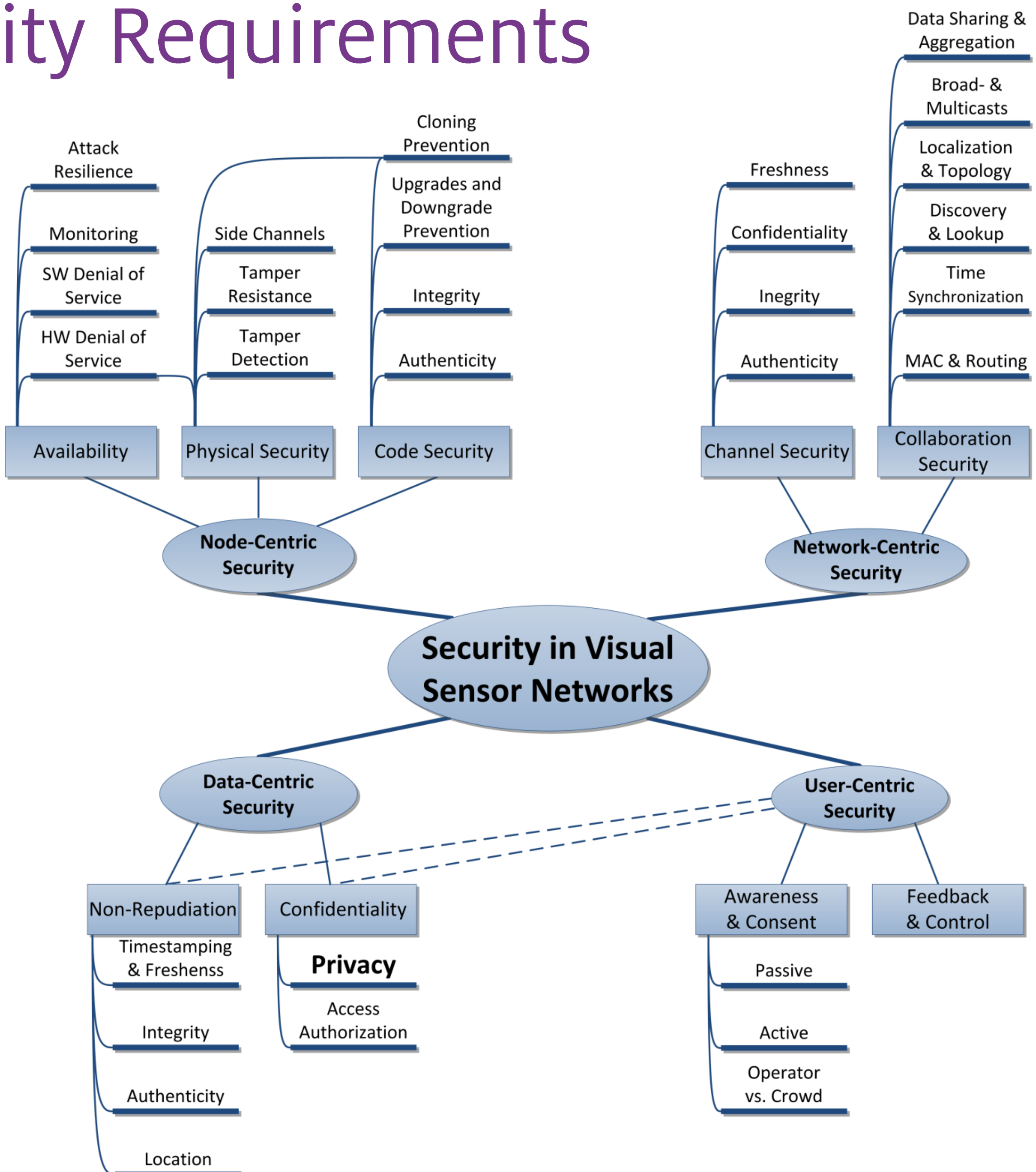
Threats and Attack Scenarios

- Illegitimate data access
  - Attacker is interested in eavesdropping the information exchange
- Illegitimate control
  - Attacker takes active measures to achieve (partial) control; might need to capture/compromise nodes of the network
- Service degradation and denial of service
  - Main goal is to reduce the availability and utility of the network
- Threats from outsiders vs. insiders
- Software vs. hardware attacks.
  - Software attacks are typically performed from remote (via communication channels) and aim at changing the software stack
  - Prevention of hardware (physical) attacks inherently difficult

Key Design Challenges

- Open system architecture
  - Clear trend from traditional closed-circuit networks to open infrastructure (Internet, WiFi etc.)
- Limited system resources
  - Tradeoff between system performance and the implemented security functionality
- Limited physical control
  - Deployment in public (unprotected) environments
- Visual data privacy
  - Images can be easily interpreted by humans and potentially reveal much more information than most other sensor data

Security Requirements



Data-Centric Security

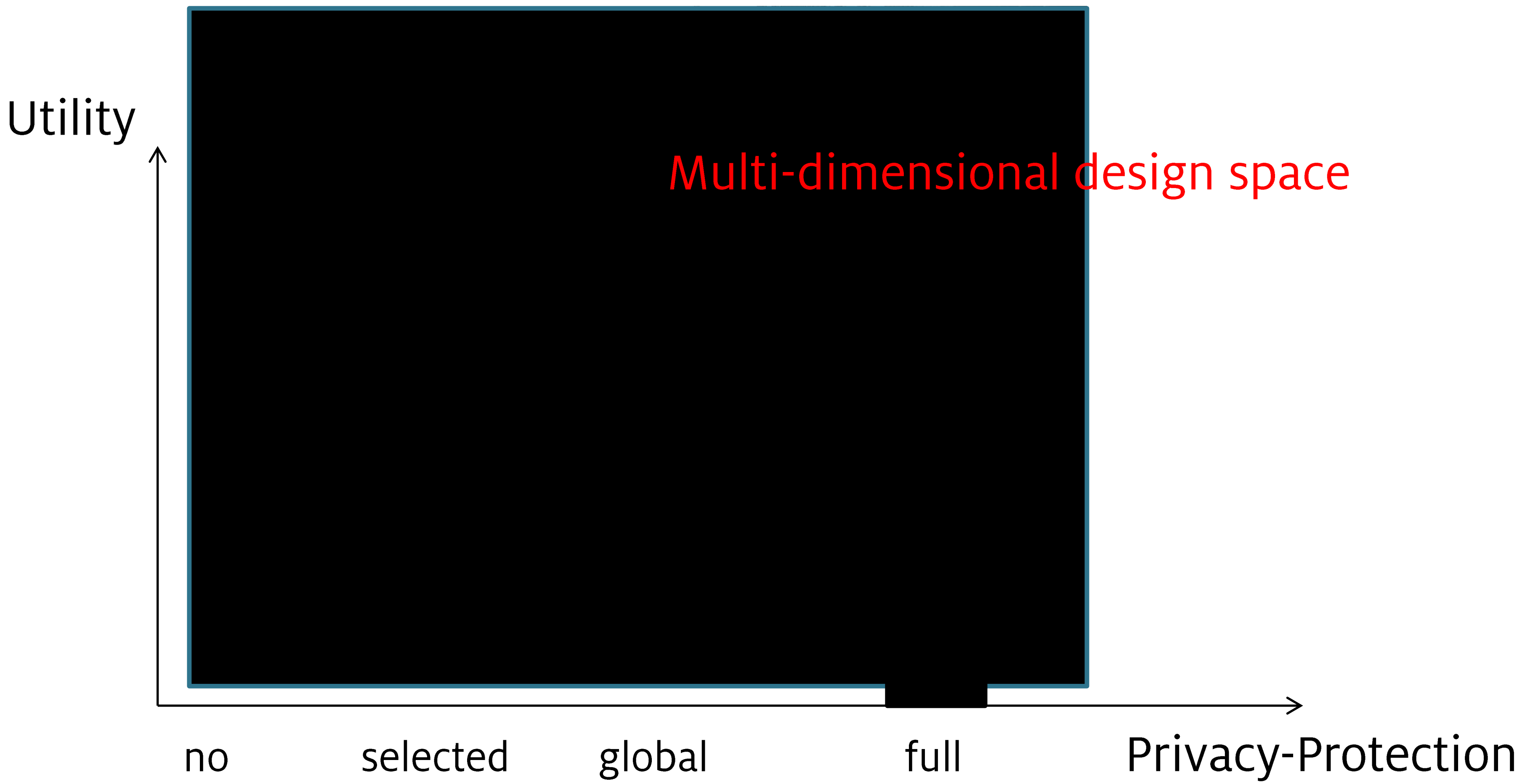
Concerned with the protection of all data made available by camera network

