Design Space Exploration for Adaptive Privacy Protection in Airborne Images

Published in: IEEE Advanced Video and Signal-based Surveillance (AVSS) 2016

Omair Sarwar[1,2], Bernhard Rinner[1], Andrea Cavallaro[2]

[1]Alpen-Adria-Universität Klagenfurt, Austria

[2]Queen Mary University of London, UK

CIS centre for intelligent sensing

ICE

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Queen Mary University of London

Outline

- Introduction and Motivation
- Literature Review
- Proposed Work
- Experimental Results
- Conclusion and Future Work

Introduction

[James, 2014]

[Leigh, 2014]

[Simon, 2014]

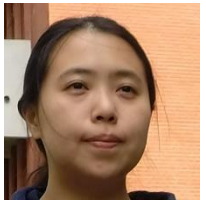
[Kurt, 2015]

Motivation

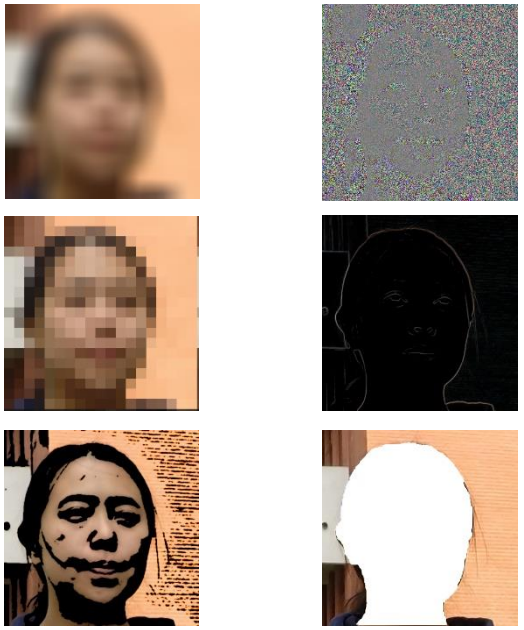
- How we can protect privacy in airborne cameras (intended for recreational applications), while maintaining high fidelity of the visual data ?
- Sub-problems
  - Exploring privacy design space
  - Configuring a privacy adaptive filter

Background

- Privacy Filters in CCTV
  - Adaptive filters
    - Pixelation [Zhao, 1998]
    - Blurring [Wickramasuriya, 2004]
    - Cartooning [Erdelyi, 2014]
    - Scrambling [Zeidler, 1994]
    - Warping [Korshunov, 2013]
  - Non-adaptive filters
    - Box [Wickramasuriya, 2004]
    - Avatar [López, 2015]
    - Edge [Zhao, 1998]
    - Transparency [Chinomi, 2008]
    - Silhouette [Tansuriyavong, 2001]



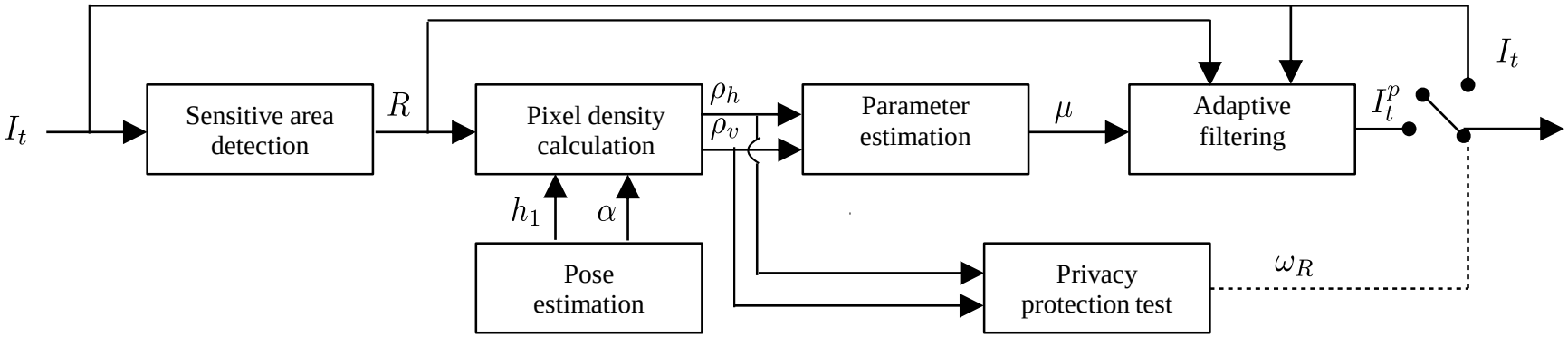
[Hsu, 2015]



