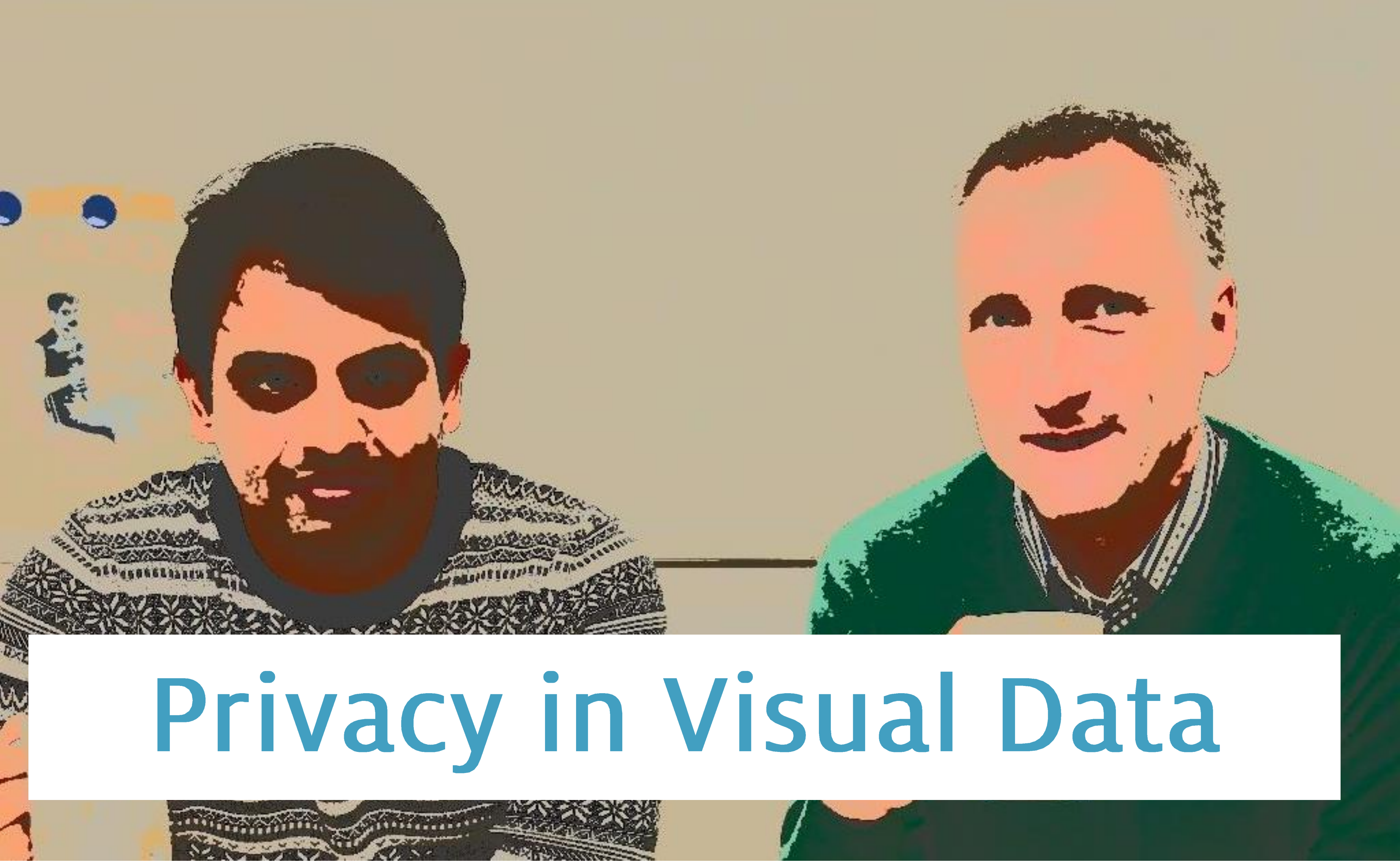


Privacy in Visual Data

Bernhard Rinner

Klagenfurt, August 11, 2017

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Institute of Networked and Embedded Systems

The Challenge of Privacy and its Protection

- Privacy is highly subjective and difficult to define
  - Related to “the ability of an individual or group to seclude themselves, or information about themselves”
- Privacy has a significant impact on society and is addressed in numerous fields
  - Warren, Brandeis. „The Right to Privacy.“ 1890.
  - „EU General Data Protection Regulation“. effective in 2018
- Privacy is increasingly at risk
  - Technological progress, change in politics, limited awareness

Privacy in Data(bases)

- Draw conclusions for the entire population (or parts of) but avoid linkage of sensitive information to individuals

Name	SSN	Age	ZIP	Sex	Disease
[redacted]		[30,39]	9***	female	Flu
[redacted]		[40,49]	9***	male	Cancer
[redacted]		[30,39]	9***	female	Flu
[redacted]		[40,49]	9***	male	Flu
…	…	…		…	…

Explicit identifier — Quasi identifier — Sensitive information

- Anonymization as key protection method
- Modify quasi identifier to achieve k anonymity

Privacy in Visual Data

Who is there?

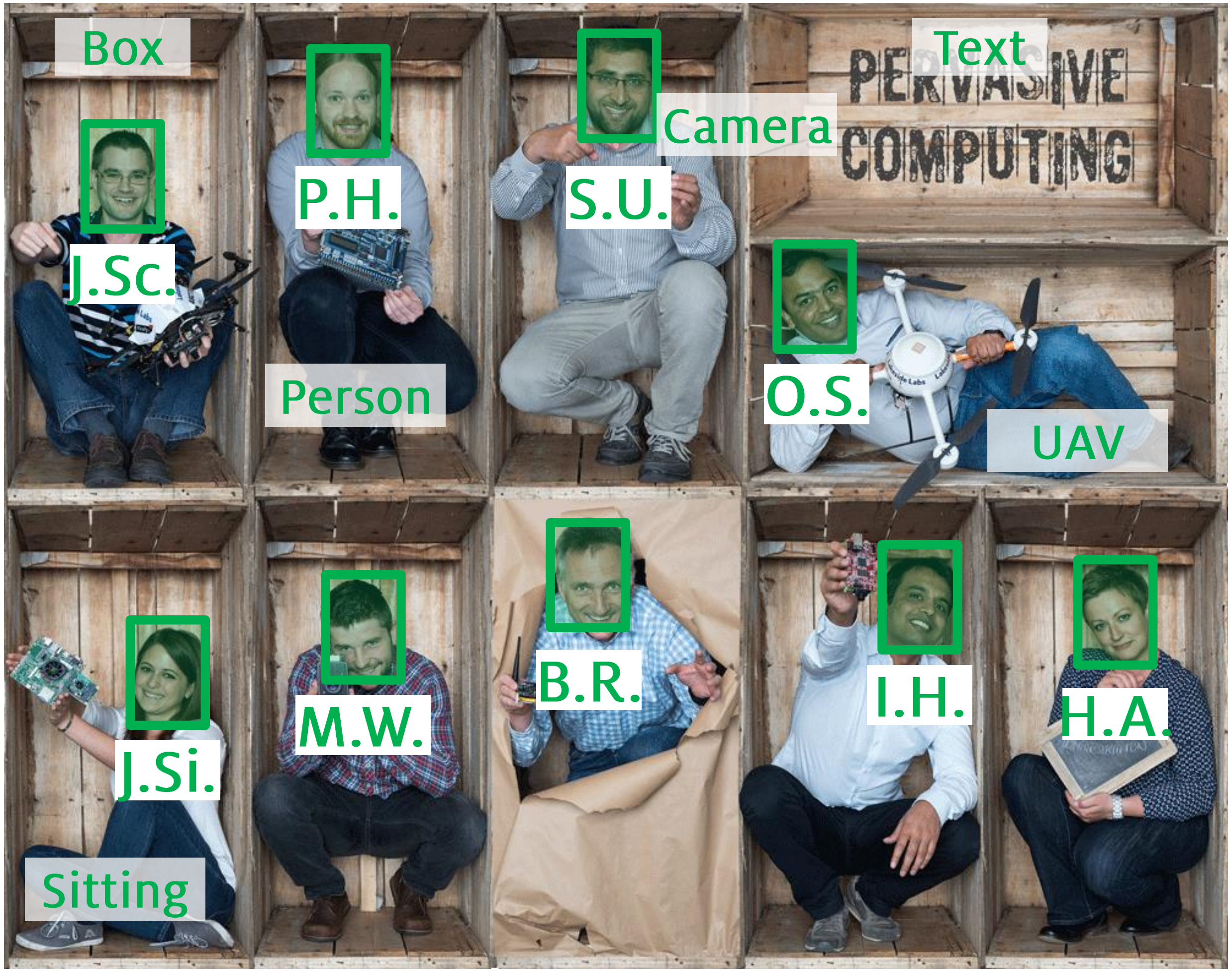
- (Quasi-)Identifiers
- Body or face regions

What is shown?

- Sensitive information
- presence,
  „show an object“
  „captured in a box“

How to avoid linkage of sensitive information to individuals?

Privacy Threats: Algorithms



Face Detection

- Where are the faces?

Face Recognition

- What are their IDs?

