

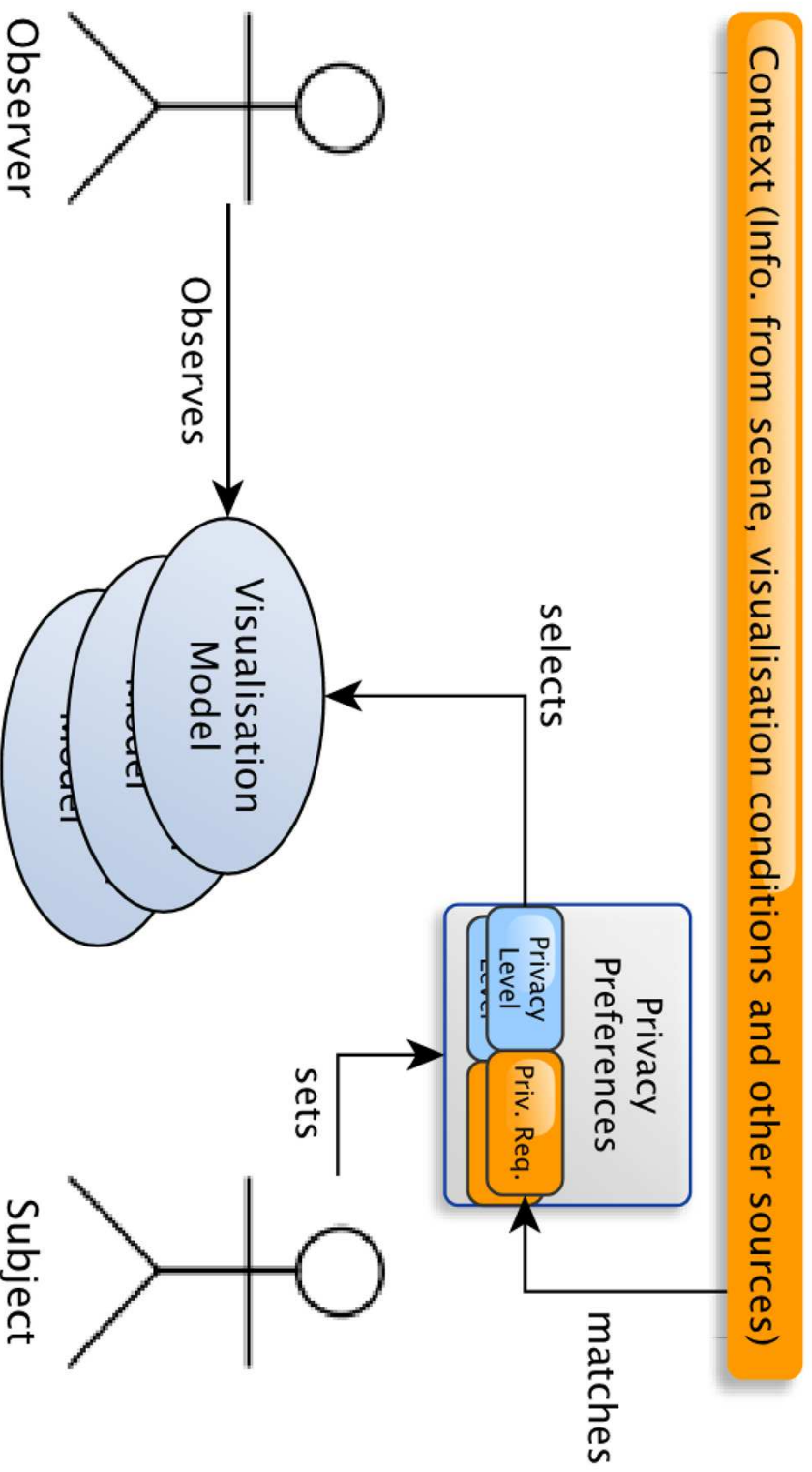
Privacy preservation in video-based AAL applications

ESR 13. Siddharth Ravi, University of Alicante

Problem Statement

- There is a need for visual data to be used for services where remote caregivers need to observe the scene
- Visual data exposes a lot of information about individuals appearing on images and videos
- There is a privacy / utility trade-off for the AAL services
- This project works on advancing a privacy by context approach.
 - Creating different privacy preserving visualizations.
 - Depending on the context of capture (Identity, appearance, location, etc) and the nature of access privilege of observer.

