



Biometric Recognition: Accuracy, Privacy, and Trustworthiness

Dr. Xiaoming Liu

Jacqueline Maria Hagan Distinguished Professor

**Department of Computer Science
University of North Carolina at Chapel Hill**



**The University
of North Carolina
at Chapel Hill**

This research is based upon work supported in part by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via 2022-21102100004. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

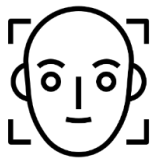
Biometrics



“Automated recognition of individuals based on their behavioral and biological characteristics”

ISO/IEC JTC1 2382-37:2012

- ***Biometrics: bios (life) + metron (measure)*** *Morris, 1875*

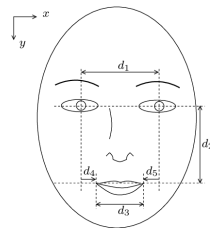


Credit: Prof. Anil Jain

History of Face Recognition

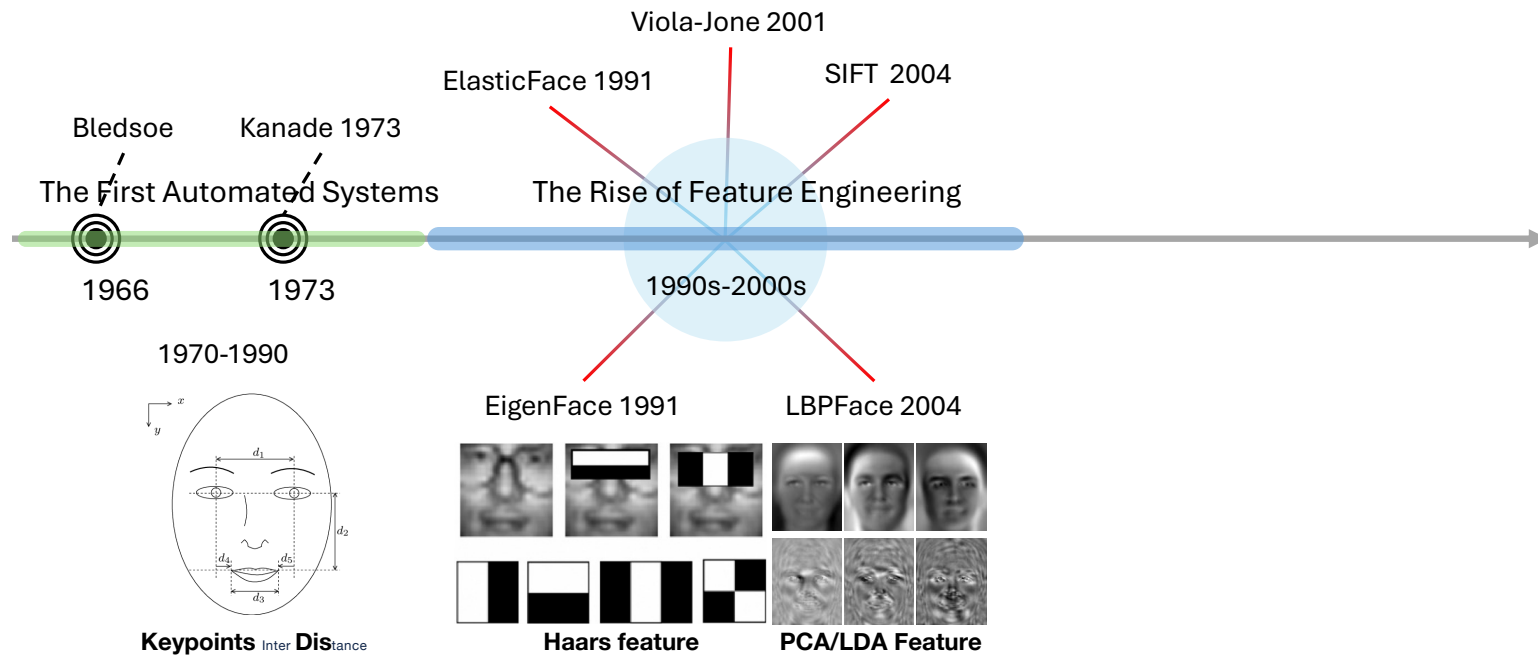


1970-1990

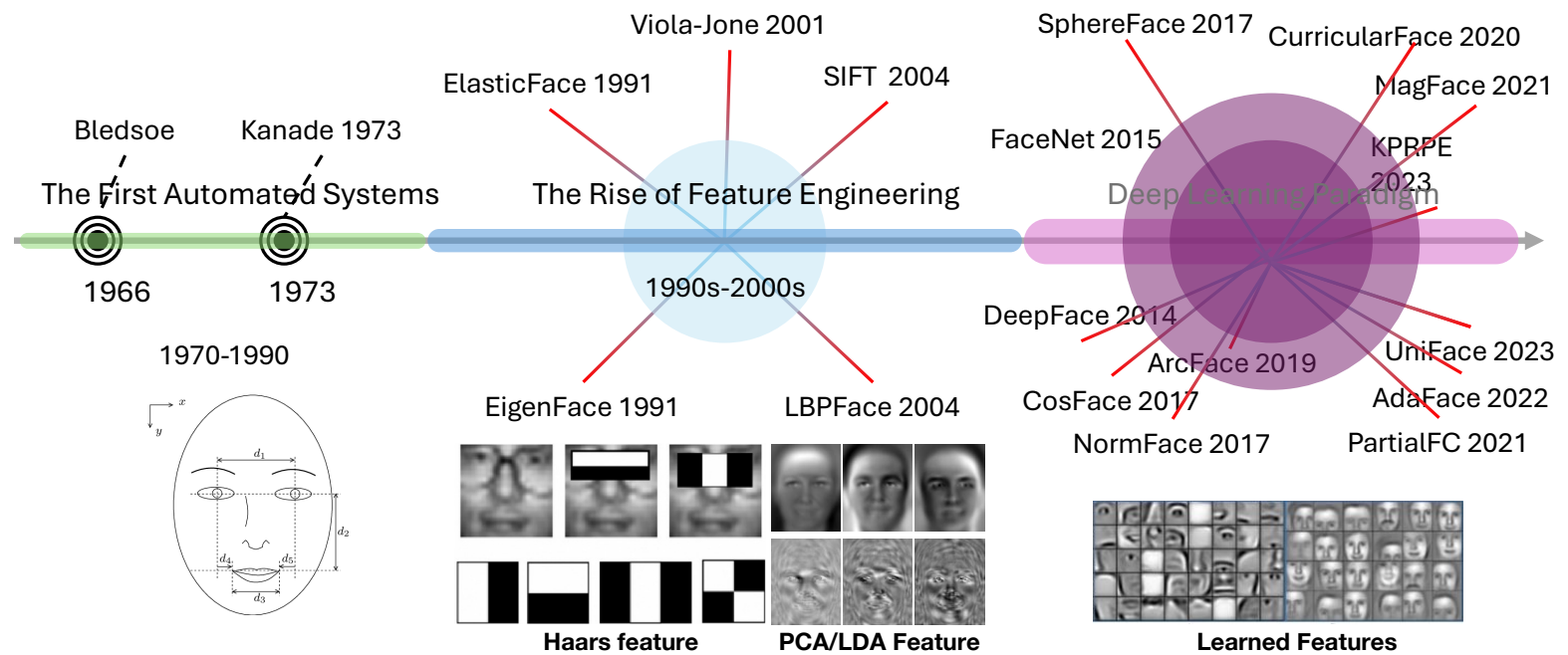


Keypoints Inter Distance

History of Face Recognition



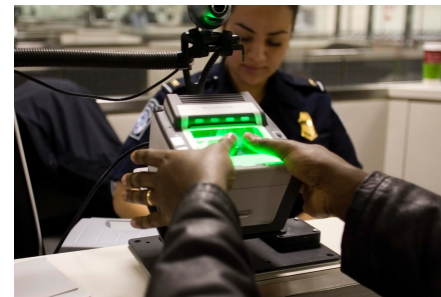
History of Face Recognition



Successful Applications of Biometric Recognition



Apple FaceID



Fingerprint



Boarding in Airports



Amazon One Palmprint