Scene Analysis

- What is shown?

Protection approach: make recognition/identification difficult

Privacy Threats: Meta-Data

EXIF Data (selected)
- Authors
- Photographers
- Date
- Image dimensions
- Camera model
- Serial number
- Focal length
- GPS position
- ....

Derived meta-data
- „Person“
- „Camera“
- „UAV“
- „Pervasive Computing“
- „Sitting“

Tipp: Query for derived meta-data

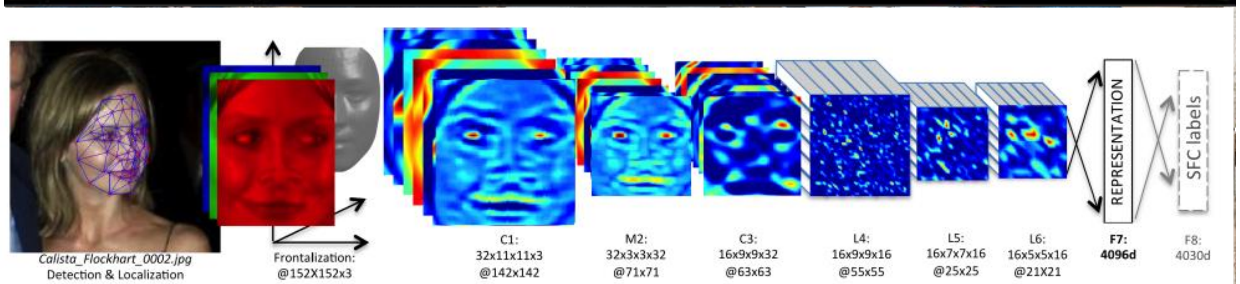
Encoded in image
- Image descriptors
- Automatically inserted by many cameras

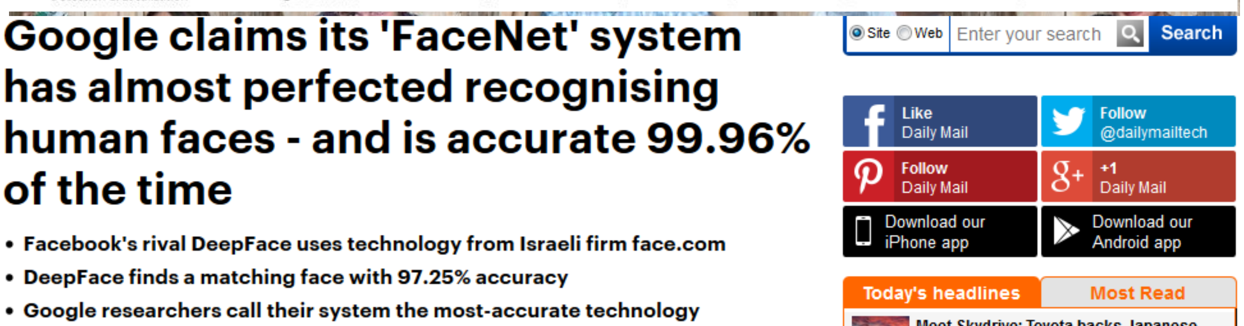
Derived from image
- Scene analysis

Linked w/ other data
- Social media
- Retrieval (search)

Protection approach: avoid storage and linkage of meta-data

Privacy Threats: Big Data





Google claims its 'FaceNet' system has almost perfected recognising human faces - and is accurate 99.96% of the time

- Facebook's rival DeepFace uses technology from Israeli firm face.com
- DeepFace finds a matching face with 97.25% accuracy
- Google researchers call their system the most-accurate technology

Data Collection

- Cloud computing, IoT

© UMass, LWF

Machine Learning

- Boost by deep learning

© Taigman et al. CVPR14

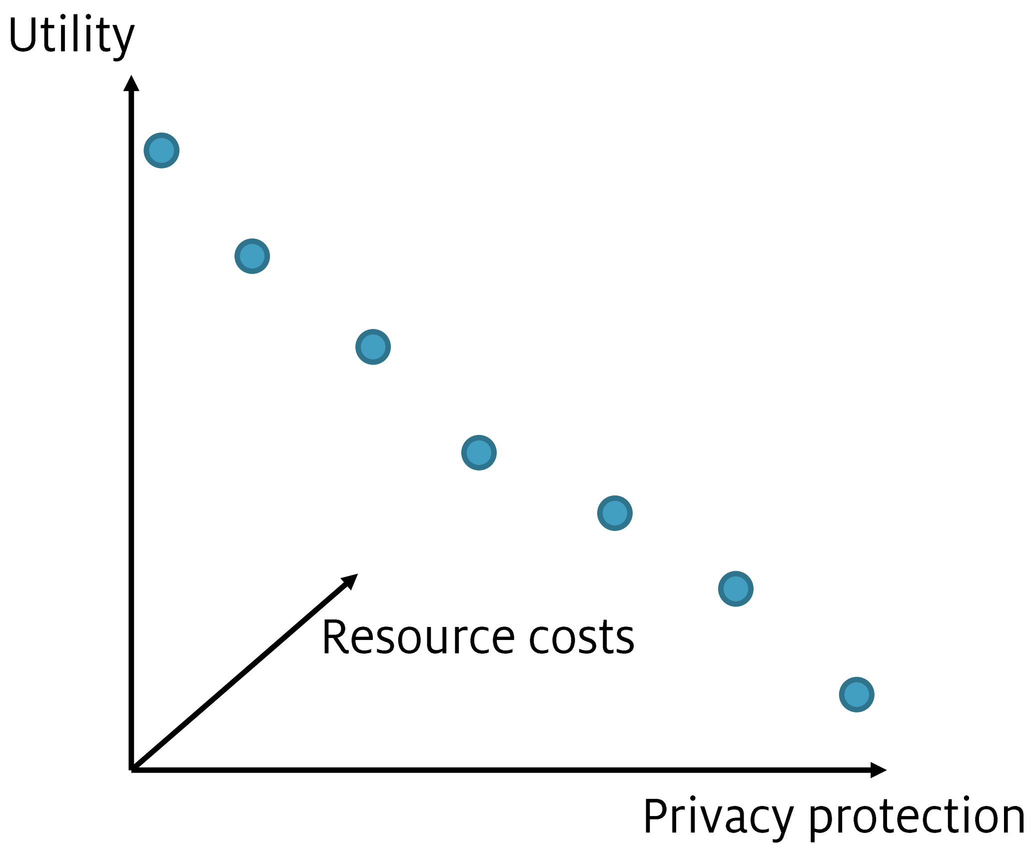
Performance

- Close to humans and steadily improving

© Daily Mail, 2015

Protection method: rely on formal frameworks

Utility and Privacy Tradeoff



Distortion as key protection method

- Blanking
- Pixelation
- Bluring
- Cartooning

Utility dependent on level of distortion

- Similarity
- Appearance
- Detectability

No single best protection method available

Our Research Focus

1. What distortion method to use?
   – Explore utiliy/privacy/cost design space
   – Adapt filter strength for optimizing utility&privacy

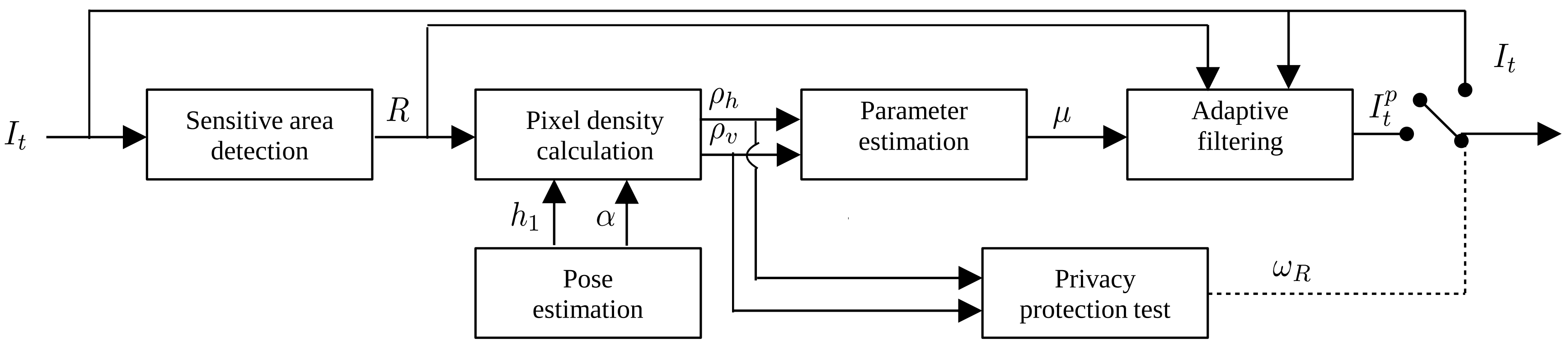
2. How to hinder privacy attacks?
   – Perform protection onboard of cameras
   – Make „reverse engineering“ difficult

3. How to securely implement privacy protection?
   – Apply security methods to maintain integrity and authenticity
   – Rely on hardware-supported protection