- Research is embedded in a higher-level structure -
 - Creating end-to-end contextual privacy preservation pipelines (ESR 14)
 - Studying the perceptions and effects of the imparted privacy (ESR 15)

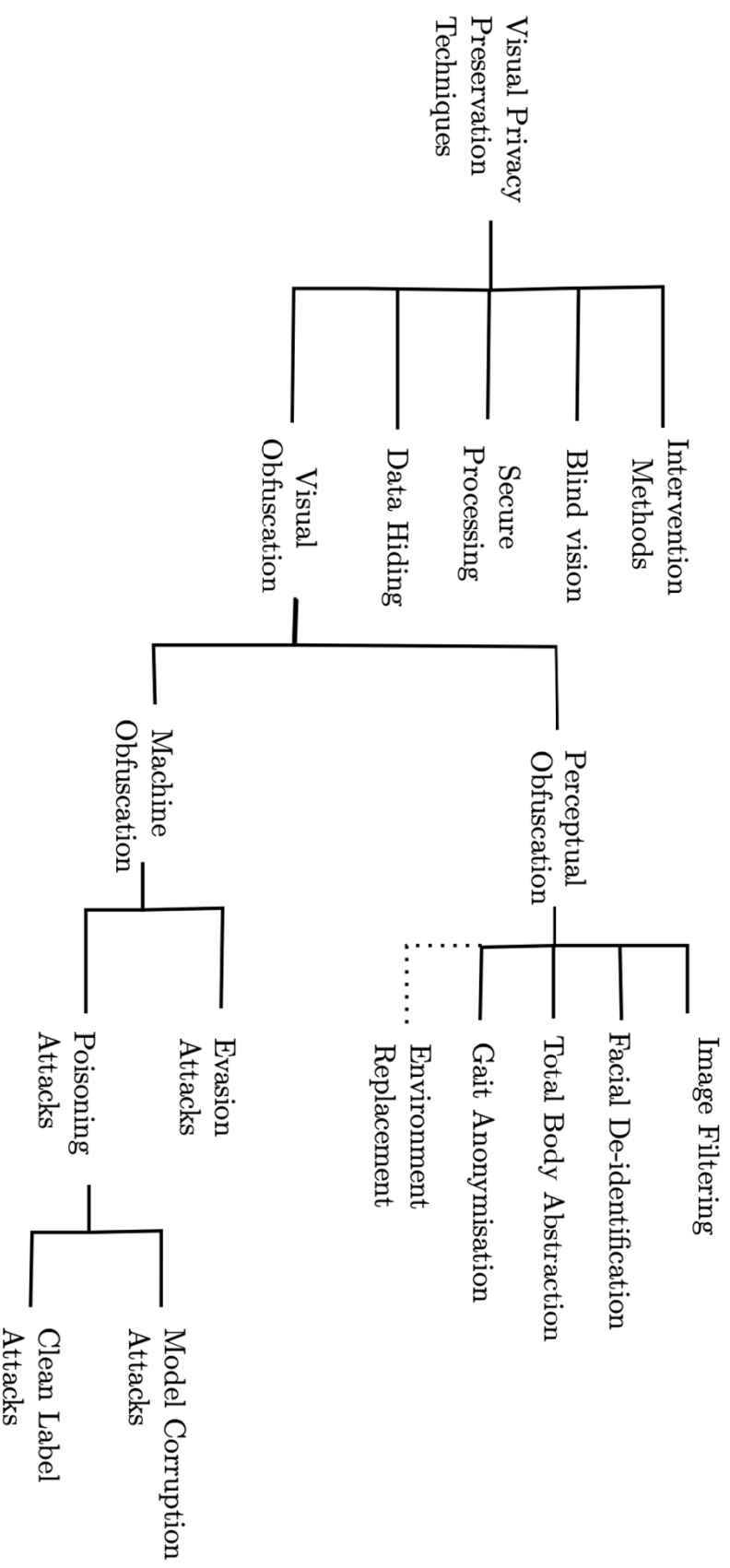




Research Conducted

- Completed a comprehensive review of the state of the art in visual privacy preservation methods
- Proposed a taxonomy with which to classify the state of the art methods
- Connected the proposed low-level taxonomy of visual privacy preservation to a high-level taxonomy created by Mihailidis and Colonna (2019) for categorizing privacy by design.

