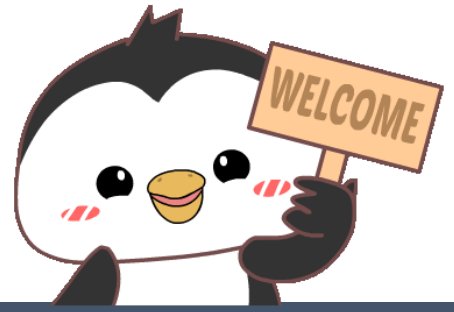
南京航空航天大學
NANJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS



Vision Access Control In Facial Identity Protection

Tao Wang

Why Protect Facial Identity?

➢ **Facial images are extensively collected and disseminated.**

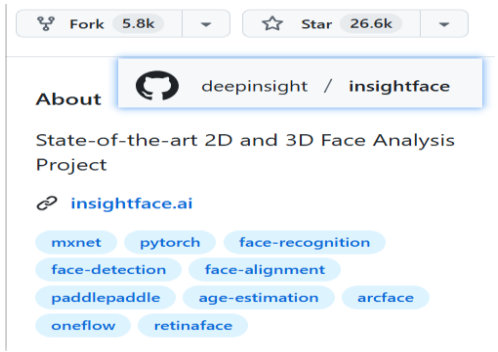
Electronic Payments

Video Surveillance

Social Photo Sharing

➢ **Deep learing-based face recognition (FR) is highly accurate and widely accessible.**

- **InsightFace** open-sourced various advanced FR models, e.g., ArcFace.
- Leading companies also open up their available APIs, e.g., **Face++**



➢ **Anyone can use FR tools to obtain facial identity without authorization.**

- Facial identity is **immutable**; once leaked by unauthorized FR, it remains leaked for life.

Location tracking

Identity fraud

Limitations of Traditional Methods

➢ **Traditional methods obscure the visual content of facial features for identity protection.**

Blurred Pixelated Masked

Limitation 1: Low Visual Naturalness-> Susceptible to Attacks

- Poor visual quality can **easily attract the attention** of adversaries
- Distinguishable visual effects also **reveal the purpose** of privacy protection.

Then, adversaries can leverage various forms of background knowledge to **infer the original identity**.

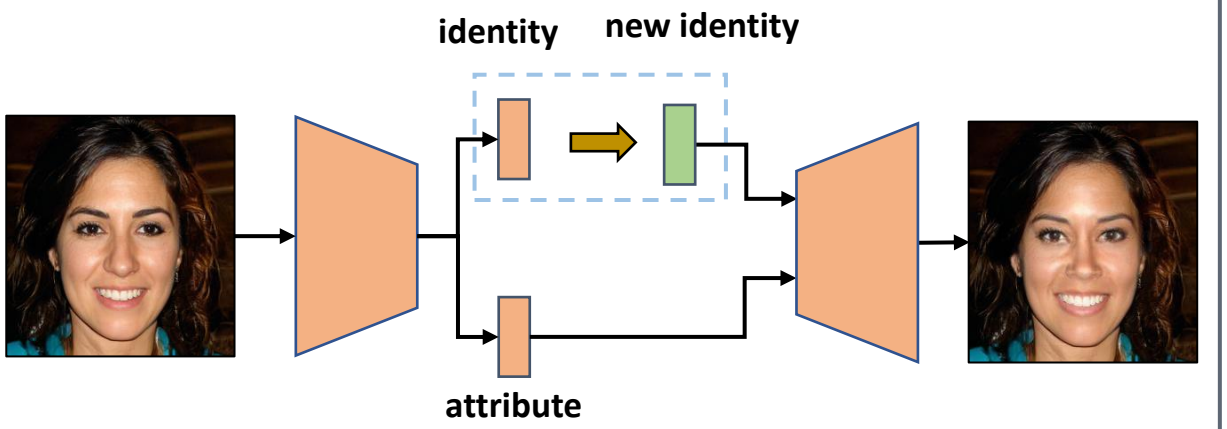
Limitation 2: Low Visual Utility

- The post-processing degradation of facial images undermines their effectiveness for **face detection and attribute recognition tasks**

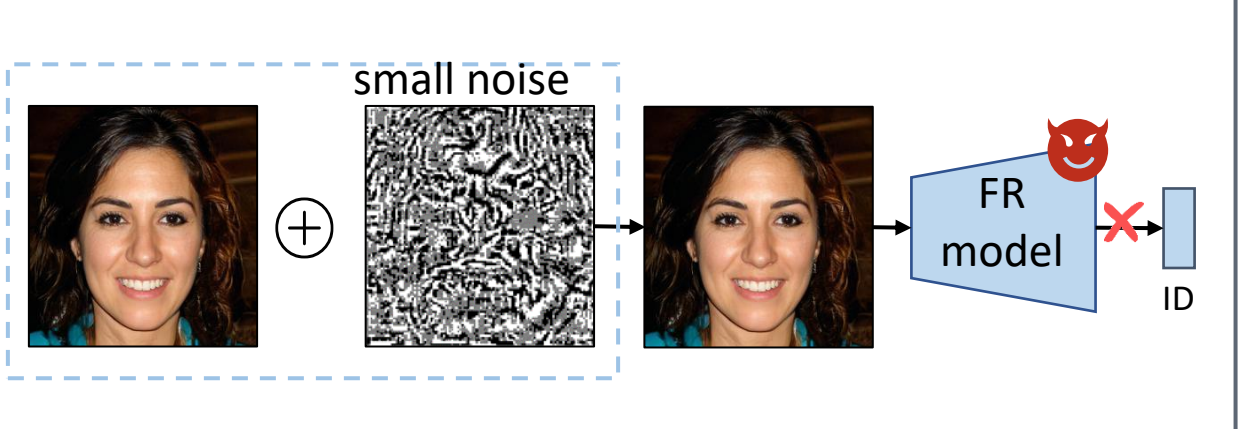
Advanced Methods

Advanced methods overcome two major limitations of traditional methods and can be categorized into two classes:

- **Synthesis-based Method**: Such methods generate a face with a new identity to replace the original face, thus removing the original identity.
- **Perturbation-based Method**: Such methods add quasi-imperceptible noise to disturb the judgment of Face Recognition (FR) models, thus concealing the original identity.