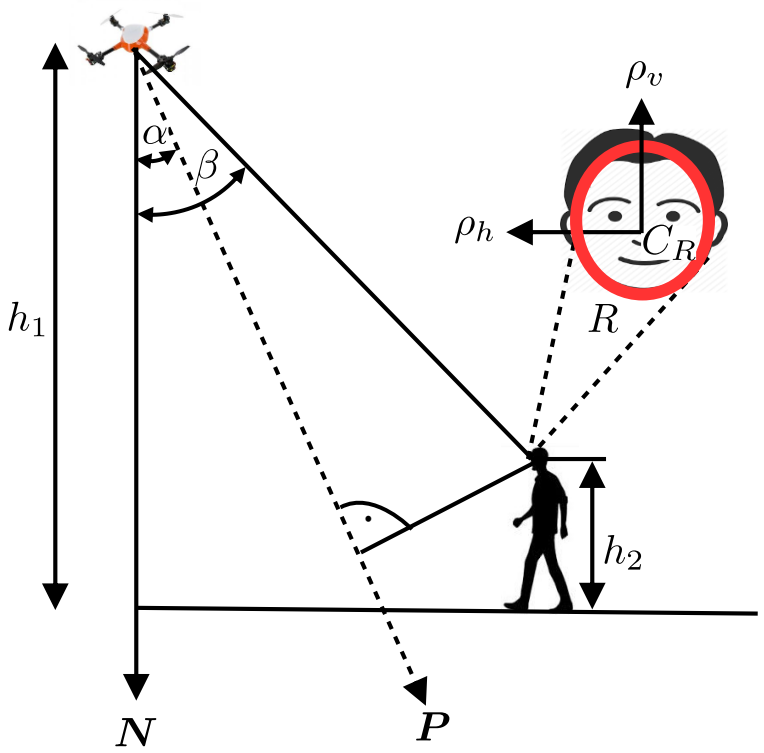
Background

- Privacy in Airborne Cameras
  - Geo-fencing
    - NoFlyZone [www.noflyzone.org]
    - Broadcast privacy beacons [Vaidya, 2015]
  - Processing ROI
    - Encrypted videos [Kim, 2014]
    - Unmanned Aerial System- Visual Privacy Guard (UAS-VPG) [Babiceanu, 2015]

