Dr. Thomas Winkler

Security & Privacy Protection in Visual Sensor Networks

ALPEN-ADRIA UNIVERSITÄT
KLAGENFURT | WIEN GRAZ

FAKULTÄT FÜR TECHNISCHE WISSENSCHAFTEN

Institute of Networked and
Embedded Systems

Pervasive Computing Group

Omnipresent Cameras

- **Billions of cameras** in private and business spaces
- A person is **caught on CCTV 300 times** / day in London [1]
- 5.9 million CCTV cameras in UK (**1 camera per 11 people**) [2]
- Various well-known domains
  - Transportation
  - Surveillance
  - Home Monitoring and assisted living
  - Entertainment

[1] C. Norris, G. Armstrong (1999): The maximum surveillance society. The rise of CCTV, Berg Publishing

[2]British Security Industry Authority (BSIA) Survey, July 2013, http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

Visual Sensor Networks

- Spatially distributed visual sensing
  - **Cooperation** between nodes (e.g., tracking)
- Share many properties with WSNs
  - E.g., in-network processing, mesh-like communication structure
  - Amount of captured data much larger
- Resource constraints
  - High computational load leaves little room for security features

Cyclops

CMUcam 4

Citric

Security and Safety

- Security vs. safety
  - **Safety** usually means protection against **unintended events** (accidents)
  - **Security** means protection against **intended events** (e.g., criminal acts)

- Main purpose of a surveillance system / VSN is to **increase security and safety**
  - Look for potentially dangerous situations (e.g., crowds in narrow spaces)
  - Deterrent (e.g., burglary)
  - Identification of individuals after an incident

- VSN security in this talk means
  Protection against attacks on the VSN itself (i.e., IT security)

Outline

- Applications and Requirements
- Threats and attack scenarios
- Security domains and classification
    - Data-centric security
    - Node-centric security
    - Network-centric security
    - User-centric security
- Case Studies

Application Requirements

- Monitoring for **enforcement**
  - Usually **reactive** (i.e., event triggered)
  - **Enforcement** applications: ticketing, speeding, tailgating, traffic light violation

  - Evidence **what** data was captured, **when** and by **whom**

    →non-repudiation

Application Requirements (cont).

- Monitoring for **private safety (and security)**
  - Home monitoring and assisted living
  - Access to personal data only by small group
  - Data **confidentiality / privacy**

Application Requirements (cont.)

- **Monitoring for public safety and security**
  - Usually proactive, **large-scale monitoring**, recording and archiving

  - Used as a **deterrent** and for **post-event analysis**
  - Usually **behavior** is sufficient
  - Confidentiality, access-authorization and non-repudiation are required

Threats and Attack Scenarios

- Illegitimate **data access**
  - Attacker is interested in **eavesdropping** and/or **manipulating** 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

Design Challenges

- **Open system architecture**
  Clear trend from traditional closed-circuit networks to open infrastructure (Internet, WiFi etc.)

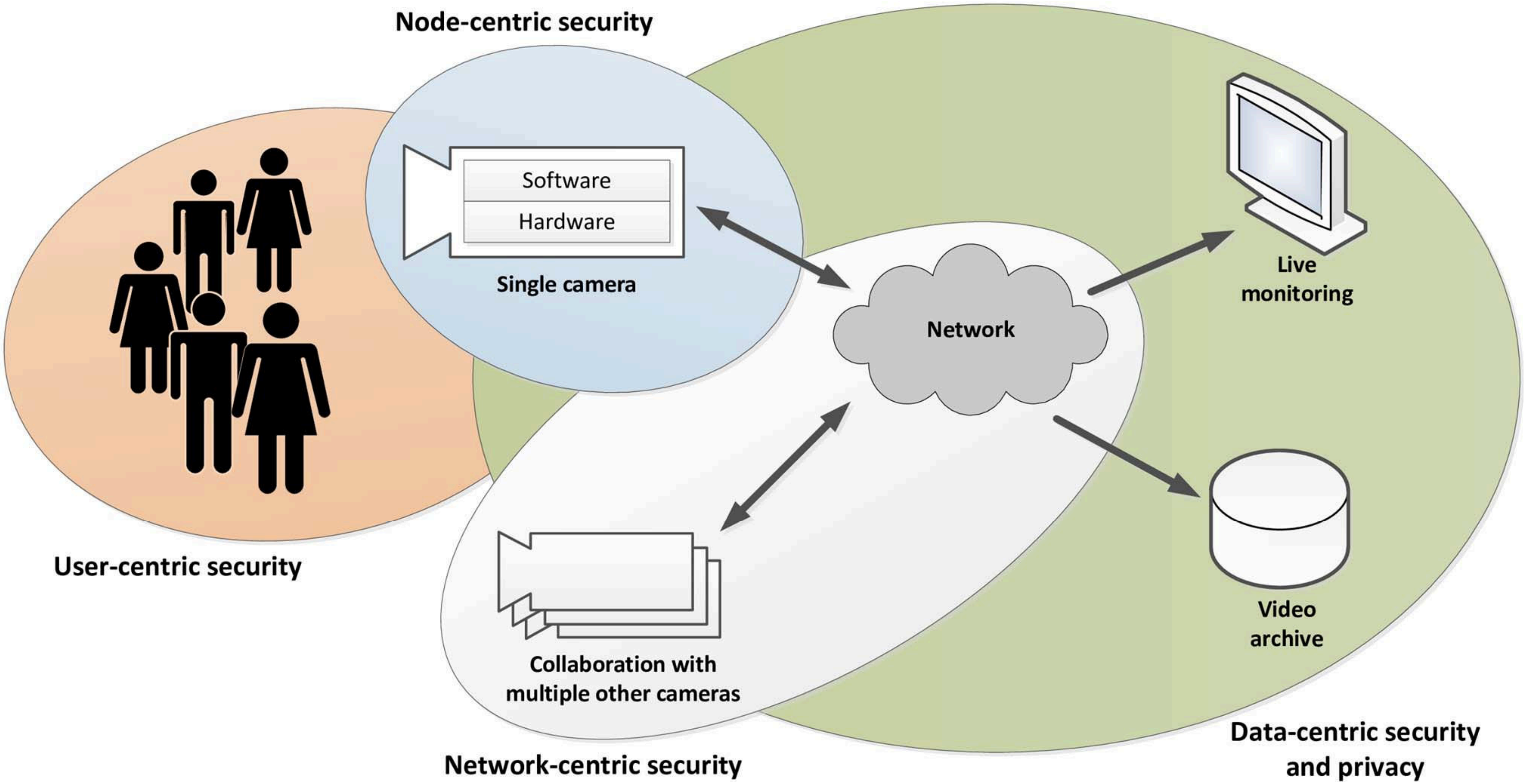
- **Limited system resources**
  Tradeoff between system performance and the implemented security functionality

- **Limited physical control**
  Deployment in public (unprotected) environments

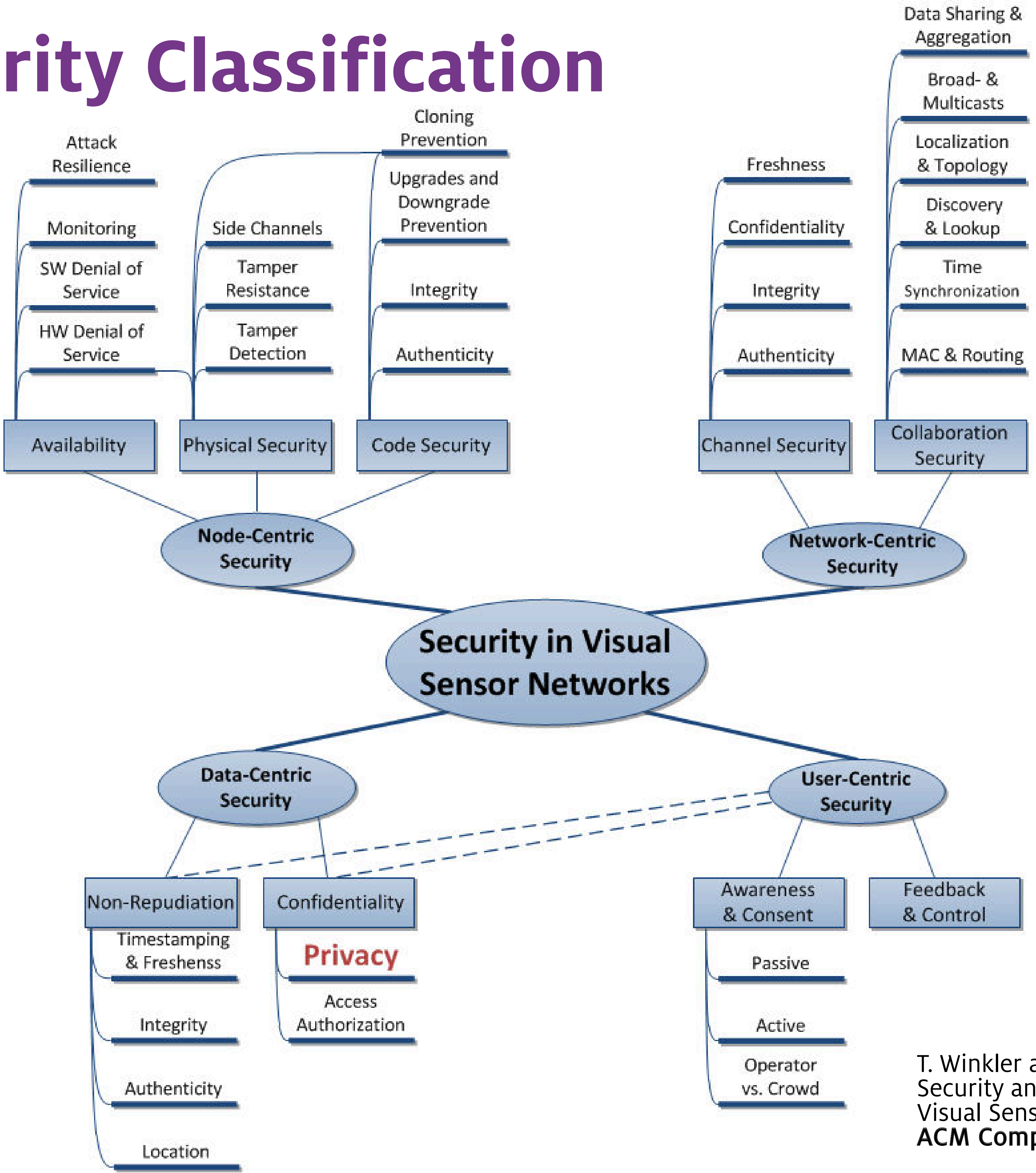
- **Visual data privacy**
  Images can be easily interpreted by humans and potentially reveal much more information than most other sensor data

Security Domains and Classification

VSN Security Domains



Security Classification



T. Winkler and B. Rinner,
Security and Privacy Protection in Visual Sensor Networks: A Survey,
ACM Computing Surveys (in print)

Data-, Node- and Network-centric Security

Data-centric Security

- Non-Repudiation
  - **Integrity**
    - Detect modifications
    - Prevent re-ordering of frames
  - **Authenticity**
  - **Freshness + Timestamping**
    - Protection against replay attacks
    - Proof when an image/video was taken
- **Location** (e.g., in enforcement applications)

- Confidentiality
  - Images/video must not be accessible by 3rd parties
  - **Privacy**: protection of sensitive data against insiders
  - **Access Authorization**
    - Limit access to persons with adequate security clearance
    - Enforce the four eyes principle for especially sensitive data

Network-centric Security

- Protection of **data transfer** within the VSN

- **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

Node-centric Security

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

- **Availability**
  - Hardware and software denial of service
  - System status monitoring
  - Attack resilience

- **Physical Security**
  - Tamper detection and resistance
  - Side channels

- **Code Security**
  - Authenticity and integrity
  - Secure updates and downgrade prevention
  - Cloning prevention

User-centric Security

User-Centric Security

- Awareness and Consent
  - **Passive vs. active** notifications
  - **Operator vs. crowd** driven approaches

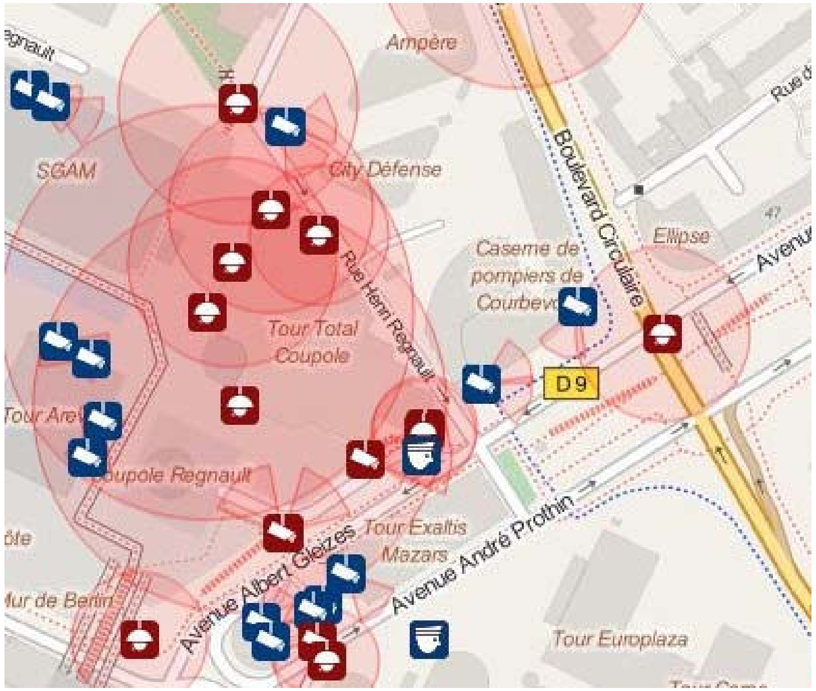
- Feedback and Control
  - Information **what cameras are doing**
  - How personal information is protected and how long it is stored
  - Information should be **easy to understand**
  - Control over distribution and use of personal data
  - Require user **permission for data disclosure** to 3rd parties