- Non-repudiation subsumes who, where and when data generated as well as detection of manipulation
  - Authenticity: provide evidence about the origin of image and videos
  - Integrity: detect manipulation of image and video data
  - Timestamping/Freshness: detect replay attacks
- Confidentiality makes sure that data cannot be accessed by an unauthorized party
  - Access Authorization: enforce access control for confidential data
  - Privacy: protection of sensitive data against misuse by legitimate users (i.e., insiders).

Privacy Protection in Images

Source: Wikipedia

Utility and Privacy-Protection Tradeoff



User-Centric Security

Concerned with transparency of security features to users

- Awareness and consent about camera network and capturing of personal data
  - Passive vs. active methods
  - Operator vs crowd driven approaches

- Feedback and control provide trusted information about functionality or even actively involve users

[Winkler, Rinner. User Centric Privacy Awareness in Video Surveillance. Multimedia Systems, Springer, 18(2), pages 99-121, 2012.]

Node-Centric Security

Concerned with the protection of camera nodes (incl. hard- and software)

- Availability
  - Hardware and software denial of service
  - System monitoring
  - Attack resilience
- Physical Security
  - Tamper detection and resistance
  - Side channels
- Code Security
  - Authenticity and integrity
  - Secure updates and downgrade prevention
  - Cloning prevention

Network-Centric Security

Concerned with the protection of data transfer within the camera network

- Channel security (for 1:1 communication)
  - Authenticity, integrity, freshness for data transmission
  - Confidentiality
- Collaboration security (beyond 1:1 communication)
  - Similar to security aspects in wireless sensor networks
  - Examples: MAC & routing, time synchronization, discovery & lookup, localization & topology control

Observations and Challenges

- Most protection approaches focus on data-centric aspects
- Reactive data delivery does not replace privacy protection
- Tradeoff between privacy protection and utility barely addressed

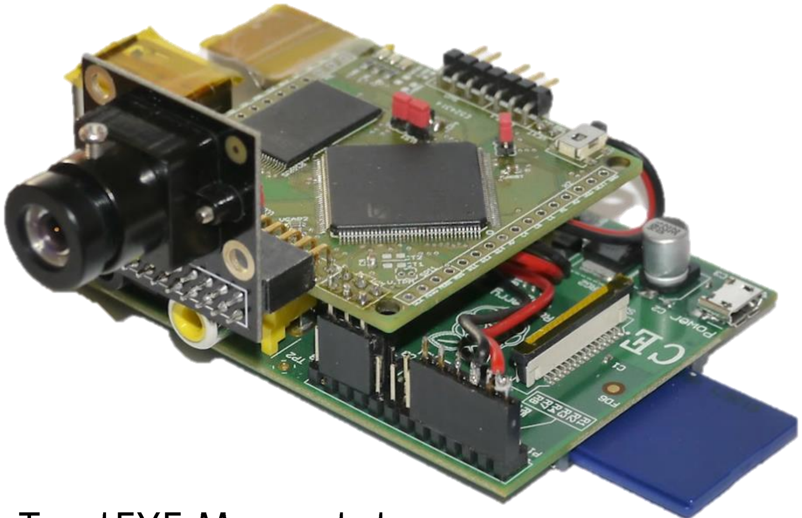
- Open research questions (examples)
  - Holistic security and privacy concept
  - Exploration of security and privacy design space (considering resource limitations)
  - Secure and trustworthy camera sensors
  - User awareness, feedback and control

Security and Privacy-protection with Smart Cameras

Principle of Smart Cameras

- Smart cameras combine
  - sensing,
  - processing and
  - communication

  in a single embedded device



TrustEYE.M4 prototype
on top of RaspberryPI

- perform image and video analysis in real-time closely located at the sensor and transfer only the results
- collaborate with other cameras in the network

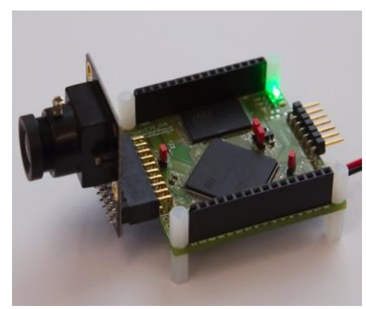
[Rinner, Wolf. A Bright Future for Distributed Smart Cameras. Proc. IEEE, 2008]

Be aware of scarce Resources

- Major resource limitations
  - Processing power
  - Communication bandwidth
  - Onboard memory
  - Energy
- Various Prototypes (with decreasing performance)

SLR Engineering
Atom Z530@ 1.6 GHz

Sony XCISX100C/XP
x86 VIA Eden ULV @ 1 GHz



TrustEYE.M4
ARM Cortex@ 168MHz

CITRIC
PXA 270@ 13-640MHz

[Rinner, Wolf. Towards Pervasive Smart Camera Networks. In Multi-Camera Networks. 2009]