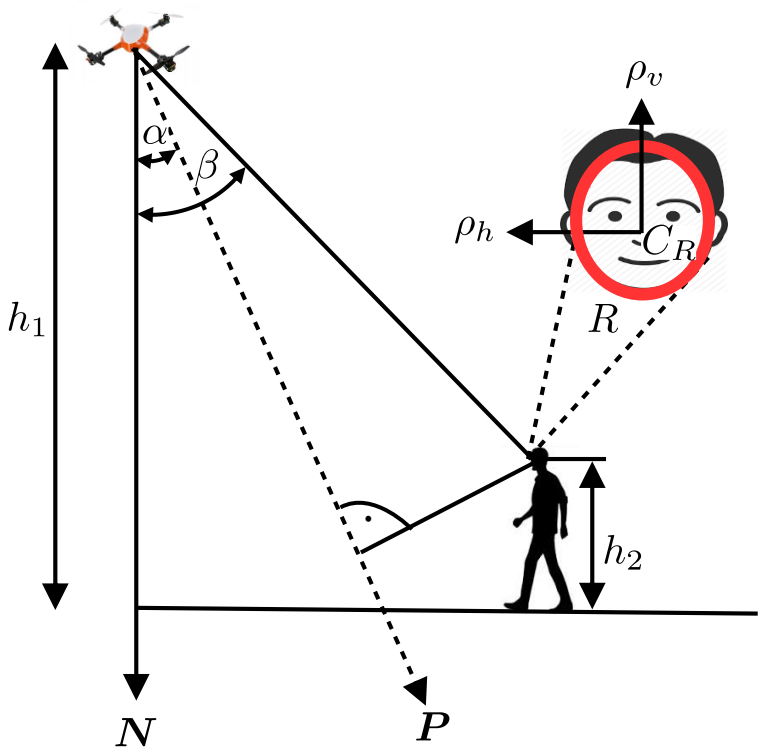
Proposed approach



Proposed approach



Proposed approach



focal length

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

horizontal pixel size

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

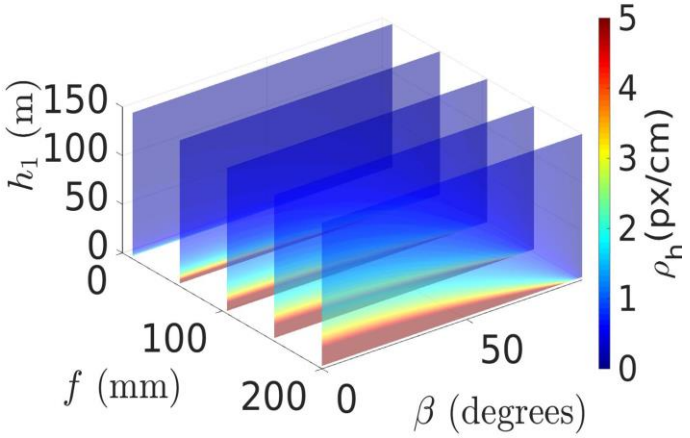
vertical pixel size

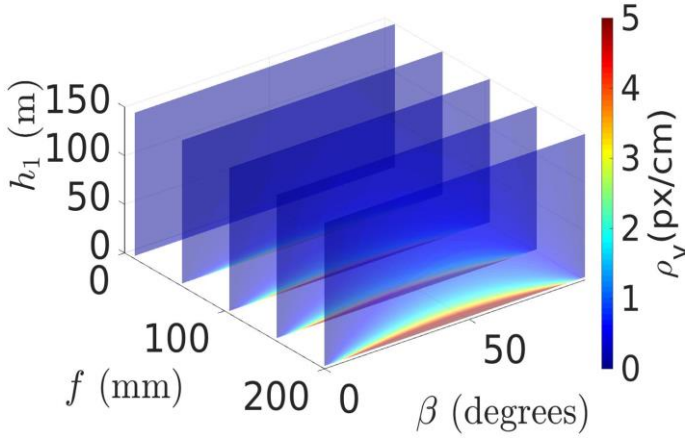
Privacy design space

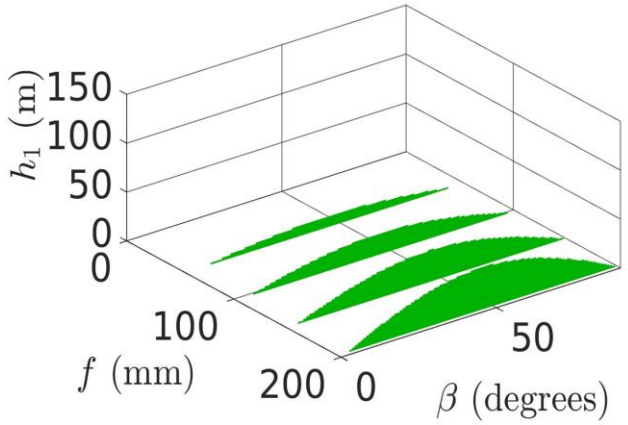
experimentally determined thresholds

$$\omega_R = \begin{cases} 1 & if \quad \rho_h > \rho_h^0 \quad \& \quad \rho_v > \rho_v^0 \\ 0 & otherwise \end{cases}$$

Analytical results (Canon EOS 5D MARK II)

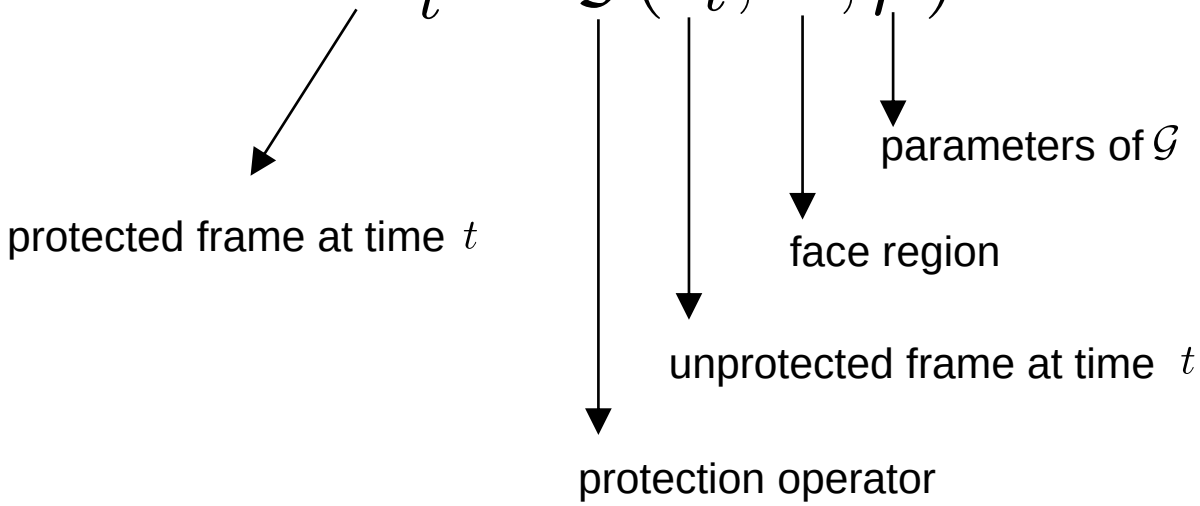






Adaptive privacy filter

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



Adaptive Gaussian blur

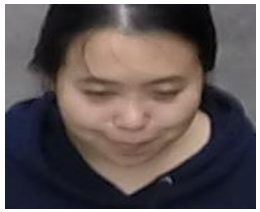
$$g(h,v) = \frac{1}{2\pi\sigma_h\sigma_v} e^{-(\frac{h^2}{2\sigma_h^2}+\frac{v^2}{2\sigma_v^2})}$$

$$\sigma_i = \frac{3\rho_i}{\pi\rho_i^0} \qquad \text{where} \quad i \in \{h,v\}$$