Generating Awareness

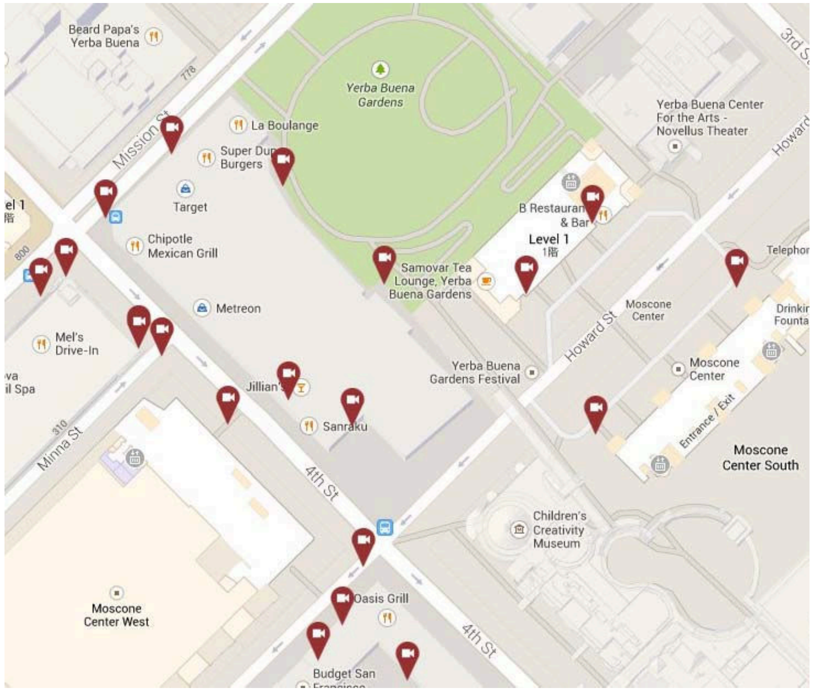
- People are made aware by **stickers and plates**

Generating Awareness (cont.)

- Illustrate **how widespread** video surveillance is
- **Increase pressure** on operators, manufacturers, governments
- **Community / crowd-based** mapping of cameras

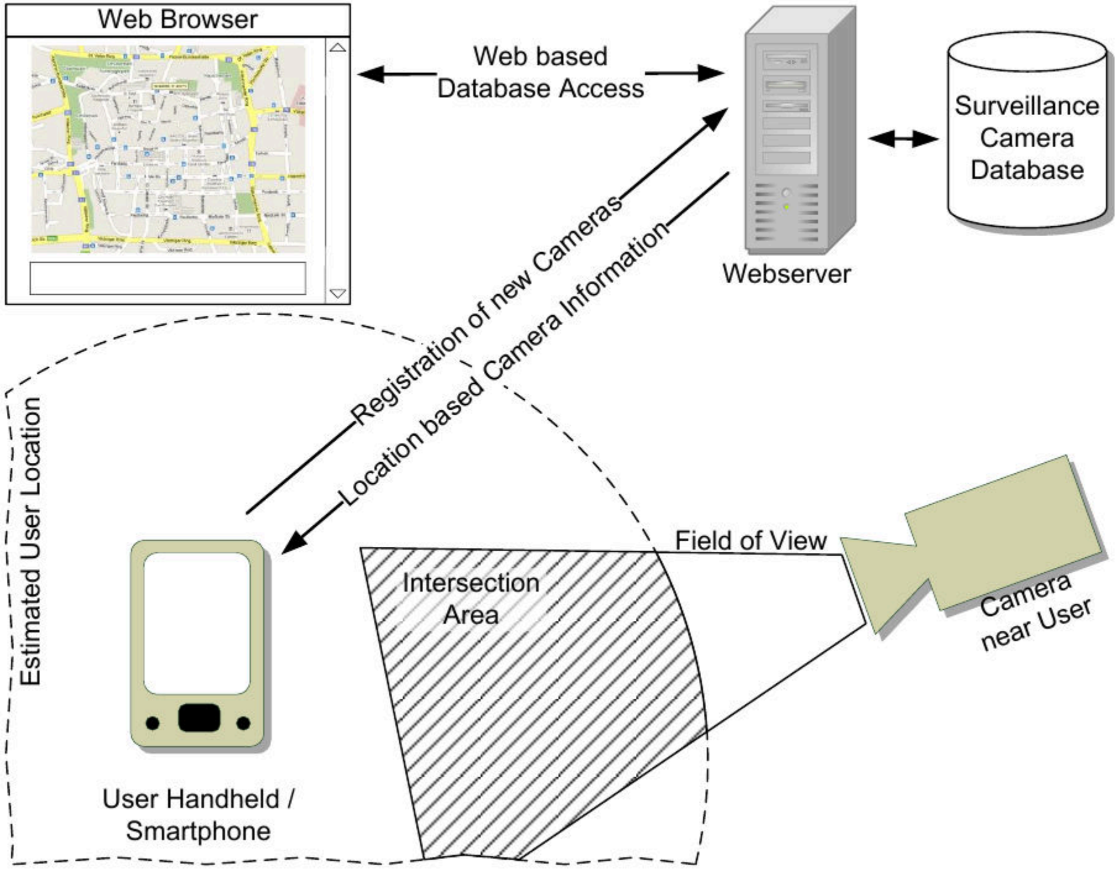


OpenStreetMap: http://osmcamera.tk/



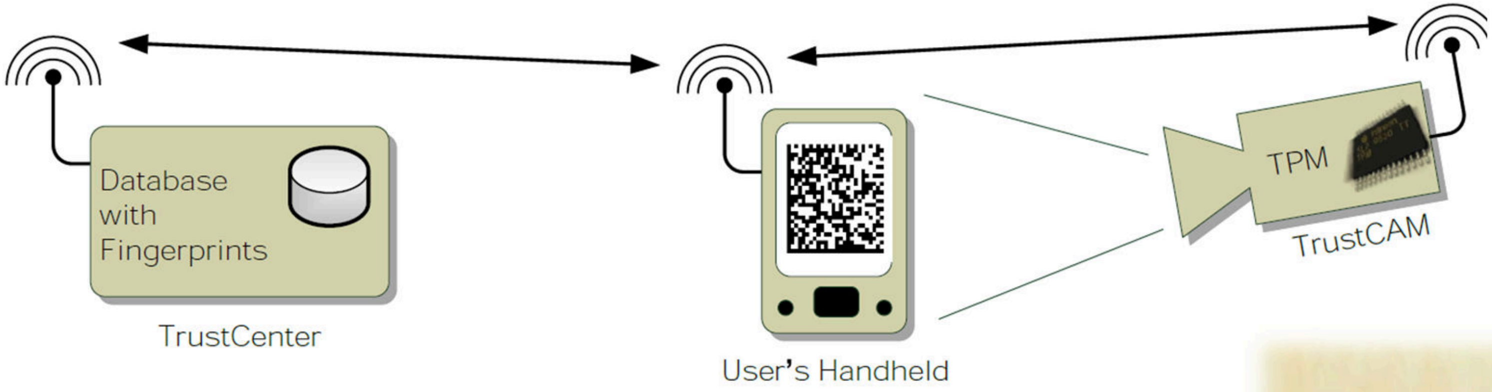
CommunityCam
http://www.videosurveillance.com/communitycam/

Active Notification and Feedback



- Location-based notification via smartphone
- Direct feedback to users about camera status

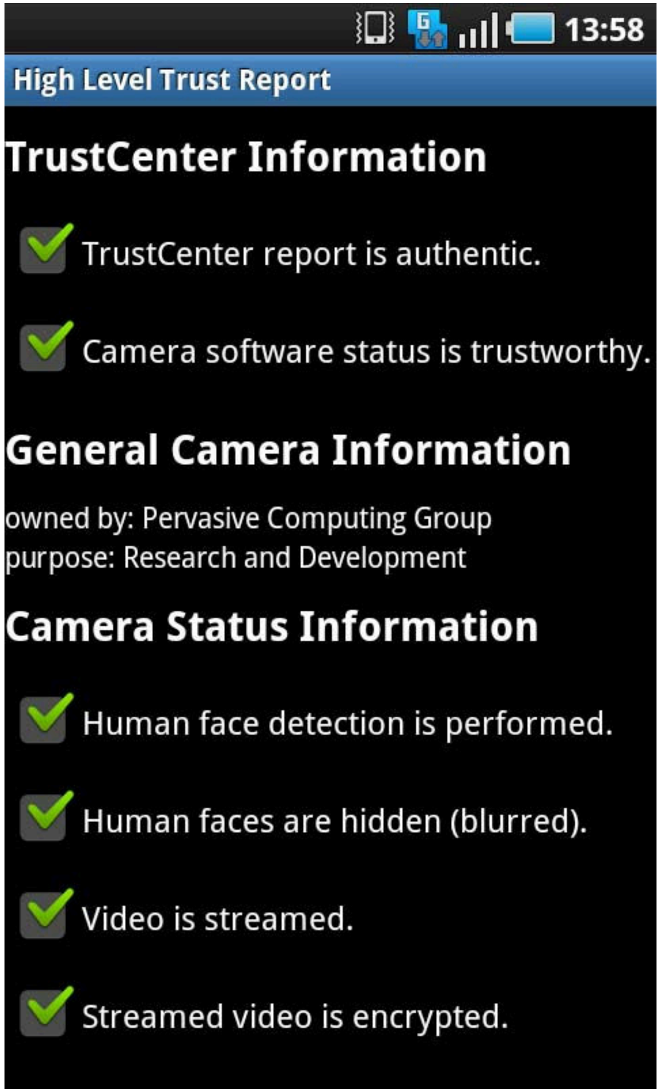
Unser Feedback



- Goal: **Trustworthy feedback to monitored persons** about camera's privacy protection
- **Visual communication** for authentication
  - Direct line of sight
  - Intuitive way to select intended camera
- Operator discloses applications to TrustCenter

T. Winkler and B. Rinner, "User Centric Privacy Awareness in Video Surveillance," Multimedia Systems Journal, vol. 18, no. 2, pp. 99–121, 2012.

Attestation Report



High Level Trust Report

TrustCenter Information

✓ TrustCenter report is authentic.

✓ Camera software status is trustworthy.

General Camera Information

owned by: Pervasive Computing Group
purpose: Research and Development

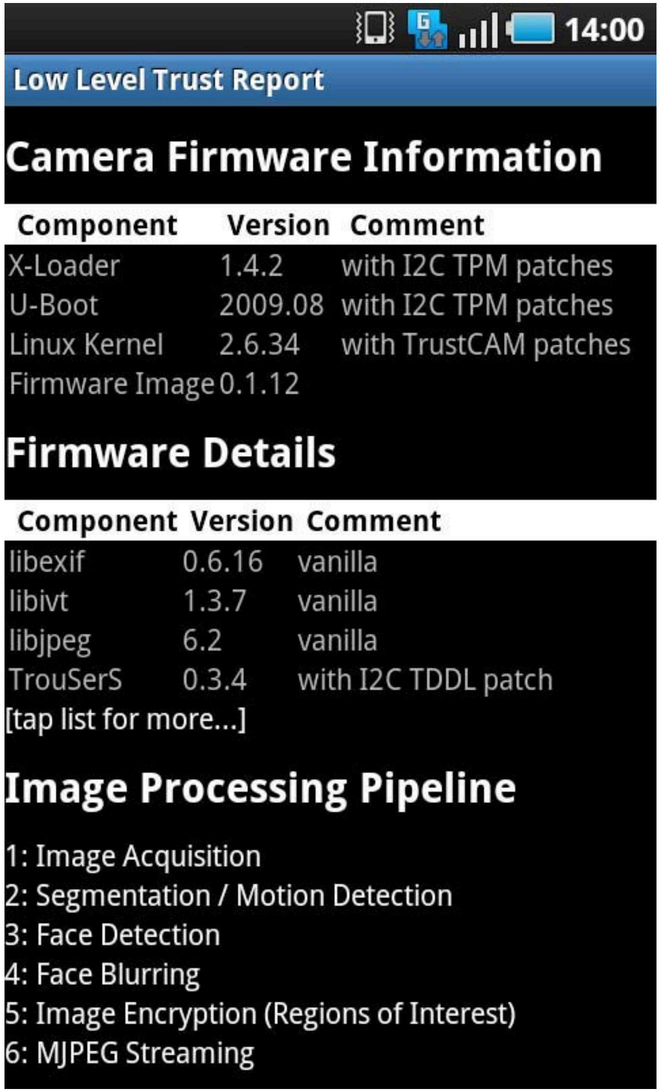
Camera Status Information

✓ Human face detection is performed.

✓ Human faces are hidden (blurred).

✓ Video is streamed.

✓ Streamed video is encrypted.



Low Level Trust Report

Camera Firmware Information

Component	Version	Comment
X-Loader	1.4.2	with I2C TPM patches
U-Boot	2009.08	with I2C TPM patches
Linux Kernel	2.6.34	with TrustCAM patches
Firmware Image	0.1.12	

Firmware Details

Component	Version	Comment
libexif	0.6.16	vanilla
libivt	1.3.7	vanilla
libjpeg	6.2	vanilla
TrouSerS	0.3.4	with I2C TDDL patch

[tap list for more...]