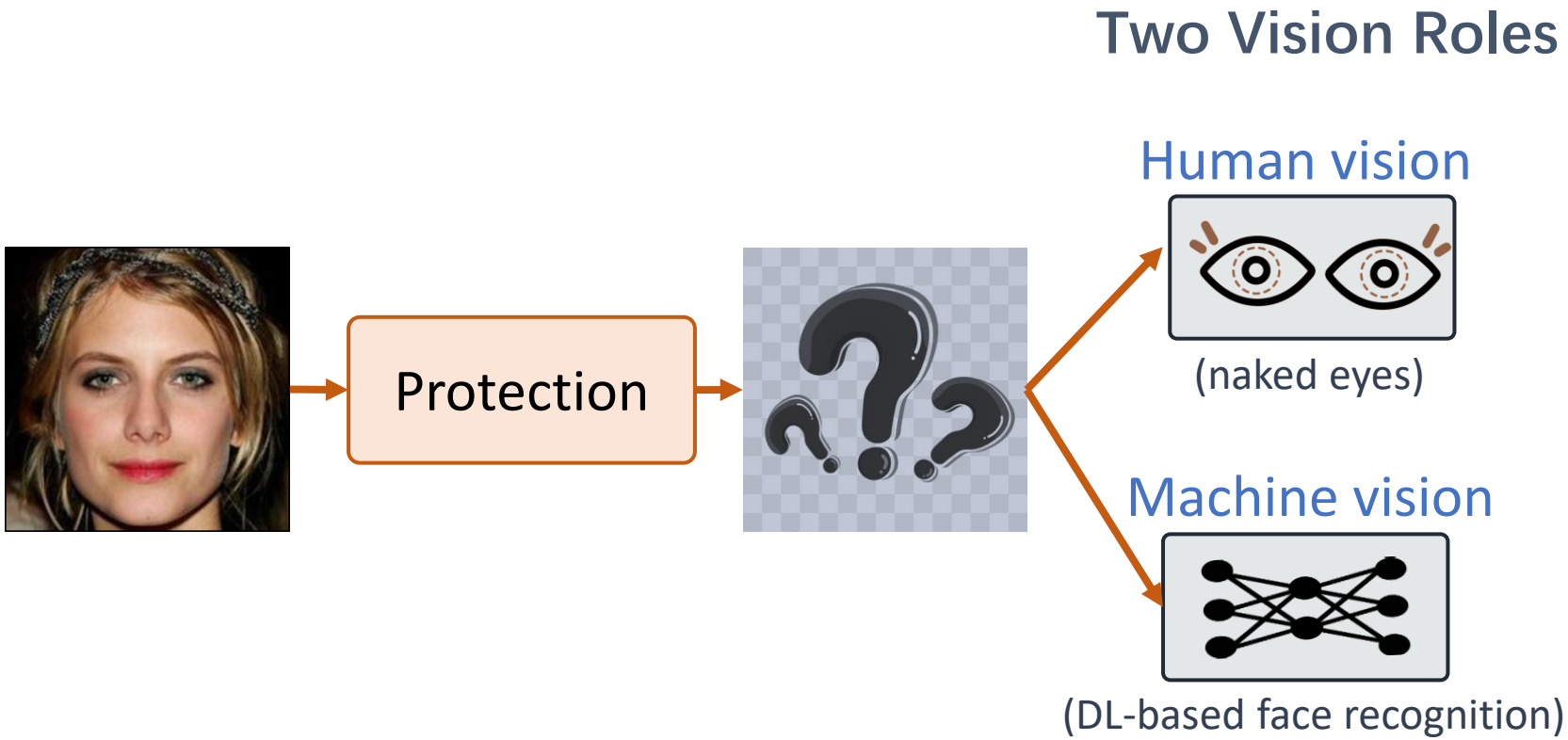
Synthesis-based Method



Perturbation-based Method

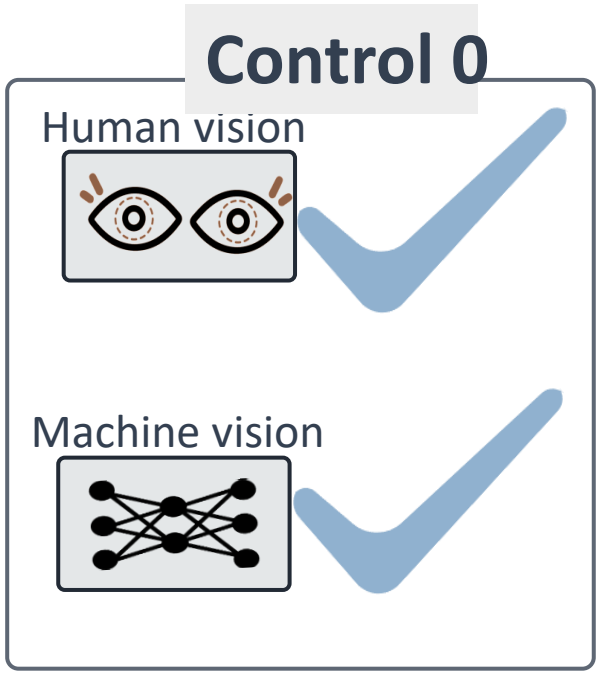
Vision Access Control in Facial Identity Protection

Who can access the real facial identity?

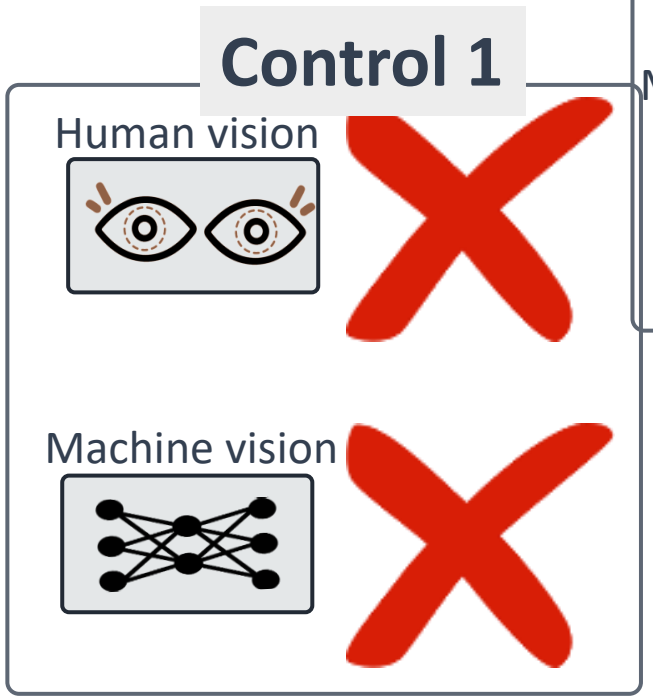


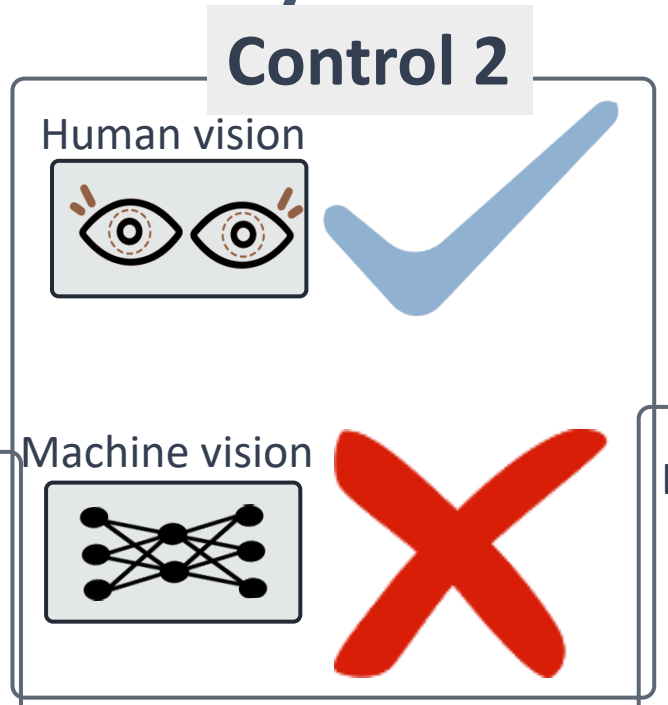
Vision Access Control in Facial Identity Protection

Who can access the real facial identity?

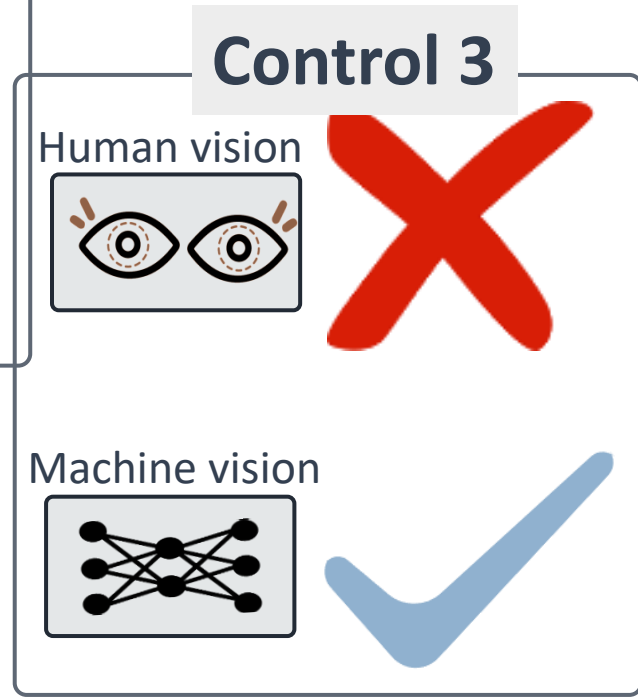


Original Version





Protected Version



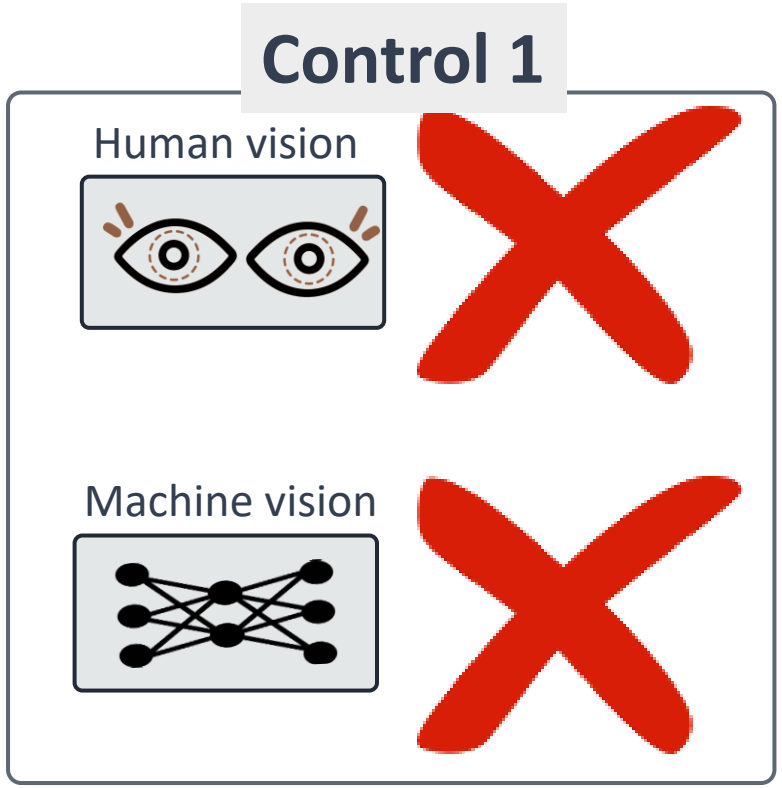
Vision Access Control in Facial Identity Protection