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

Standard deviation of anisotropic Gaussian function $g(h,v)$

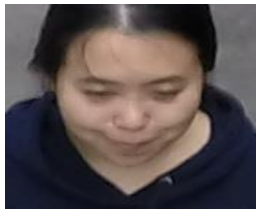
Adaptive Gaussian blur example



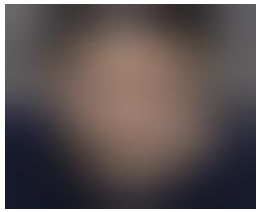
$(5.03, 3.88)$

Original

Adaptive Gaussian blur example



$(5.03, 3.88)$



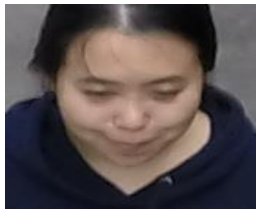
$(121, 105)$

Original

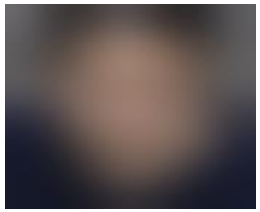
Fixed*

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

Adaptive Gaussian blur example



$(5.03, 3.88)$



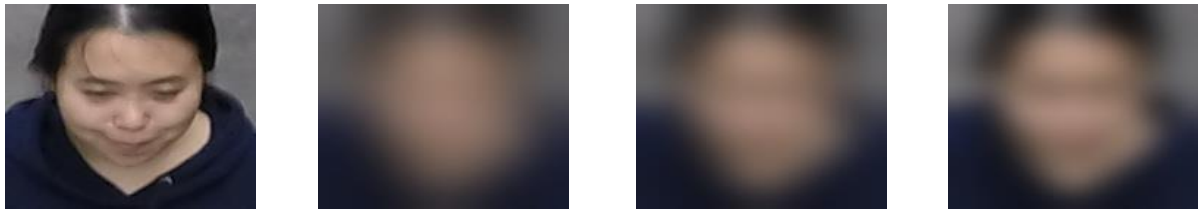
$(121, 105)$

$(99, 77)$

Original Fixed* Over*

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

Adaptive Gaussian blur example

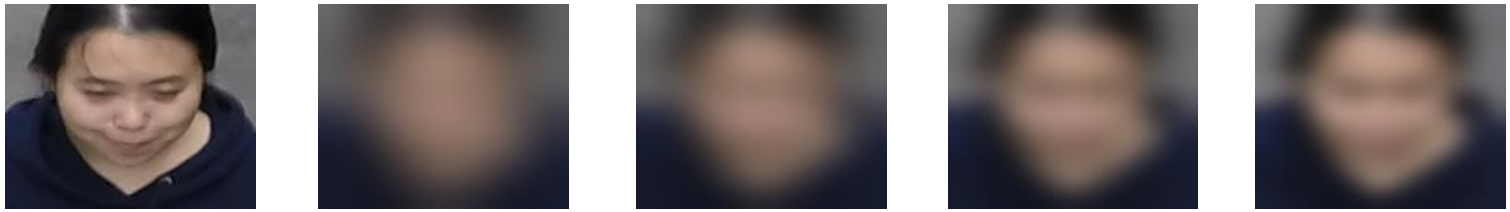


$(5.03, 3.88)$ $(121, 105)$ $(99, 77)$ $(75, 57)$

Original Fixed* Over* Optimal*

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

Adaptive Gaussian blur example



$(5.03, 3.88)$ $(121, 105)$ $(99, 77)$ $(75, 57)$ $(59, 47)$

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

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

Experimental set-up

- Dataset “Face Recognition on Drones: Issues and Limitations [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.

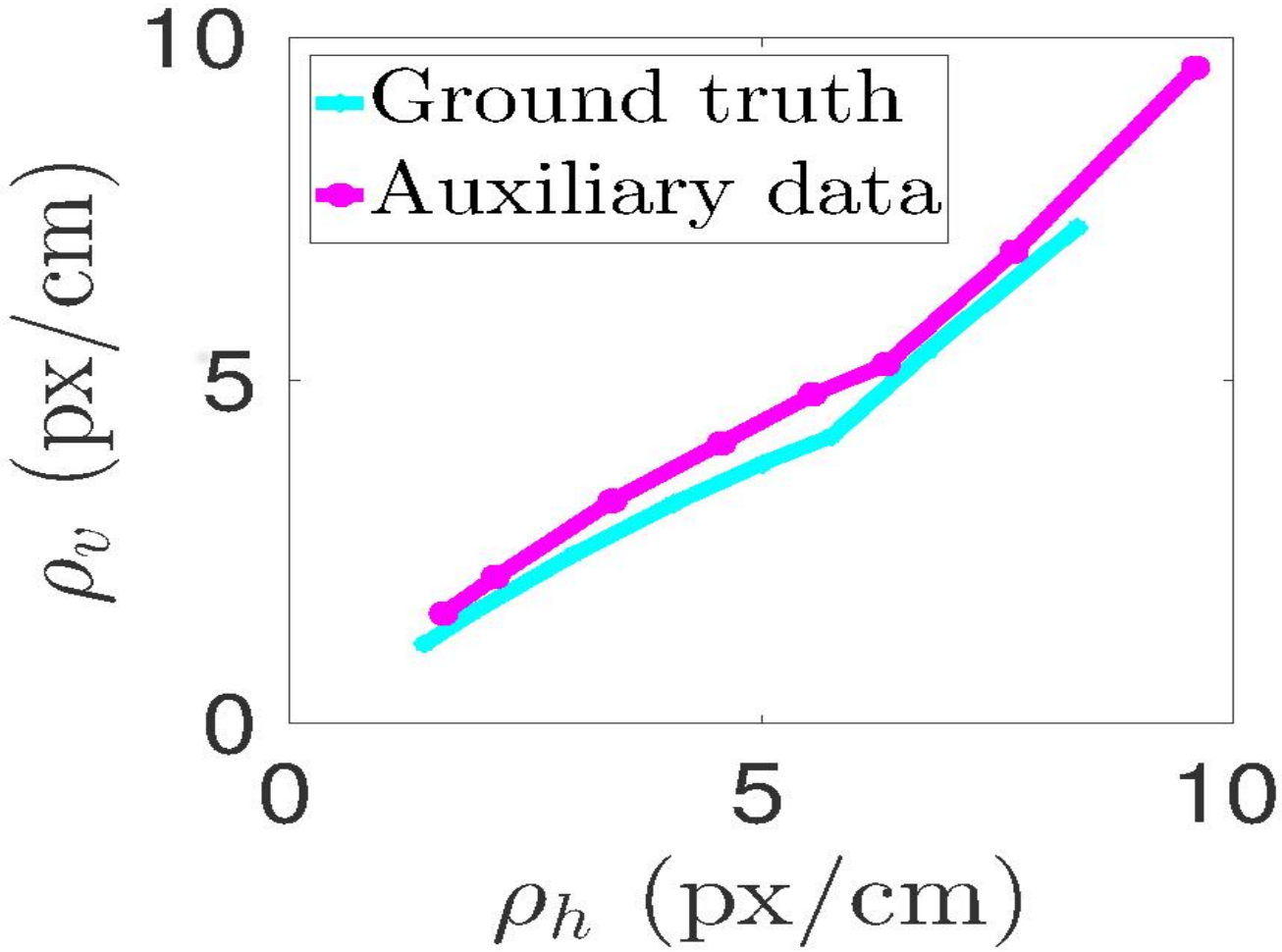
Experimental set-up

- Dataset “Face Recognition on Drones: Issues and Limitations [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.
- Privacy measurement:
  - Linear Discriminant Analysis (LDA) face recognizer [Belhumeur, 1997]
  - Local Binary Patterns Histograms (LBPH) face recognizer [Ahonen, 2006]