Image Processing Pipeline

1: Image Acquisition
2: Segmentation / Motion Detection
3: Face Detection
4: Face Blurring
5: Image Encryption (Regions of Interest)
6: MJPEG Streaming

Privacy Protection

Privacy Protection

- Privacy is a **subset of confidentiality** and denotes protection of sensitive data against **insiders**

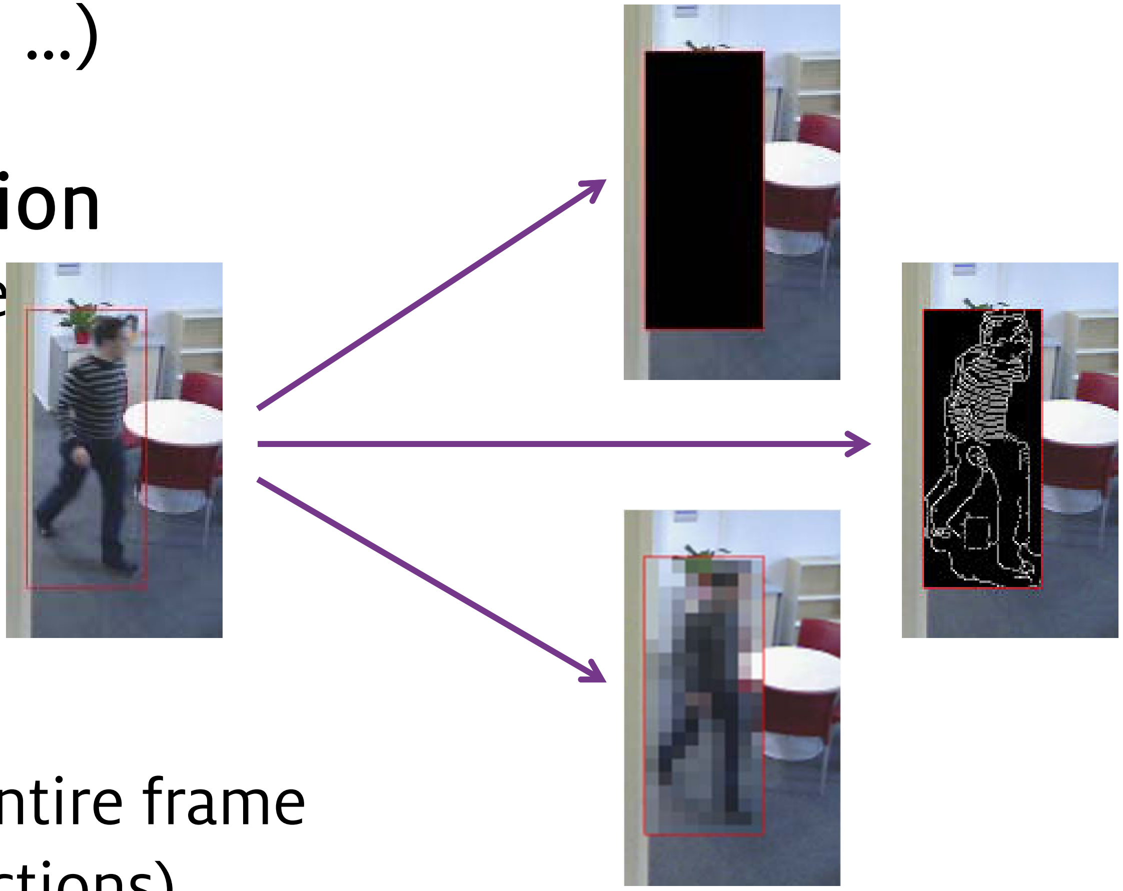
- For **monitoring** purposes **behavior** is usually more important than identity

- Only under special circumstances (e.g., law violations) identities are important

- Goal: **Hide identity** information during normal operation but **make it recoverable** (under controlled conditions)

Privacy Protection Approaches

- **Data abstraction** (e.g., stick figures) and **data obfuscation** (e.g., blurring, pixelization, morphing, scrambling, …)
- **Object-based protection**
  - Detection of sensitive re (e.g., human faces)



- **Global protection**
  - Uniform protection of entire frame (insensitive to mis-detections)

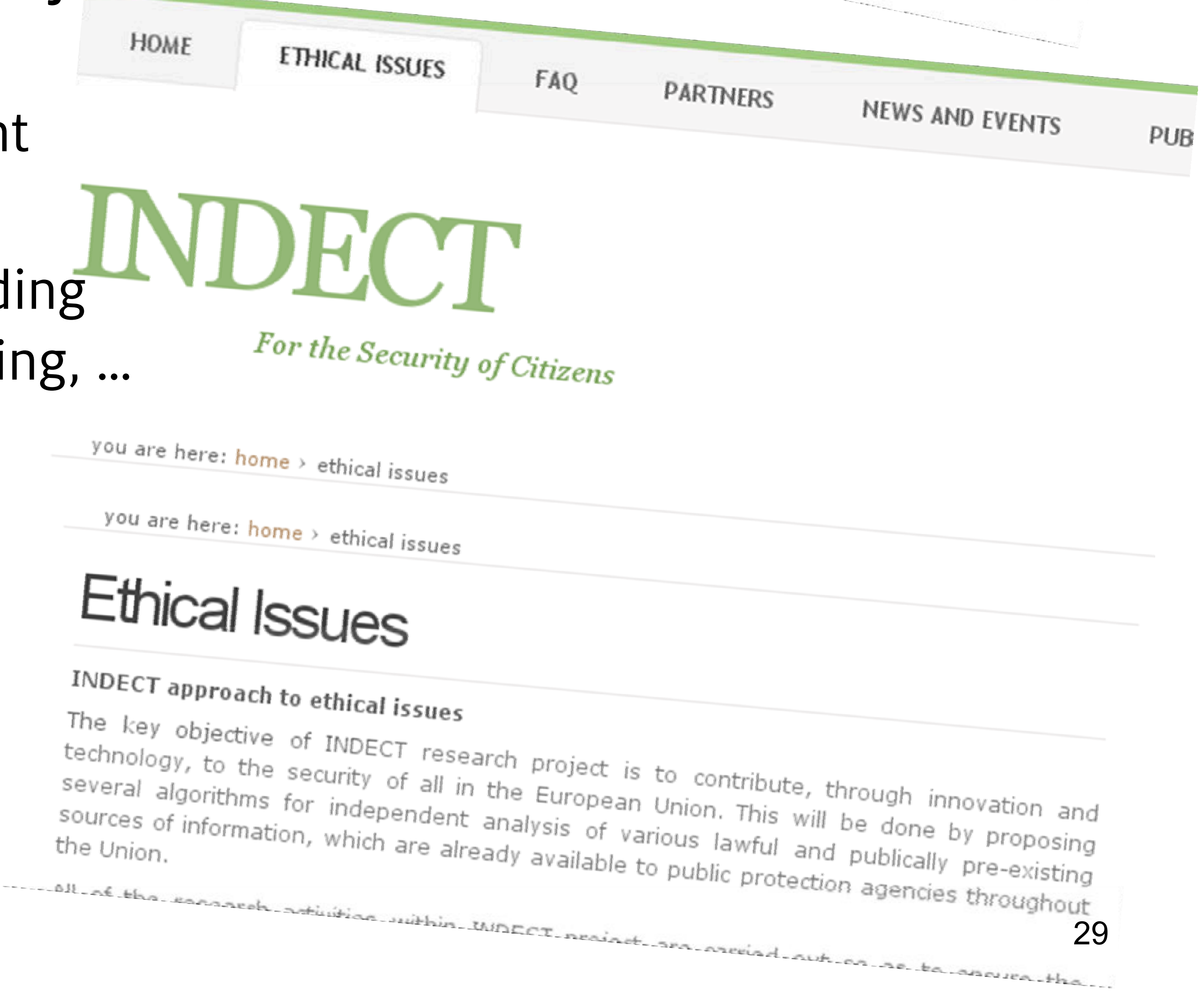
Privacy vs. Surveillance

- On the one hand
  - **Number of cameras** is increasing rapidly
  - Surveillance as a **useful tool** (e.g., Boston bombings)

- On the other hand
  - In Europe **concerns about personal privacy** seem to increase
  - Extreme forms: **vandalism against CCTV** cameras (“Camover”)

Privacy vs. Surveillance

- Online petitions against **INDECT EU research project**
- **Goal:** automatic threat detection and intelligent monitoring
- Different sources including CCTV, network monitoring, …



INDECT

For the Security of Citizens

you are here: home › ethical issues

you are here: home › ethical issues

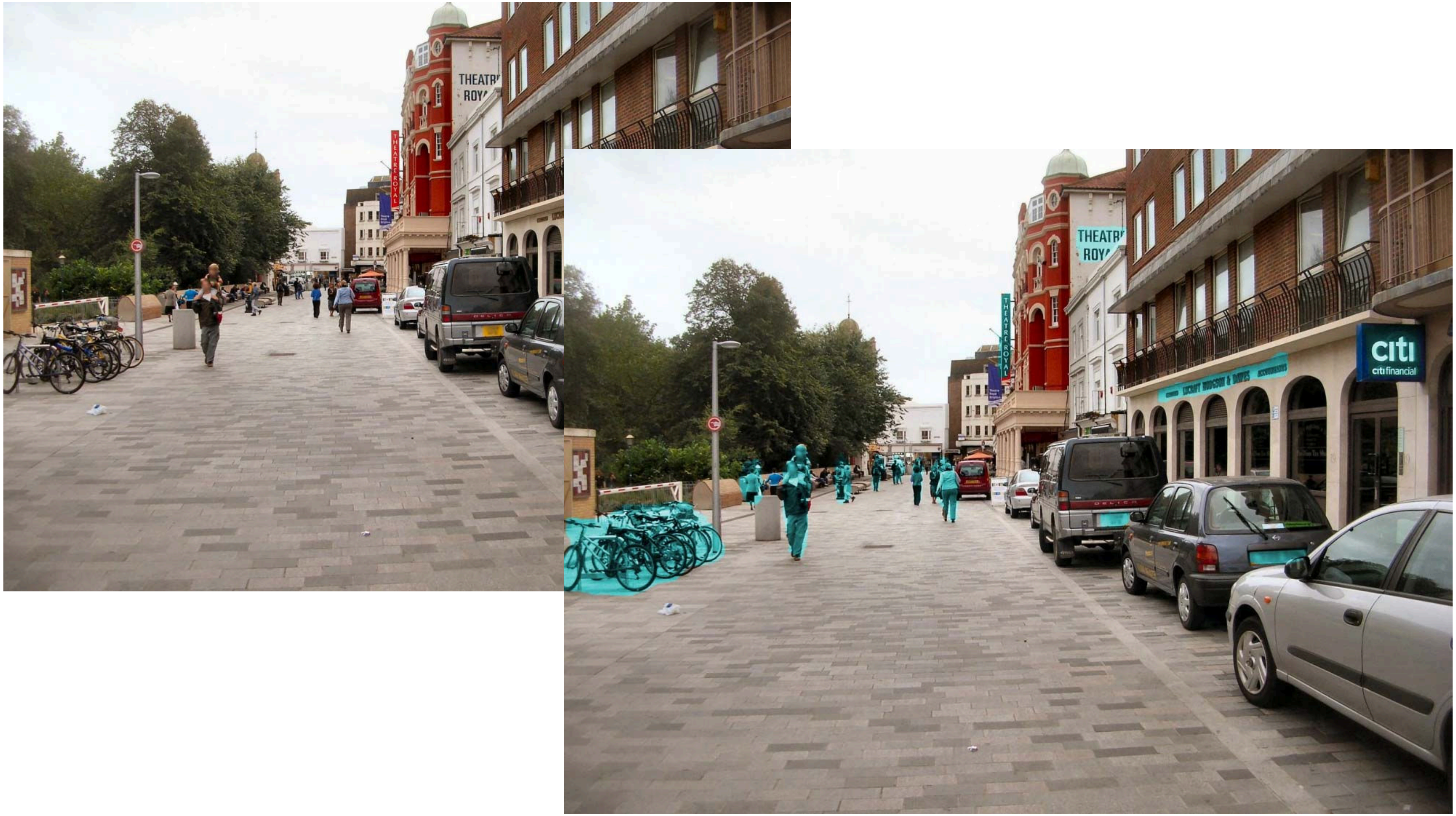
Ethical Issues

INDECT approach to ethical issues

The key objective of INDECT research project is to contribute, through innovation and technology, to the security of all in the European Union. This will be done by proposing several algorithms for independent analysis of various lawful and publically pre-existing sources of information, which are already available to public protection agencies throughout the Union.