TrustCAM - Security-enabled Embedded Smart Camera

Goals and Assumptions

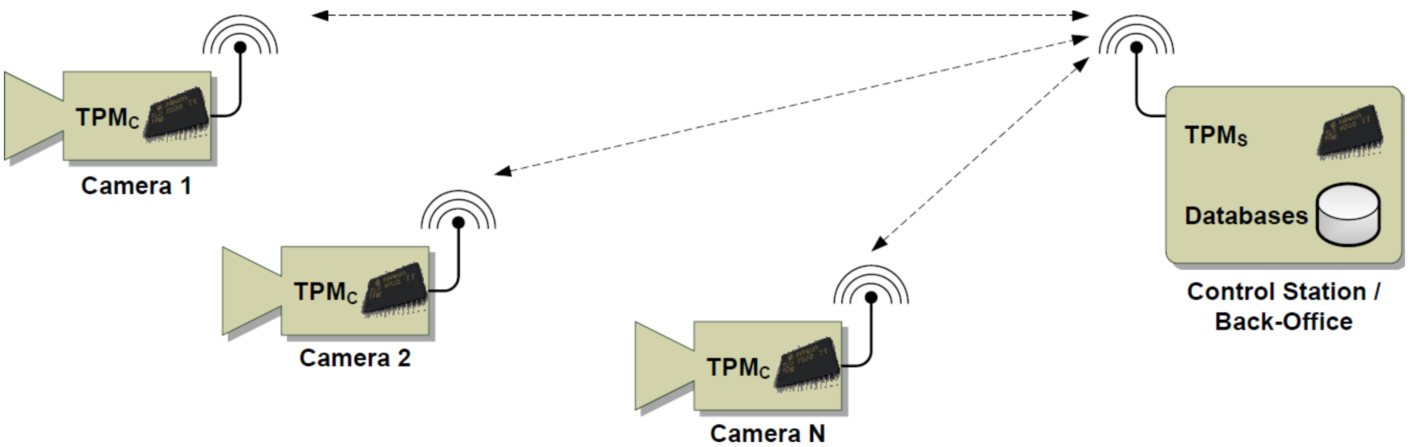
- We present a system level approach that addresses the following security issues:
  - Integrity: detect manipulation of image and video data
  - Authenticity: provide evidence about the origin of image and videos
  - Confidentiality: make sure that privacy sensitive image data cannot be accessed by an unauthorized party
  - Multi-level Access Control: support different abstraction levels and enforce access control for confidential data

- Considered attack types: only software attacks

[Winkler, Rinner. Security Embedded Smart Cameras with Trusted Computing. EURASIP Journal on Wireless Communications and Networking. 2011]

TPM-based Approach

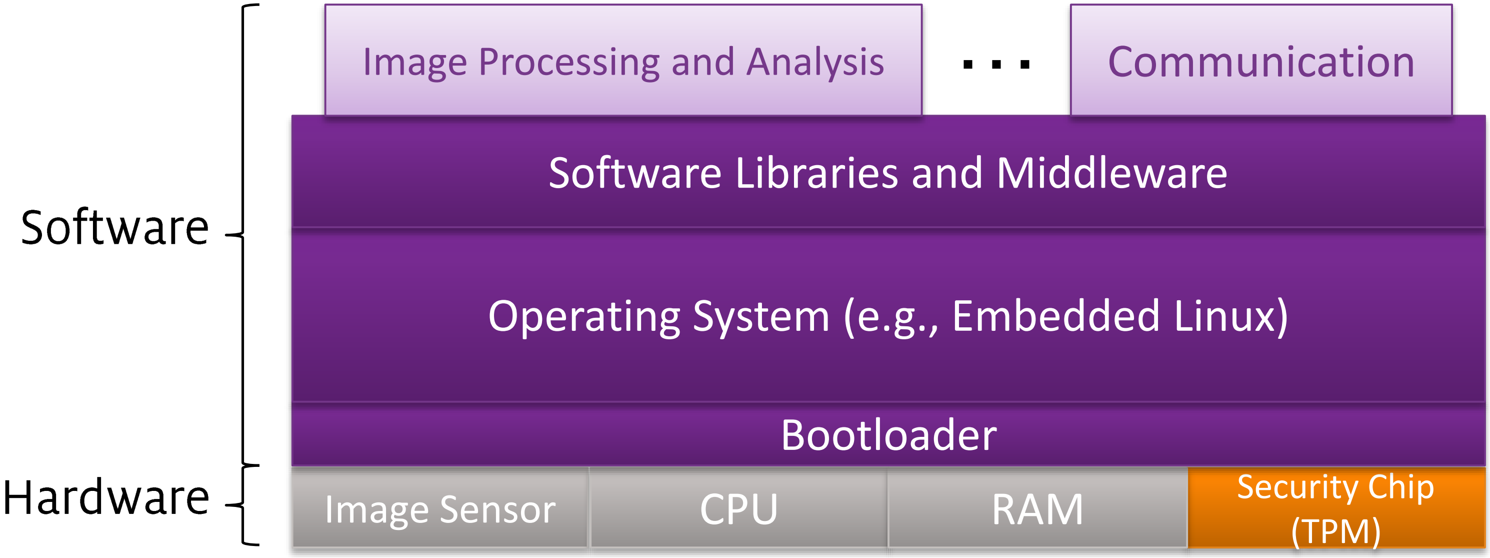
- Bringing of Trusted Computing concepts into cameras
- Trusted Platform Modules (TPMs) are well defined, readily available and cheap



- TC is an open industry standard
- TPMs are available from many manufacturers, but have performance limitations

Hardware Security Anchor

- Trusted Platform Module (TPM) at a glance
  - Secure storage for cryptographic keys
  - Data encryption, digital signatures
  - System status monitoring and reporting (measurement + attestation)
  - Unique platform ID