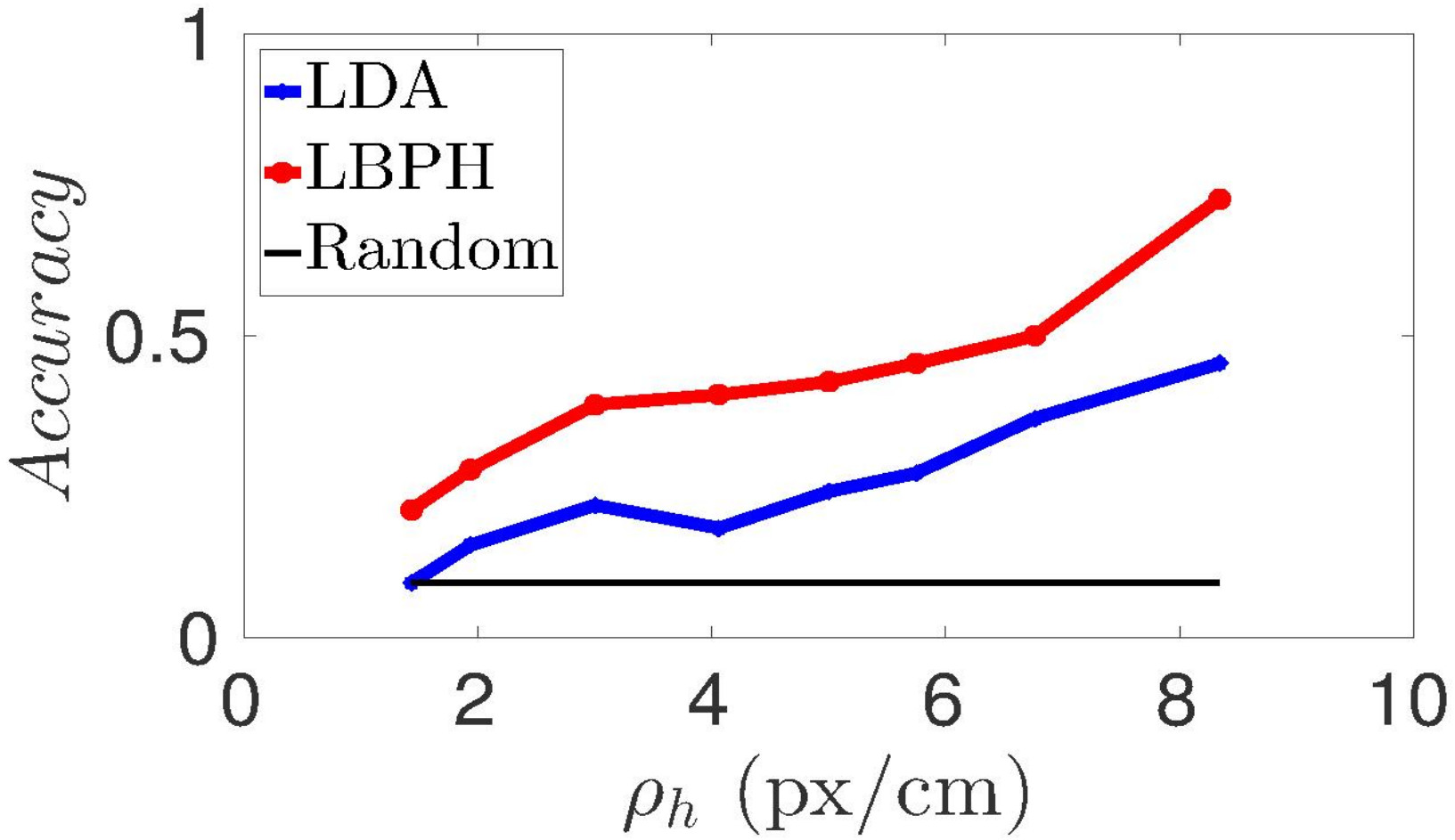
Experimental set-up

- Dataset “Face Recognition on Drones: Issues and Limitations [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.
- Privacy measurement:
  - Linear Discriminant Analysis (LDA) face recognizer [Belhumeur, 1997]
  - Local Binary Patterns Histograms (LBPH) face recognizer [Ahonen, 2006]
- Fidelity measurement:
  - Peak Signal to Noise Ratio (PSNR)
  - Structural Similarity Index Metric (SSIM) [Wang 2004]