Control 1

With two Limitations

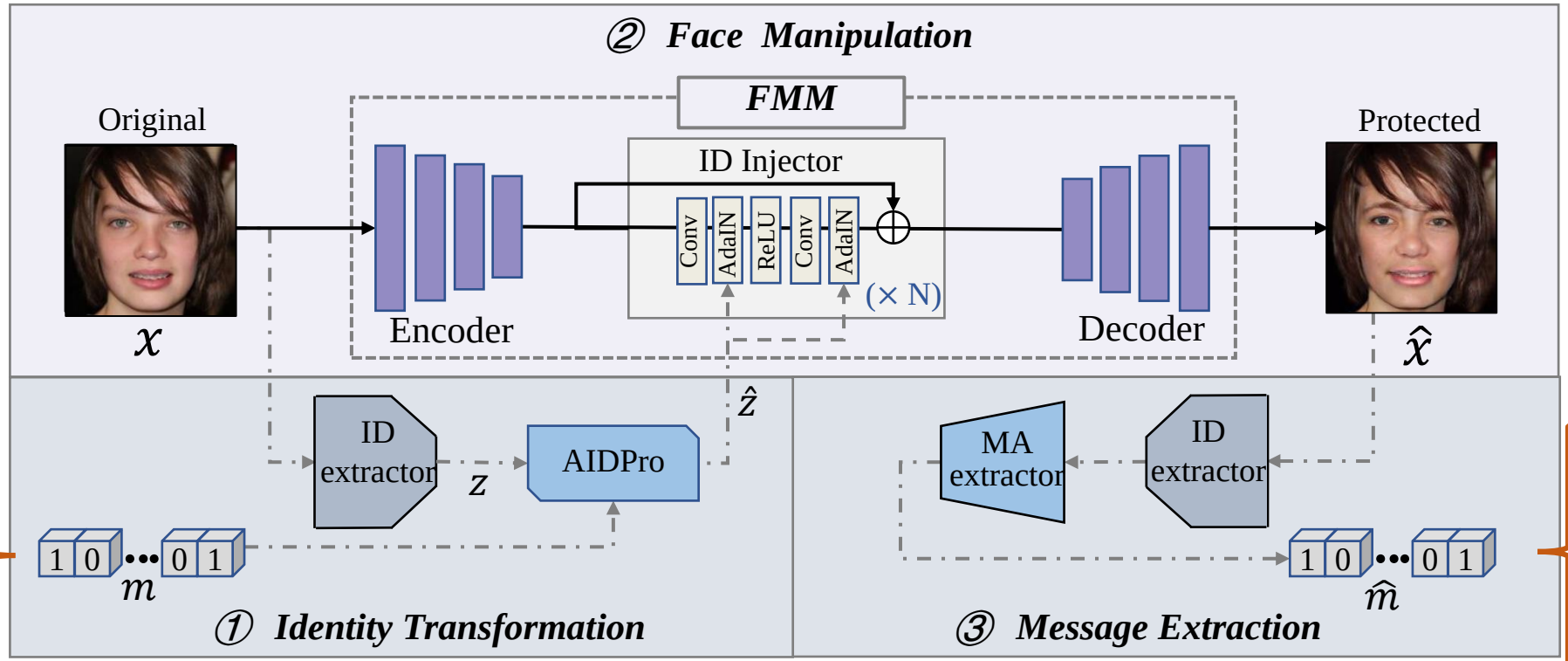
Traditional Method

Synthesis-based Method



Our Work 1

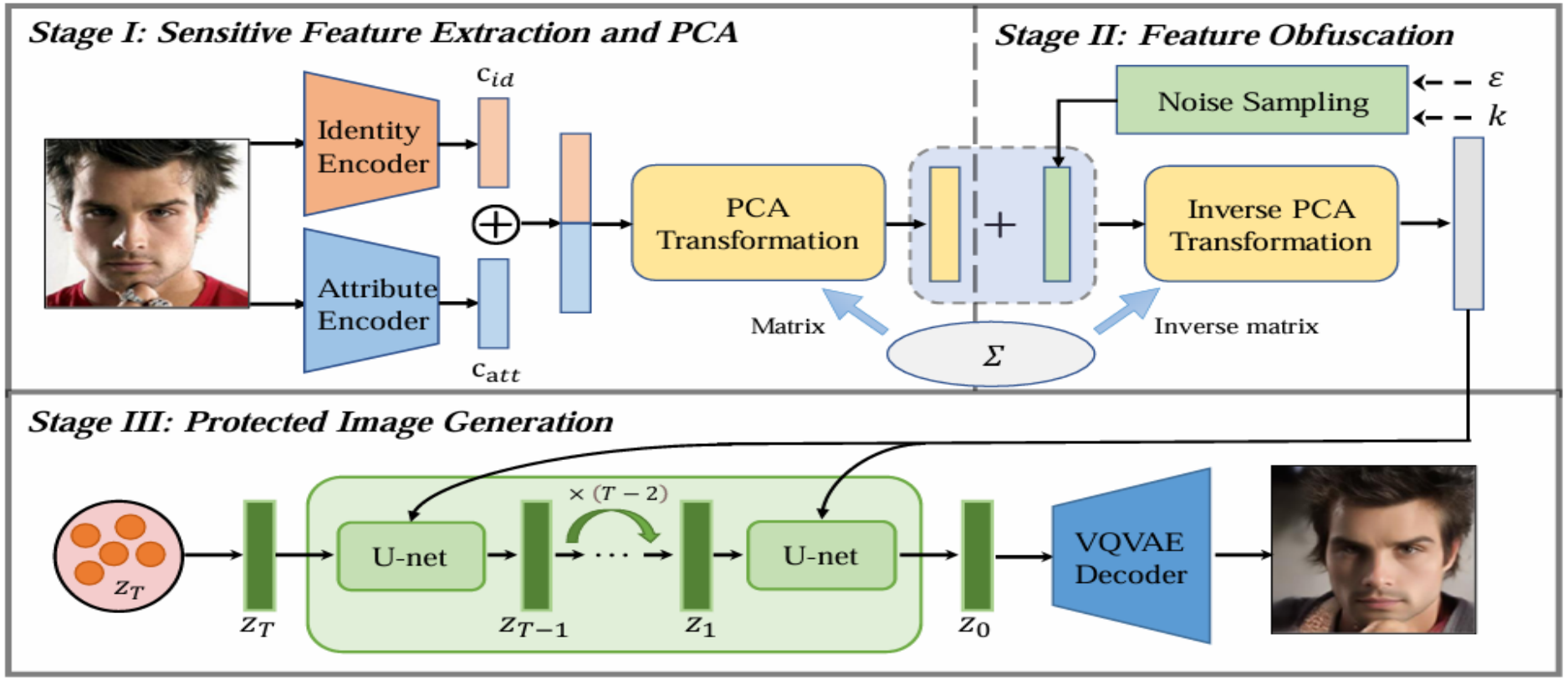
Control 1 Inserting a usable message in a robust way, while synthesizing a new face for privacy protection.



[2025 IEEE TIFS] **Tao Wang**, Wenying Weng*, Xiangli Xiao, et al. Beyond Privacy: Generating Privacy-Preserving Faces Supporting Robust Image Authentication. *IEEE Transactions on Information Forensics and Security*

Our Work 1

Control 1 Introducing a improved differential privacy mechanism, while synthesizing a new face for privacy protection.