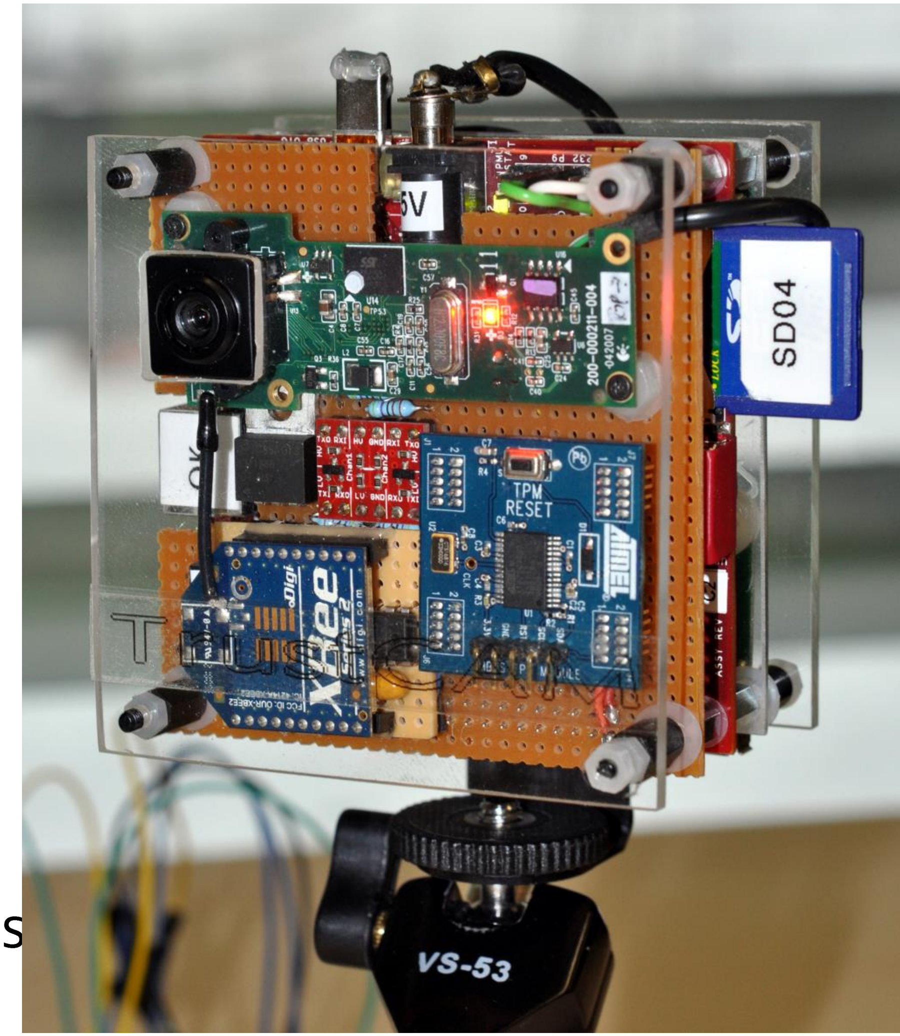


Implemented Security Features

- Trusted boot where camera software stack is “measured” and the status is securely reported to operator
- Integrity and authenticity guarantees using non-migratable, TPM-protected RSA keys
- Freshness/timestamping for outgoing images via TPM-protected tick (counter) sessions

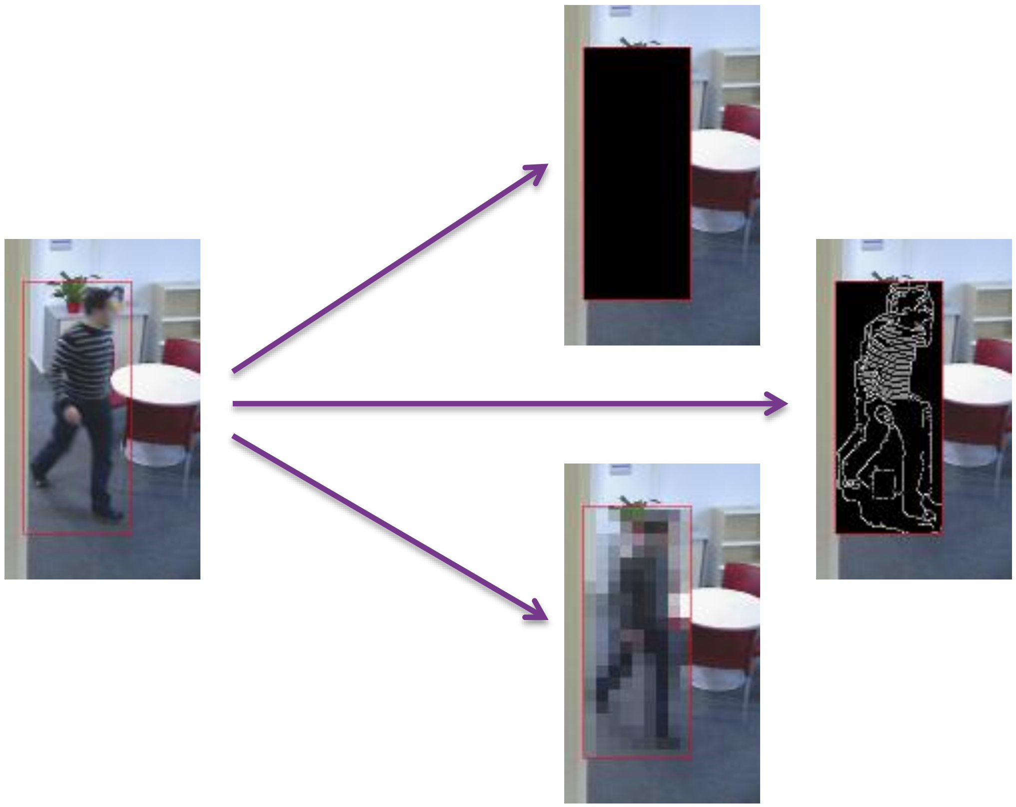
Hardware Prototype

- TI OMAP 3530 CPU:
  ARM @ 480MHz and
  DSP @ 430MHz
- 256MB RAM,
  SD-Card as mass storage
- VGA color image sensor
- wireless: 802.11b/g WiFi and 802.15.4 (XBee)
- LAN via USB (primarily
  used for debugging)
- Atmel hardware TPM on I2C bus



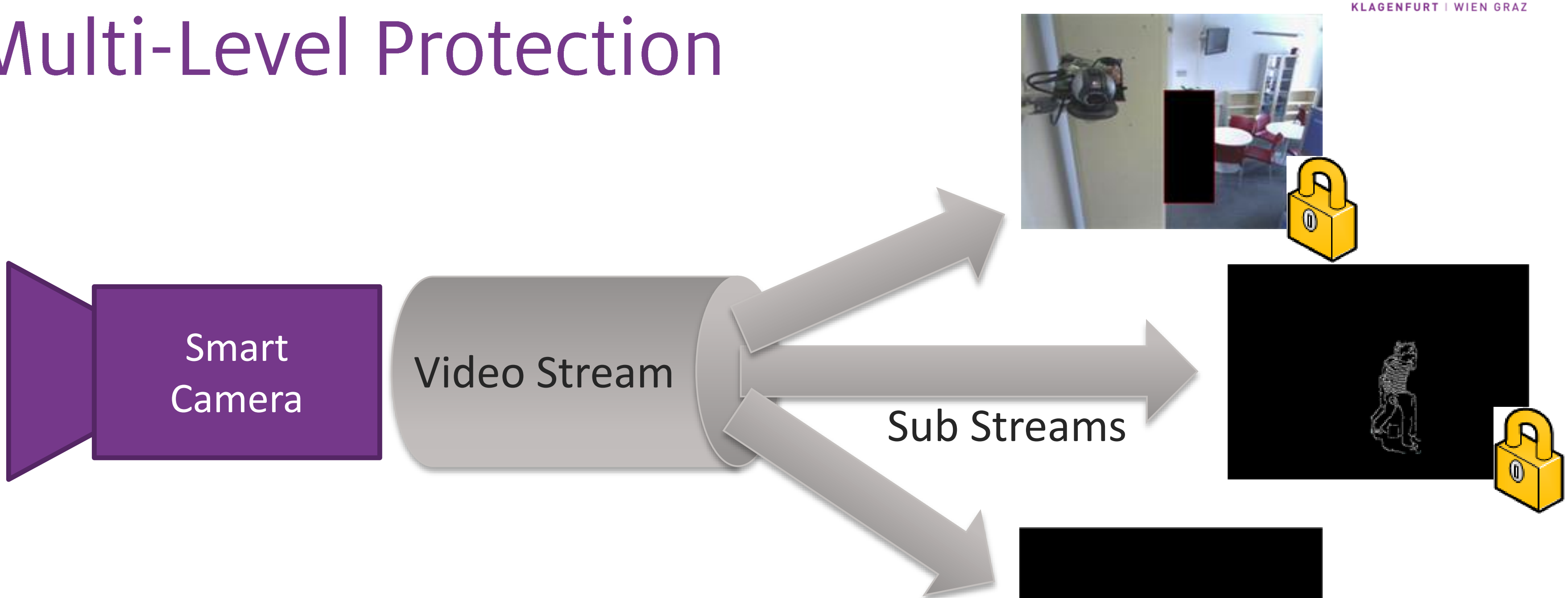
Privacy Protection Approaches

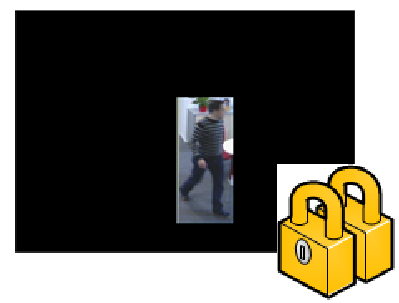
- Protection as an inherent feature of the camera
- Object-based protection: Identification of sensitive data (e.g., human faces)
- Data abstraction and obfuscation