Accuracy: Recognition at a Distance



BRIAR: The subject in the figure consented to publication.

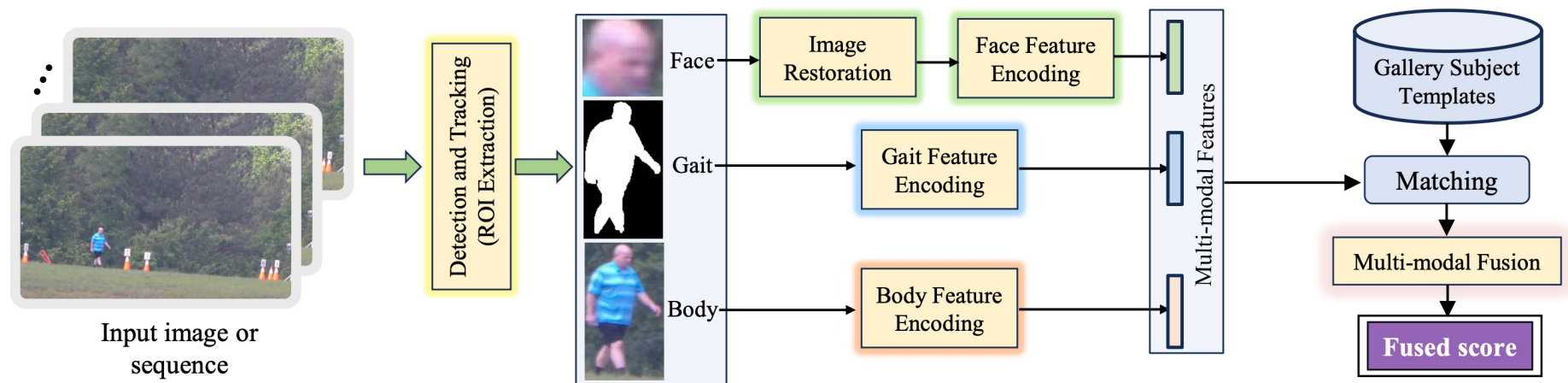
BRIAR



- One of the largest Biometrics projects in US, 4.5 years!
- Sponsored by IARPA
- 7 full teams and 2 partial teams in phase 1
- 5 teams in phase 2
- 2 teams in phase 3: MSU and STR
- Advancing the SOTA in face, body, gait recognition, multi-modality fusion, AIGC, and image restoration

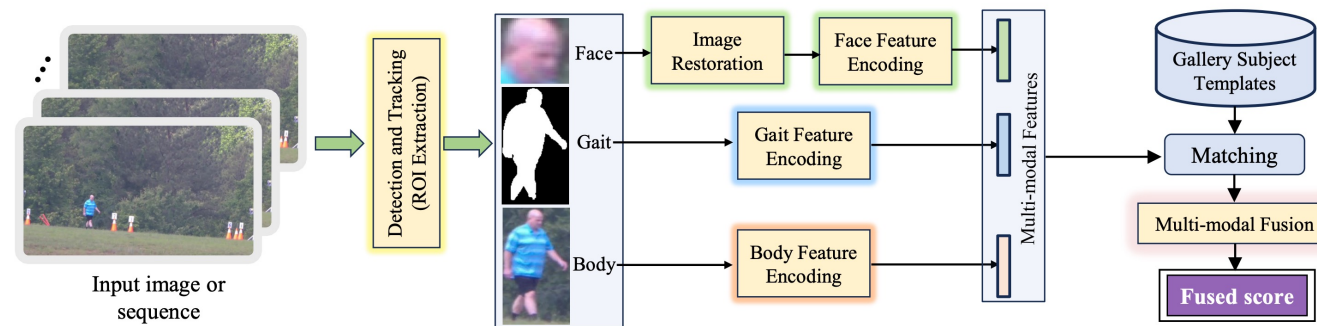


MSU BRIAR System - FarSight





Five Categories of FarSight Algorithms



- Face Recognition
- Person Reidentification (Body Recognition)
- Gait Recognition
- Multi-modality Fusion
- Unified model

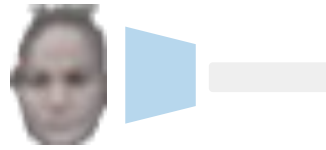


FarSight Algorithms - Face

- **Generic matcher:**

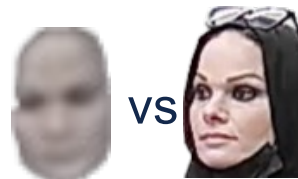
AdaFace

(CVPR'22, Oral)



- **Domain adaption:**

CFSM (ECCV'22)



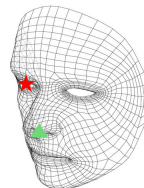
- **Video-based reco:**

CAFace (NeurIPS'22)



- **Landmark assisted reco**

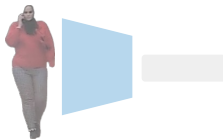
KP-RPE (CVPR'24)



FarSight Algorithms - ReID



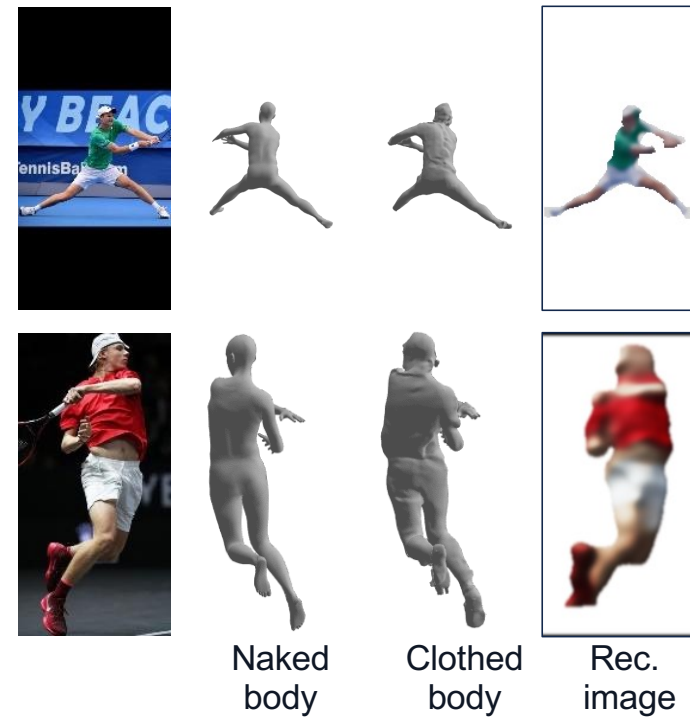
- **3D body matching**
(ICCV'23)