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

#1 Adapt Blur to Target Resolution

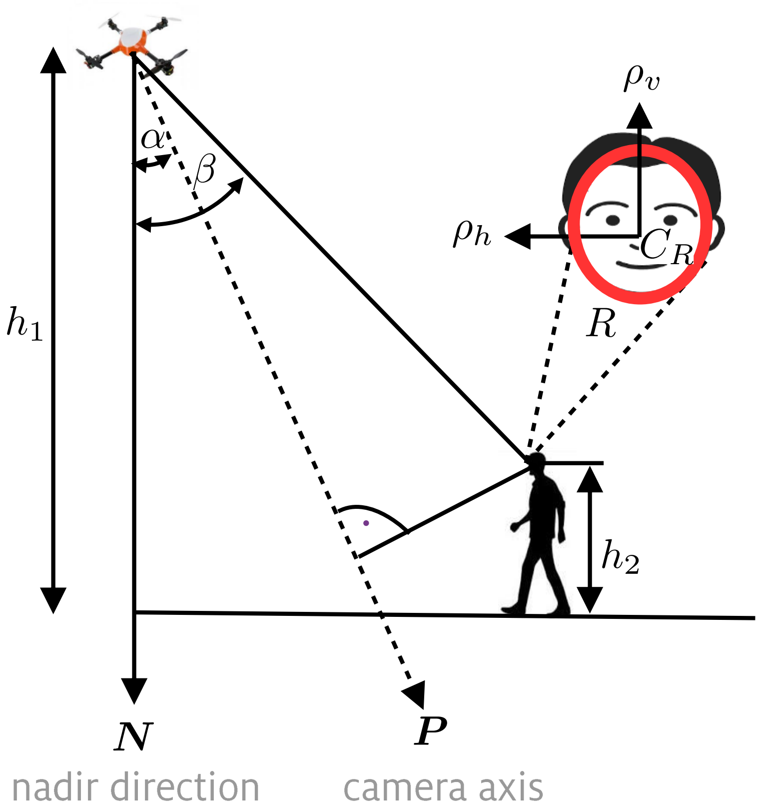
- Privacy design space exploration with adaptive filtering
  - Determine target‘s pixel density based on camera pose
  - Decide whether target is inherently protected
  - Configure privacy protection filter
  - Perform adaptive filtering
- Studied for aerial images



[Sawar, Rinner, Cavallaro. [Design Space Exploration for Adaptive Privacy Protection in Airborne Images](). In Proc. AVSS 2016.]

Pixel Density Estimation

- Horizontal and vertical density at target center



focal length

$$\rho_h = \frac{f\,cos(\beta)}{p_h(h_1 - h_2)}$$

horizontal pixel size

$$\rho_v \approx \frac{f\,cos(\beta)sin(\beta)}{p_v(h_1 - h_2)}$$

vertical pixel size

Adaptive Privacy Filter

- Configure filter G so that privacy protection is increased while fidelity is maintained

$$I_t^p = \mathcal{G}(I_t, R, \mu)$$

filter strength

face region

unprotected frame at time t

filter operator

- Determine filter strength μ such that the pixel resolution in the protected image is just below the threshold

Gaussian Blur as Privacy Filter

- Approximated anisotropic Gaussian kernel

$$g(v,h) = \frac{1}{2\pi\sigma_v\sigma_h} e^{-\left(\frac{v^2}{2\sigma_v^2}+\frac{h^2}{2\sigma_h^2}\right)}$$

with

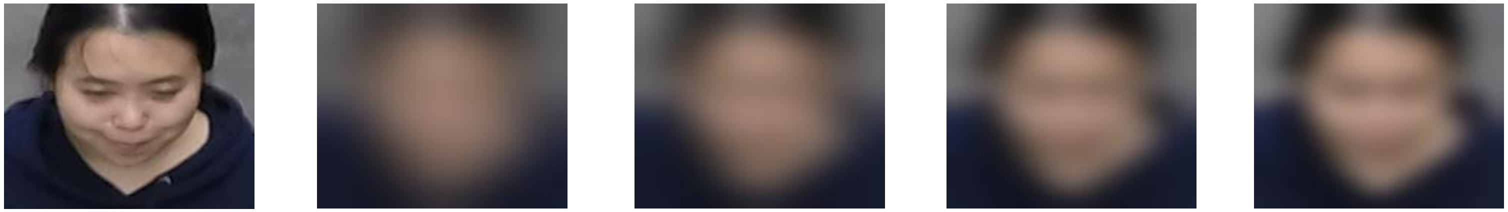
$$\sigma_i = \frac{3\rho_i}{\pi\rho_i^0} \;\; where \;\; i \,\epsilon\, \{v,h\}$$

- Filtering with kernel size

$$\mu_i = 2\lceil 3\sigma_i \rceil + 1$$

useful information in I_t^p is reduced to the threshold ρ_i^o

Adaptive Gaussian Blur Example



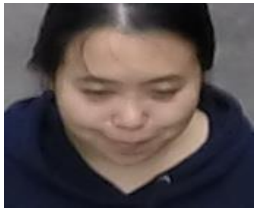
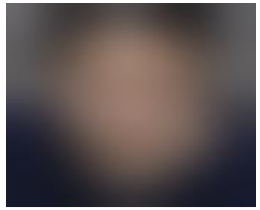
ρ: (5.03, 3.88) | μ: (121, 105) | μ: (99, 77) | μ: (75, 57) | μ: (59, 47)

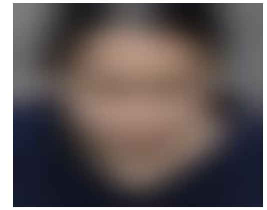
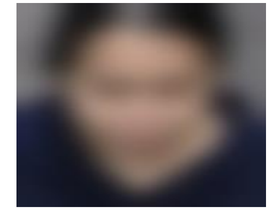
Original | Fixed | Over | Optimal | Under

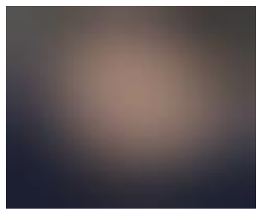
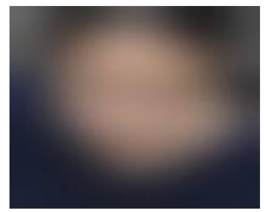
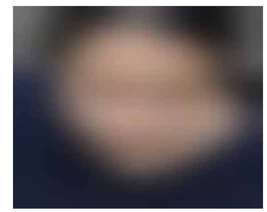
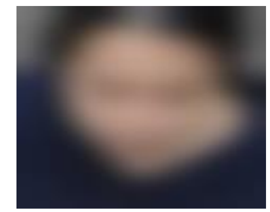
Gaussian blur for LDA face recognizer

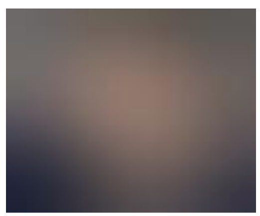
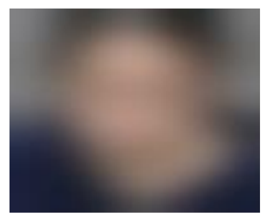
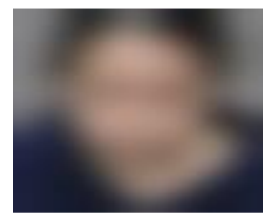
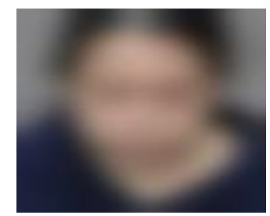
Fixed: w.r.t. highest pixel density image in the data

Adaptive Gaussian Blur Example


ρ: (5.03, 3.88)

μ: (121, 105)

μ: (99, 77)

μ: (75, 57)

μ: (59, 47)


ρ: (3.96, 2.87)

μ: (121, 105)

μ: (75, 57)

μ: (59, 43)

μ: (47, 35)


ρ: (3.06, 2.28)

μ: (121, 105)

μ: (61, 45)

μ: (45, 35)

μ: (37, 29)

Original | Fixed* | Over* | Optimal* | Under*

*Gaussian Blur for LDA face recognizer
Fixed: w.r.t. highest pixel density image in the data

Experimental Setup

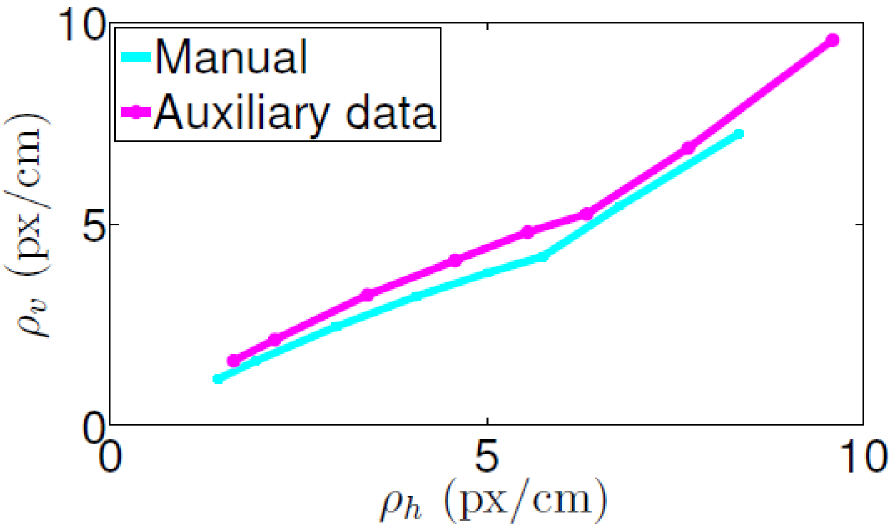
- Dataset from [Hsu, 2015]
  - Population size: 11 persons
  - Test data: 693 (63 x 11) images collected from 63 different positions.
  - Training data: 121 images i.e. 11 images of each person.