- Global protection techniques: Uniform protection of entire frames (insensitive to misdetections of computer vision)

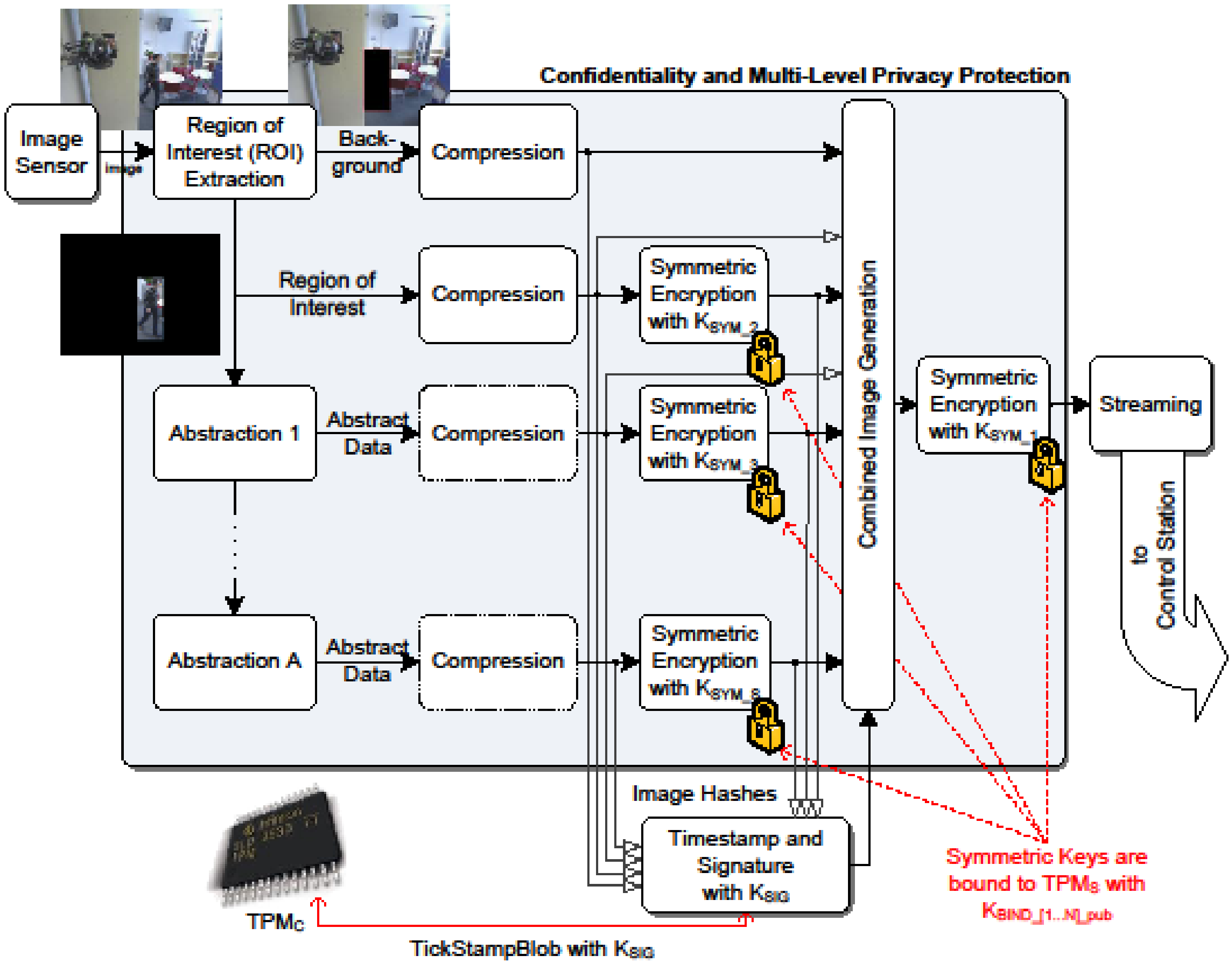
Multi-Level Protection





- Video stream contains sub streams
- Every sub stream is encrypted
  - Hardware-bound cryptographic keys
- Recovery of identities only via four eyes principle

Processing Flow



Implementation and Results

Signature Performance
▪ SHA1 runtime: less than 2ms for less than 30kB of Data ▪ TPM signature runtime: approx. 800ms ▪ additional TPM overheads: approx. 50ms

- Image signing using TPM: SHA1 of image + TPM signature
- TPM too slow to sign every frame
- Approach: accumulate the SHA1 hash of F frames and use TPM to sign this accumulated sum
- Verification also has to be done for the frame groups
- Additional property: group signature ensures correct frame order

Control Station

- Video viewer prototype
- Abstracted regions of interest
- Frame groups signatures embedded as custom EXIF data
- History: circular buffer with last 64 frames
  - Unverified frames: orange
  - Verified frames: dark green
  - Last frame of group: light green