- **CLIP 3D Re-ID**
(CVPR'24)



- **MoE for ReID**
(CVPR'25)





FarSight Algorithms - Gait

- **Human OF**
(CVPR'25, highlight)



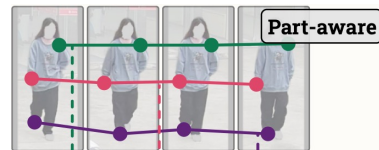
- **BigGait**
(CVPR'24)



- **BiggerGait**
(NeurIPS'25)



- **GaitMax**
(CVPR'26, highlight)



FarSight Algorithms – 3D Flow



H-Flow Self-supervised Human Scene Flow via Physics-inspired Joint Multi-modal Learning

Multi-view Renderings of the Ballet Reconstruction Zero-Shot Inference



Input Frames



H-Flow
Ours



Zero MSF
General Scene Flow

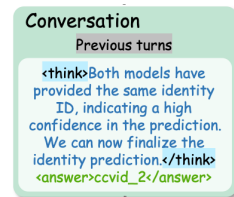


FarSight Algorithms - Fusion

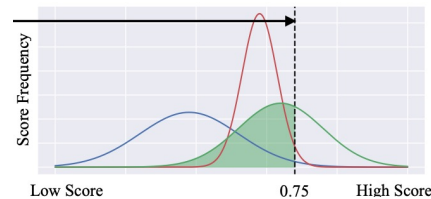
- **MoE for fusion:**
(ICCV'25)



- **Agent for fusion:**
(CVPR'26)



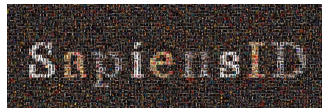
- **Open-set Biometrics:**
(ECCV'24)



FarSight Algorithms - Unified



- **Unified human recognition**
(CVPR'25)

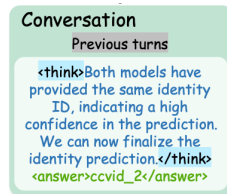


- **SapiensID 2.0**
(Under review)

Highlights: Biometrics vs Foundation Models

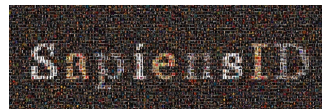


- **Agent for fusion:**
(CVPR'26)



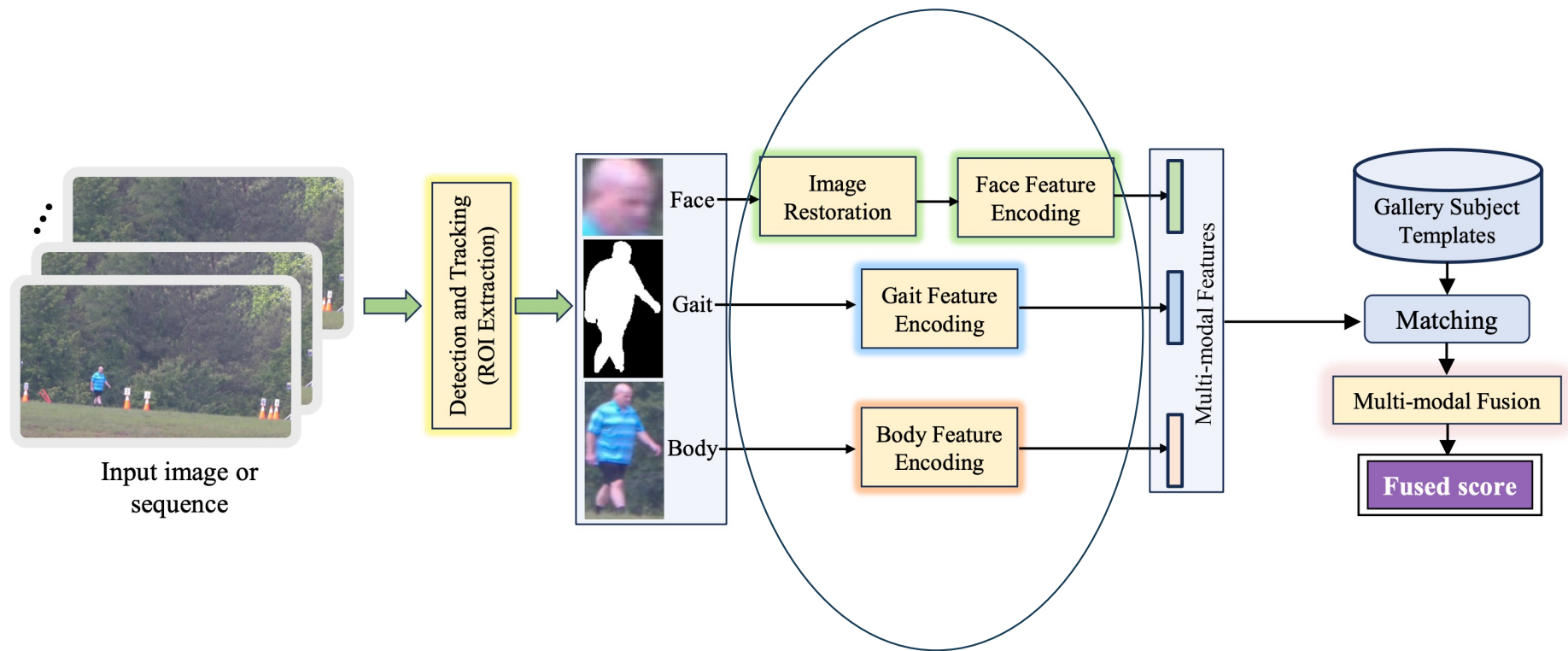
← Novel usage of pre-trained FM

- **Unified human recognition**
(CVPR'25)