- Popular face recognizers for privacy measurement:
  - Linear Discriminant Analysis (LDA) [Belhumeur, 1997]
  - Local Binary Patterns Histograms (LBPH) [Ahonen, 2006]

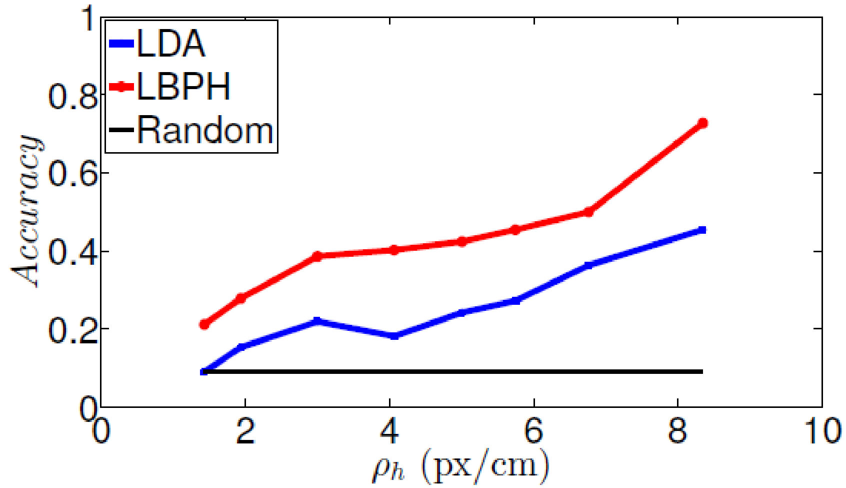
- Fidelity measurement:
  - Peak Signal to Noise Ratio (PSNR)
  - Structural Similarity Index metric (SSIM) [Wang 2004]

Original data

- Pixel density of faces
  - Range [1.15, 9.8] px/cm



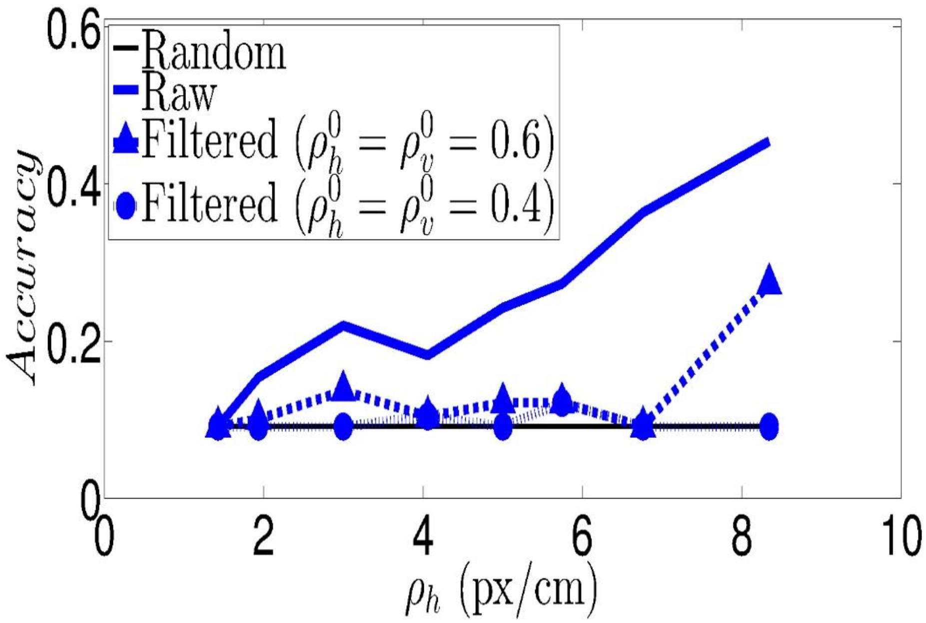
- Face recognition accuracy
  - Performance of LDA & LBPH
  - Random classifier for threshold identification