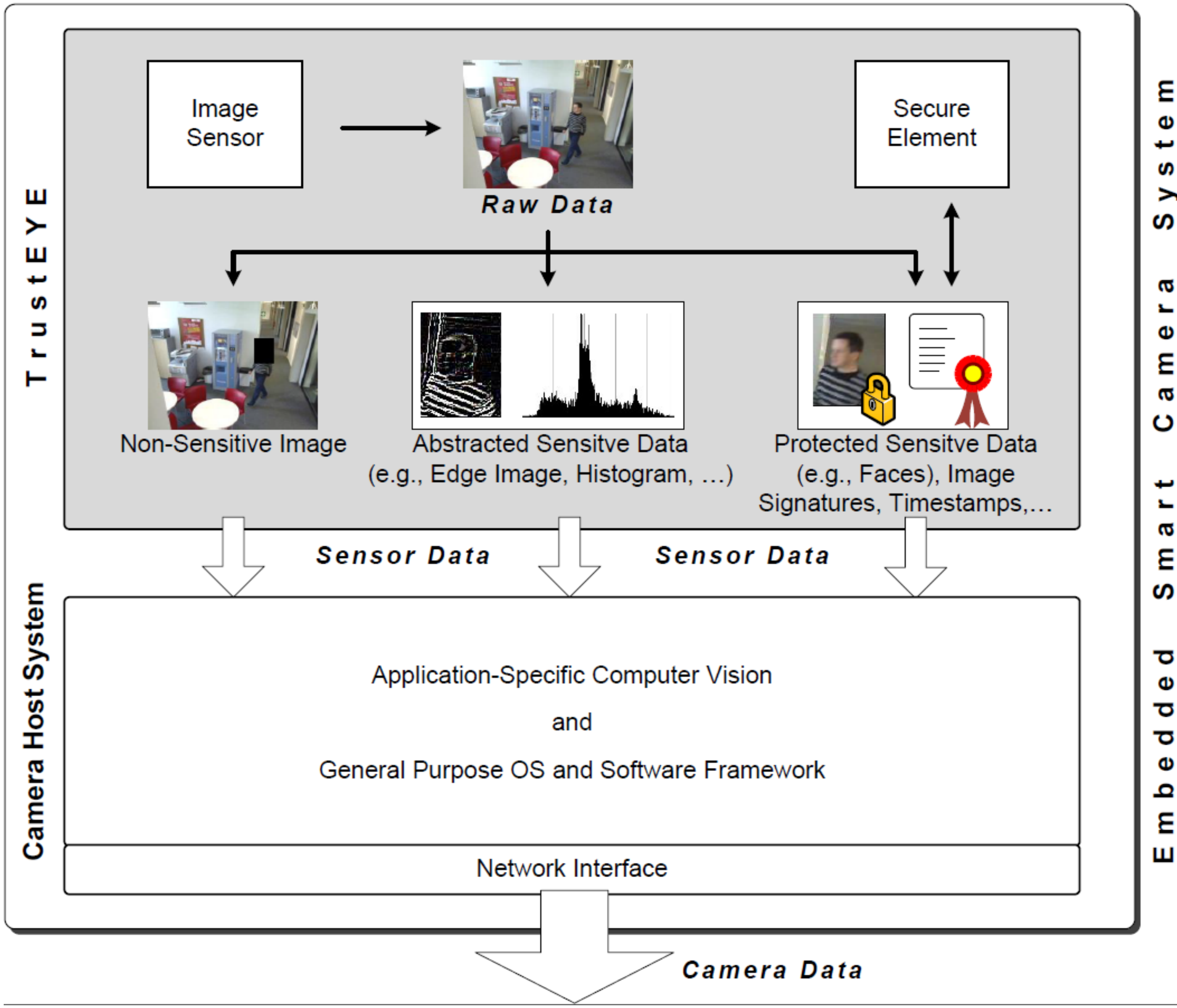
From TrustCAM to TrustEYE

- Vision: Trustworthy Sensing - security and privacy protection as a feature of the image sensor instead of the camera

- Benefits:
  - Sensor delivers protected and pre-filtered data
  - Strong separation btw. trusted and untrusted domains
  - Camera software does no longer have to be trustworthy
  - Security can not be bypassed by application developers
  - TrustEYE is anchor for secure inter-camera collaboration

[Winkler, Rinner. Sensor-level Security and Privacy Protection by embedding Video Content Analysis. In Proc. DSP 2013]
http://trusteye.aau.at/

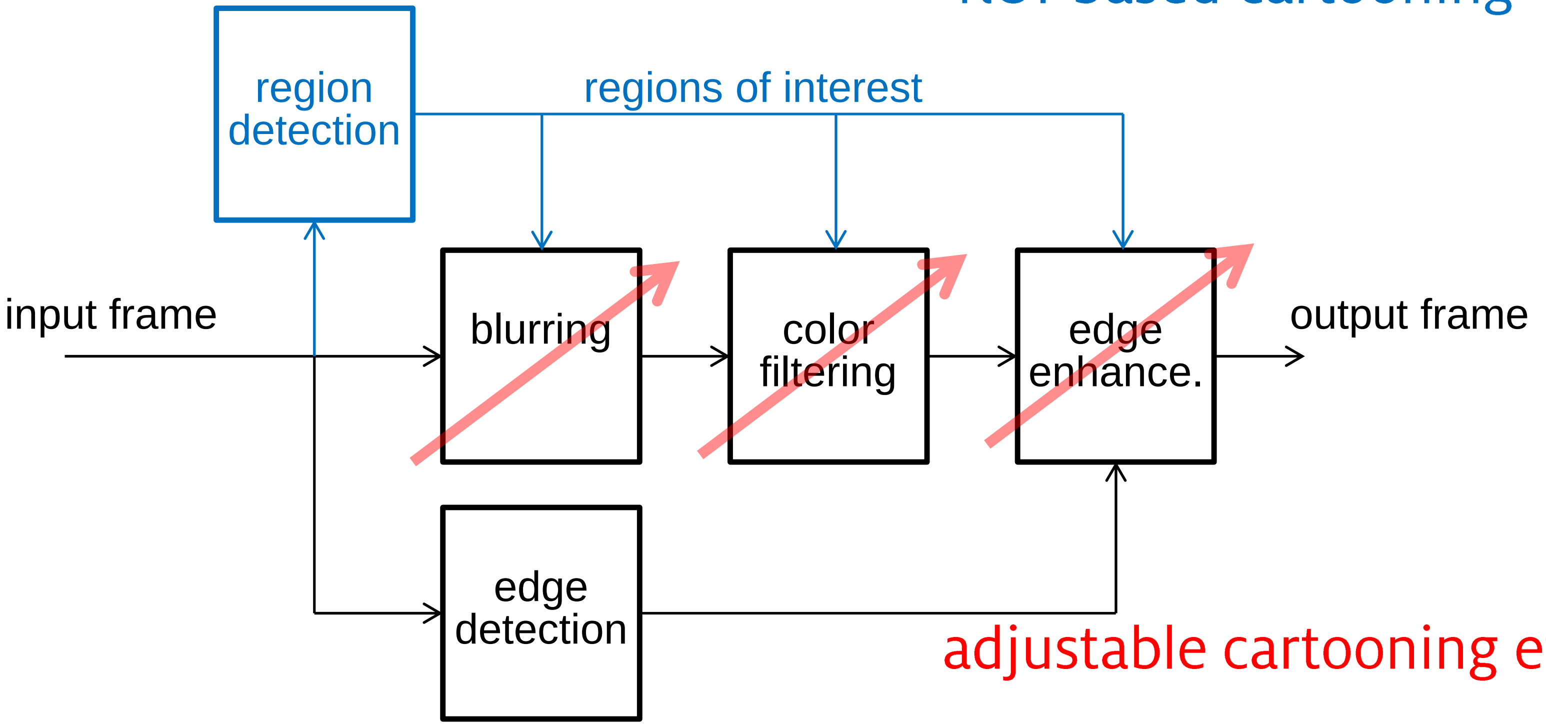
TrustEYE Overview



Privacy Protection by Cartooning

- Abstract parts or entire image by blurring and color filtering
- Cartooning pipeline

ROI-based cartooning



adjustable cartooning effect

- Embed cartooning as privacy feature into smart cameras

ROI-based Cartooning

(c) MediaEval Dataset

Cartooning of detected faces

- Privacy protection depends on performance of region detectors (faces, persons etc.)
- Adapting the filter characteristic beneficial

[Erdelyi et al. Serious Fun: Cartooning for Privacy Protection. In Proc. MediaEval 2013.]