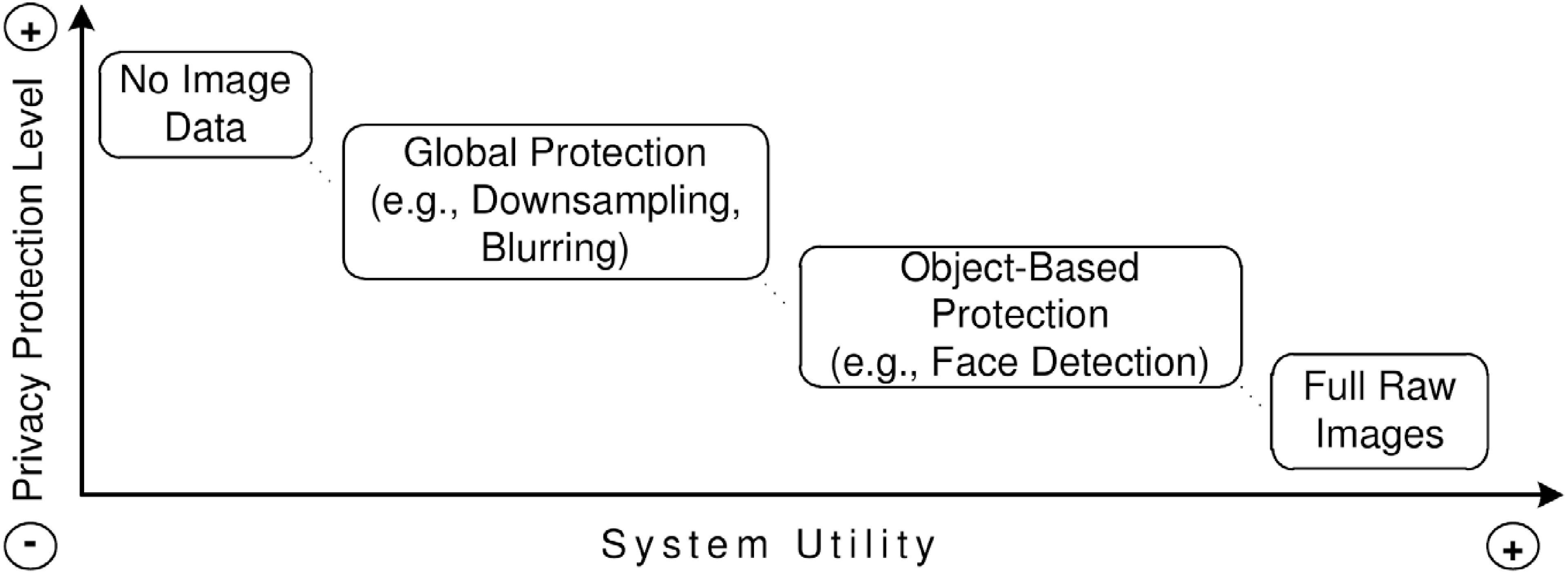
All of the research activities within INDECT project are carried out so as to ensure the

Primary vs. Secondary Identifiers



Source: Wikipedia

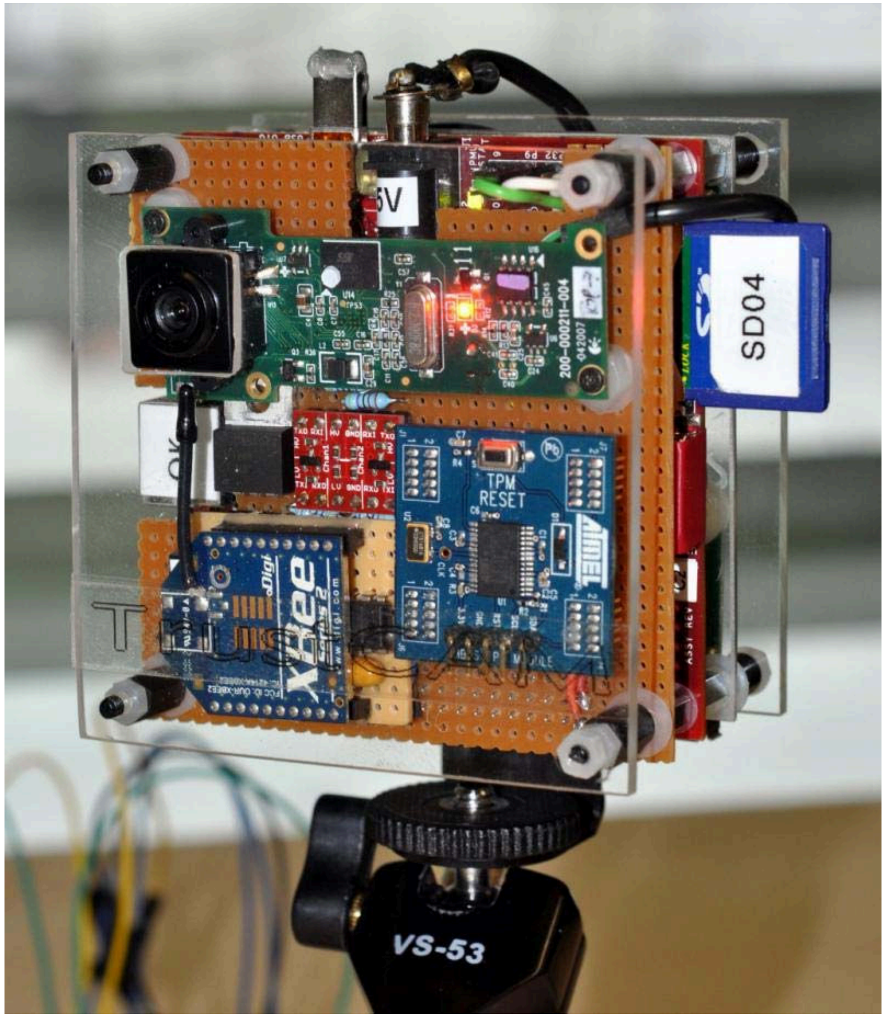
Balancing Privacy and Utility


+
Privacy Protection Level
No Image Data
Global Protection (e.g., Downsampling, Blurring)
Object-Based Protection (e.g., Face Detection)
Full Raw Images
-
System Utility
+

Case Studies

A trustworthy Camera

- OMAP 3530 CPU (ARM+DSP)
- Hardware security solution
- Linux OS + custom middleware
- Trusted boot, continuous system monitoring, secure video streaming, …

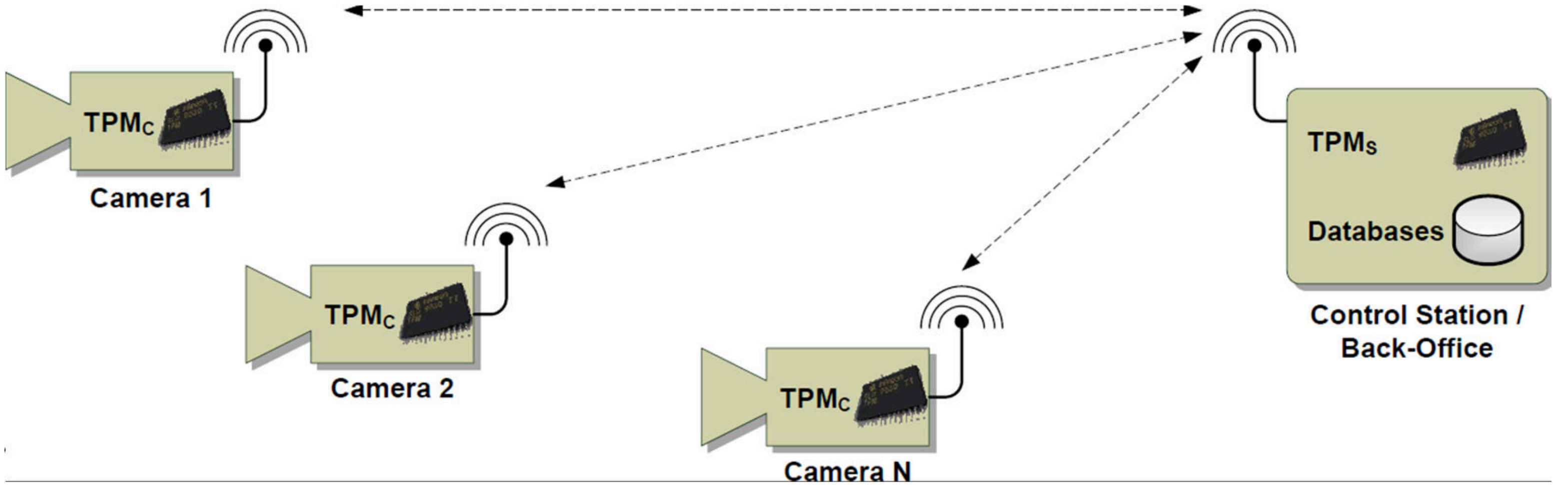


TrustCAM Prototype

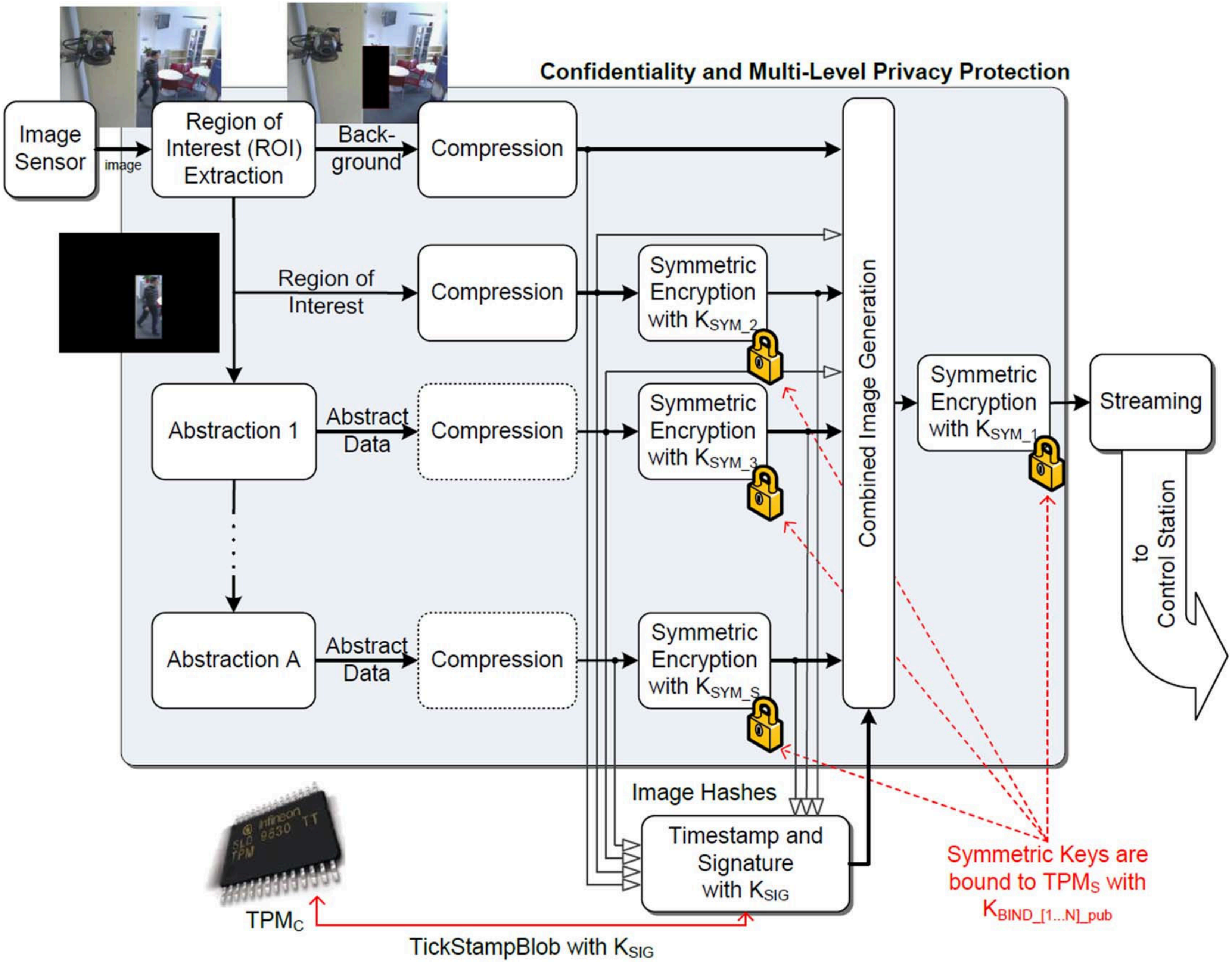
T. Winkler and B. Rinner, "Securing Embedded Smart Cameras with Trusted Computing," EURASIP J. Wirel. Commun. Netw., vol. 2011, p. 20, 2011

TrustCAM Security Features

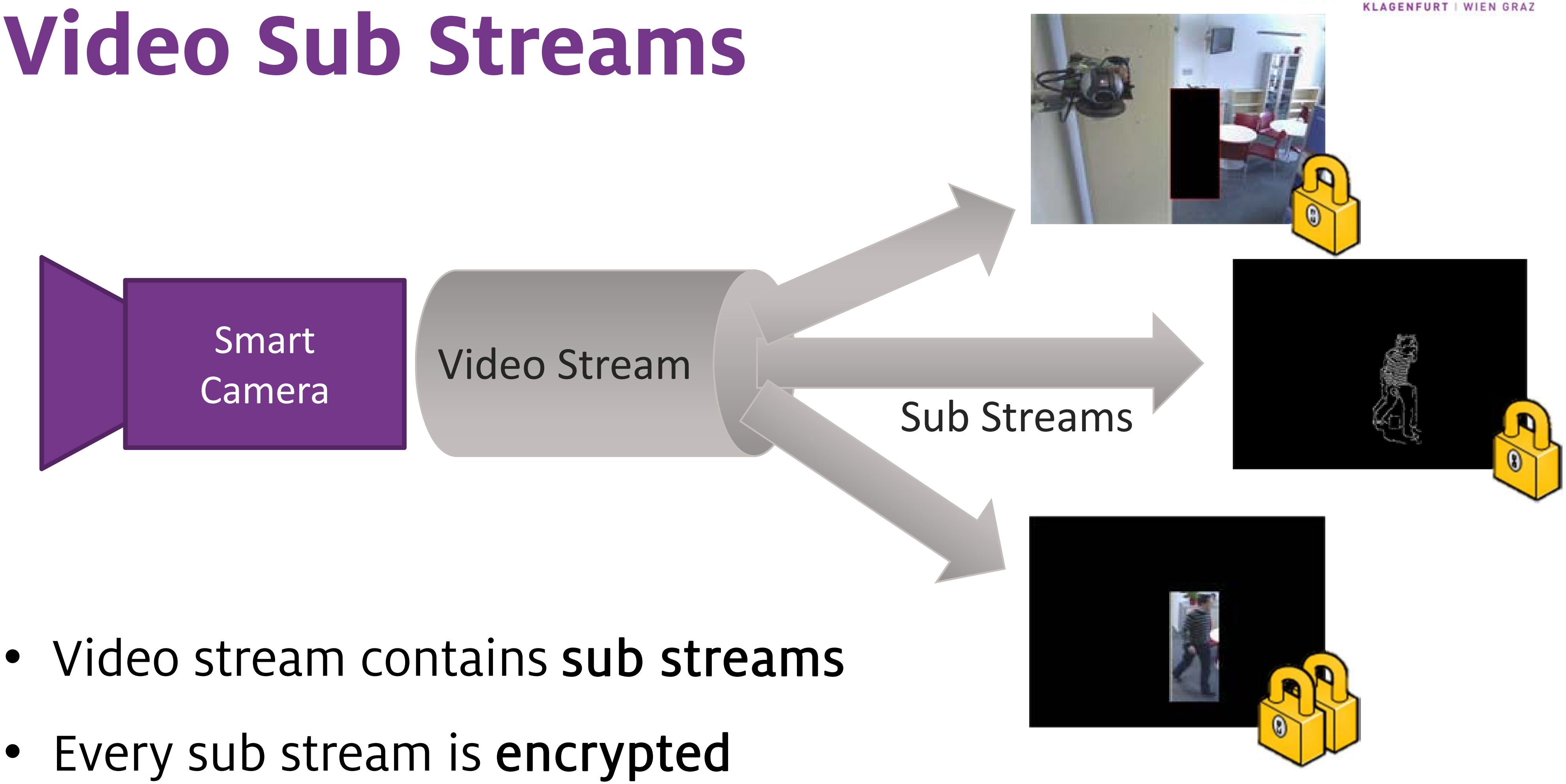
- **Trusted boot**: software stack is “measured” and reported
- **Integrity and authenticity** guarantees using non-migratable, **TPM-protected RSA keys**
- **Freshness/timestamping** for outgoing images via TPM-protected **tick (counter) sessions**
- **Encryption** of outgoing data (confidentiality + privacy)