Privacy of adaptively blurred Faces

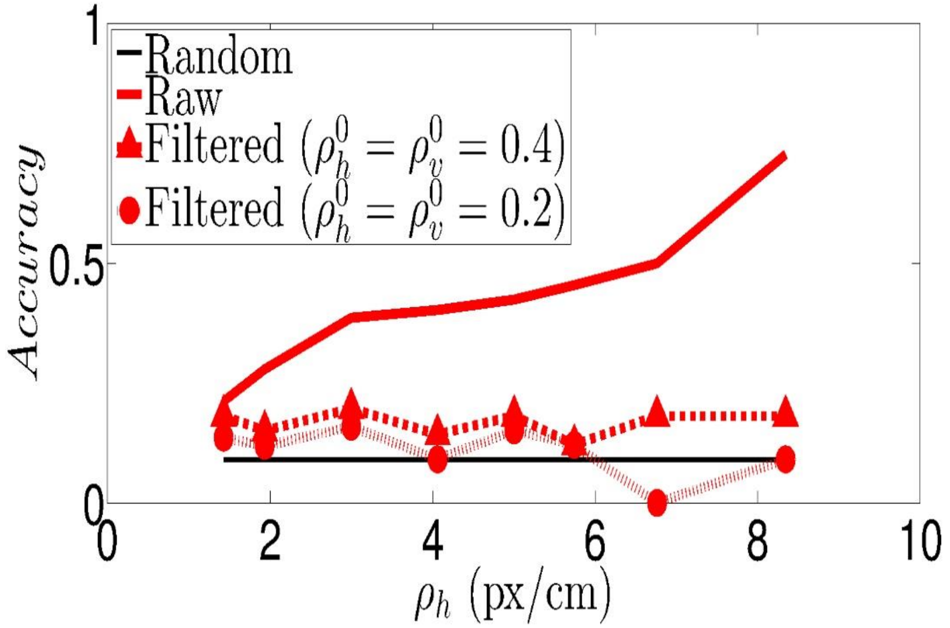
LDA face recognizer

Thresholds: 0,6 & 0.4 px/cm



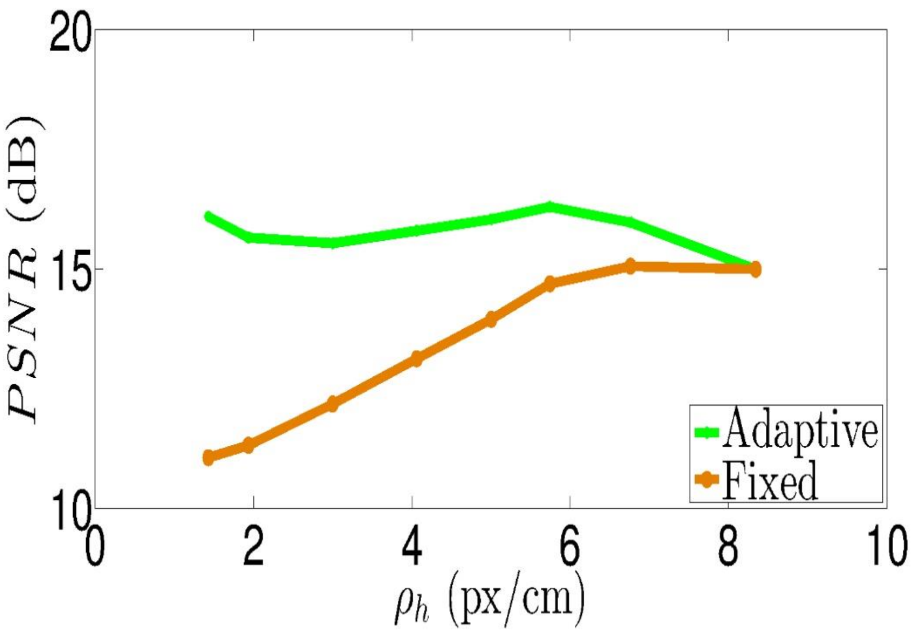
LBPH face recognizer

Thresholds: 0.4 & 0.2 px/cm

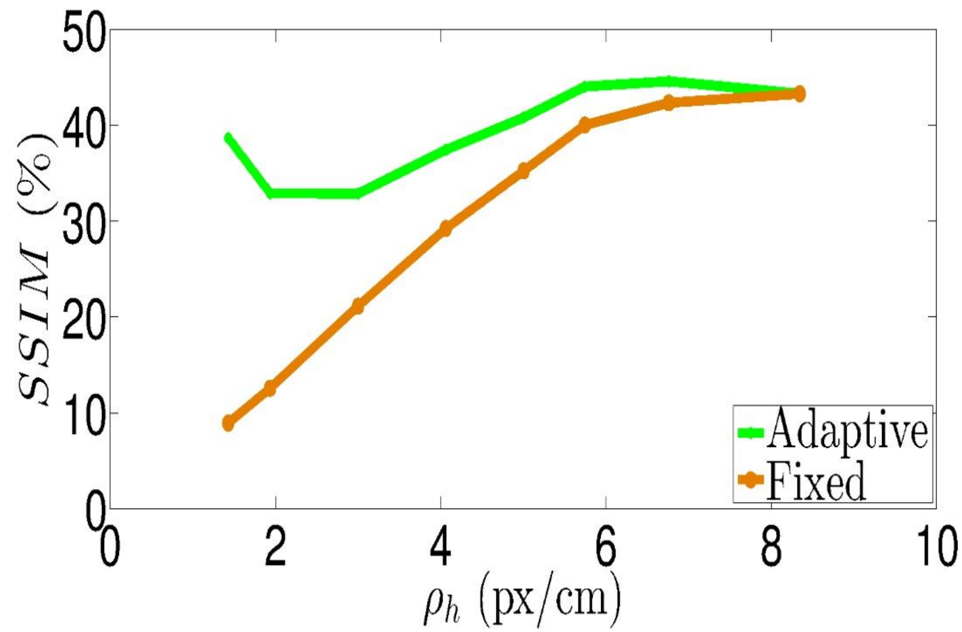


Fidelity Comparison

Peak Signal to Noise Ratio

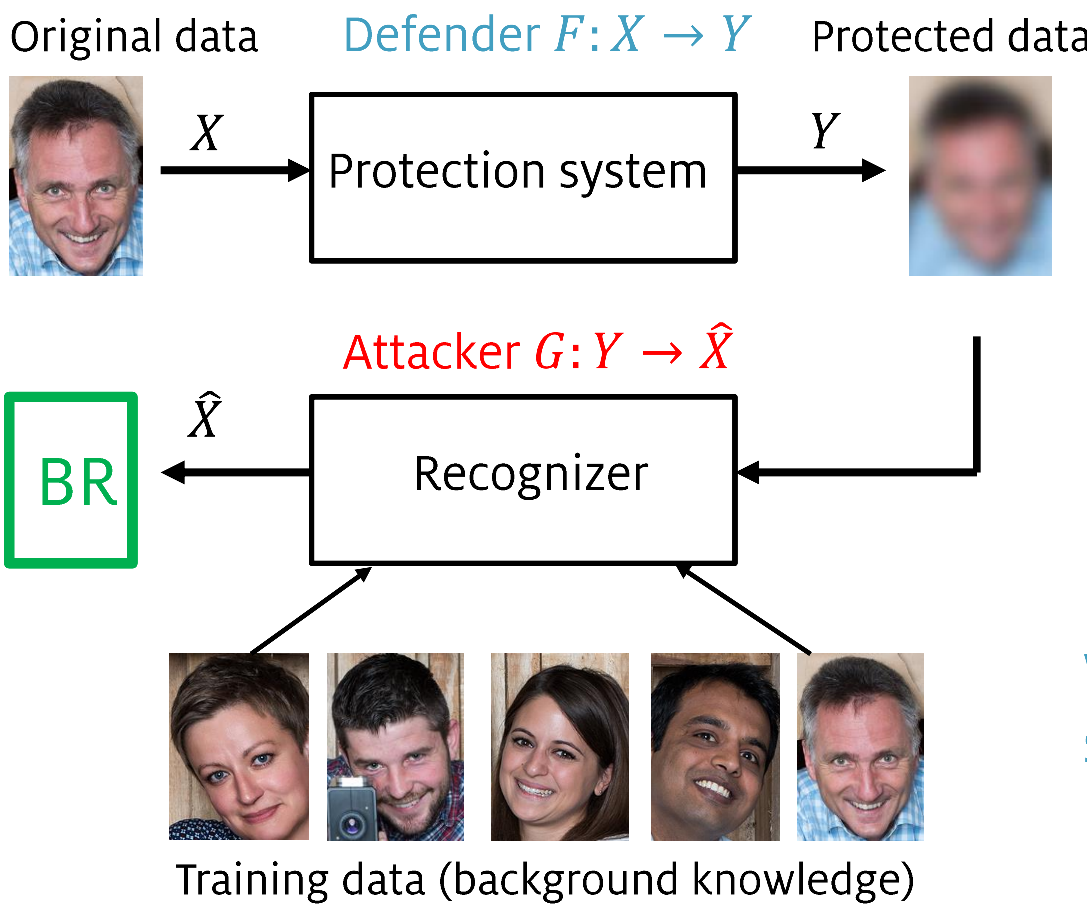


Structural Similarity Index



#2 Hinder Privacy Attacks

Modelling privacy protection systems



Distortion (utility)

$$D = \lambda(X; Y)$$

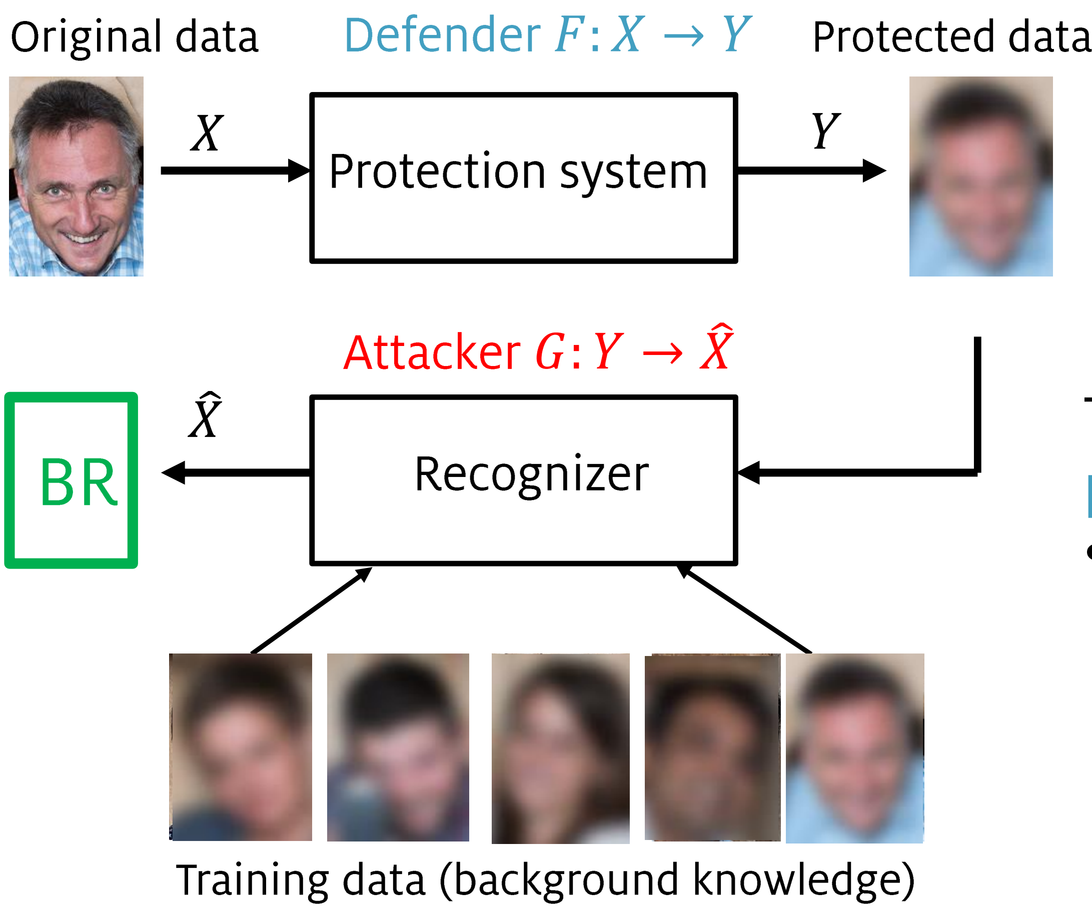
Information leakage (privacy protection)

$$L = \lambda(X; \hat{X})$$

What if the attacker has some knowledge about F?