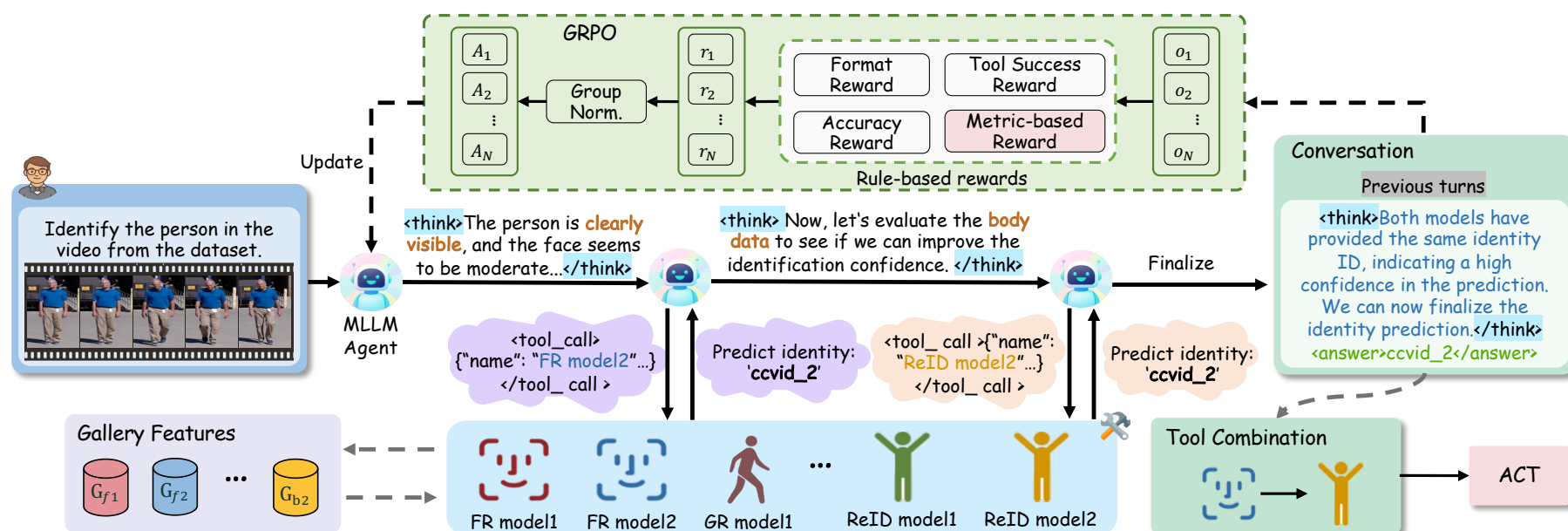


← FM for Biometrics

MSU BRIAR System - Fusion



FusionAgent



Unified Biometric Recognition: Motivation



Can one model perform comparison across different body pose and visual area?

WebBody Dataset



4 Million Labeled Images

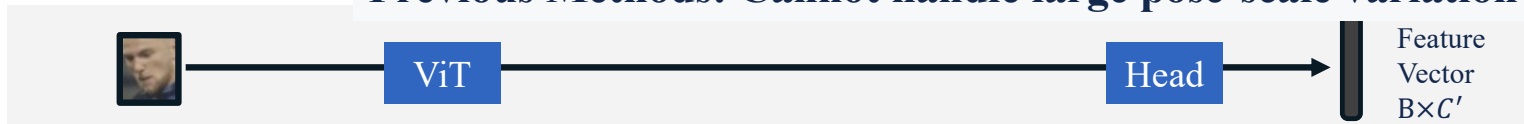
263,920 Subjects

Large Pose–Scale Variation

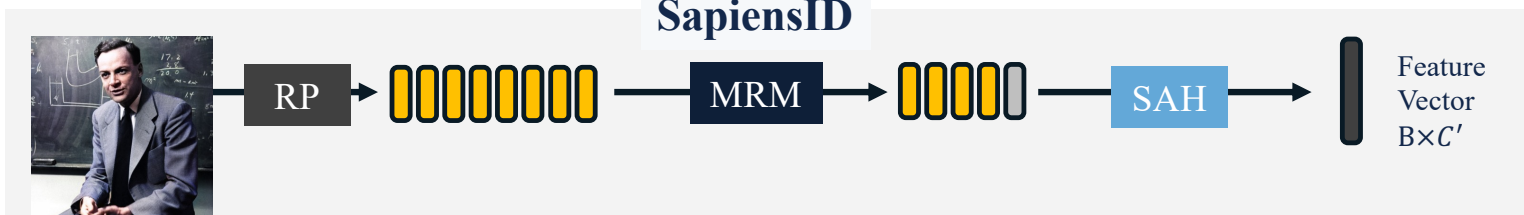
Overview



Previous Methods: Cannot handle large pose-scale variation



SapiensID



SapiensID proposes 3 things to **handle large pose and scale variation**.

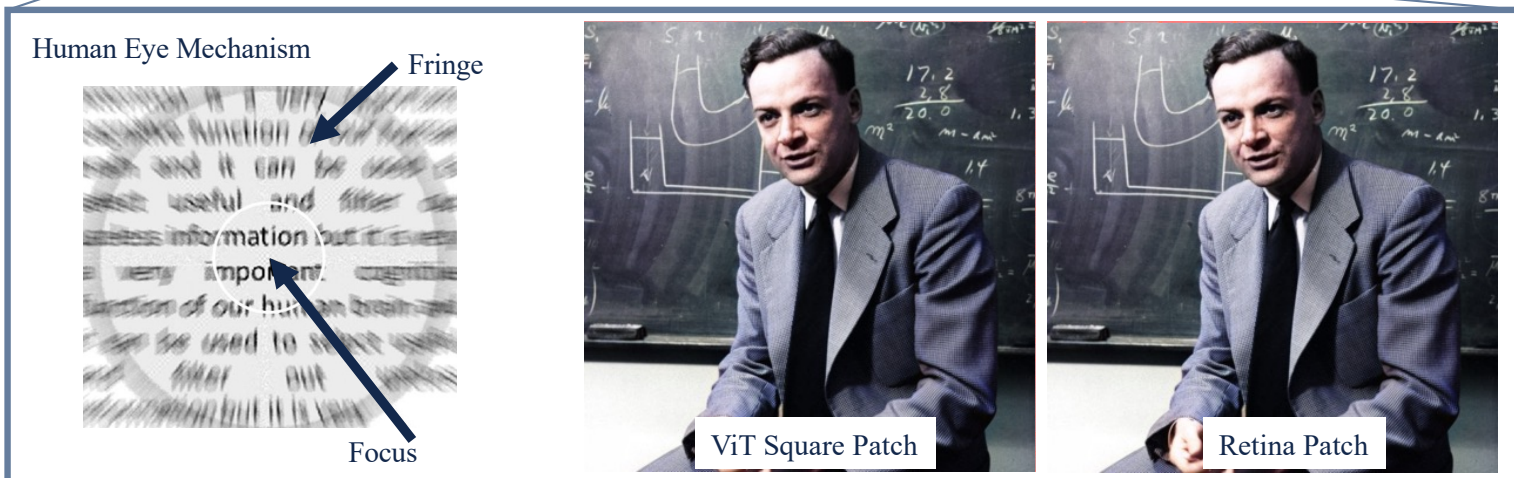
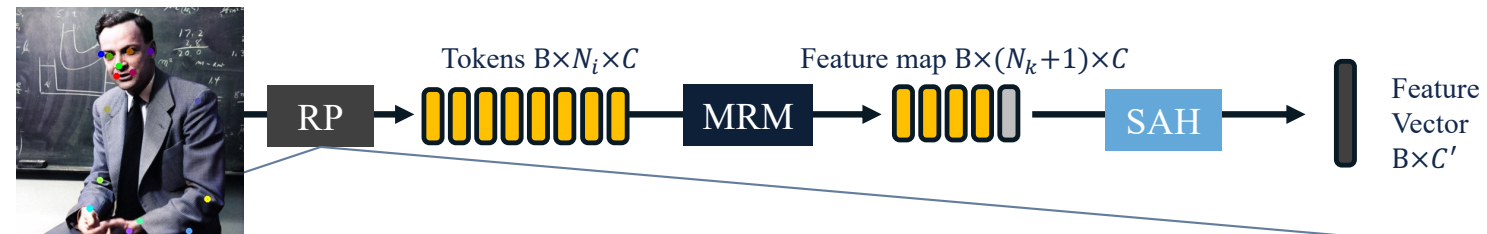
RP: Retina Patch