Adjustable Global Cartooning

original

cartooning (small)

cartooning (std)

cartooning (strong)

Evaluating Privacy/Utility Tradeoff

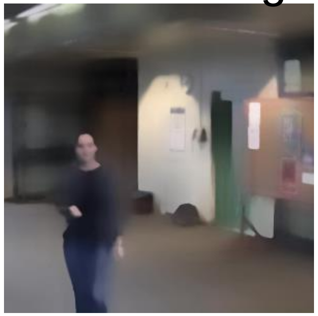
- Establish an objective evaluation framework among key dimensions, i.e.,
  - Privacy protection — Identification of objects of interest
  - Utility — Detection/tracking of objects
  - Appearance — Structural similarity with unprotected frame
  - Resource consumption — Achievable frame rate
- Measure the performance using standard CV algorithms with protected videos (and use labeled test data as ground truth)
  - Independently for each frame
  - Measure protection among object‘s traces

[Erdelyi et al. Adaptive Cartooning for Privacy Protection in Camera Networks. In Proc. IEEE AVSS, 2014]

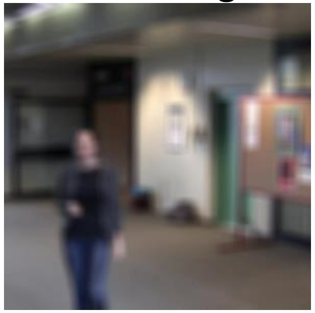
Comparison of Global Filter Approaches

- Performance of standard CV algorithms compared to unprotected video or other protection filters