Parrot Attacks

Attacker knows (learns) the protection filter (eg. blurring filter)



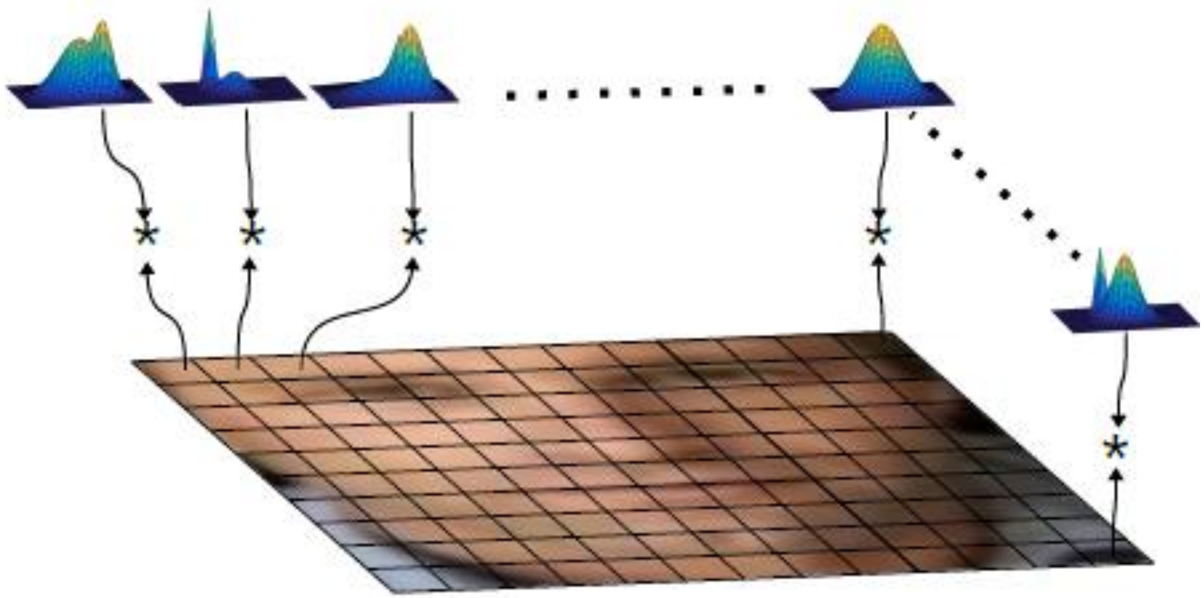
Train the recognizer in protected domain

- increase of information leakage

Adaptive Blurring with Spatial Hopping (AHGMM)

Pseudo-randomly change filter parameters for small patches to hinder

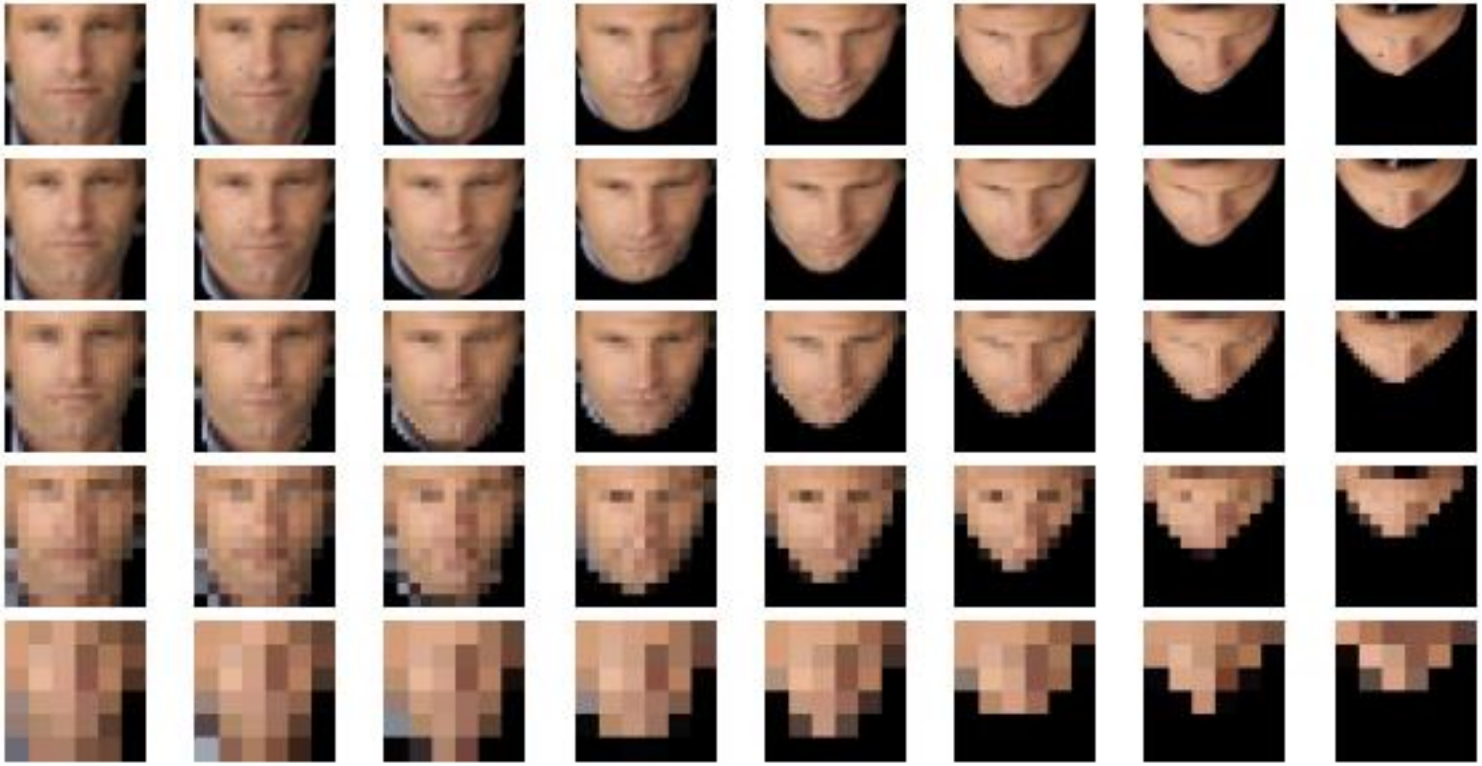
- Estimation of filter parameter
- Reconstruction of original image



[Sawar, Rinner, Cavallaro. [Adaptive Hopping Gaussian Mixture Model for Privacy-Preserving Aerial Photography](). Under review 2017.]

Experimental Setup

- Labelled Faces in the Wild Dataset
  - Population size: 5749 persons
  - Expanded for aerial imagery
    40 instances for each person (variation in pitch angle and resolution)



Experimental Setup (2)

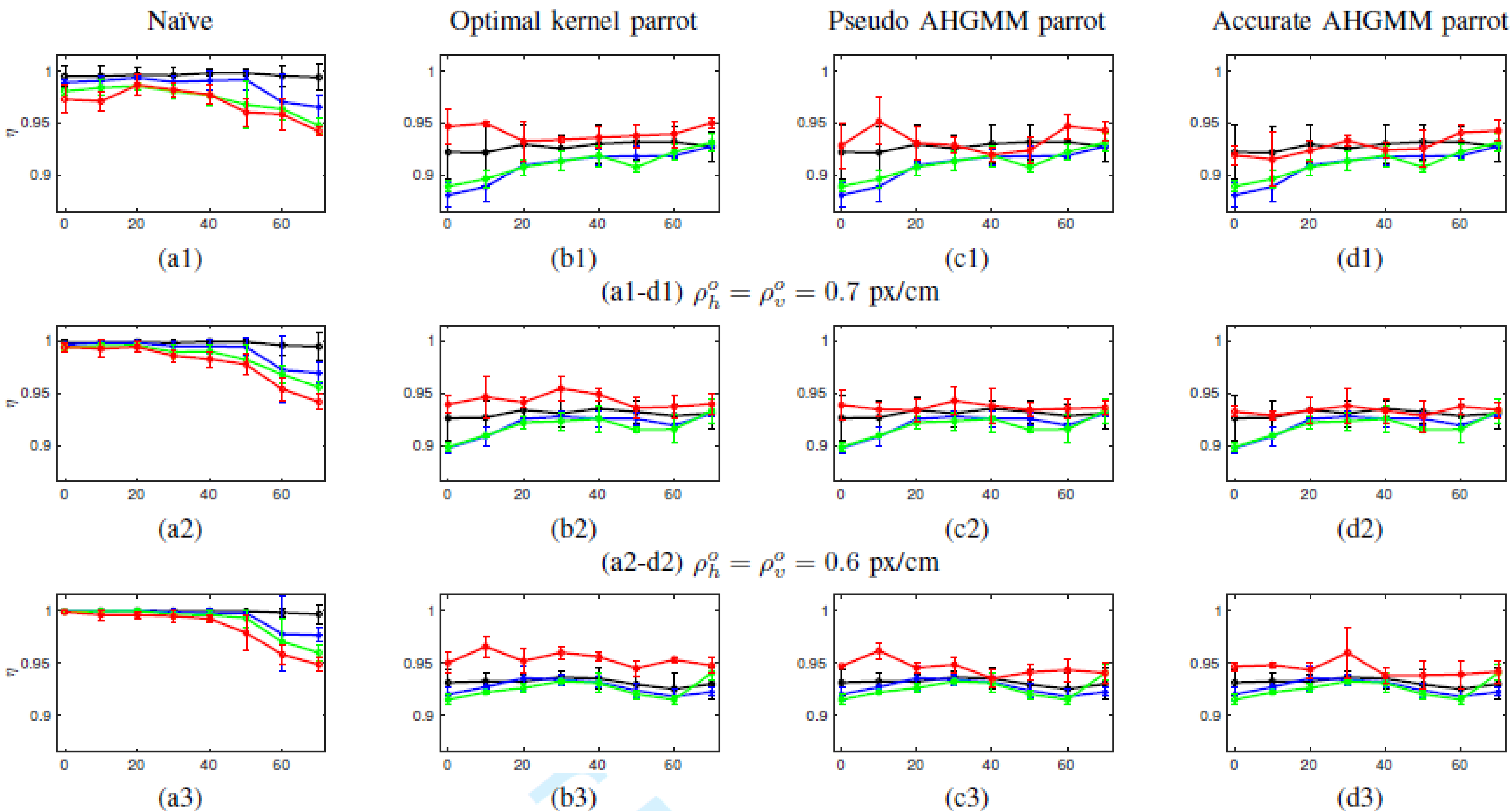
- Privacy attack scenarios
  - Naïve: training with raw data
  - Parrot: training with AHGMM filtered data (3 variants)
  - Pitch angle is known by attacker as background
  - Tested with 380000 face images in total