Processing Flow of Streaming App


Confidentiality and Multi-Level Privacy Protection
Image Sensor
image
Region of Interest (ROI) Extraction
Back-ground
Compression
Region of Interest
Compression
Symmetric Encryption with K_{SYM_2}
Abstraction 1
Abstract Data
Compression
Symmetric Encryption with K_{SYM_3}
Abstraction A
Abstract Data
Compression
Symmetric Encryption with K_{SYM_S}
Combined Image Generation
Symmetric Encryption with K_{SYM_1}
Streaming
to Control Station
Image Hashes
Timestamp and Signature with K_{SIG}
TPM_C
TickStampBlob with K_{SIG}
Symmetric Keys are bound to TPM_S with $K_{BIND\_[1...N]\_pub}$

Video Sub Streams



Smart Camera

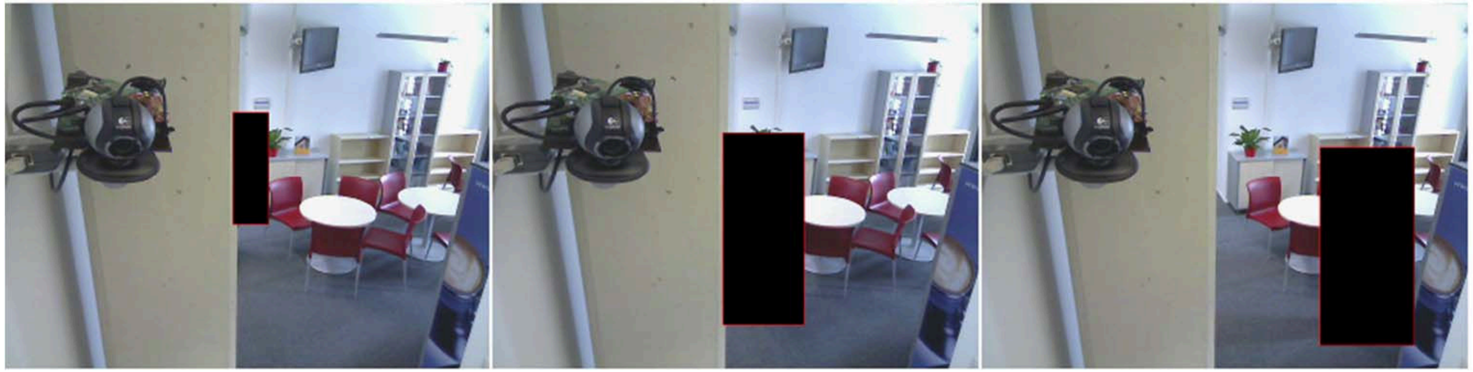
Video Stream

Sub Streams

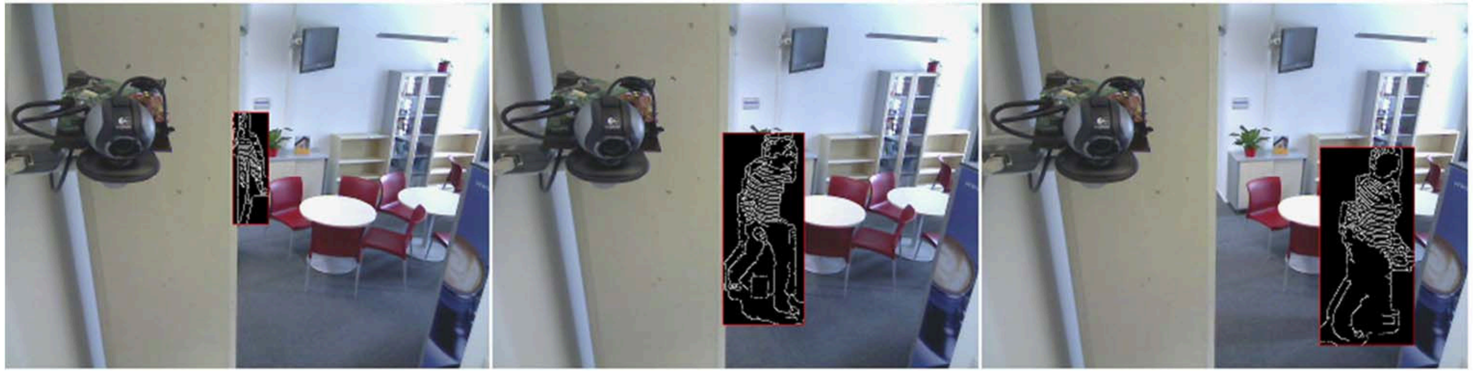
- Video stream contains **sub streams**
- Every sub stream is **encrypted**
  - **Hardware-bound** cryptographic keys
- Recovery of identities only via **four eyes principle**

Multi-Level Privacy Protection

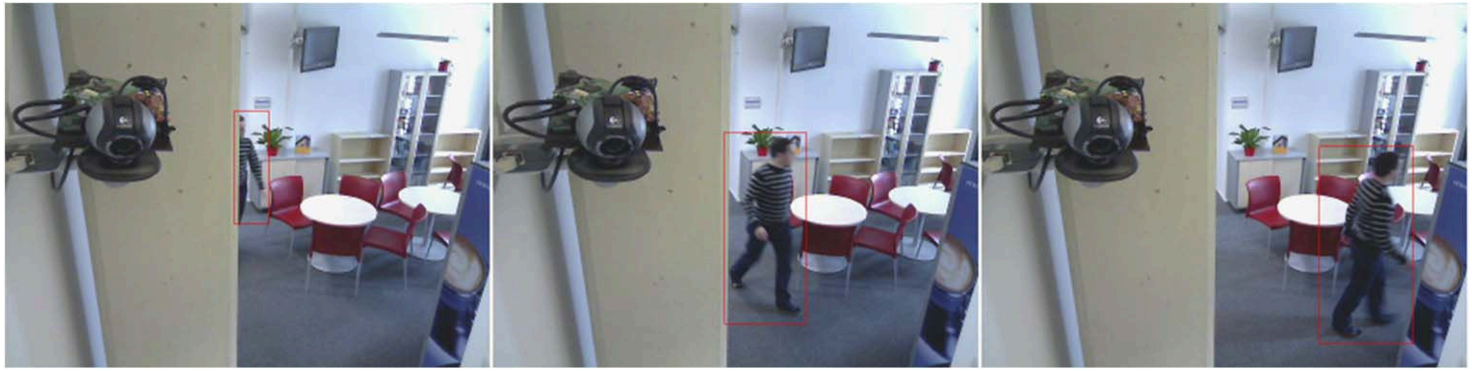
Level 0
no access to
motion regions



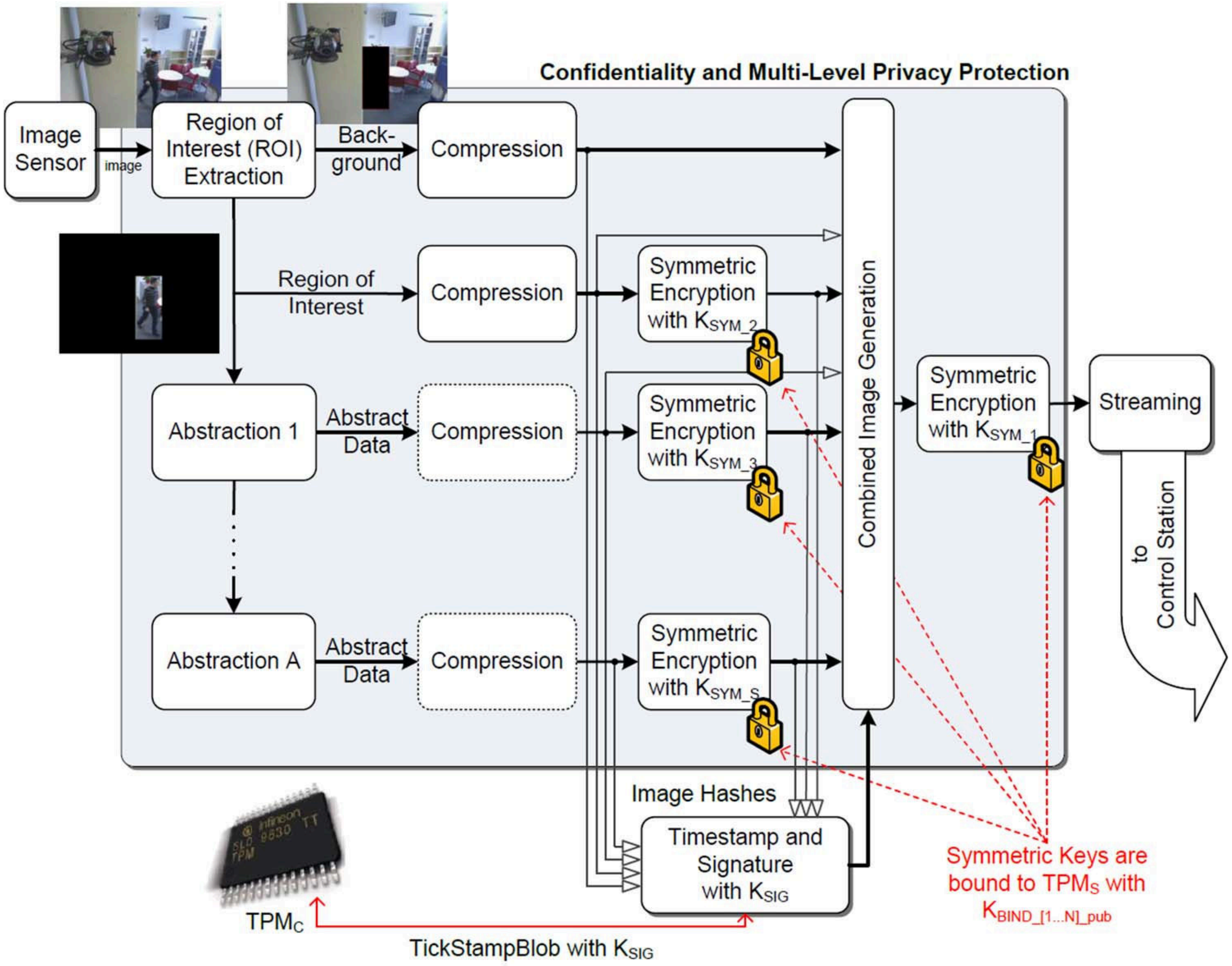
Level 1
access to
abstracted
motion regions



Level 2
full access to
motion regions



TrustCAM – Lessons Learned



Confidentiality and Multi-Level Privacy Protection
Image Sensor
image
Region of Interest (ROI) Extraction
Back-ground
Compression
Region of Interest
Compression
Symmetric Encryption with K_SYM_2
Abstraction 1
Abstract Data
Compression
Symmetric Encryption with K_SYM_3
Abstraction A
Abstract Data
Compression
Symmetric Encryption with K_SYM_S
Combined Image Generation
Symmetric Encryption with K_SYM_1
Streaming
to Control Station
Image Hashes
Timestamp and Signature with K_SIG
TPM_C
TickStampBlob with K_SIG
Symmetric Keys are bound to TPMs with K_BIND_[1...N]_pub