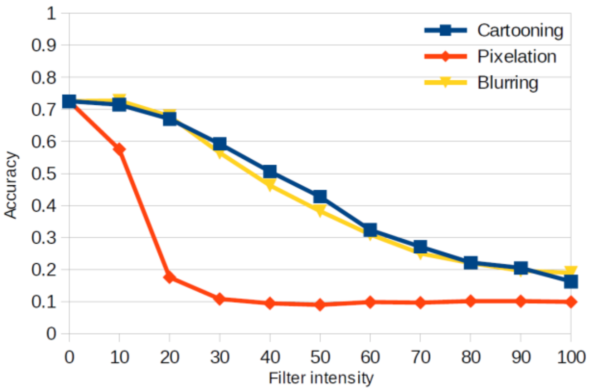
Cartooning



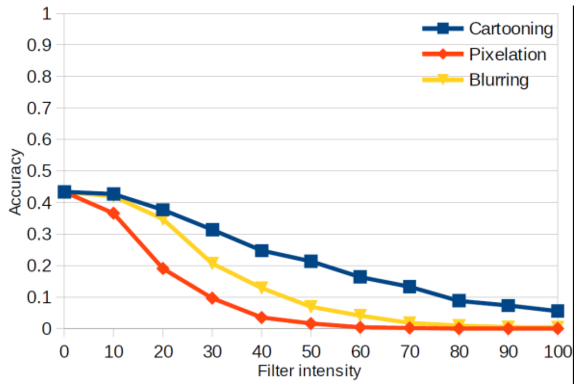
Blurring



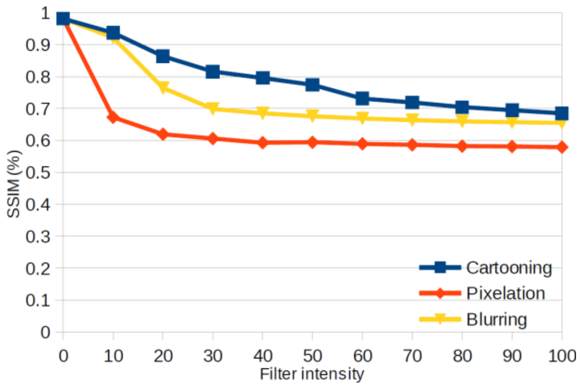
Pixelation



Protection: object re-identification performance

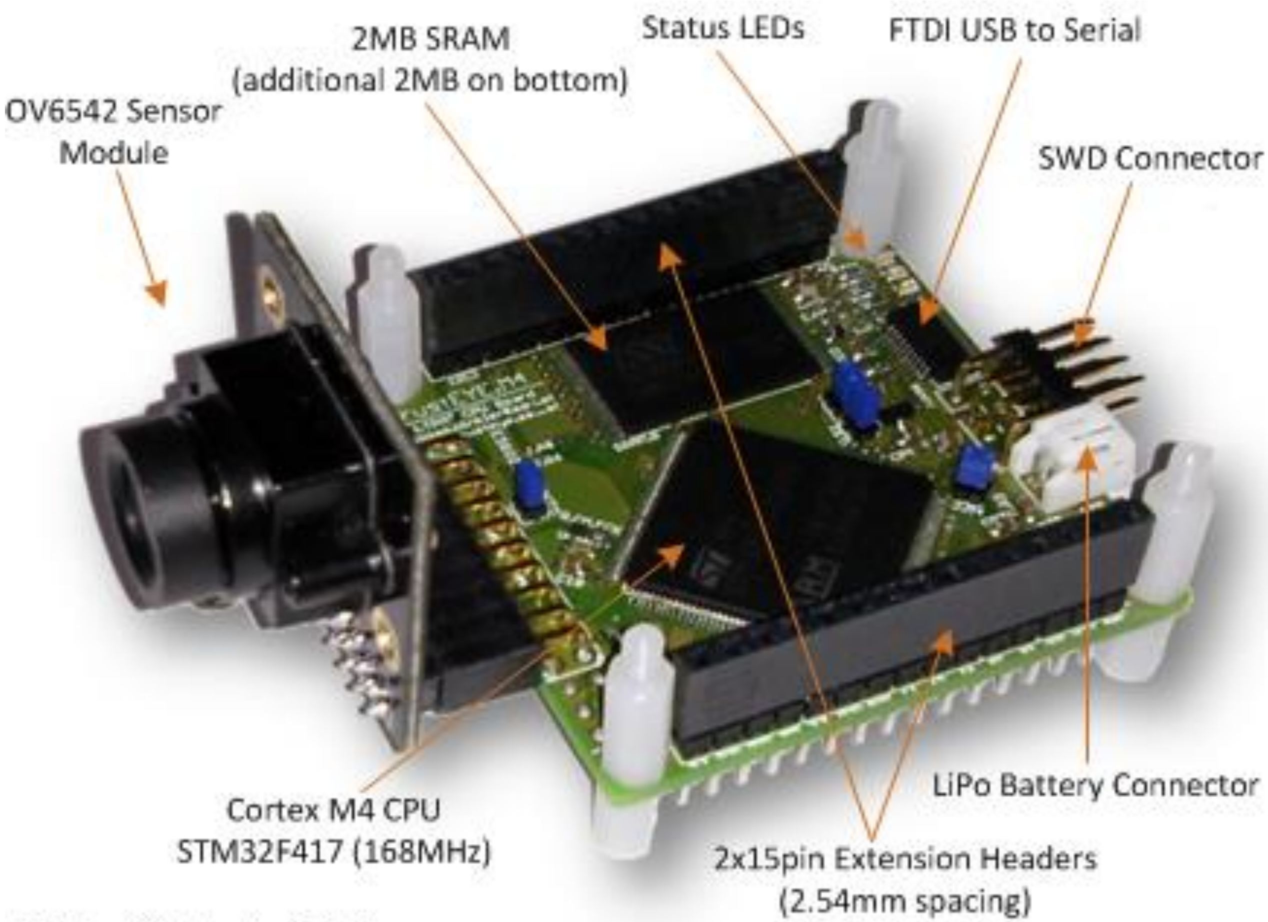


Utility: object detection performance



Appearance: structural similarity index

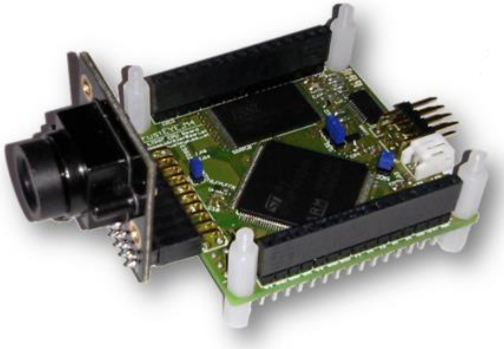
TrustEYE.M4 Architecture



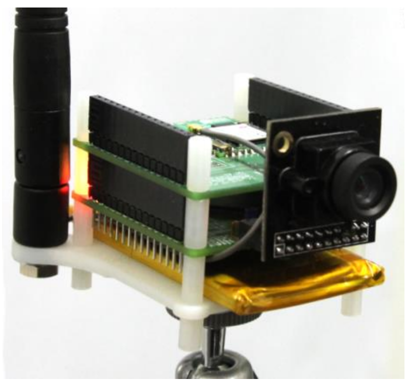
Bottom Side (not visible):
2MB SRAM, TPM Security IC, Power Management IC
(LiPo Charger), Micro USB Connector, Reset Button

TrustEYE.M4 Prototypes

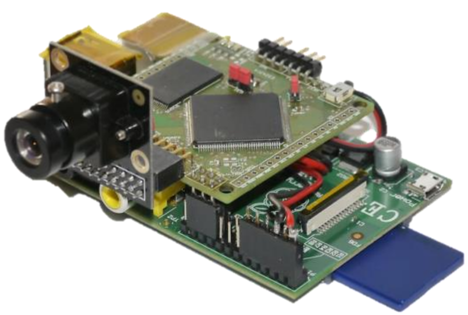
- Processing board (50x50 mm)
  - ARM Cortex M4 @ 168MHz
  - 4 MB SRAM
  - TPM IC: ST33TPM12SPI via SPI
  - Keil RTX RTOS



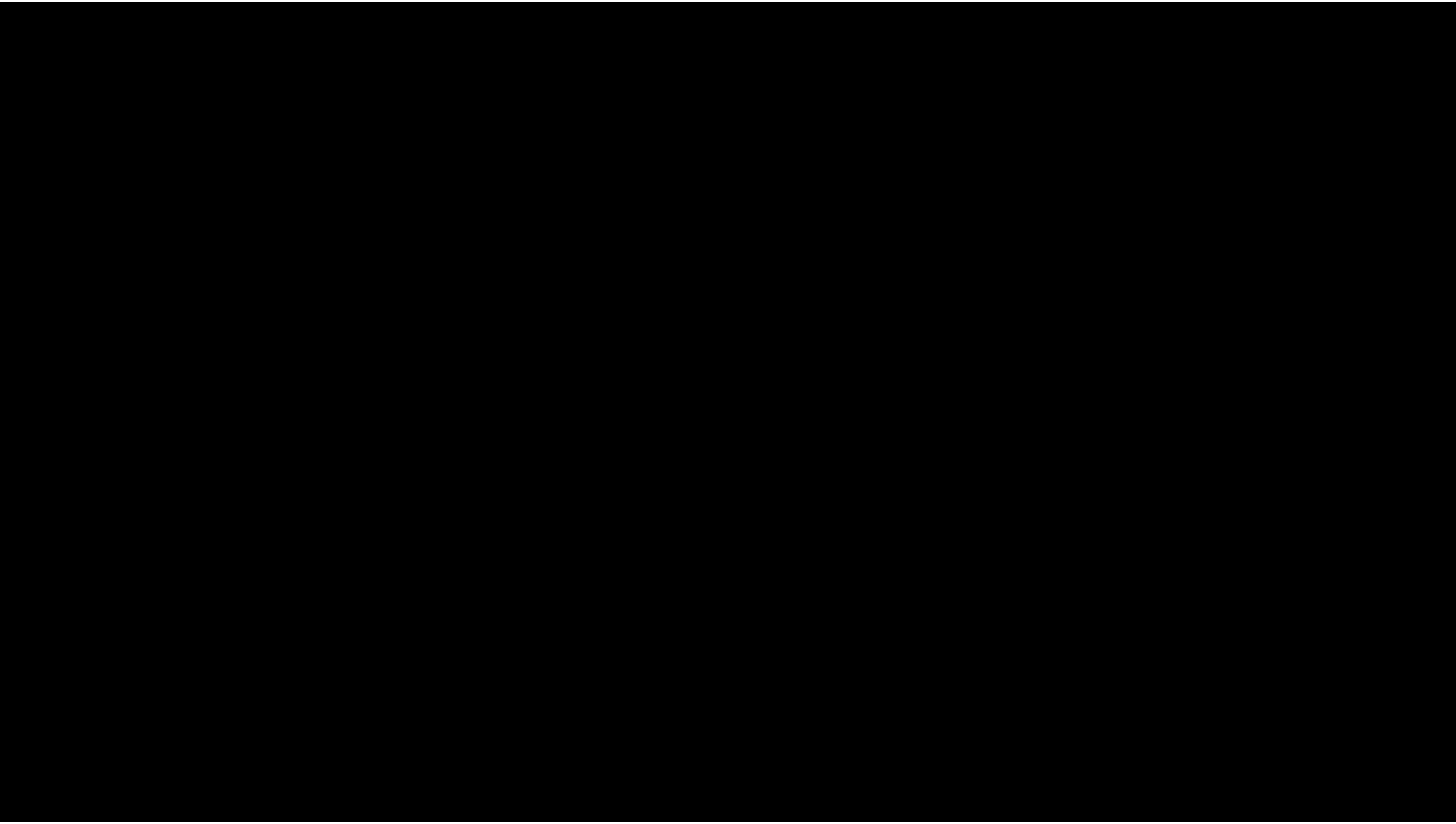
- WiFi extension board (50x50 mm)
  - Redpine Signals RS9110-N-11-02
  - 802.11 b/g/n
  - Encryption: WPA2-PSK, WEP
  - Interconnect: SPI bus on 15pin ext. header



- RaspberryPI mounting option
  - Interconnect: SPI bus via dedicated RPI
  - Daterate: 32 Mbit/s



TrustEYE in Action



ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Summary

- Security and privacy protection (in camera networks) is a highly relevant and requires a holistic (including non-technical) concept
- Our approach protects image data "at the sensor" and exploits dedicated hardware to provide security at
  - data,
  - node and
  - network level
- Prototypes have been developed and demonstrate the feasibility of the approach

Acknowledgements & Further Information

Pervasive Computing group

Institute of Networked and Embedded Systems

http://nes.aau.at

http://bernhardrinner.com