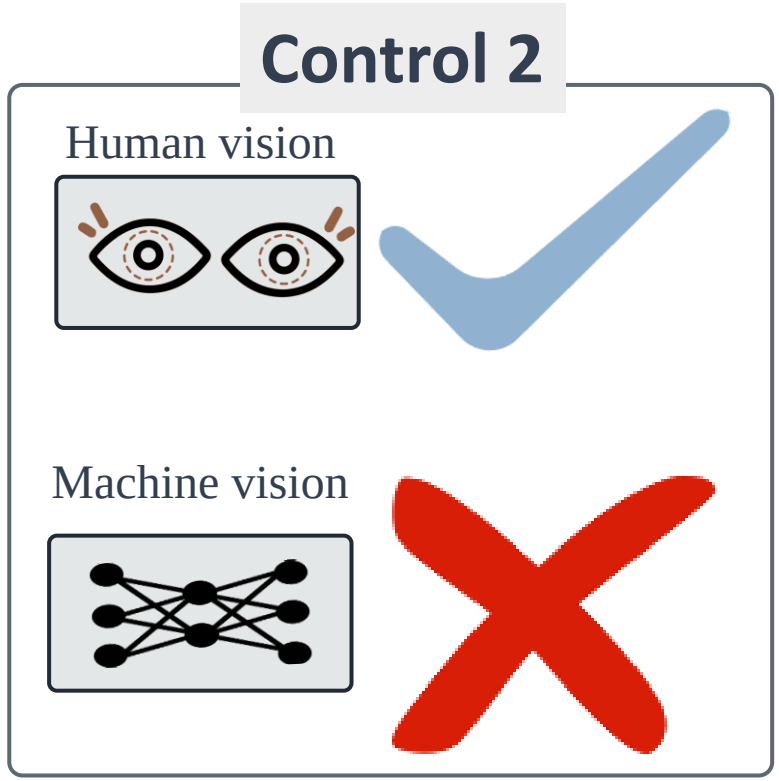


[2025 IEEE TPAMI] Yushu Zhang, Junhao Ji*, **Tao Wang**, et al. Make Identity Indistinguishable: Utility-Preserving Face Dataset Publication with Provable Privacy Guarantees. *IEEE Transactions on Pattern Analysis and Machine Intelligence*

Vision Access Control in Facial Identity Protection

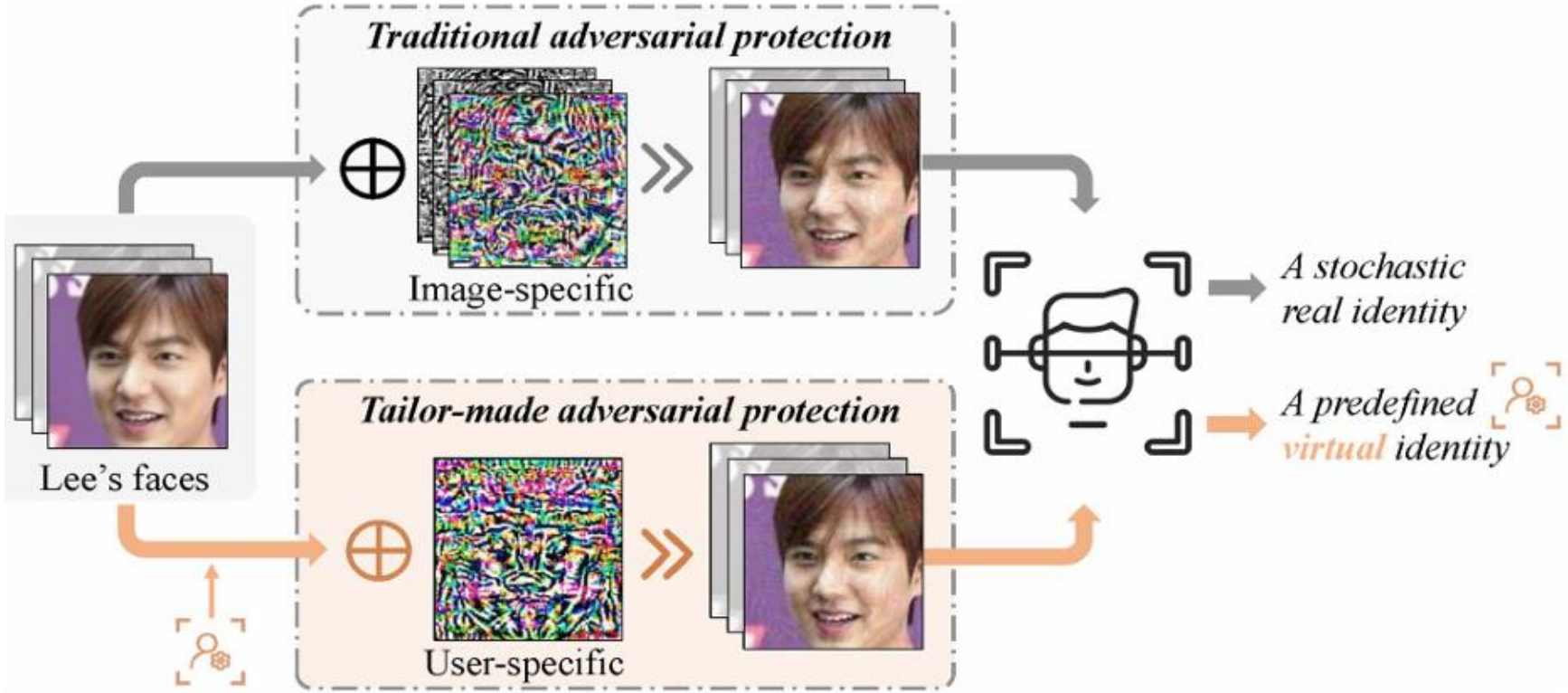
Control 2

Perturbation-based Method



Our Work 2

Control 2 Generate a user-specific (not image-specific) perturbation to conceal identity for machine vision, link to a predefined identity

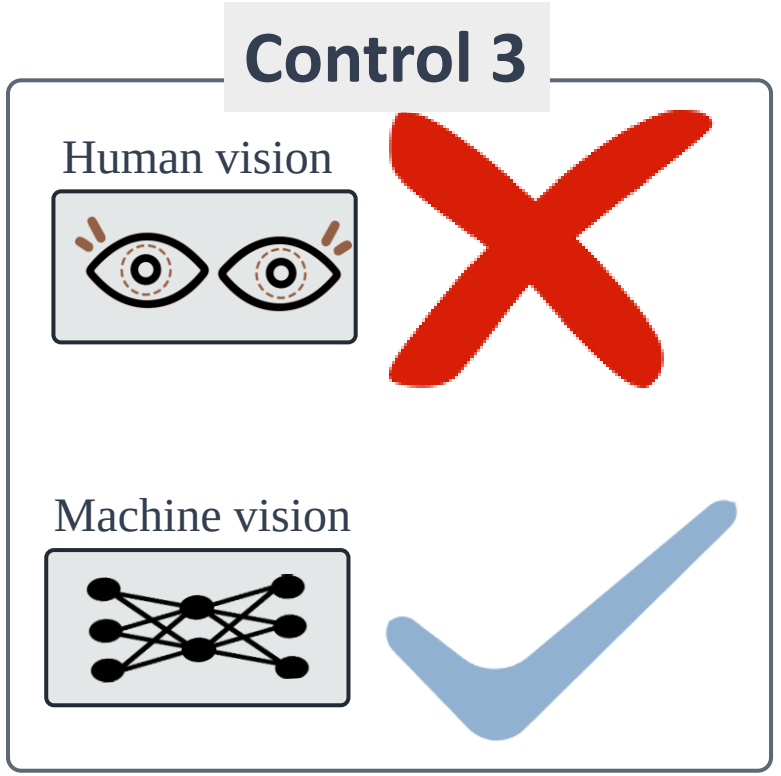


[2025 IEEE TDSC] Yushu Zhang, Zixuan Yang, **Tao Wang***, et al. Tailor-made Face Privacy Protection via Class-wise Targeted Universal Adversarial Perturbations. *IEEE Transactions on Dependable and Secure Computing*

Vision Access Control in Facial Identity Protection

Control 3

Our work: Identity Hider

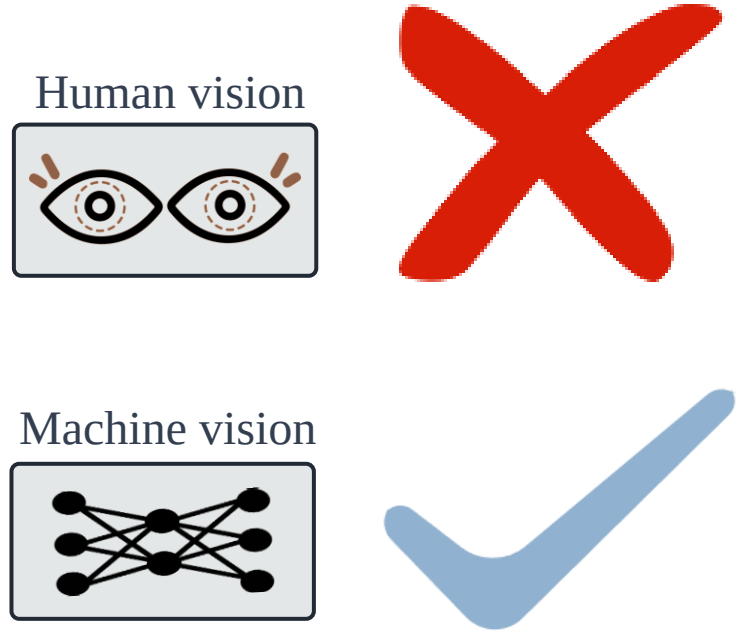


Attention!