- Lack of separation
- Developer responsibility
- Implicitly trusted components

TrustEYE - Secure sensing

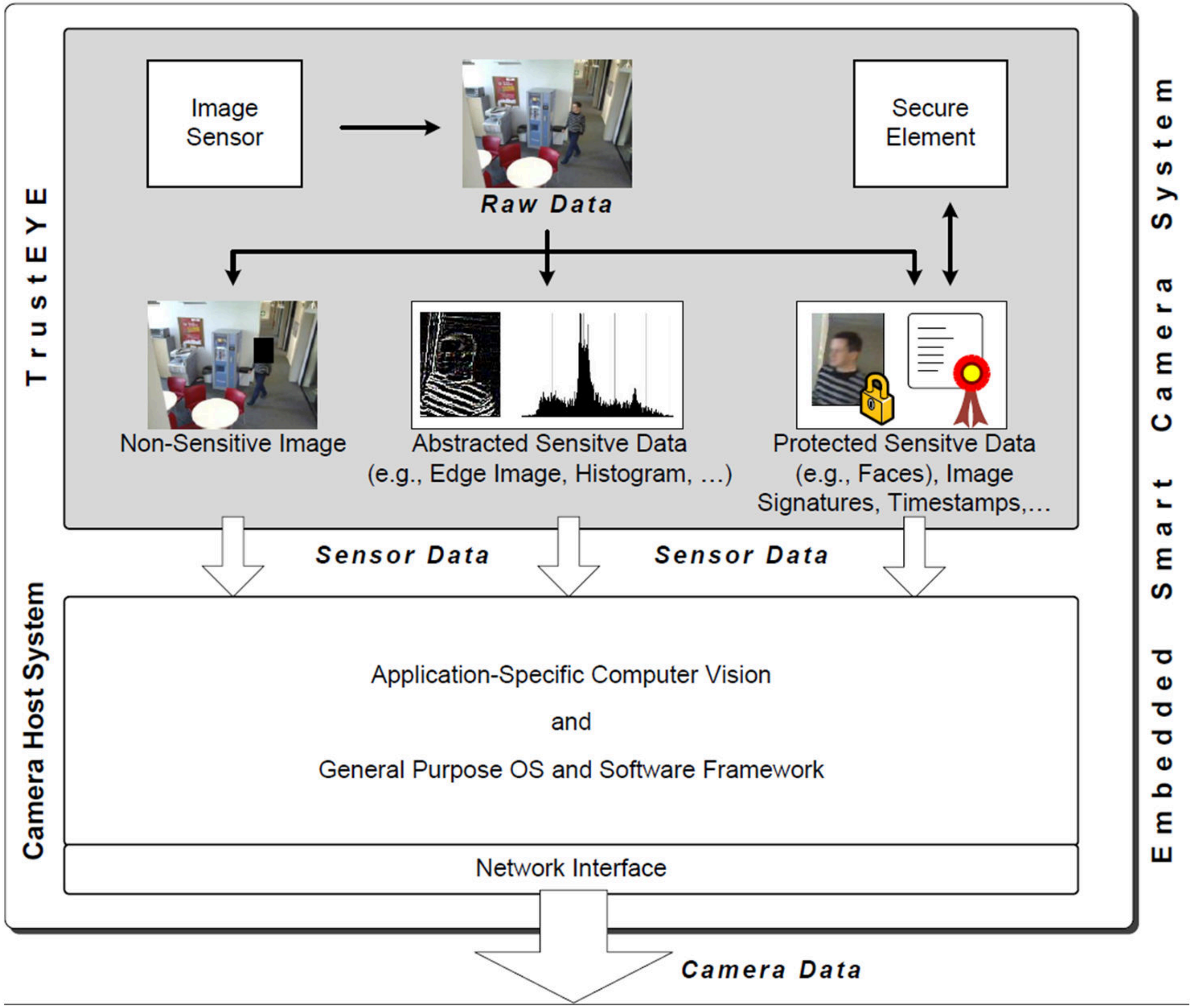
Vision: **Trustworthy Sensing** - security and privacy protection as a **feature of the image sensor** instead of the camera

TrustEYE website: http://trusteye.aau.at

TrustEYE Approach & Benefits

- **Strong separation** btw. trusted and untrusted domains
- **Secure sensing unit**: delivers protected and pre-filtered data
- **Camera host system**: “User applications”, networking, …
  - Access only to pre-processed and filtered data
  - Camera software does no longer have to be trustworthy
  - Protection no longer in the sole hands of app developers
- Security **can not be bypassed** by application developers
- TrustEYE as **anchor for secure inter-camera collaboration**

TrustEYE Overview



Challenges

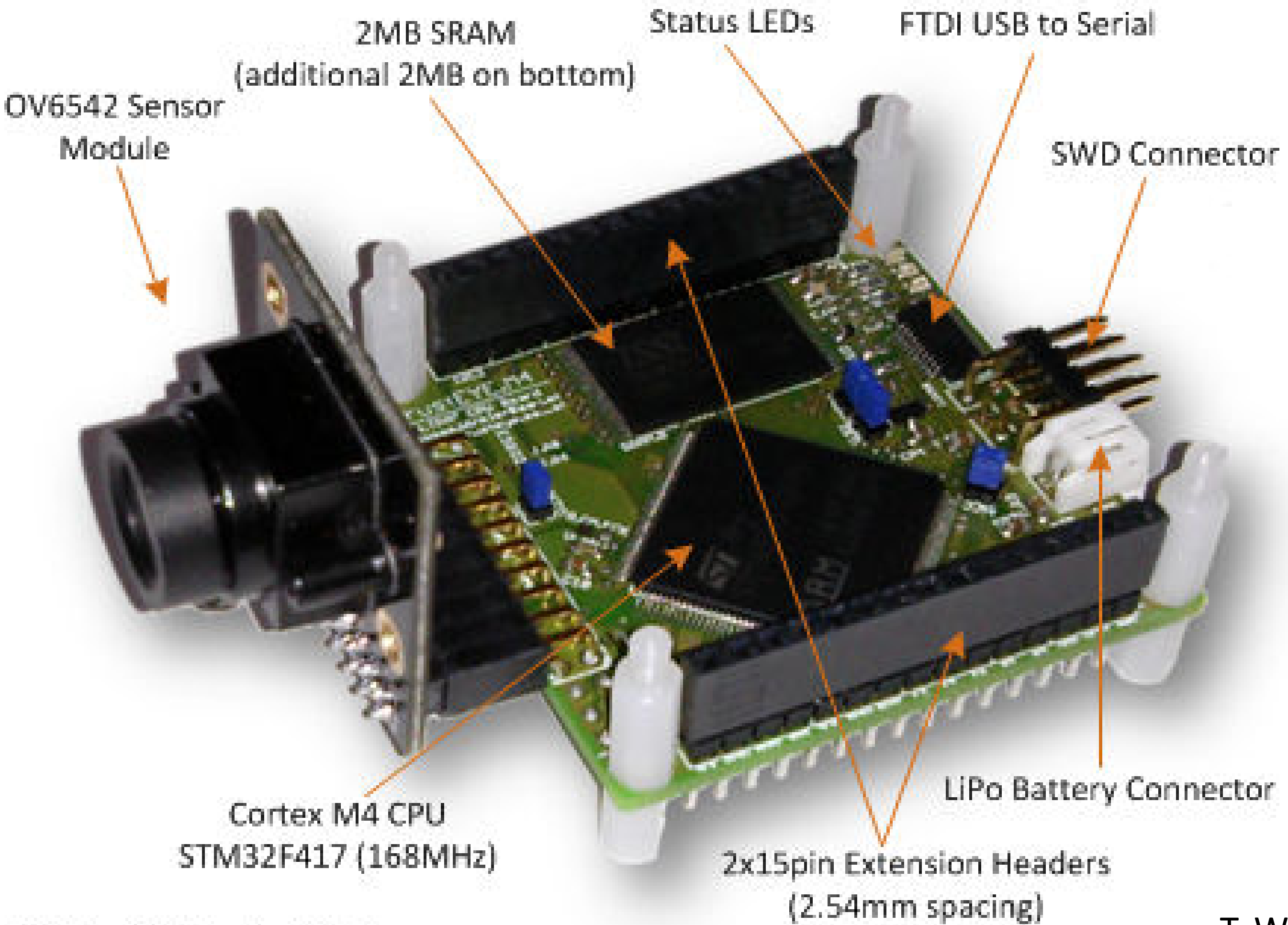
- Security and privacy protection at the **sensor level**
  => techniques for **resource-limited** environments
- Strong **boundary protection**
- **Privacy** vs. **Utility** tradeoff & design space exploration
- **Controlled flexibility**
- **Secure cooperation** in multi-camera scenarios

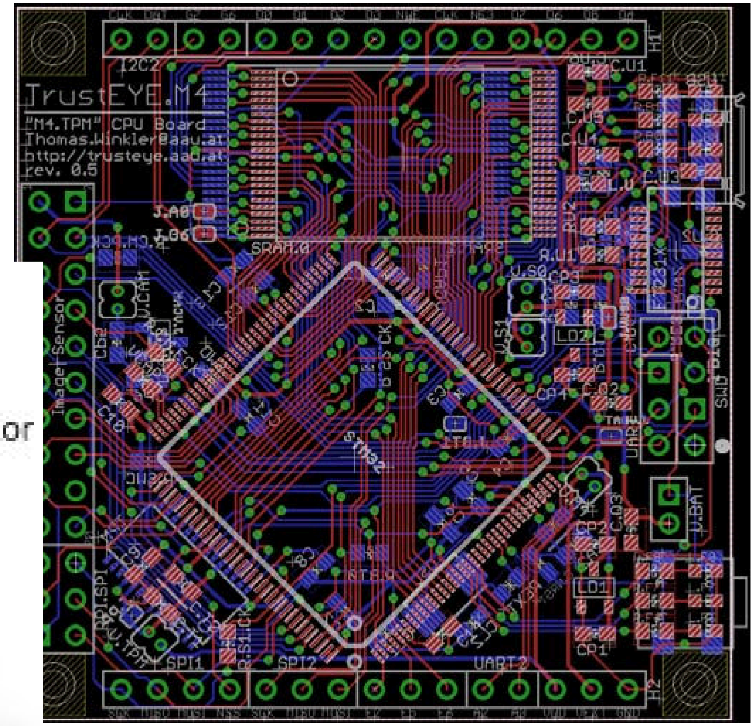
TrustEYE Architecture Variants

- **ASIC**: Sensor + dedicated logic on a chip
- **SoC**: Sensor, dedicated logic + programmable component (microcontroller and/or FPGA fabric) on a chip
- **Virtualization**: Hardware assisted, software-base separation

	ASIC	SoC	Virtualization
Performance	+	~ / +	+
Separation	+	+	~
Flexibility	-	~ / +	+
Sensor Replacement	+	+	-
Developer Involvement	+	+	~ / +

TrustEYE.M4 Platform



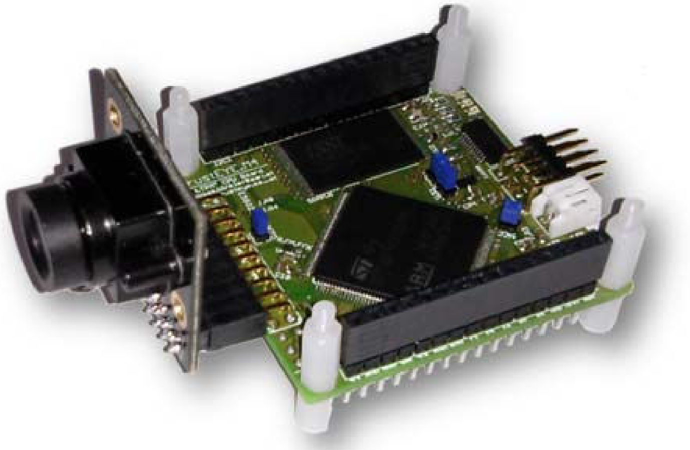


Bottom Side (not visible):
2MB SRAM, TPM Security IC, Power Management IC (LiPo Charger), Micro USB Connector, Reset Button

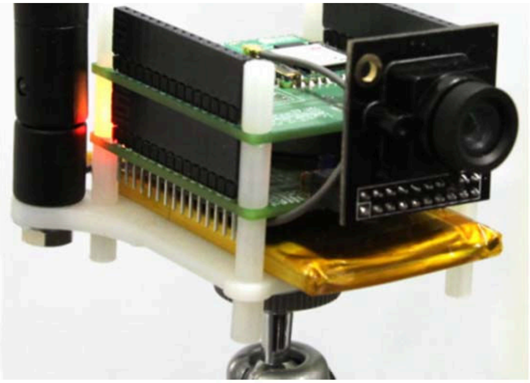
T. Winkler, Á. Erdélyi, and B. Rinner,
"TrustEYE.M4: Protecting the Sensor - not the Camera,"
in Proceedings of the AVSS, 2014,

TrustEYE.M4 Variants

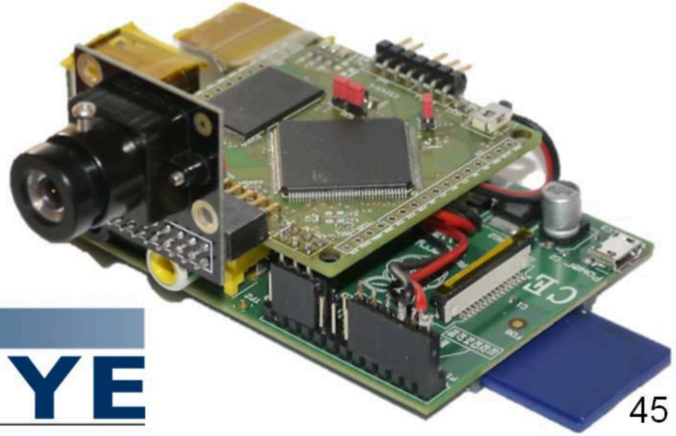
- Processing board (50x50 mm)
  - ARM Cortex M4 @ 168MHz, 4MB SRAM
  - TPM IC: ST33TPM12SPI via SPI
  - FreeRTOS; GCC-ARM toolchain



