

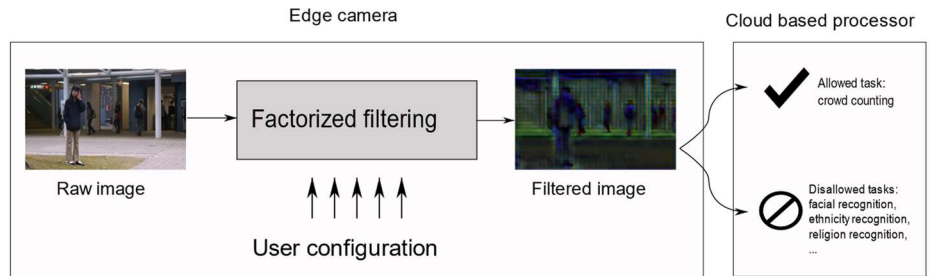
# Privacy-Aware Video Processing

Sander De Coninck, Wei-Cheng Wang, Sam Leroux, Pieter Simoens  
Sander.DeConinck@UGent.be, UGent - imec



Video processing is often **cloud-based**:

- Cameras and cloud computing are inexpensive
- Processing on edge devices is difficult
  - Fewer computational resources
  - More susceptible to wear and tear
  - Vulnerable during processing
- However, high risk of:
  - **Function creep**
  - **Malicious usage**

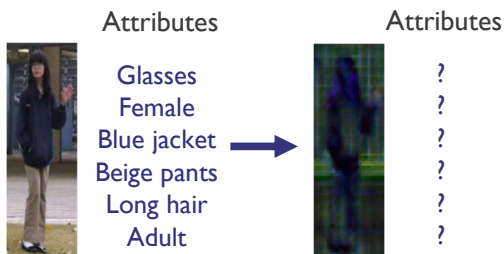
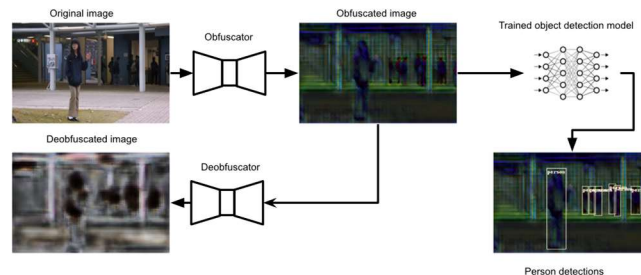


**Solution?** → Use a lightweight filter to remove sensitive aspects of data before sending to the cloud for processing

## Use case: privacy-aware pedestrian detection

How can we **filter** data?

By employing **adversarial training** to obtain an **opt-in** version of the data: Only allow pedestrian detection while removing as much information as possible.



How can we **verify privacy**?

By testing out **Pedestrian Attribute Recognition (PAR)** ability on obfuscated frames

How can we make it **edge-friendly**?

By making the obfuscation process **lightweight** and **generalizable across multiple cameras**

## Results

Dataset	Utility Person AP	PAR Performance			
		Jia et al. [1]		VTB [2]	
		Original	Obfuscated	Original	Obfuscated
ShanghaiTech Campus	89.16	72.85	57.74	74.57	55.74
Avenues	89.62	76.28	66.51	80.73	66.40
WILDTRACK	81.33	75.53	57.04	75.77	58.82

We can maintain a relative pedestrian detection accuracy of around 90%

While heavily reducing the ability to learn sensitive attributes to near random (50%) performance

[1] J. Jia, H. Huang, X. Chen, and K. Huang, "Rethinking of Pedestrian Attribute Recognition: A Reliable Evaluation under Zero-Shot Pedestrian Identity Setting," Nov. 2021, arXiv:2107.03576 [cs]. [Online]. Available: <https://arxiv.org/abs/2107.03576>

[2] X. Cheng, M. Jia, Q. Wang, and J. Zhang, "A Simple Visual-Textual Baseline for Pedestrian Attribute Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 10, pp. 6994–7004, Oct. 2022, conference Name: IEEE Transactions on Circuits and Systems for Video Technology.

**Limitations:**

- Coupled with object detection model
- Reliant on other models to evaluate privacy

**Future work:**

- Implementation in Trusted Execution Environments
- Using non-stationary cameras (e.g., smart cars)



AI FLANDERS  
BUILDING OUR DIGITAL FUTURE

WWW.FLANDERSAIRESARCH.BE

imec IDLab  
INTERNET & DATA LAB