Unlike **privacy-preserving face recognition (PPFR)**, the results they generate lack naturalness and visual utility.

With two Limitations

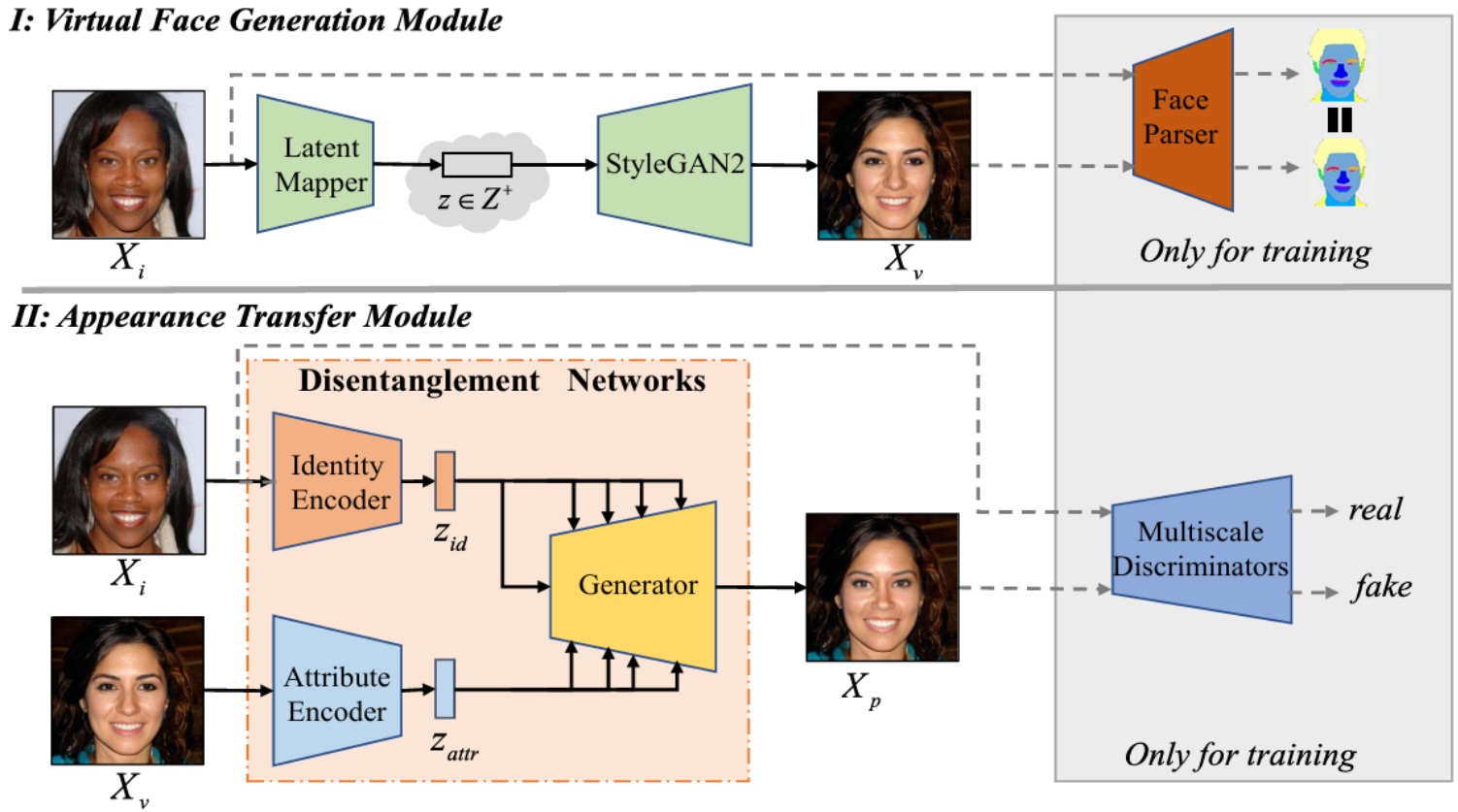
Privacy-preserving face recognition



[2024 ACM MM] Zixuan Yang, Yushu Zhang*, **Tao Wang**, et al. Once-for-all: Efficient Visual Face Privacy Protection via Person-specific Veils. *ACM International Conference on Multimedia*

Our Work 3

Control 3 Generate a virtual appearance and replace the original appearance, concealing identity for human vision

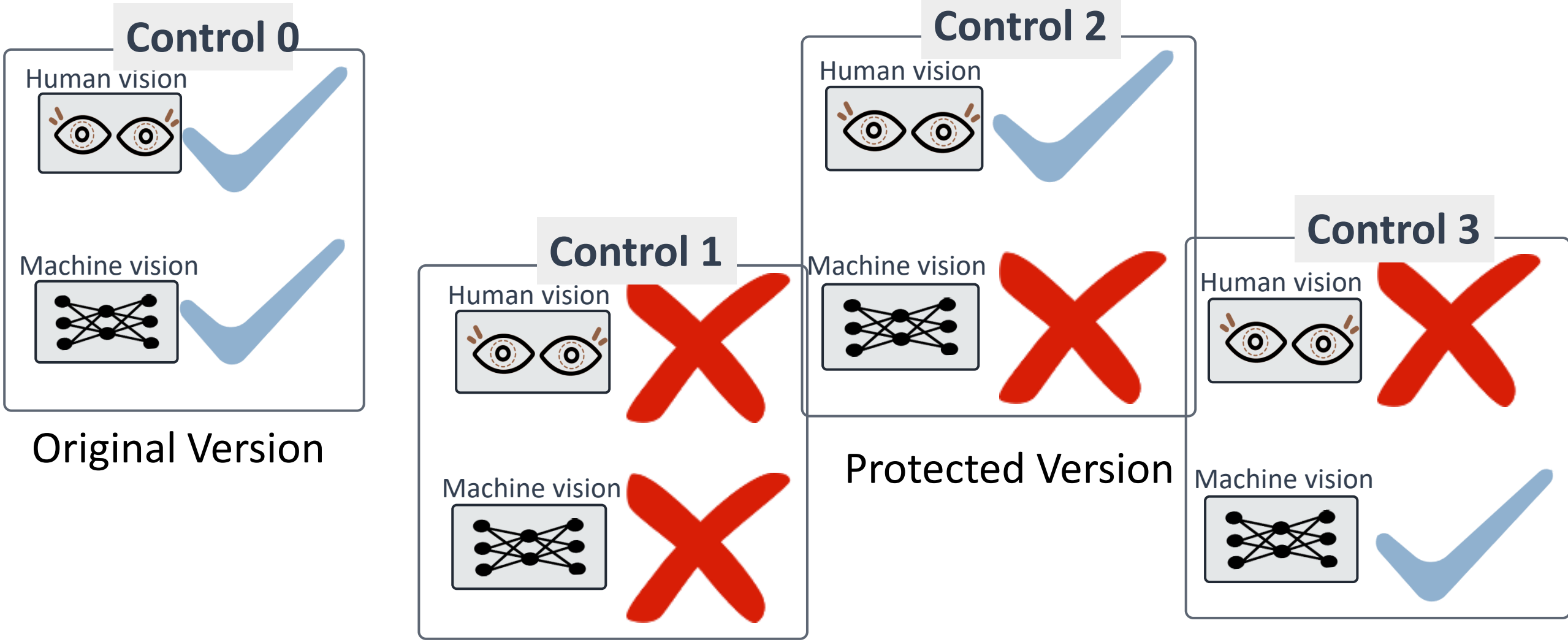


(keep a similar semantic maps to preserve visual utility)

[2025 IEEE TBIOM] Tao Wang, Yushu Zhang*, Zixuan Yang, et al. Seeing is not Believing: An Identity Hider for Human Vision Privacy Protection. *IEEE Transactions on Biometrics, Behavior, and Identity Science*

Sub-Summary

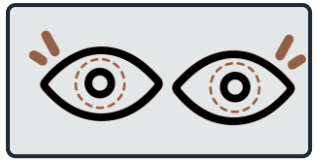
Who can access the real facial identity?