MRM: Masked Recognition Model

SAH: Semantic Attention Pooling

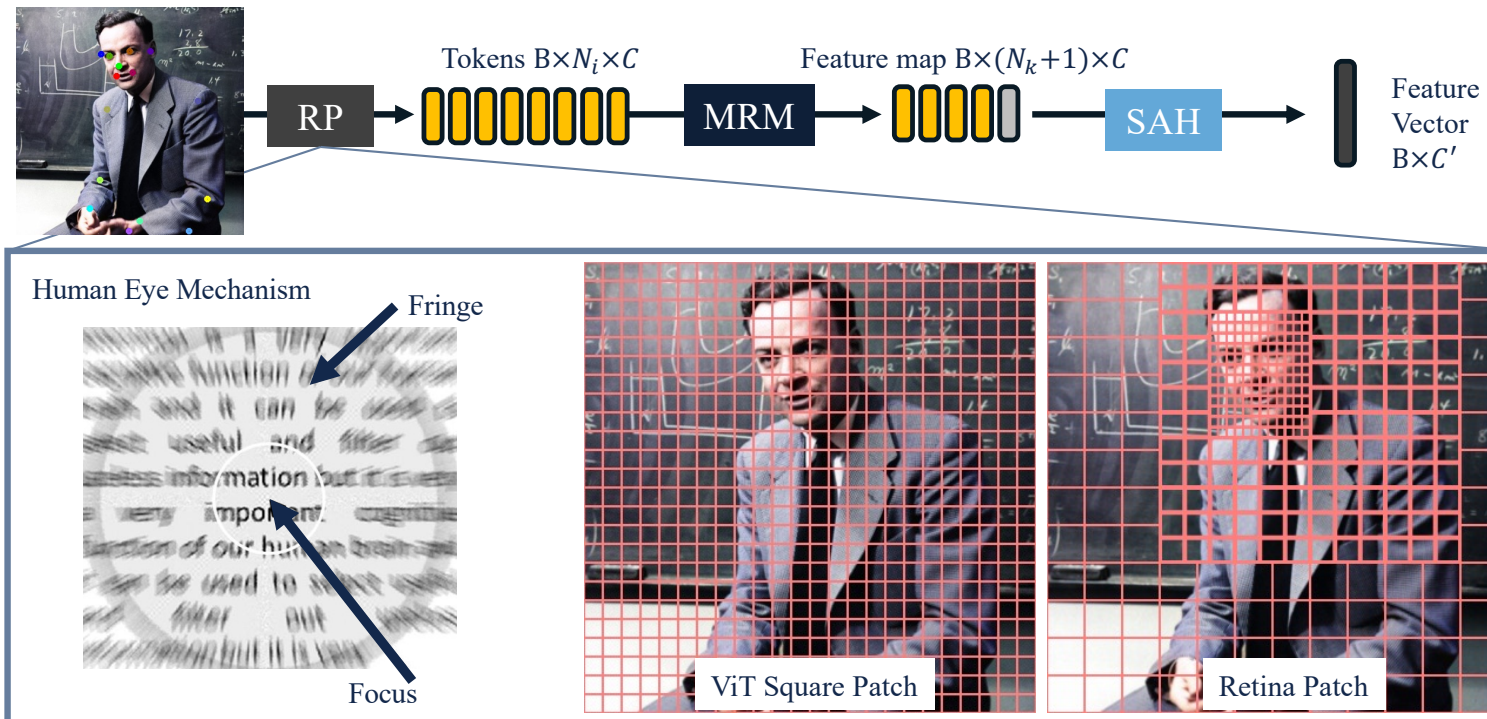


1. Retina Patch

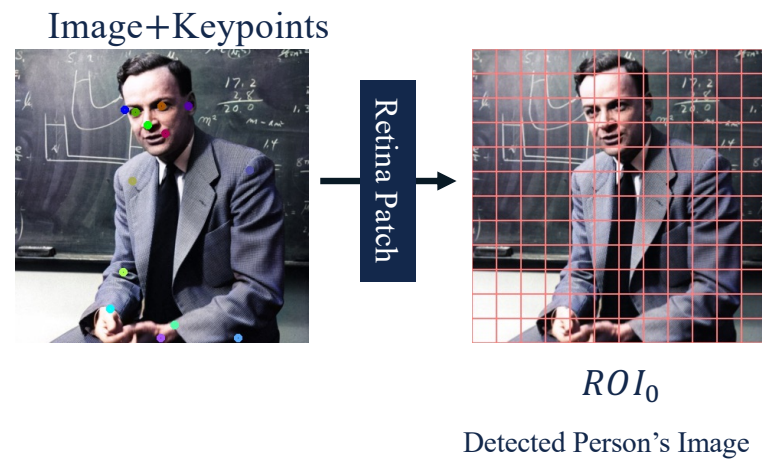