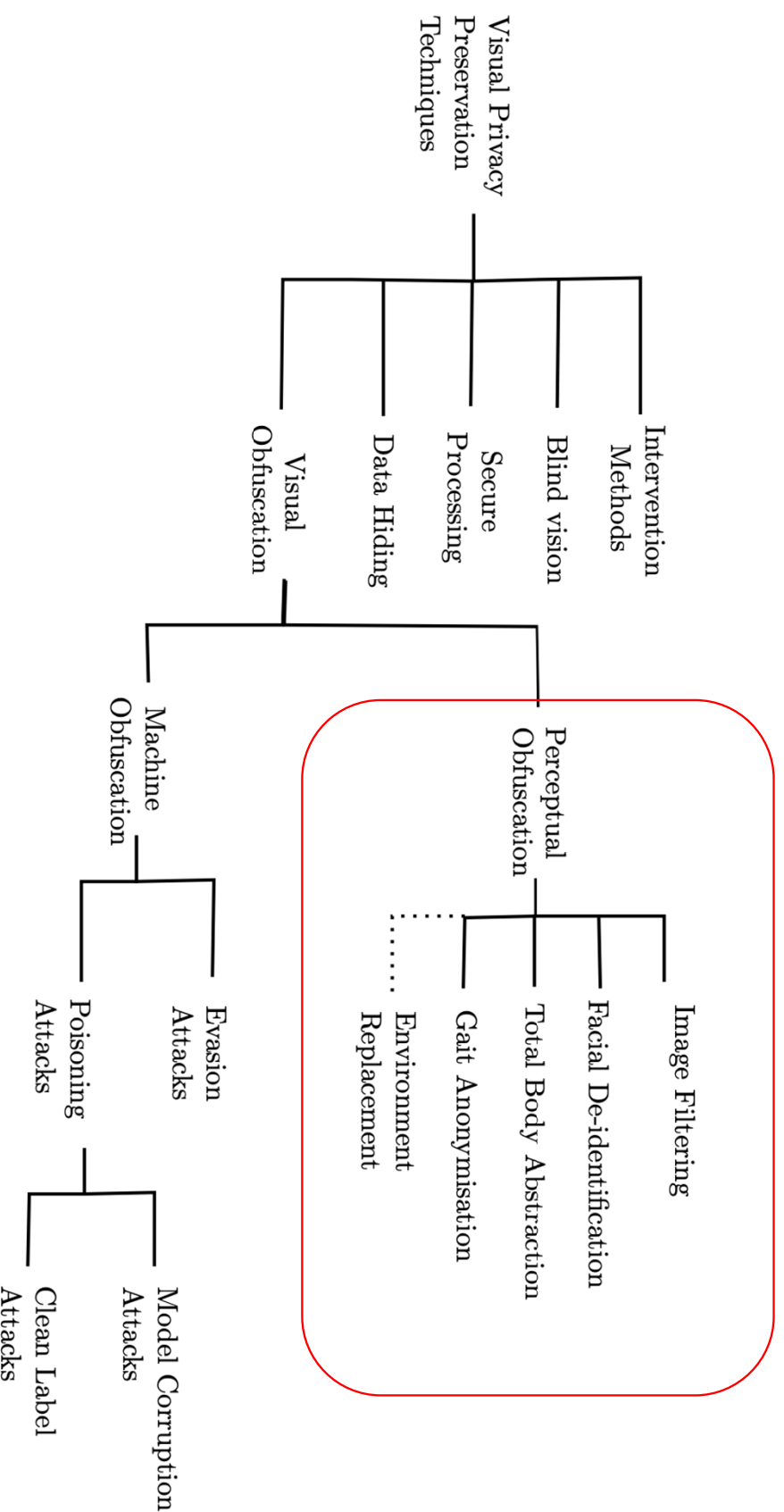
A Low-level Taxonomy of Methods

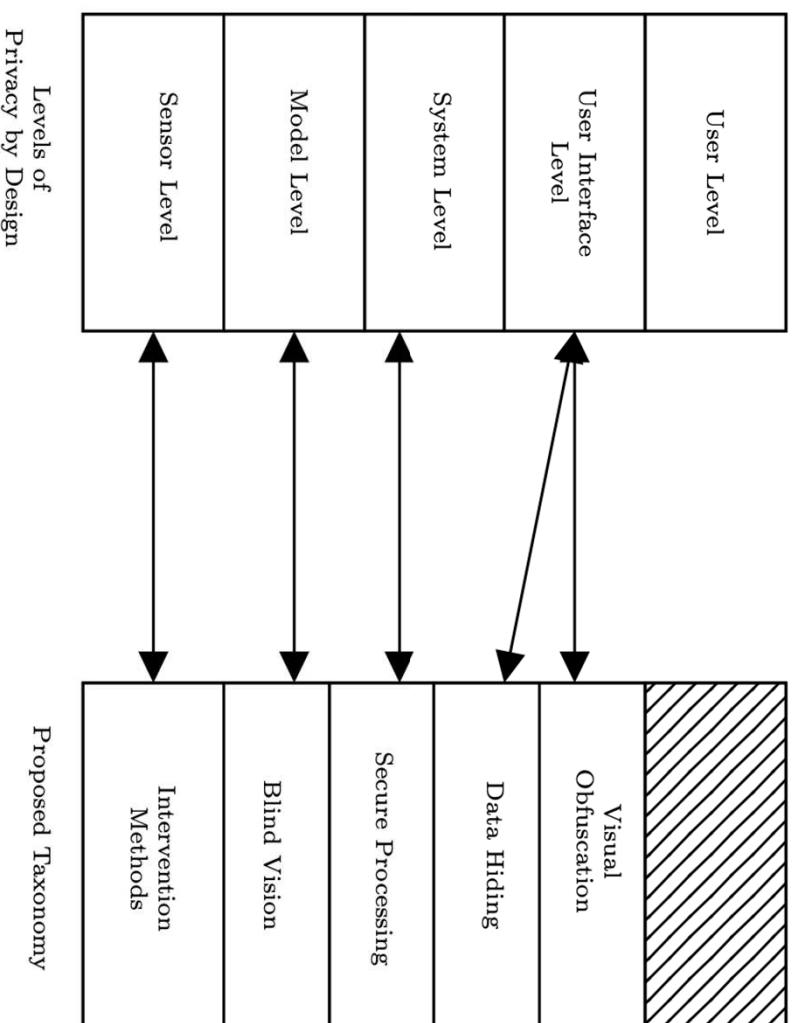


- Intervention methods prevent collection of information at sensor level.
- Blind vision - Uses Secure multiparty computation cryptography techniques hide data and algorithms from providers of each.
- Secure Processing – similar to blind vision, but without using secure multiparty computation.
- Data Hiding - schemes through which sensitive attributes can be privately hidden/embedded in the image itself.