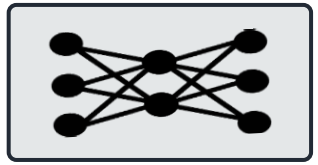
Thought

Are there any other options for access control?

Human vision

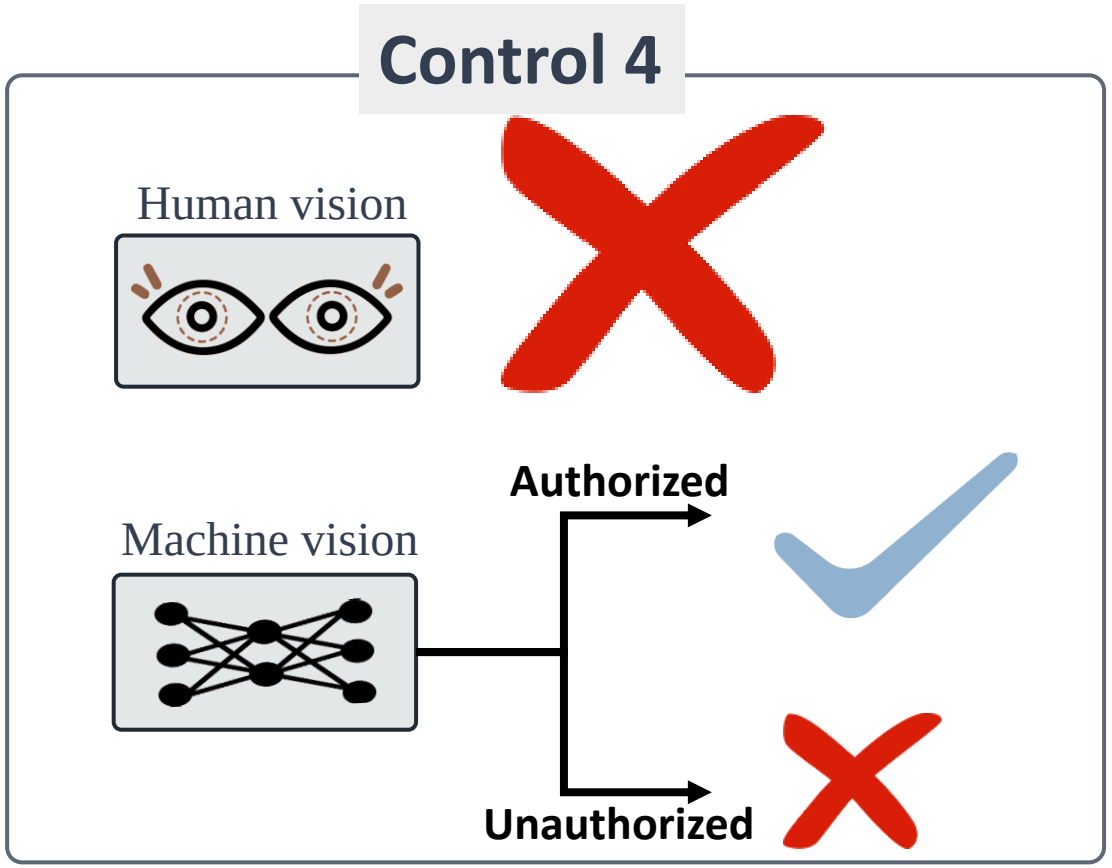


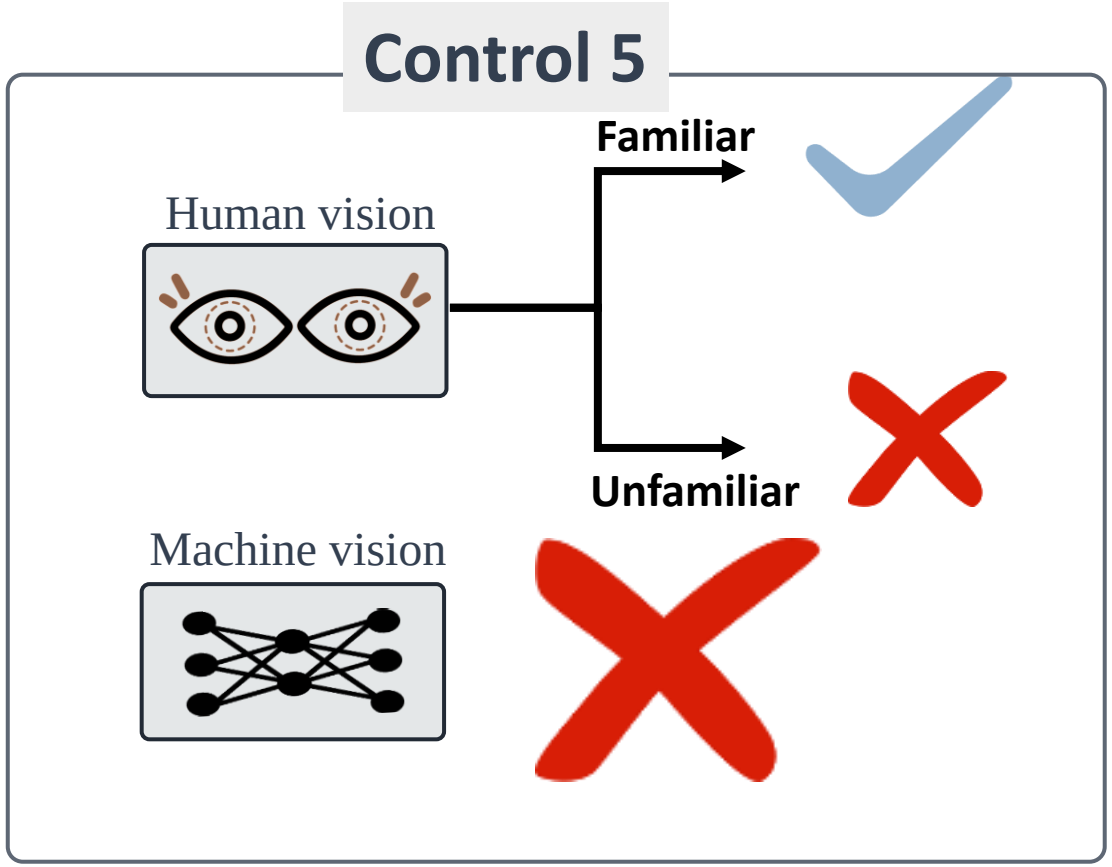
Machine vision



Vision Access Control in Facial Identity Protection

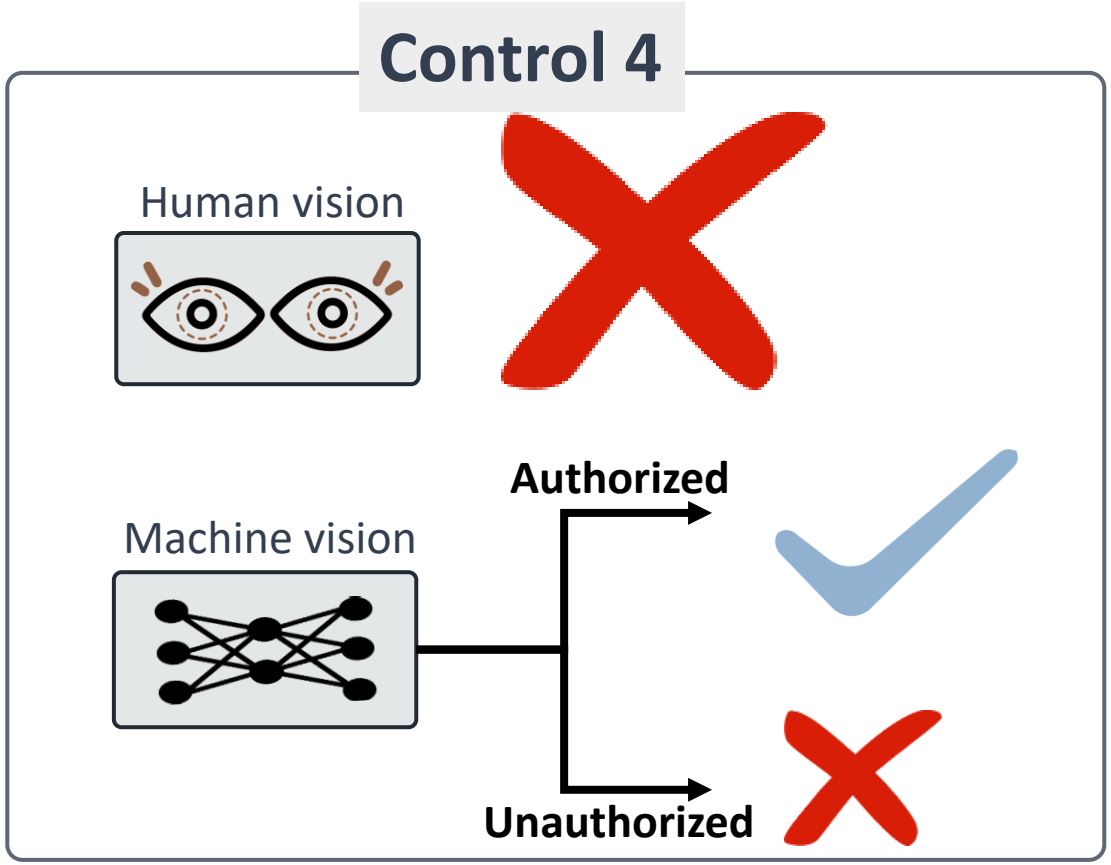
Who can access the real facial identity?





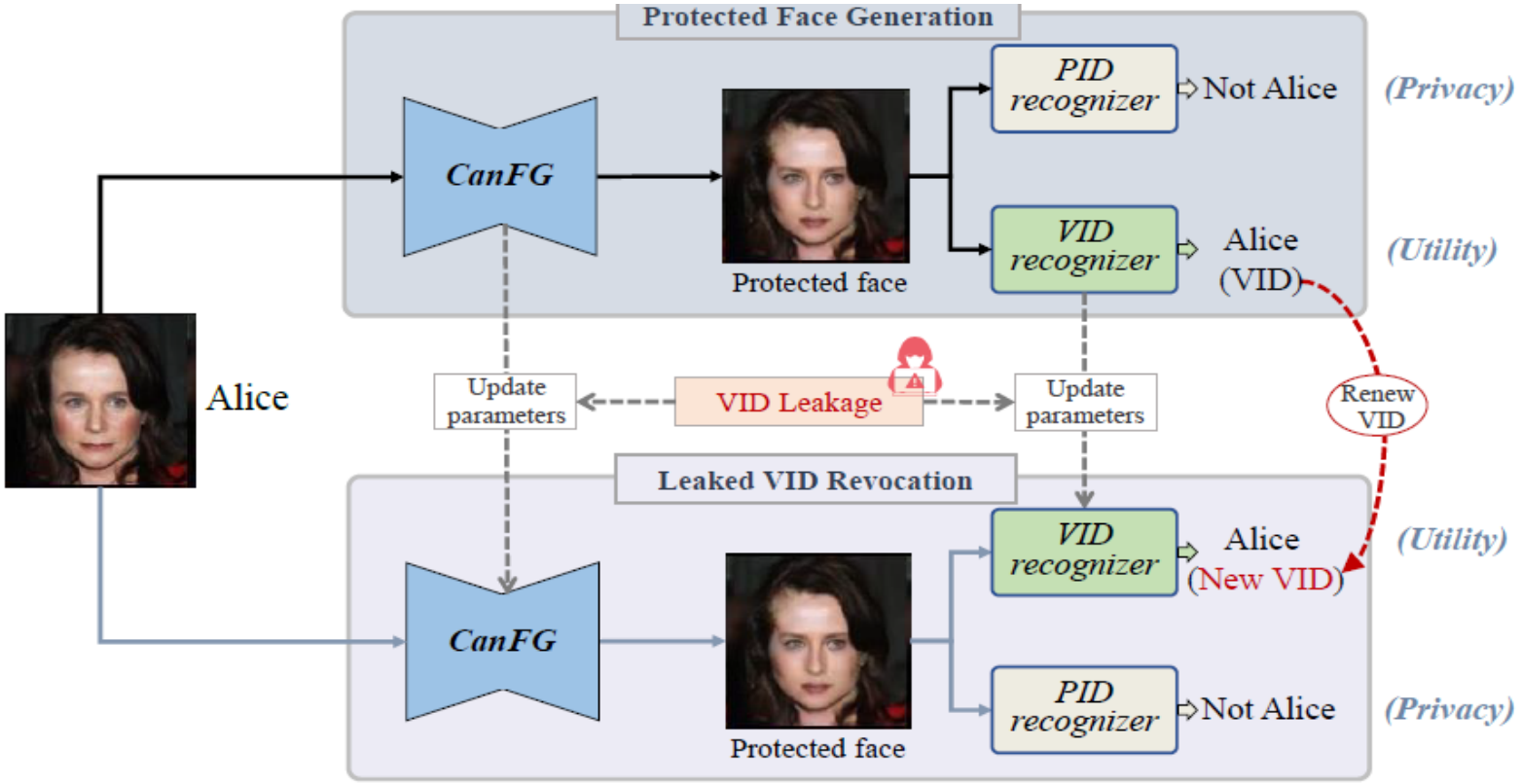
Vision Access Control in Facial Identity Protection

Who can access the real facial identity?



Our Work 4

Control 4 Embedding virtual identity for cancelable FR (only the right recognizer can extract), while synthesizing a new face