1. Retina Patch



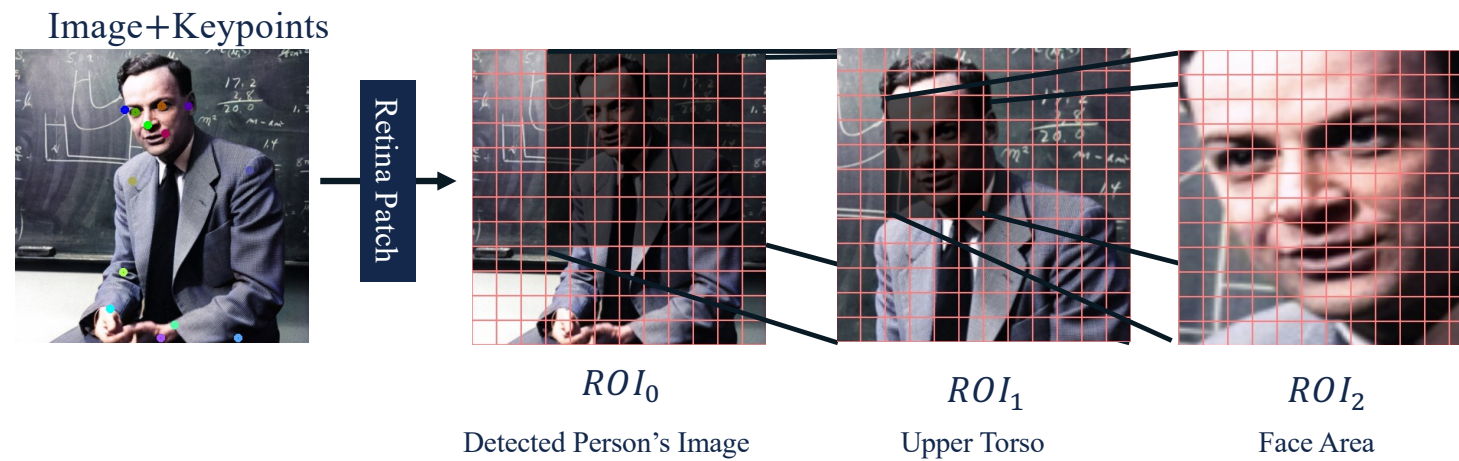
1. Retina Patch



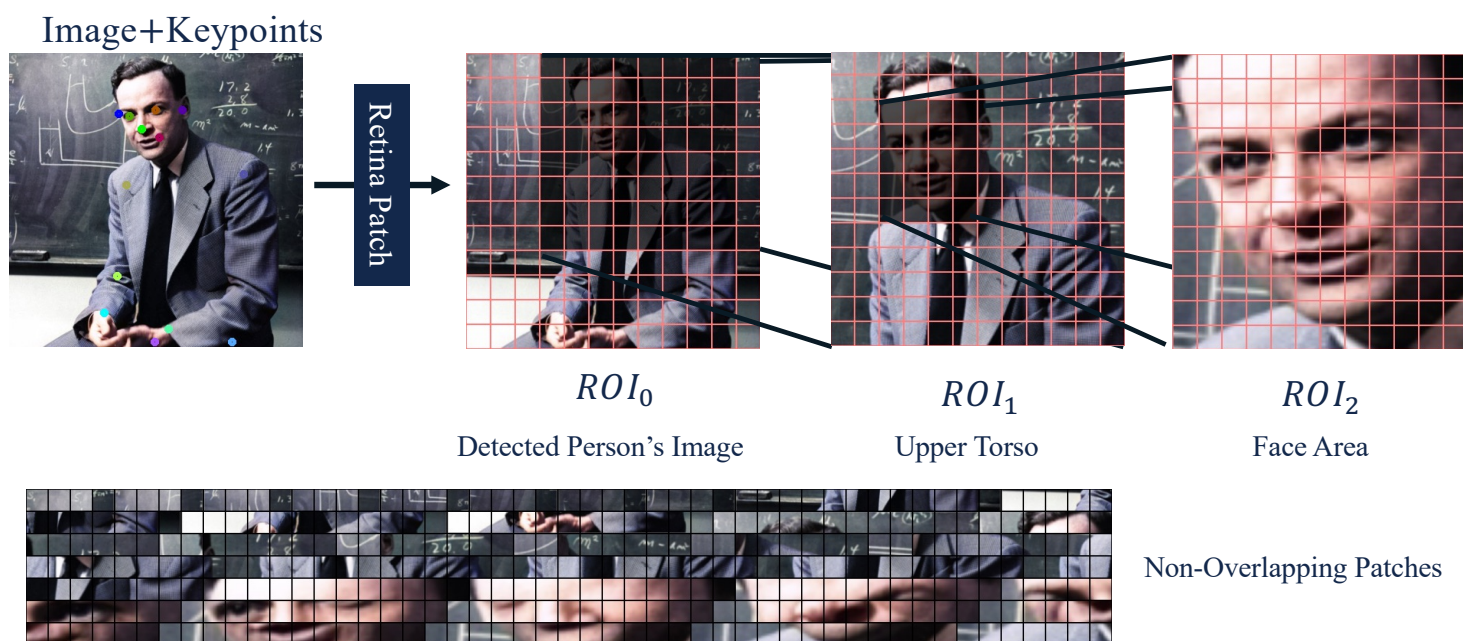
1. Retina Patch



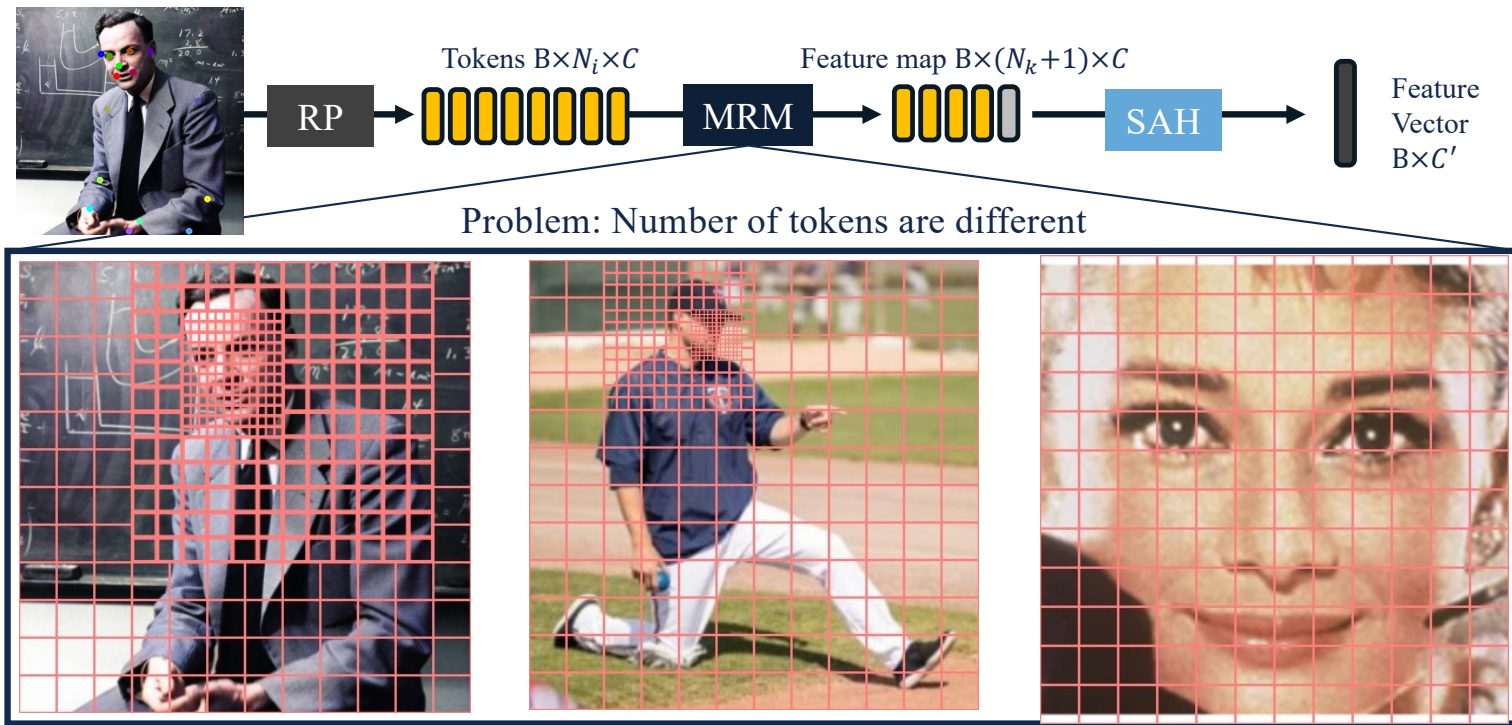