1. A Low-level Taxonomy of Visual Privacy Preservation Techniques







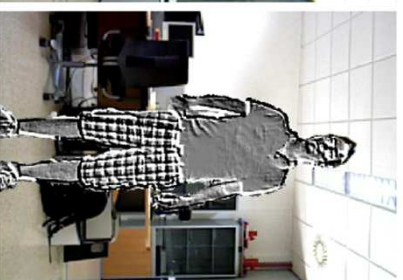
Original



Pixelate



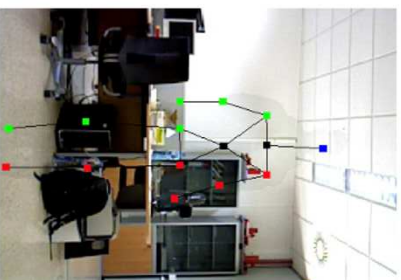
Blur



Emboss



Silhouette



Skeleton

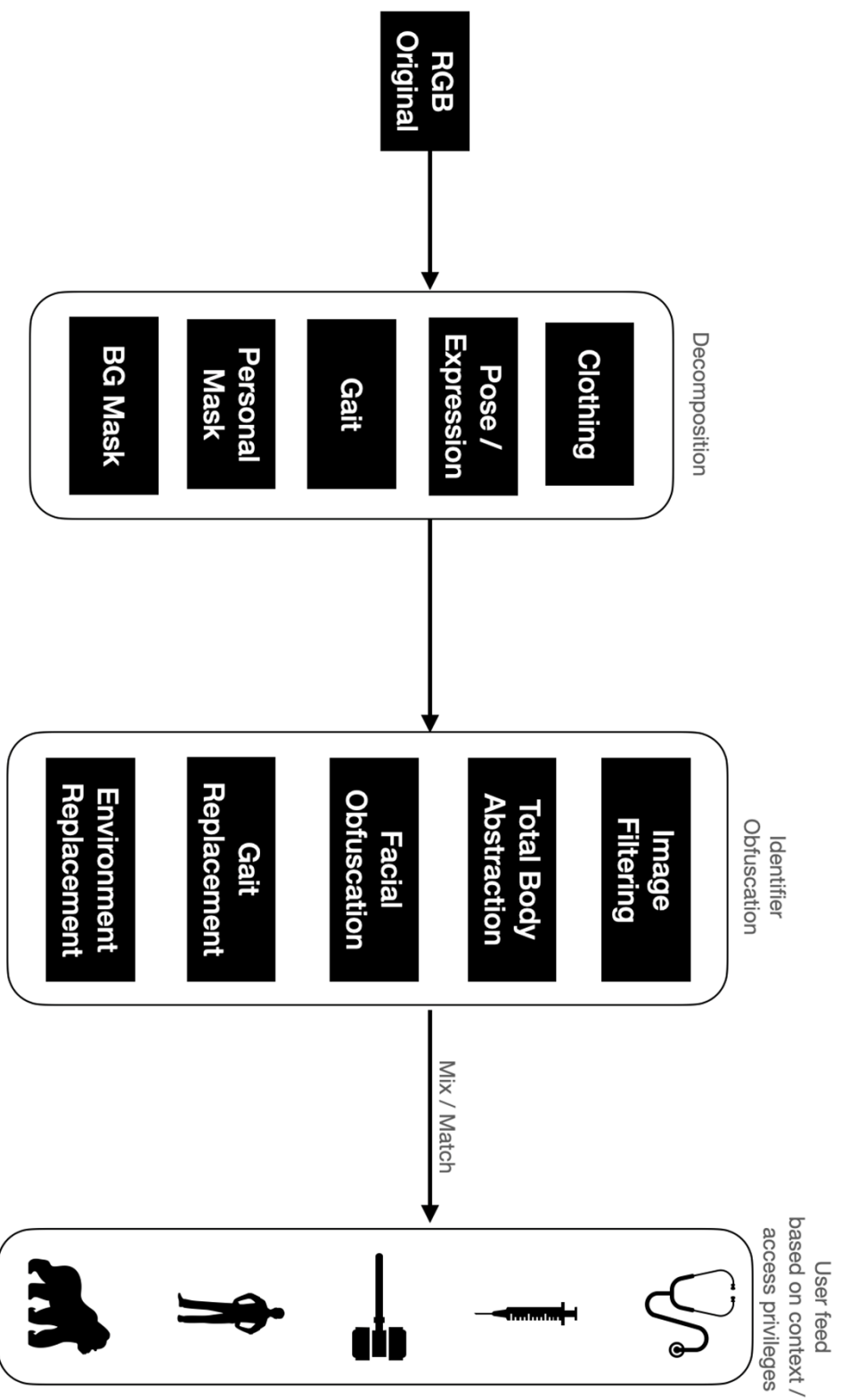


Avatar