- OpenFace recognizer for privacy measurement:
  - Verificiation test (600 persons with 10x cross validation)

- Fidelity measurement:
  - Peak Signal to Noise Ratio (PSNR)
  - Structural Similarity Index metric (SSIM) [Wang 2004]

Privacy Evaluation

- Comparison with 3 state-of-the-art privacy filters (-AHGMM)
  - Charts: privacy level η vs. pich angle; rows: different filter thresholds



(a1-d1) $\rho_h^o = \rho_v^o = 0.7$ px/cm

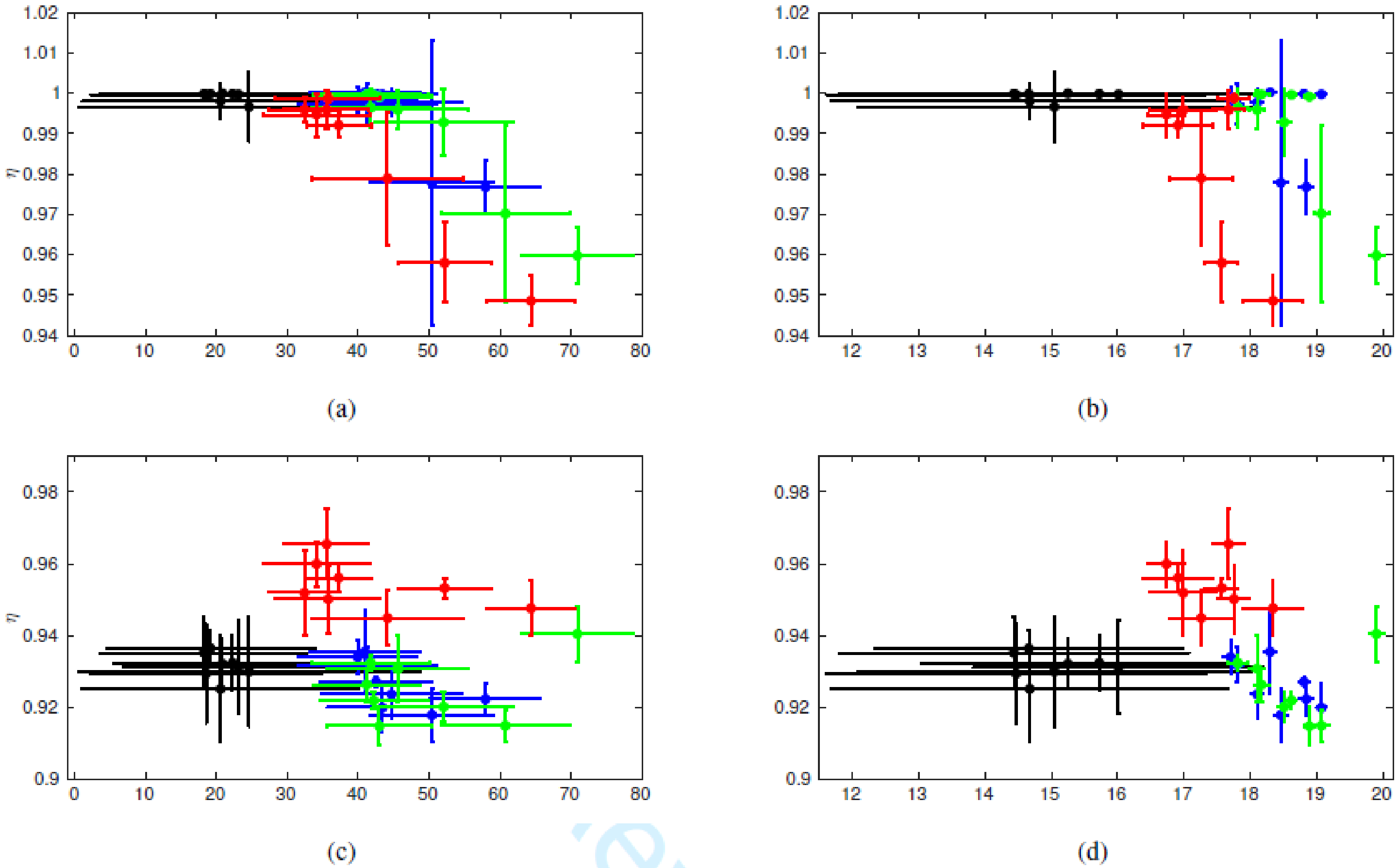
(a2-d2) $\rho_h^o = \rho_v^o = 0.6$ px/cm

(a3-d3) $\rho_h^o = \rho_v^o = 0.5$ px/cm

Privacy/Utility Tradeoff

- Privacy level vs. utility compared with 3 privacy filters (-AHGMM)

SSIM (%) PSNR (dB)



(a) (b) (c) (d)