1. Retina Patch



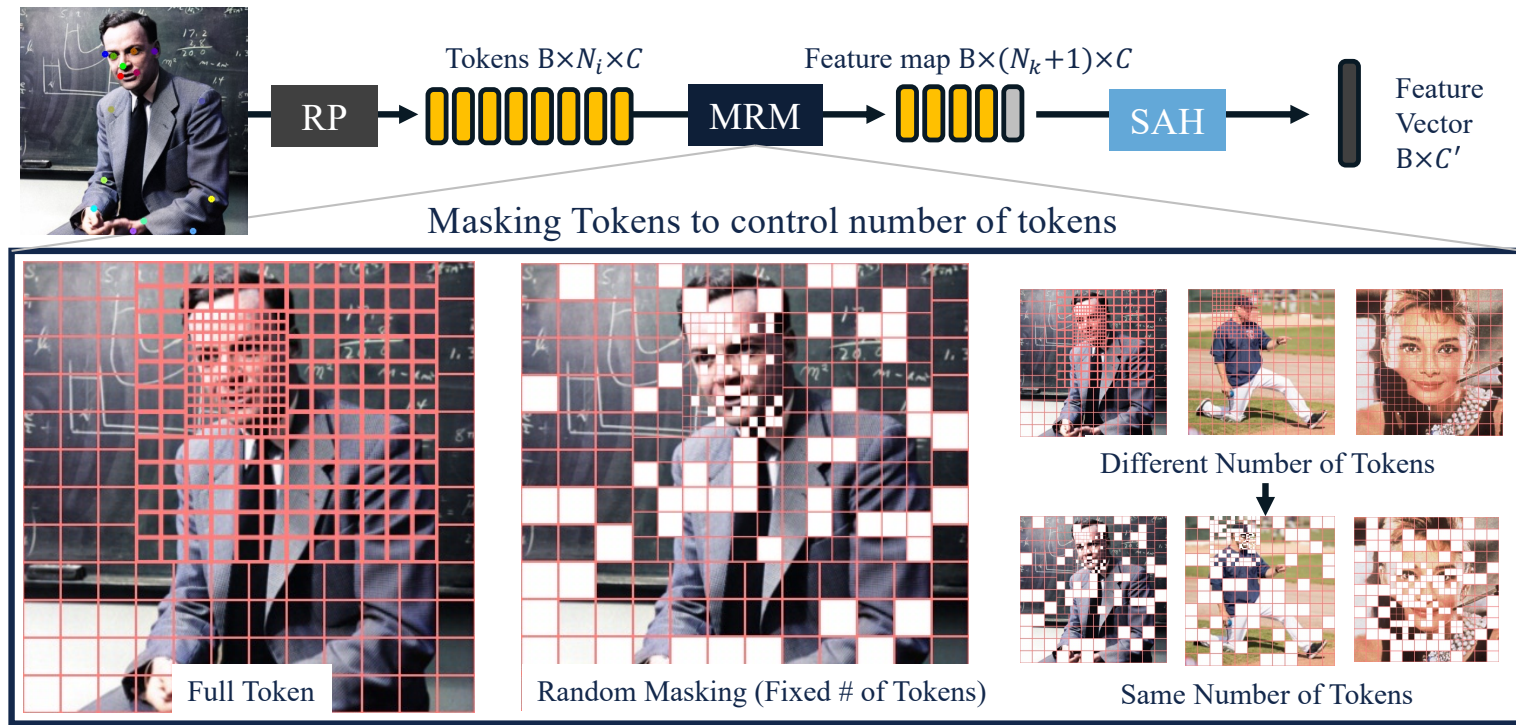
1. Retina Patch



1. Retina Patch

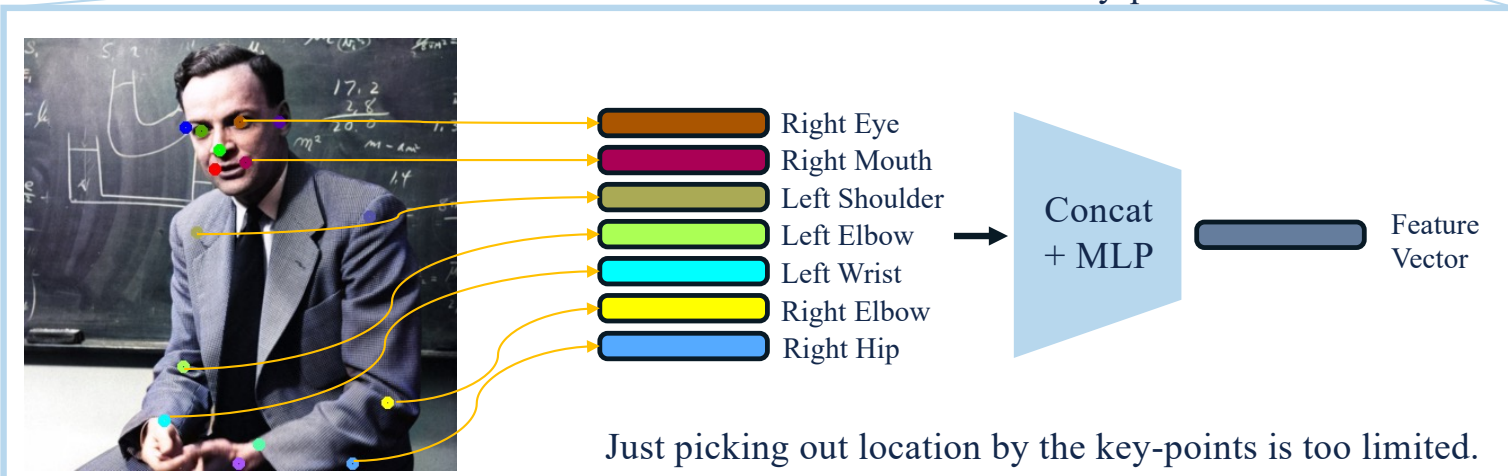
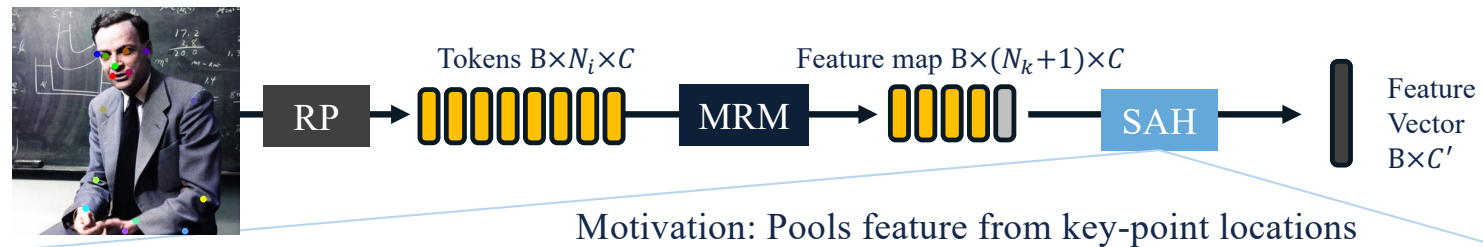