- 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

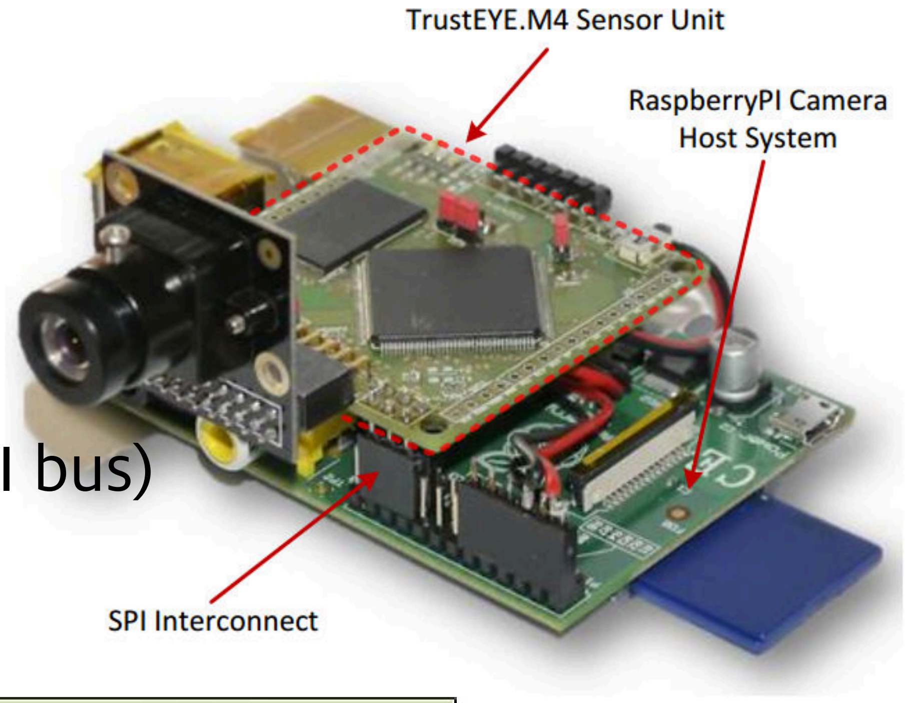


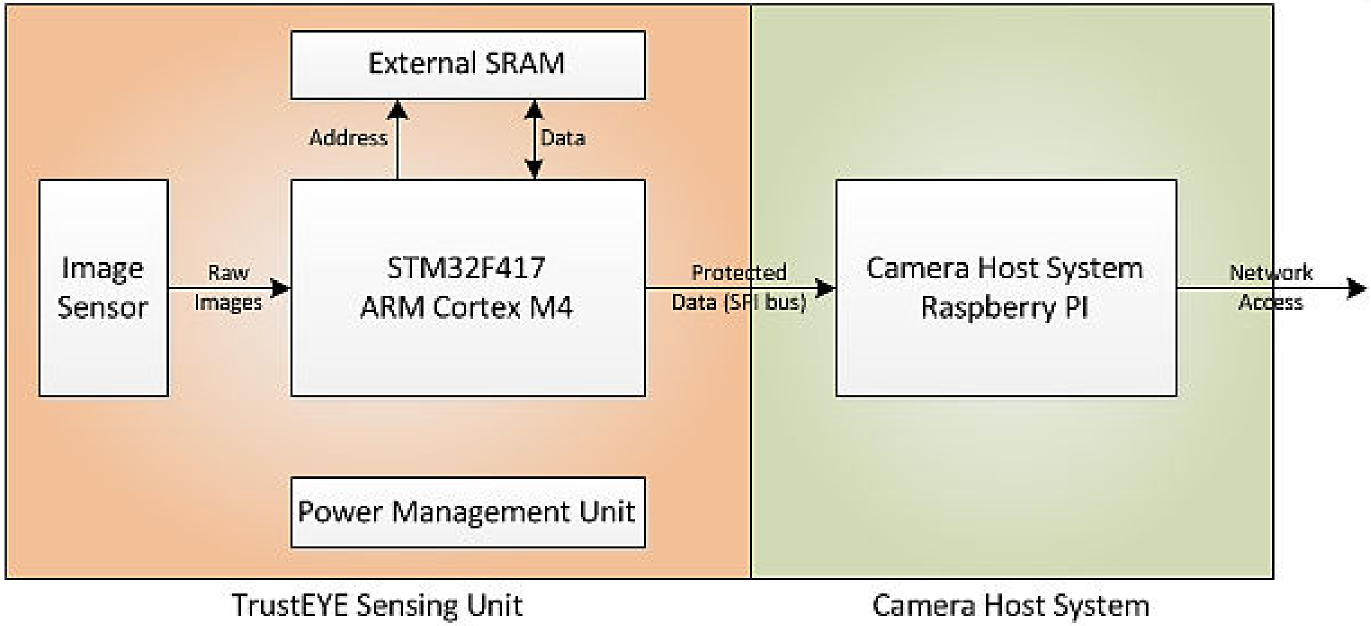
- RaspberryPI mounting option
  - Interconnect: SPI bus via dedicated RPI
  - Daterate: 32 Mbit/s



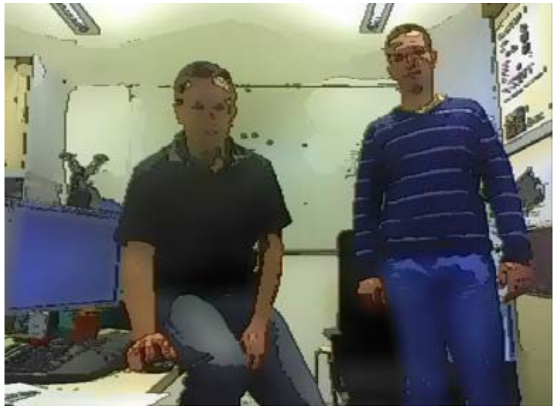
Secure Sensing Unit

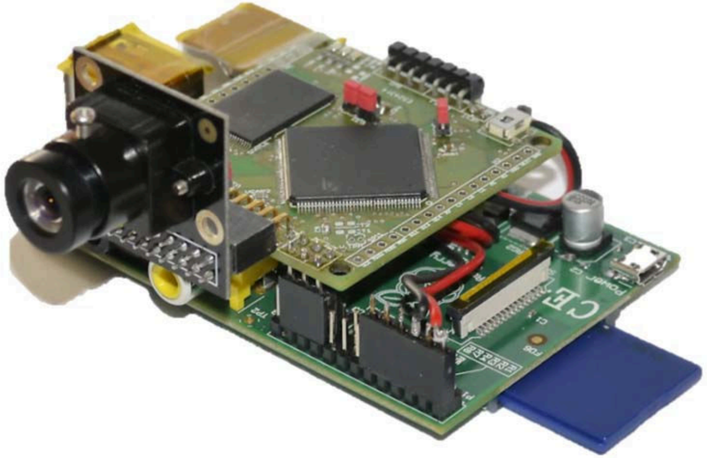
- TrustEYE secure sensing unit
- RaspberryPI as **camera host system**
- Dedicated RPI mating connector (SPI bus)
- SPI datarate: 32Mbit/s

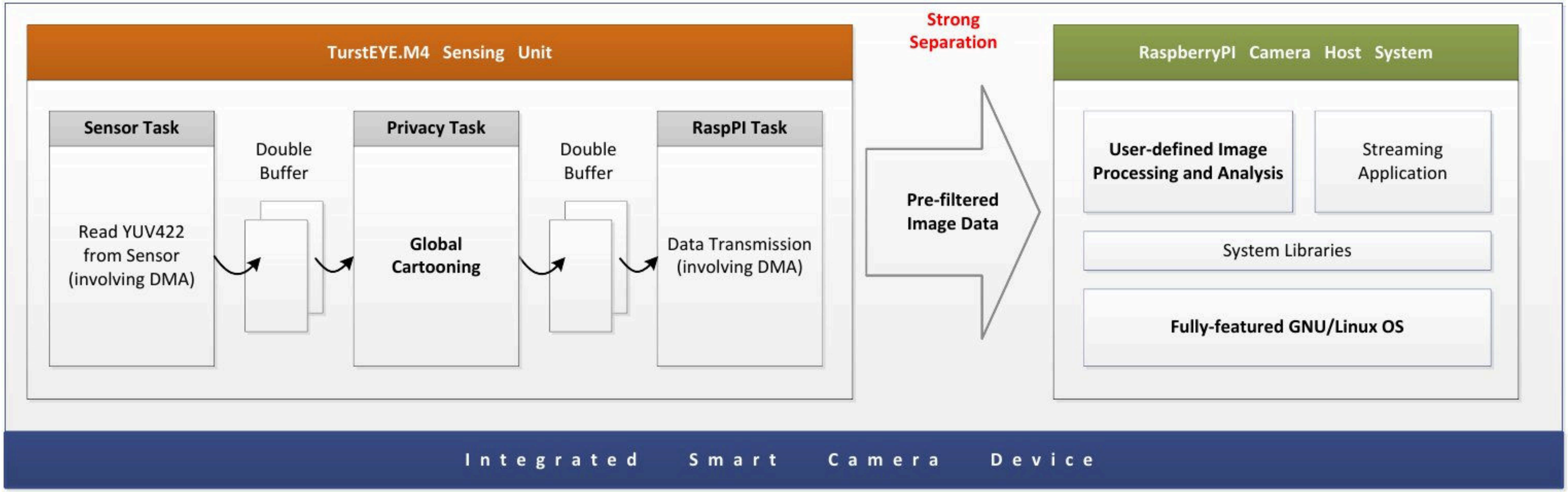




Privacy Protection by Sensor-Level Cartooning







TurstEYE.M4 Sensing Unit

Sensor Task

Read YUV422 from Sensor (involving DMA)

Double Buffer

Privacy Task

Global Cartooning

Double Buffer

RaspPI Task

Data Transmission (involving DMA)