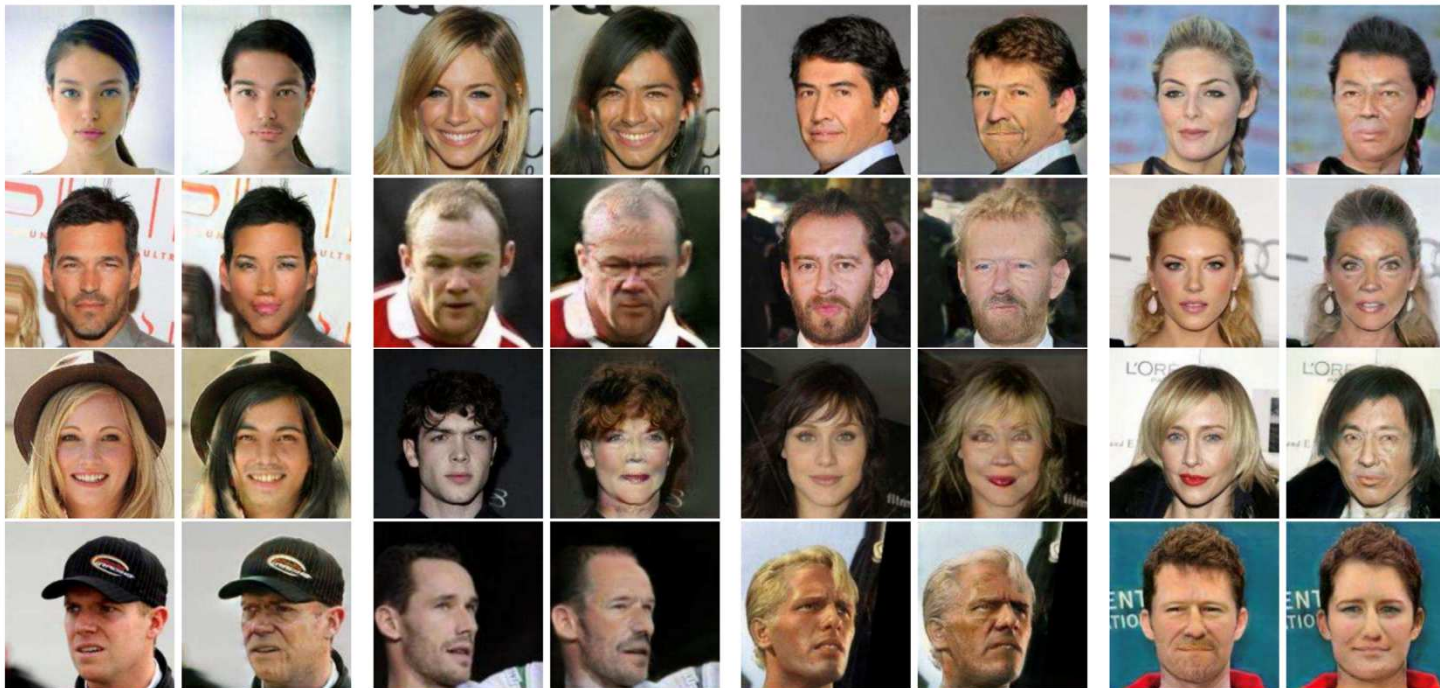
Invisibility

Privacy Preservation Pipeline





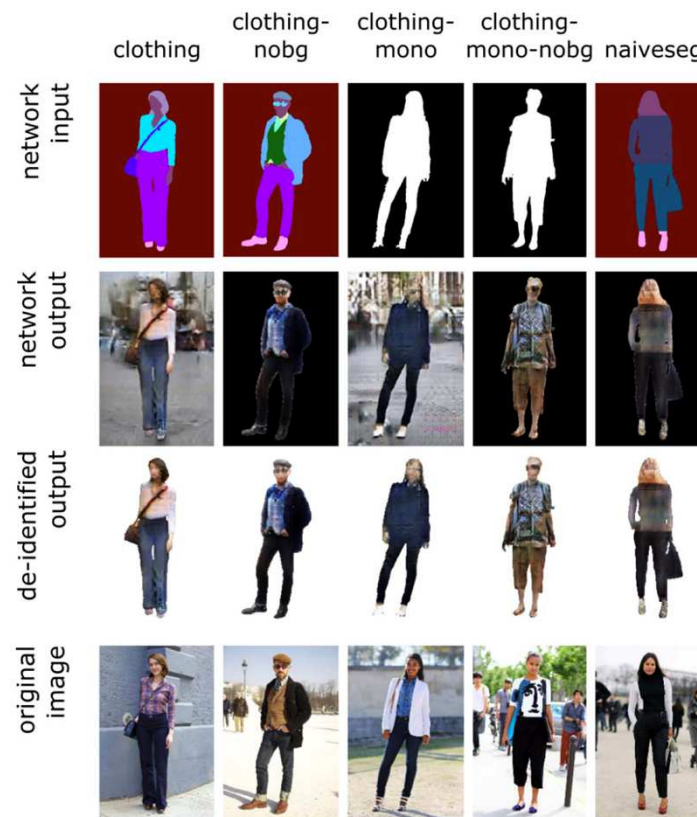
Li, T., Lin, L., 2019. AnonymousNet: Natural face de-identification with measurable privacy, in: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops



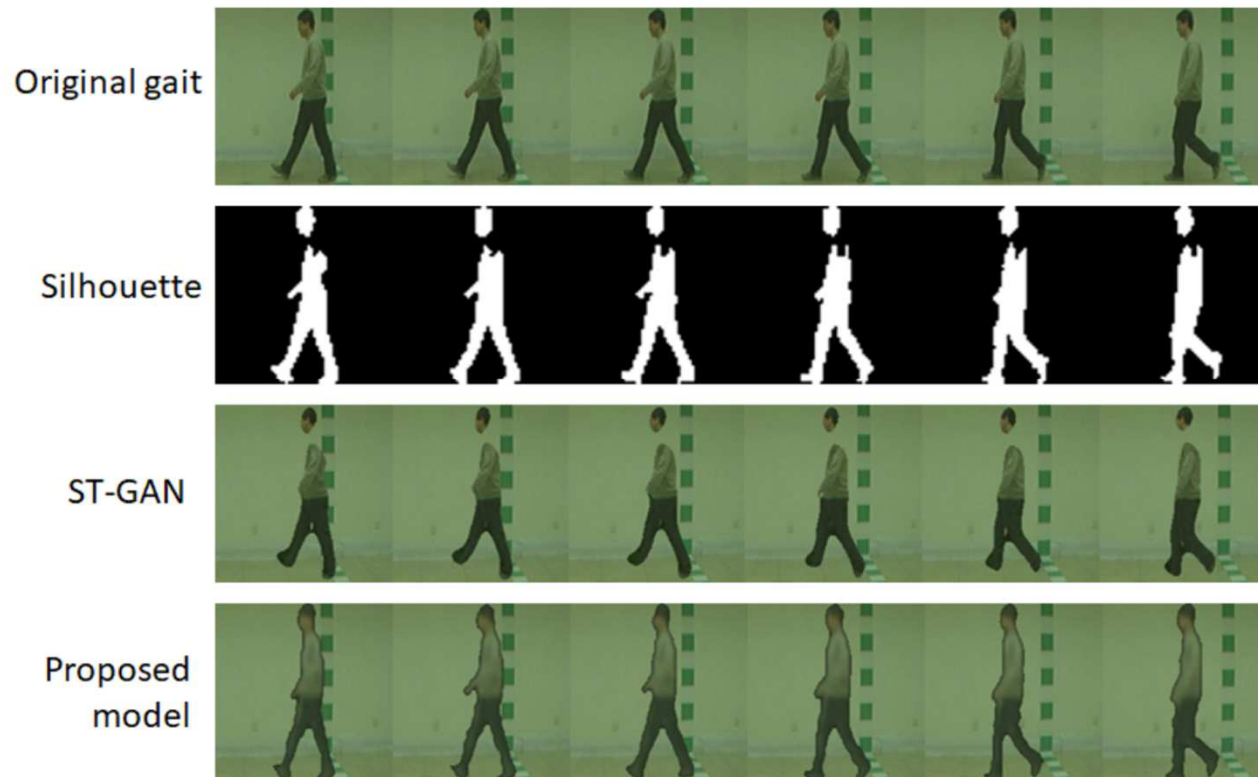
Total Body Abstraction

15

Brkic, K., Sikiric, I., Kalafatic, Z., 2017. I Know That Person: Generative Full Body and Face De-identification of People in Images, in: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops



Tieu, N.D.T., 2019. An RGB gait anonymization model for low-quality silhouettes, in: 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2019.