Naive attack

Parrot attack

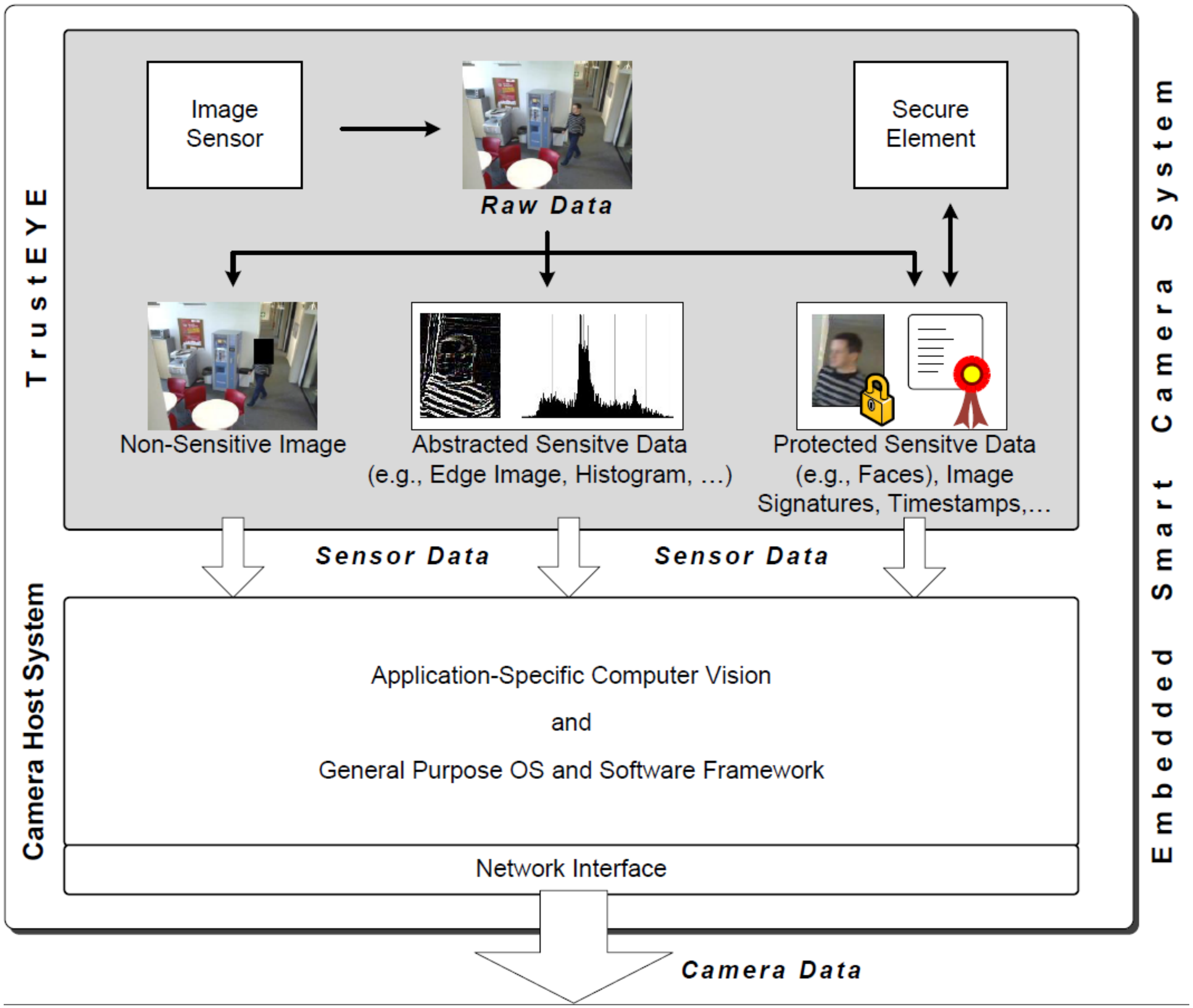
#3 Secure and Privacy-aware Camera

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

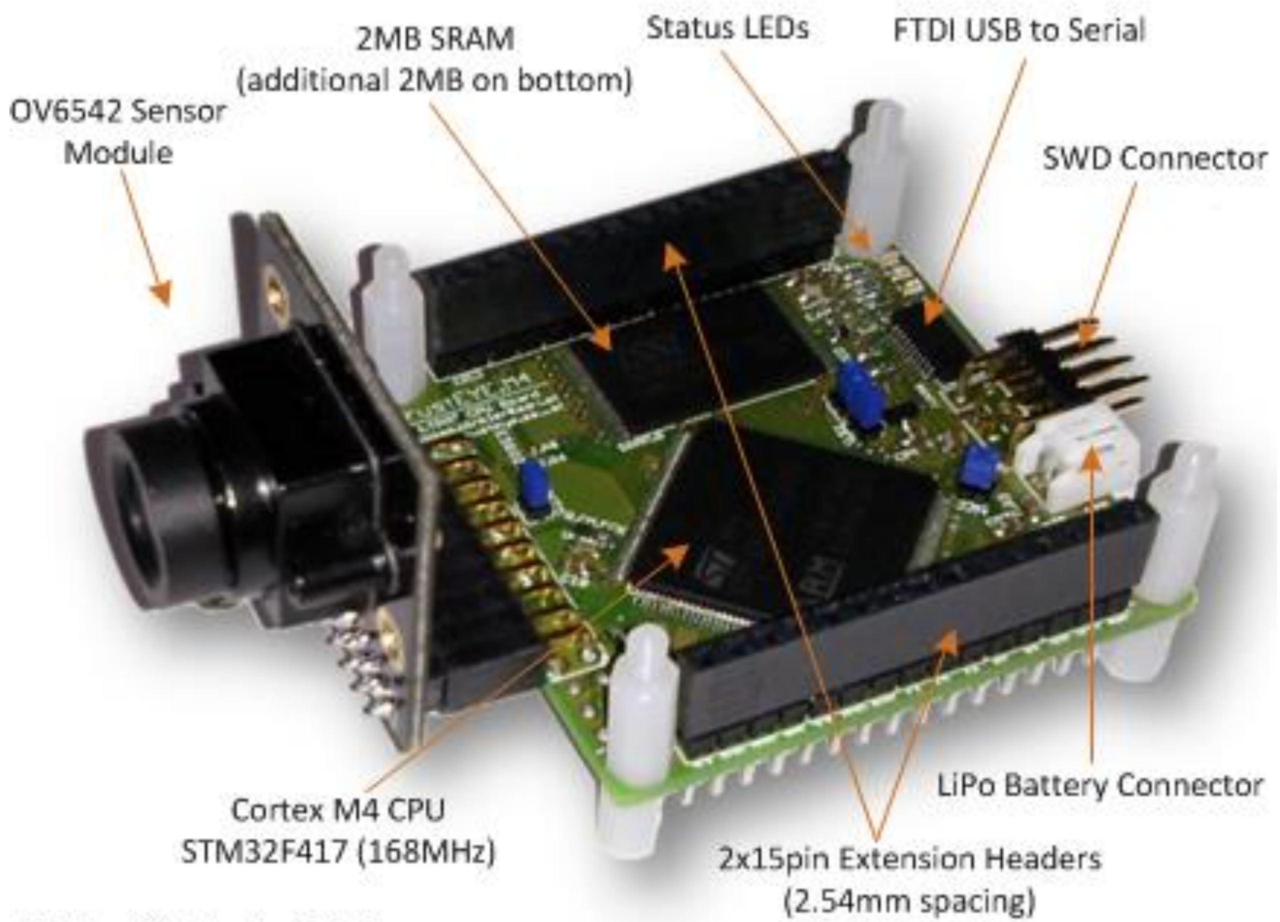
- Benefits:
  - Sensor delivers protected and pre-filtered data
  - Strong separation btw. trusted and untrusted domains
  - Camera software does no longer have to be trustworthy
  - Security can not be bypassed by application developers
  - TrustEYE is anchor for secure inter-camera collaboration

[Winkler, Erdelyi, Rinner. TrustEYE.M4: Protecting the Sensor - not the Camera. In Proc. AVSS 2014]
http://trusteye.aau.at/

TrustEYE Architecture

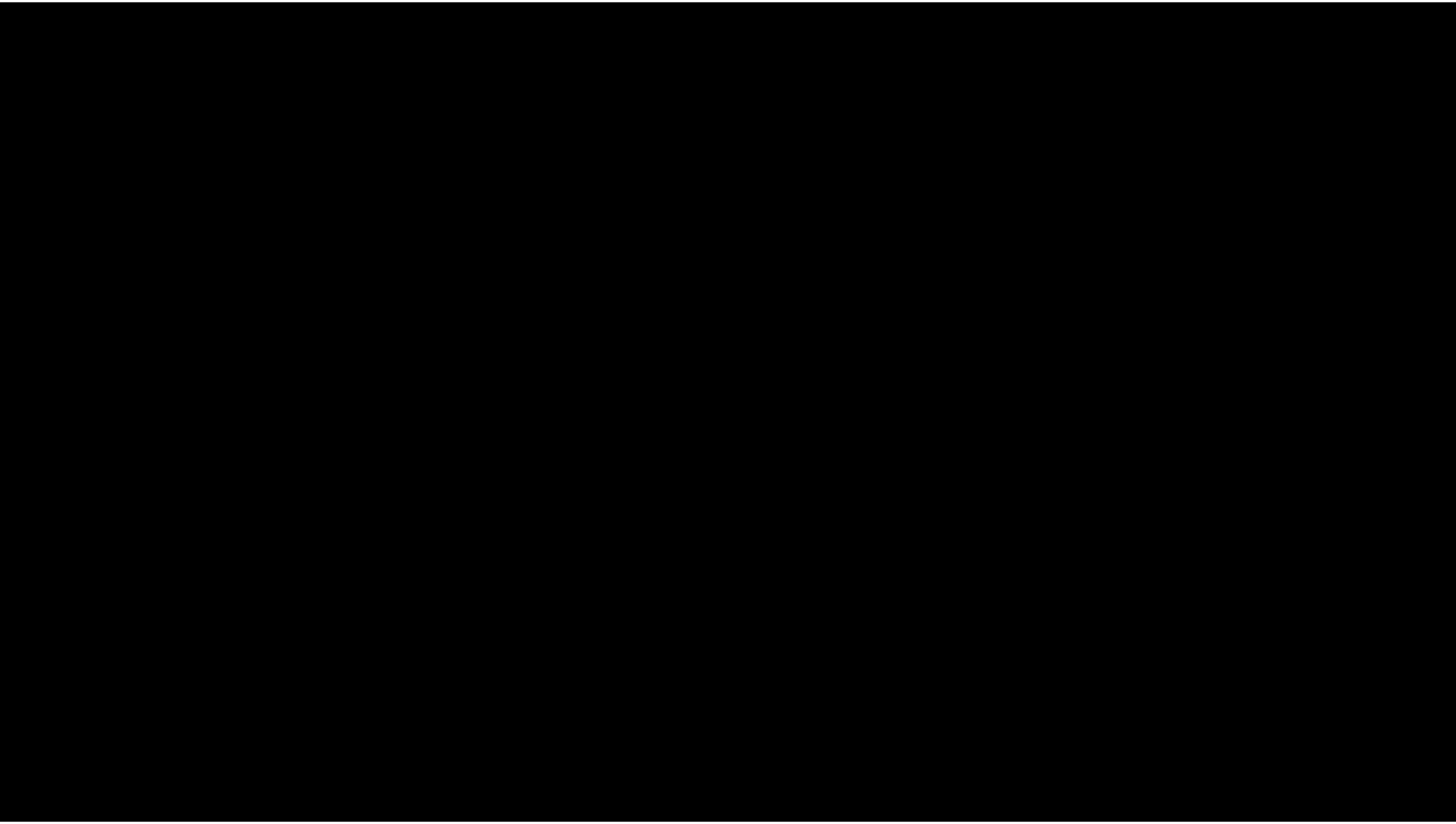


TrustEYE Platform



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

TrustEYE Demo



Conclusion

- Privacy protection important for commercial and private aerial imaging
- No single best protection method available. Tradeoff between protection, utility and resource usage
- Mostly image distortion used for protection, some can adapt the filter strength to scene
- Increase privacy awareness

Acknowledgements

Pervasive Computing group

Institute of Networked and Embedded Systems

http://nes.aau.at

http://bernhardrinner.com

Funding support

- KWF/FWF "Trustworthy Sensing and Cooperation in Visual Sensor Networks"
- FFG "Progressing towards Secure, Cooperating Smart Cameras"