Strong Separation

Pre-filtered Image Data

RaspberryPI Camera Host System

User-defined Image Processing and Analysis

Streaming Application

System Libraries

Fully-featured GNU/Linux OS

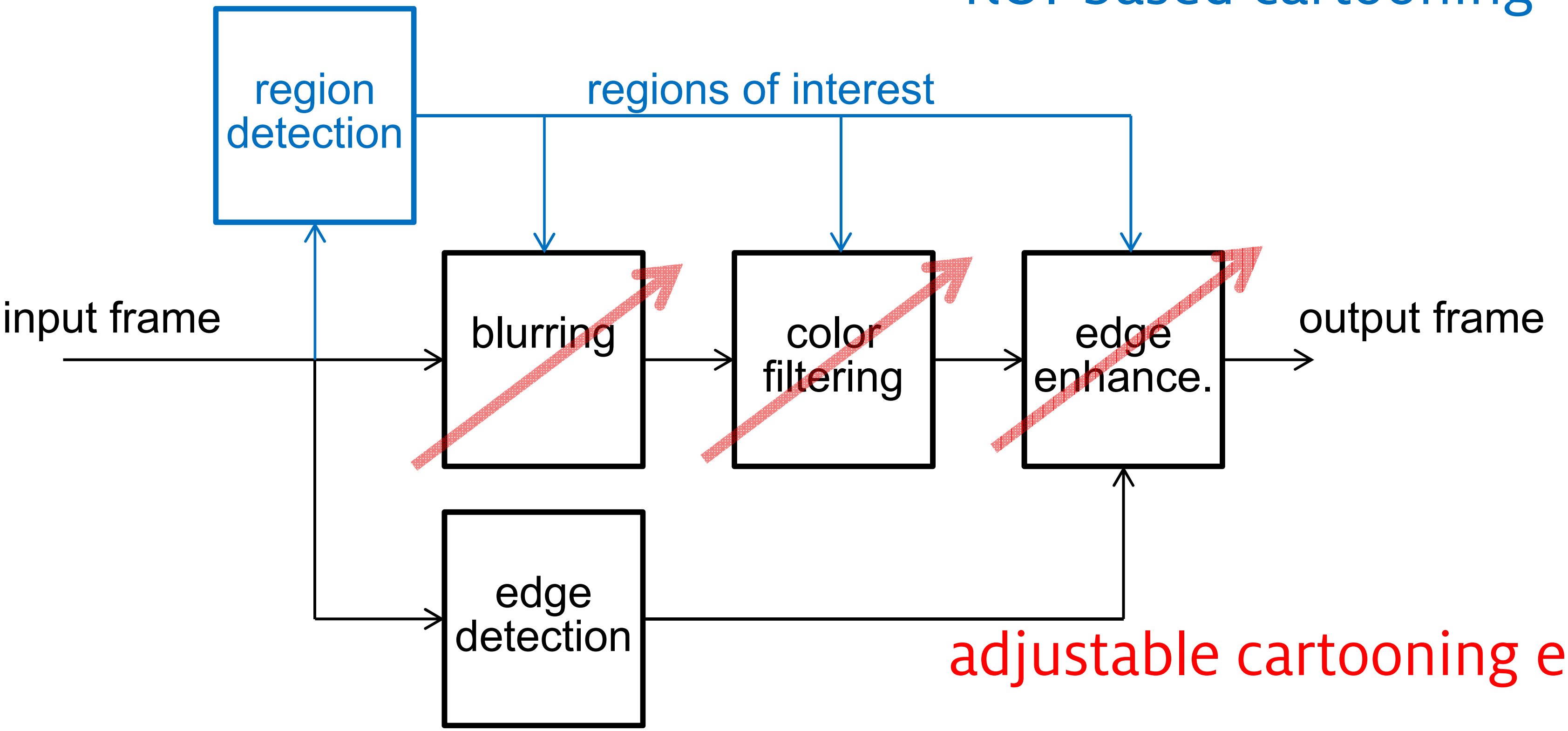
Integrated Smart Camera Device

Cartooning Example

Cartooning Pipeline

- Obfuscate (parts of) image by cartoon effect

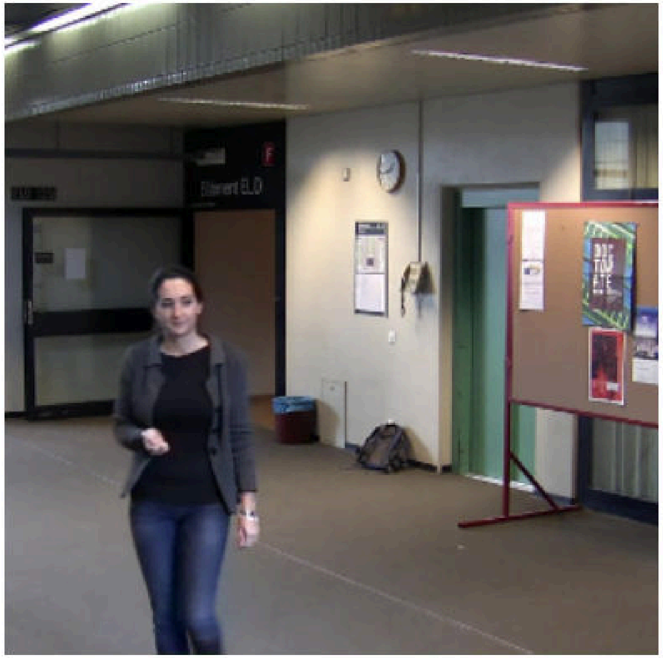
ROI-based cartooning



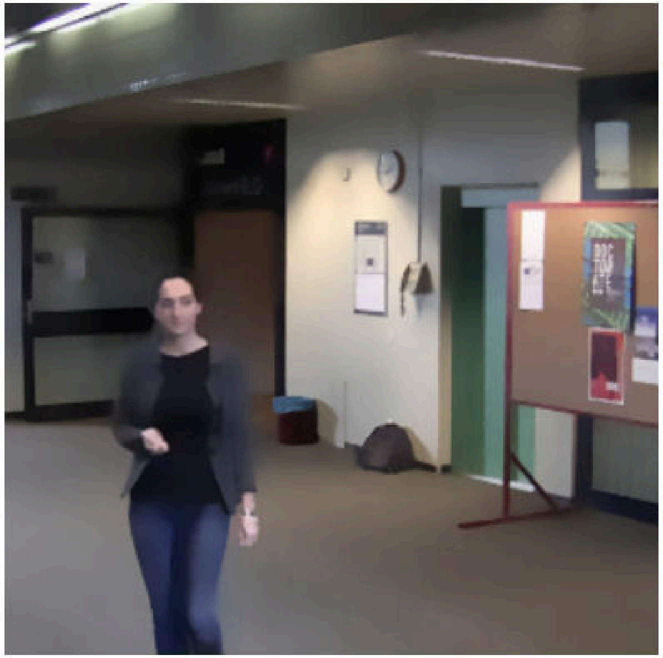
adjustable cartooning effect

Á. Erdélyi, T. Barát, P. Valet, T. Winkler, and B. Rinner, "Adaptive Cartooning for Privacy Protection in Camera Networks," in Proceedings of the AVSS, 2014

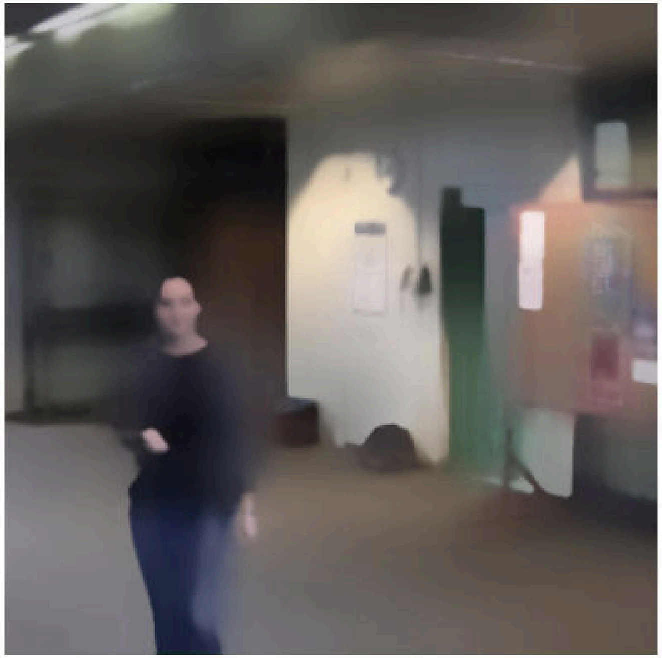
Adjustable Global Cartooning



small



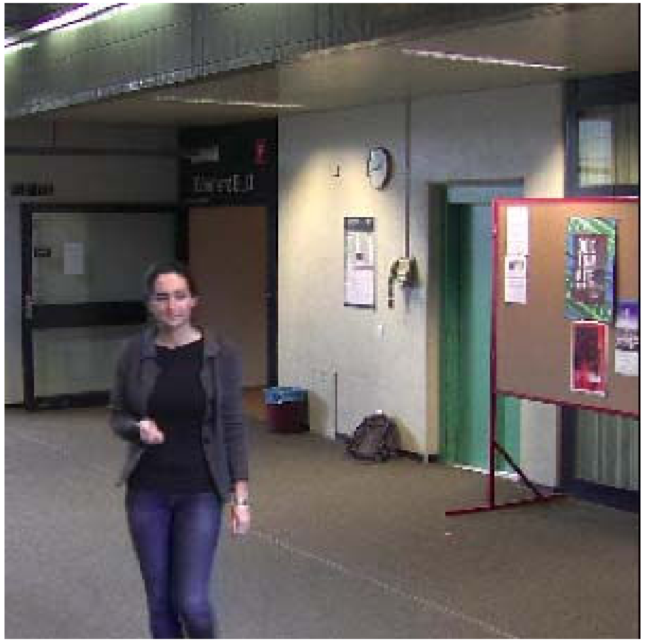
medium

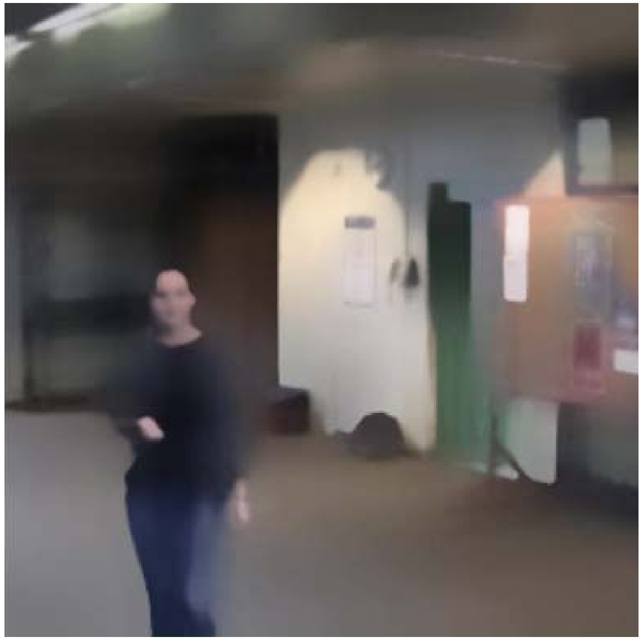


strong

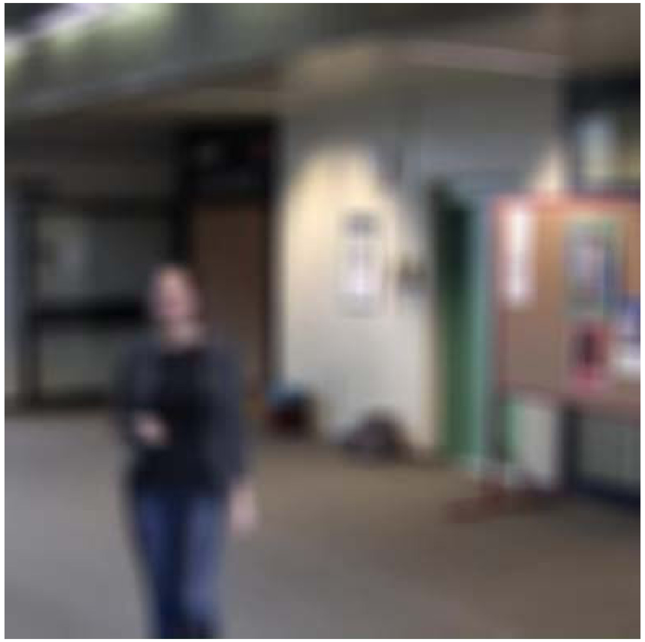
- Cartooning strength is adjustable depending on system requirements; also online

Visual Comparison

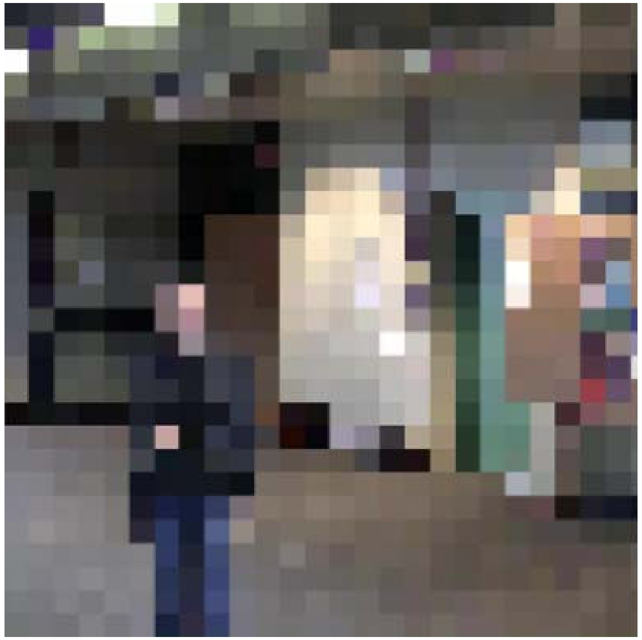




Cartooning



Blurring



Pixelation

Privacy/Utility Tradeoff

- Subjective, user-based evaluation

  P. Korshunov, S. Cai, and T. Ebrahimi, “Crowdsourcing Approach for Evaluation of Privacy Filters in Video Surveillance,” in Proceedings of the International Workshop on Crowdsourcing for Multimedia, 2012, p. 6.

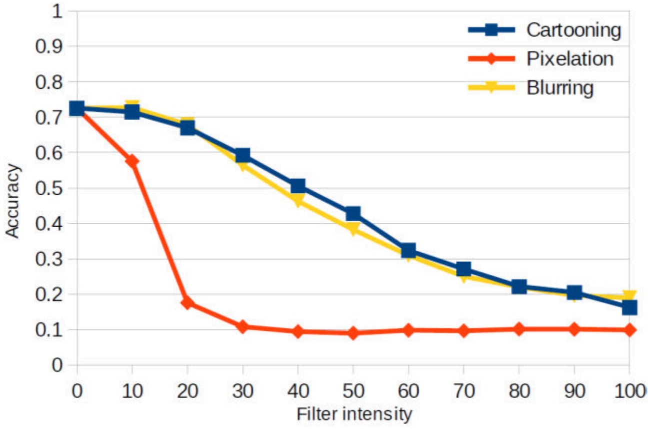
- Development of objective evaluation framework among key dimensions, i.e.,
  - Privacy protection
  - Utility
  - Appearance (pleasantness)
  - Resource consumption

- Measure the performance using standard CV algorithms with protected videos (and use labeled test data as ground truth)
  - Evaluation based on PeVid dataset

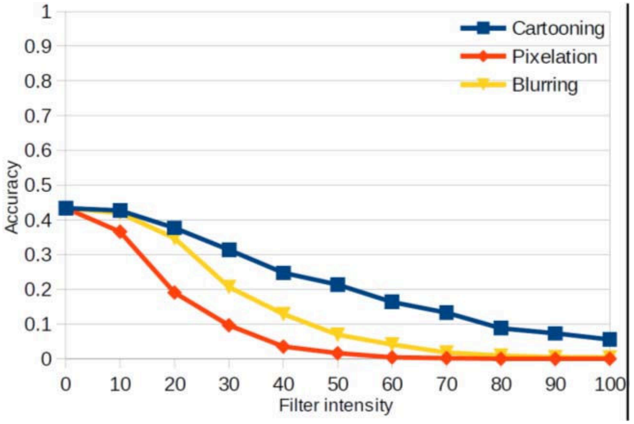
    P. Korshunov and T. Ebrahimi. PEViD: Privacy Evaluation Video Dataset at Applications of Digital Image Processing XXXVI. In Proceedings of SPIE, 2013.

Comparison of Global Filter Approaches

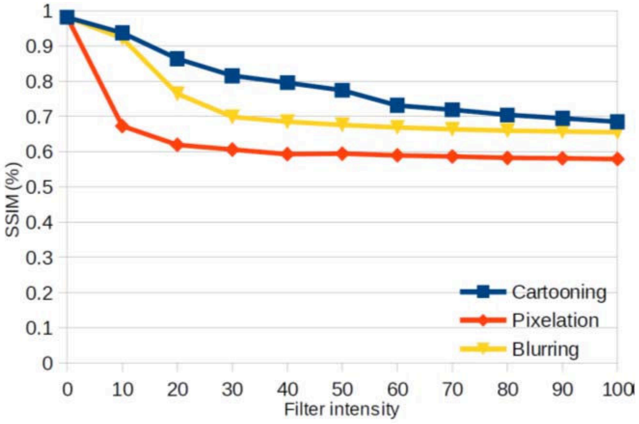
- Performance of standard CV algorithms compared to unprotected video or other protection filters



Protection: object re-identification performance



Utility: object detection performance



Appearance: structural similarity index

Cartooning Demo

- Embedded implementation on TrustEYE.M4
- Frame rate: 12fps
- Power consumption: ~440mA

Summary and Discussion

Summary (cont.)

- Security and privacy should be **up-front design considerations**
- A **holistic concept** is needed that takes into account also **non-technical dimensions**
- Key goals are typically **confidentiality** / privacy and **non-repudiation**
- Security aspects can be broken down into **node-, data-, network- and user-centric security**
- Within this scheme **privacy** is a **sub-aspect of confidentiality**

Summary (cont.)

- **TrustEYE** - moving security to the **sensor level**
  - Separation of **trusted and untrusted components**
  - Protection **can not be bypassed**
  - Exploring the **privacy vs. utility** tradeoff
  - Exploits **hardware-security** features

- Adjustable (global) **cartooning** as one way to protect privacy
  - Feasible even very close to the sensor
  - Privacy / utility tradeoff still under evaluation

Thank you for your attention!

Questions?