2. Fairness of visual privacy preservation methods

17

- Collaborated with ESR11 for a study of the fairness of various visual privacy preservation methods
- Studied the impact that obfuscation algorithms such as blurring and pixelation have on protecting the identity along the lines of races and gender.



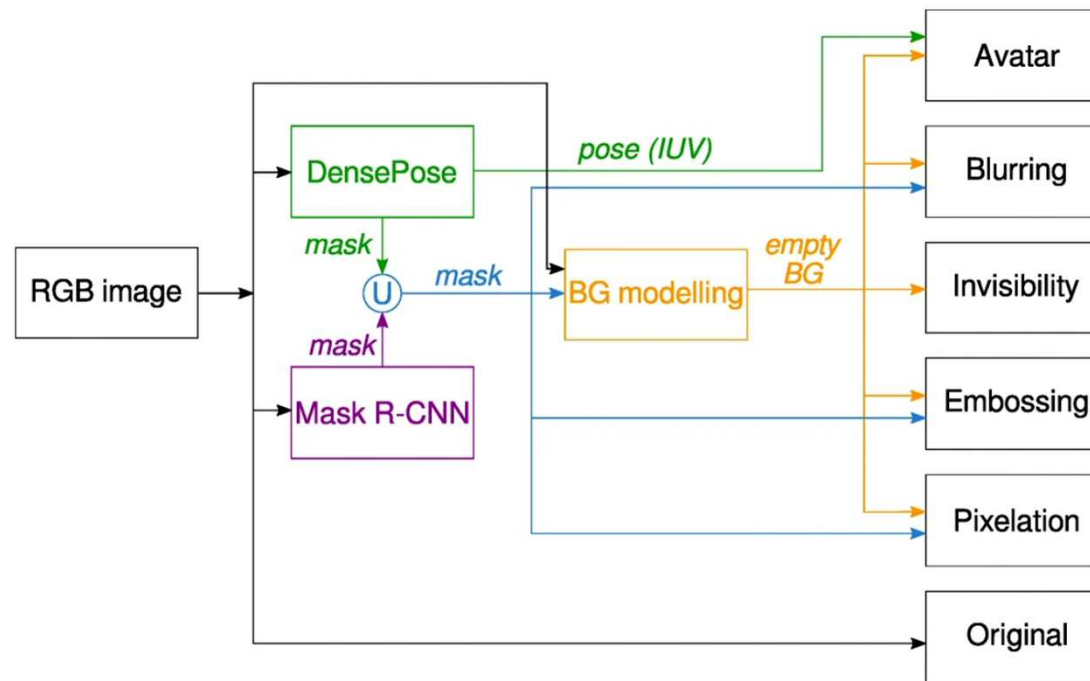
Current Work

- Most privacy preservation methods work on standard RGB images.
- Disadvantages – Occlusions, obtrusive
- Omnidirectional cameras can be preferable, but machine learning models cannot be used for privacy preservation.
- Dataset that synchronizes various cameras and wearable devices (kinects, an omnidirectional camera, an egocentric camera, an empathica wearable device).
- Created a test set for development, worked on the pipeline and setup for recording.

Privacy Preservation with Omnidirectional images



Steganography based data hiding for reversible obfuscation inside a monitoring pipeline



Securely private broadcasting of images obfuscated using a cycleGAN-based domain translation.

- Using GANs to learn a cyclical transformation from normal images to a target optimally blurred image and back
- Embedding targeted noise to create a secure one-to-one mapping between encoder and decoder.



Future Work

- Post constructing the dataset – creating reversible context-based obfuscation algorithms to operate on visuals from omnidirectional cameras.
- Creating a framework for a fair and private image obfuscation.
- Creating privacy metrics through analysis from a legal perspective (secondment, Stockholm University)
- Analysing the effects of visual privacy preservation from a sociological perspective.
- Also been accepted to a startup incubator program

Thank you!

Siddharth Ravi

University of Alicante

Siddharth.ravi@ua.es