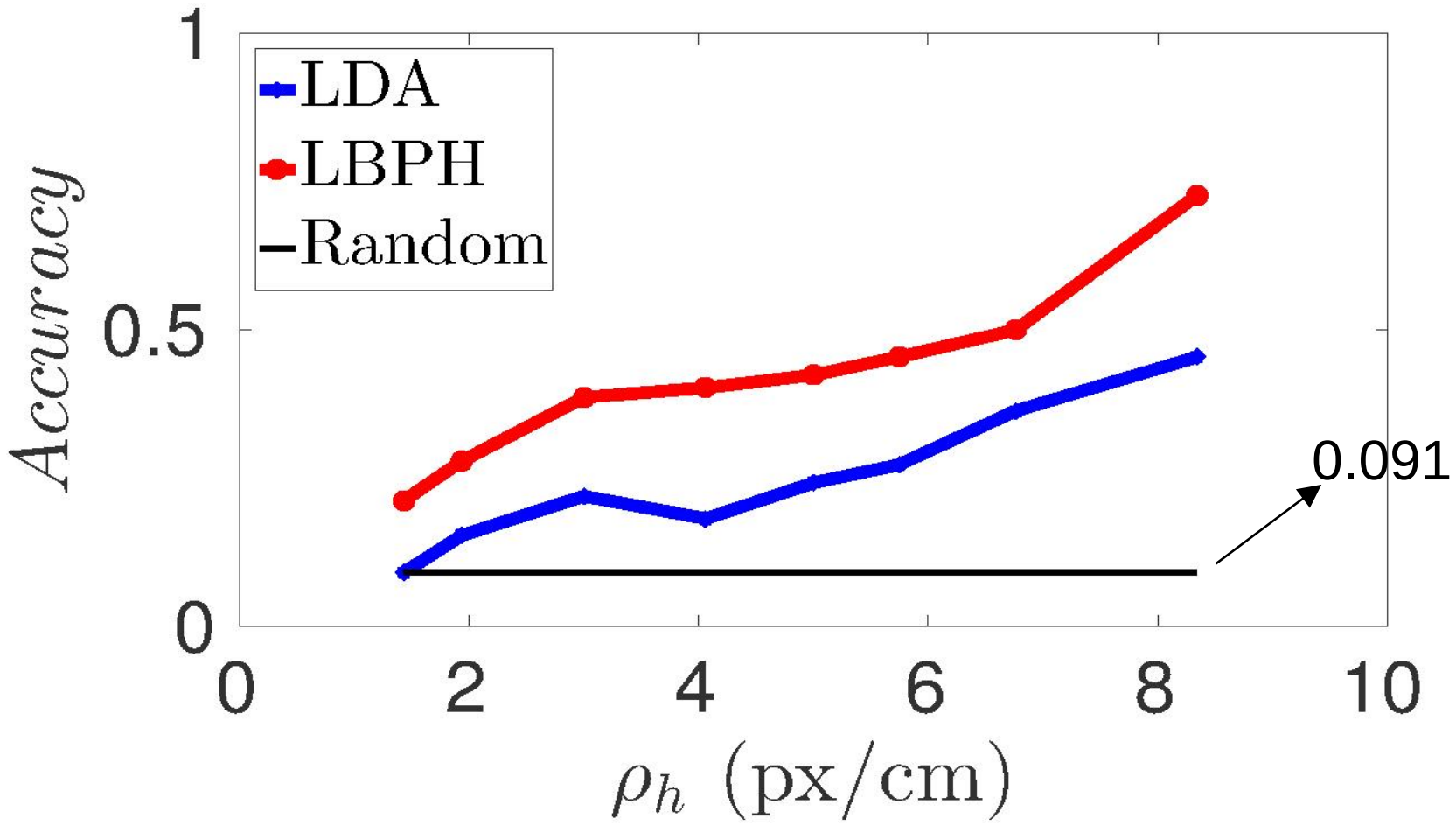
Pixel density of selected data



Recognition accuracy

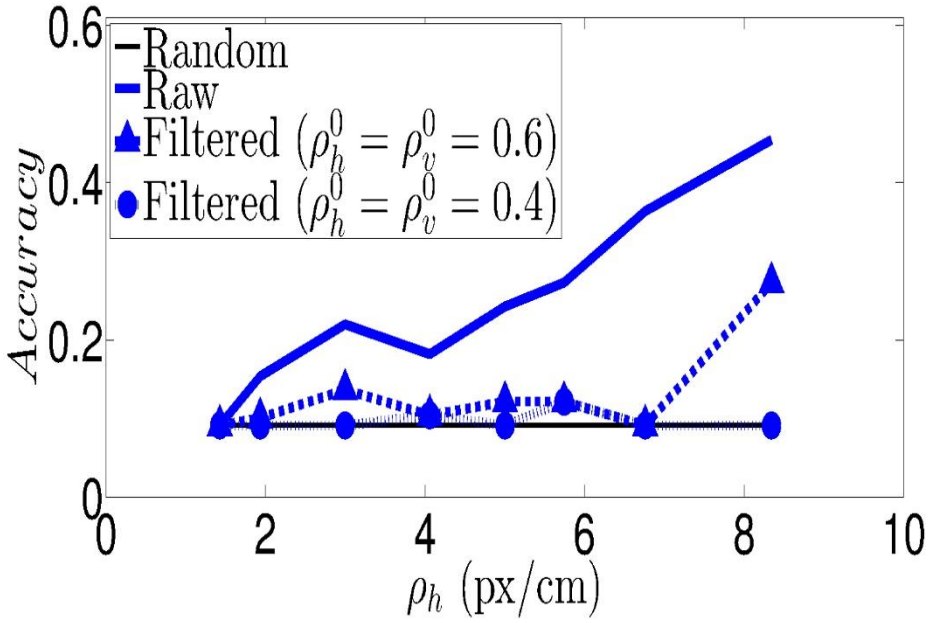


Recognition accuracy

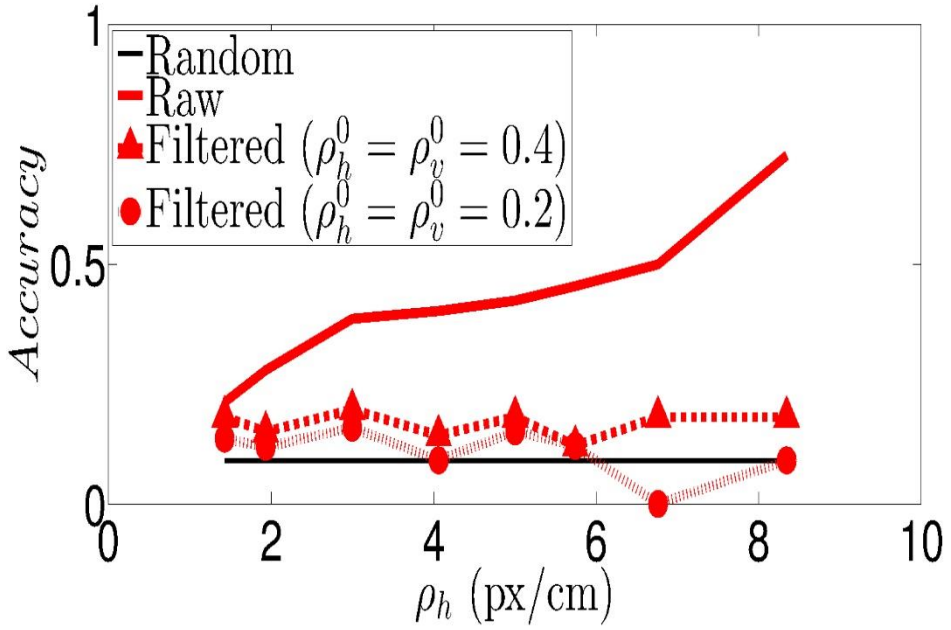


Adaptive Gaussian filter

LDA face recognizer

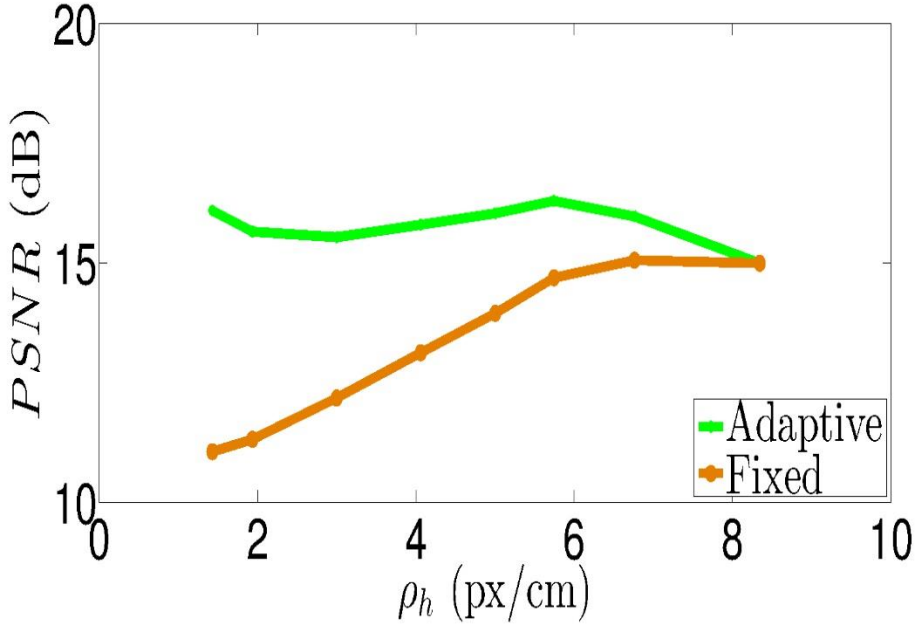


LBPH face recognizer

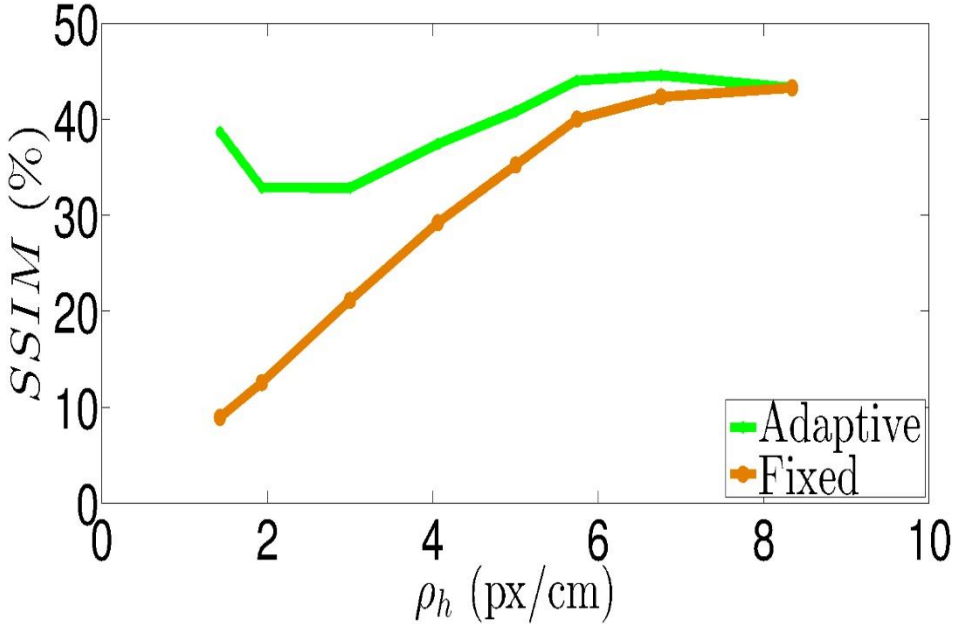


Fidelity measurement

Peak Signal to Noise Ratio (PSNR)



Structural Similarity Index Metric (SSIM)



Conclusions

- Separated inherently protected and unprotected space.
- Proposed an adaptive filtering approach, which provides high fidelity while still providing same amount of privacy protection as fixed filter.