[2024 ACM MM] **Tao Wang**, Yushu Zhang*, Xiangli Xiao, et al. Make Privacy Renewable! Generating Privacy-Preserving Faces Supporting Cancelable Biometric Recognition. *ACM International Conference on Multimedia*

Our Work 4

[2024 ACM MM] **Tao Wang**, Yushu Zhang*, Xiangli Xiao, et al. Make Privacy Renewable! Generating Privacy-Preserving Faces Supporting Cancelable Biometric Recognition. *ACM International Conference on Multimedia*

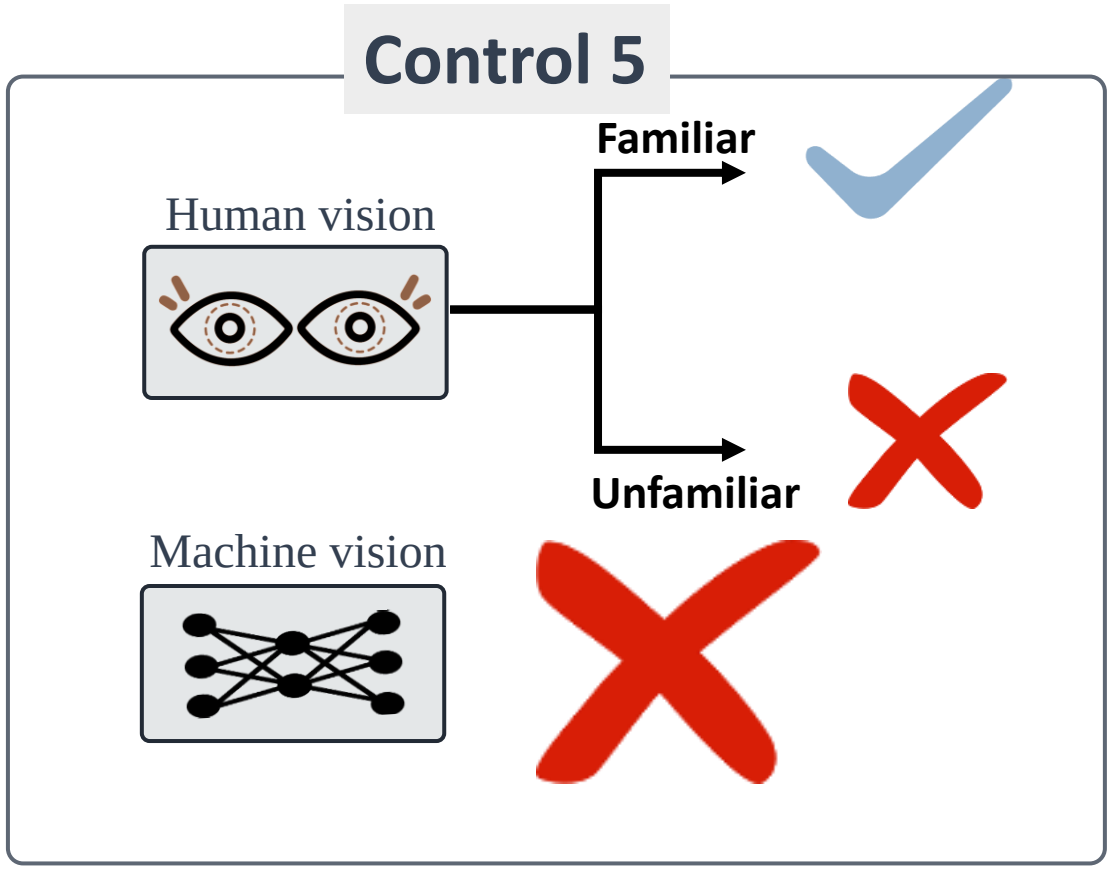
This work is also the first to generate faces (not features) with cancelable biometrics, and a work[2025IJCB] attempted to improve upon it.