- Future Work
  - Super resolution attack.
  - Benchmarking with recent face recognition algorithms.
  - Developing/testing with data set having large population size.

References

[James, 2014] James Trew, Airdog drone serves as your loyal action sports cameraman ”https://www.engadget.com/2014/06/16/airdog-drone/”. [Last accessed: 2016-08-01].

[Simon, 2014] Simon MacMichael”Drones - the next big thing in cycle safety, or a case of too much blue sky thinking?” http://road.cc/content/news/109510-drones-next-big-thing-cycle-safety-or-case-too-much-blue-sky-thinking [Last ac- cessed: 2016-08-01].

[Leigh, 2014] Leigh Giangreco ”Drones why they’re still popular on Delmarva” http://www.delmarvanow.com/story/news/local/delaware/2014/10/31/delmarva-drone-popularity/18266053/. [Last accessed: 2016-04-07].

[Kurt, 2015] Kurt Repanshek ”Scofflaws Piloting Drones In The National Park System ” http://www.nationalparkstraveler.com/2015/04/scofflaws-piloting-drones-national-park-system26476. [Last accessed: 2016-08-01].

[Wickramasuriya, 2004] J. Wickramasuriya, M. Datt, S. Mehrotra, and N. Venkatasubramanian. Privacy Protecting Data Collection in Media Spaces. In Proc. Int. Conf. on Multimedia, pages 48–55, New York, NY, USA, October 2004.

[Korshunov, 2013] P. Korshunov and T. Ebrahimi. Using warping for privacy protection in video surveillance. In Proc. Int. Conf. on Digital Signal Processing (DSP), pages 1–6, Fira, Santorini, Greece, July 2013.

[7] F. Dufaux and T. Ebrahimi, Scrambling for video surveillance with privacy, in Computer Vision and Pattern Recognition Workshop, 2006. CVPRW 06. Conference on, pp. 160160, June 2006.

[www.noflyzone.org] ”Enter your address below to create a No Fly Zone over your home. Its free!”. https://www.noflyzone.org/. [Last ac- cessed: 2016-03-24].

[Chinomi, 2008] K. Chinomi, N. Nitta, Y. Ito, and N. Babaguchi. PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstraction. In Proc. Int. Conf. on Advances in Multimedia Modeling, pages 144–154, Kyoto, Japan, January 2008.

[Erdelyi, 2014] A. Erdelyi, T. Barat, P. Valet, T. Winkler, and B. Rinner. Adaptive cartooning for privacy protection in camera networks. In Proc. Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS), pages 44–49, Seoul, Korea, August 2014.

[Lpez, 2015] Padilla-Lpez, J.R.; Chaaraoui, A.A.; Gu, F.; Flrez-Revuelta, F. Visual Privacy by Context: Proposal and Evaluation of a Level-Based Visualisation Scheme. Sensors 2015, 15, 12959-12982.

[Babiceanu, 2015] R. Babiceanu, P. Bojda, R. Seker, and M. Alghumgham. An onboard UAS visual privacy guard system. In Proc. Integrated Communication, Navigation, and Surveillance Conf. (ICNS), pages J1:1–J1:8, Herdon, VA, USA, April 2015.

[Kim, 2014] Y. Kim, J. Jo, and S. Shrestha. A server-based real-time privacy protection scheme against video surveillance by unmanned aerial systems. In Proc. Int. Conf. on Unmanned Aircraft Systems (ICUAS), pages 684–691, Orlando, FL, USA, May 2014.

[Vaidya, 2015] T. Vaidya and M. Sherr. Mind your (R, Φ)s: Location-Based Privacy Controls for Consumer Drones. In Proc. Intern. Workshop on Security Protocols, pages 91–104, Cambridge, UK, March 2015.

[Hsu, 2015] H.-J. Hsu and K.-T. Chen. Face Recognition on Drones: Issues and Limitations. In Proc. First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, DroNet ’15, pages 39–44, Florence, Italy, May 2015

[Belhumeur, 1997] P.N.Belhumeur,J.P.Hespanha,andD.J.Kriegman. Eigenfacesvs.Fisherfaces: RecognitionUsingClassSpecificLinearProjection.IEEETrans.onPatternAnalysisandMachine Intelligence, 19(7):711–720, July 1997.

[Ahonen, 2006] T. Ahonen, A. Hadid, and M. Pietikainen. Face Description with Local Binary Patterns: Application to Face Recognition. IEEE Trans. on Pattern Analysis and Machine Intelligence, 28(12):2037–2041, December 2006.

[Wang, 2004] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. Image quality assessment: from error visibility to structural similarity. IEEE Trans. on Image Processing, 13(4):600– 612, April 2004.

[Zeidler, 1994] D. Zeidler and J. Griffin, General Instrument Co., "Method and apparatus for television signal scrambling using block shuffling," US patent 5321748, June, 1994.

[Zhao, 1998] Qiang Alex Zhao and John T. Stasko. Evaluating image filtering based techniques in media space applications. In *Proceedings of conference on Computer supported cooperative work* . Pages 11-18, Seattle, Washington, USA, 1988.

[] Suriyon Tansuriyavong and Shin-ichi Hanaki. Privacy protection by concealing persons in circumstantial video image. In *Proceedings of the 2001 workshop on Perceptive user interfaces* (PUI '01). Pages 1-4, Orlando, Florida, USA, 2001.