FaceAnonyMixer: Cancelable Faces via Identity Consistent Latent Space Mixing

Mohammed Talha Alam[1], Fahad Shamshad[1], Fakhri Karray[1,2], Karthik Nandakumar[1,3]
[1]Mohamed Bin Zayed University of Artificial Intelligence, UAE
[2]University of Waterloo, Canada [3]Michigan State University, USA
{mohammed.alam, fahad.shamshad, fakhri.karray, karthik.nandakumar}@mbzuai.ac.ae

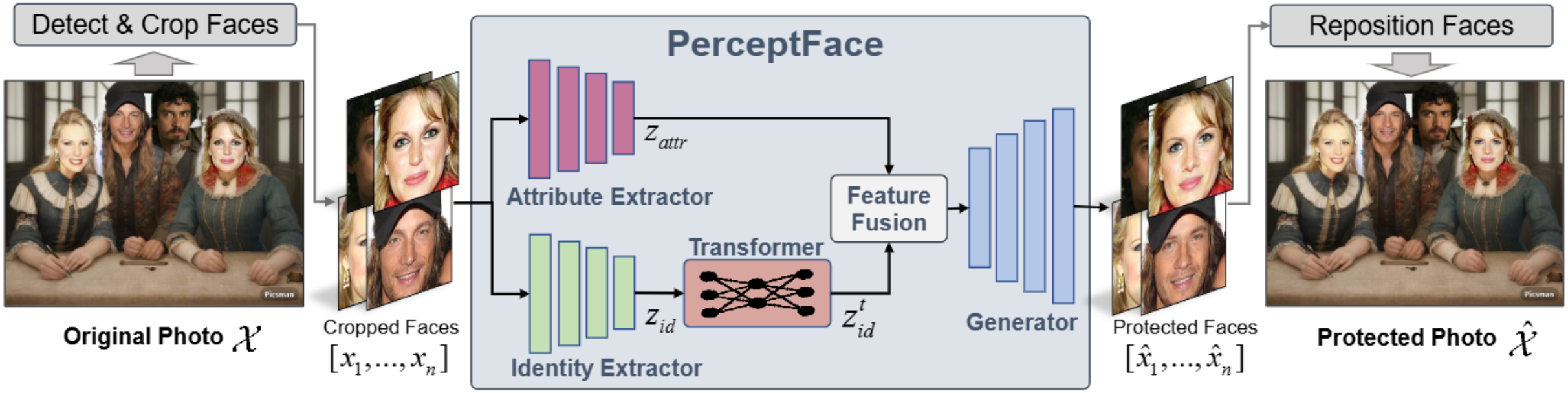
Vision Access Control in Facial Identity Protection

Who can access the real facial identity?



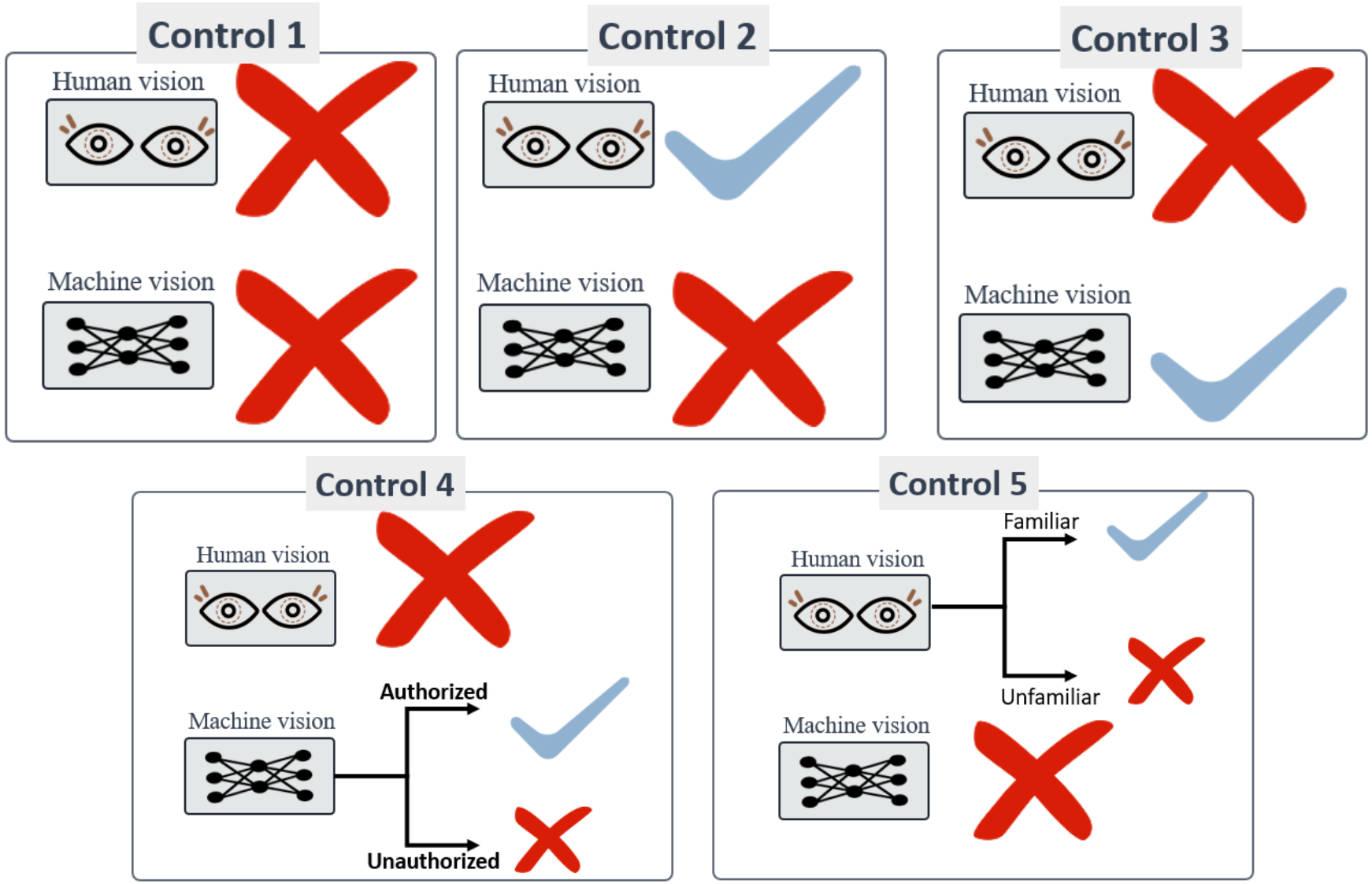
Our Work 5

Control 5 Alter identity for blocking FR models, reduce alterations in certain areas with high perceptual sensitivity



[2025 Arxiv] **Tao Wang**, Yushu Zhang*, Xiangli Xiao, Kun Xu, Lin Yuan, Wenying Wen, and Yuming Fang. Make Identity Unextractable yet Perceptible: Synthesis-Based Privacy Protection for Subject Faces in Photos

Summary


Control 1
Human vision
Machine vision
Control 2
Human vision
Machine vision
Control 3
Human vision
Machine vision
Control 4
Human vision
Machine vision
Authorized
Unauthorized
Control 5
Human vision
Familiar
Unfamiliar
Machine vision

End

Thank You!

I sincerely appreciate the time and insightful guidance from everyone today.