2. Masked Recognition Model



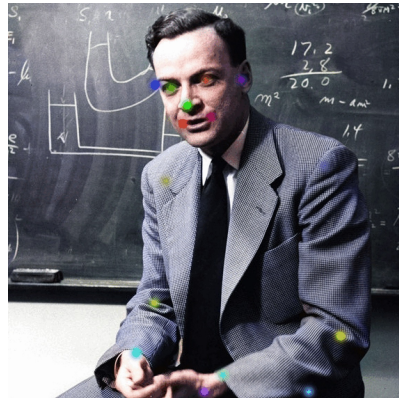
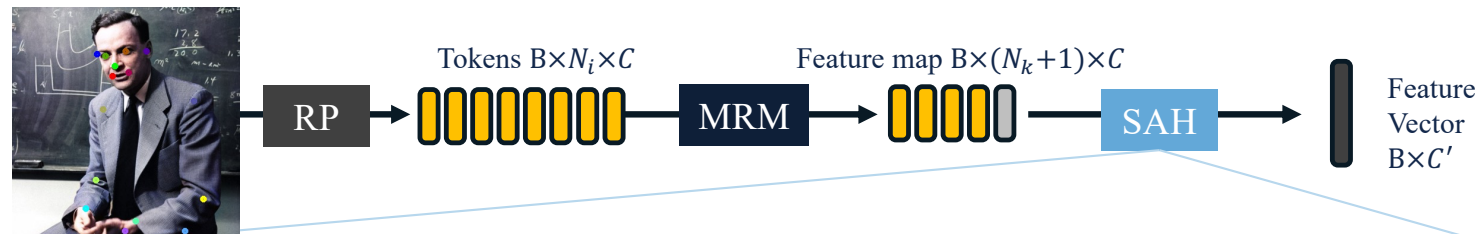


3. Semantic Attention Pooling

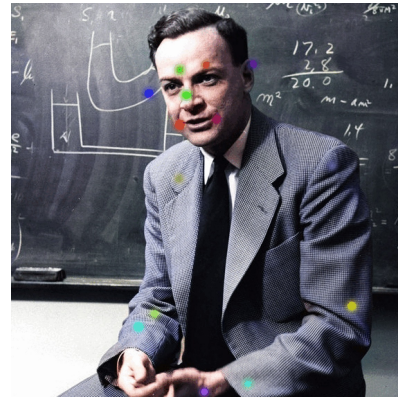




3. Semantic Attention Pooling



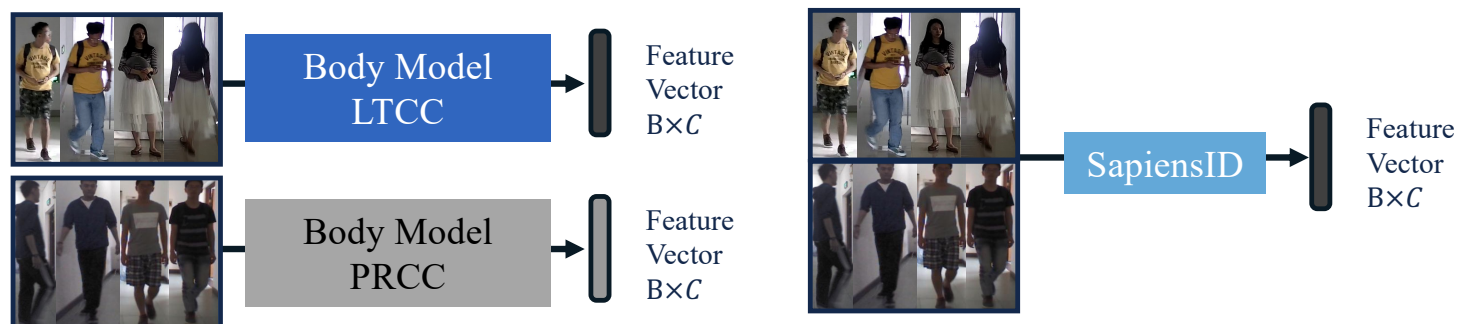
Learns Attention Size



Learns Attention Offset Location

Attention for learning the appropriate size and offset locations from **keypoints**.

Performance



Method	Train Data	Avg	LTCC Top1	PRCC Top1	CCVID Top1	CCDA Top1	Celeb-ReID Top1
CAL [19]	LTCC	38.26	38.01	37.00	74.97	3.91	37.42
CAL [19]	PRCC	32.02	6.38	55.69	71.61	2.85	23.59
CAL [19]	LTCC+PRCC	38.65	33.16	45.39	73.89	3.74	37.11
CLIP3DReID [46]	LTCC	40.11	41.84	40.81	76.28	4.31	37.31
CLIP3DReID [46]	PRCC	33.06	6.63	62.40	69.32	3.17	23.82
HAP [74]	LU4M+LTCC	33.07	25.00	26.14	41.64	4.56	30.28
HAP [74]	LU4M+PRCC	31.16	29.08	38.05	45.73	5.13	37.79
HAP [74]	WebBody4M (Ours)	52.11	22.70	54.93	88.34	28.80	65.78
SapiensID (Ours)	WebBody4M (Ours)	72.89	42.35	78.75	88.72	61.84	92.80

Performance



Method	AdaFace-ViT [32]	SapiensID (Ours)
Train Data	WebBody4M-FaceCrop	WebBody4M
LFW [24]	99.82	99.82
CPLFW [79]	95.12	94.85
CFPFP [54]	99.19	98.74
CALFW [80]	96.07	95.78
AGEDB [52]	97.97	97.33
Face Avg	97.63	97.31
LTCC [55]	21.70	72.01
Market1501 [77]	7.81	88.18
Body Avg	14.76	80.10
Combined Avg	56.19	89.80

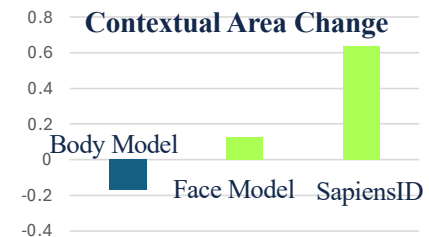
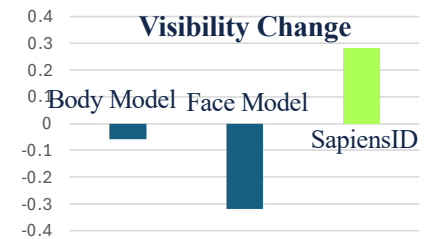
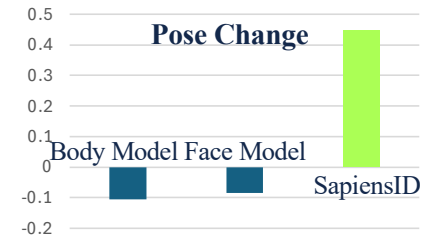
Analysis

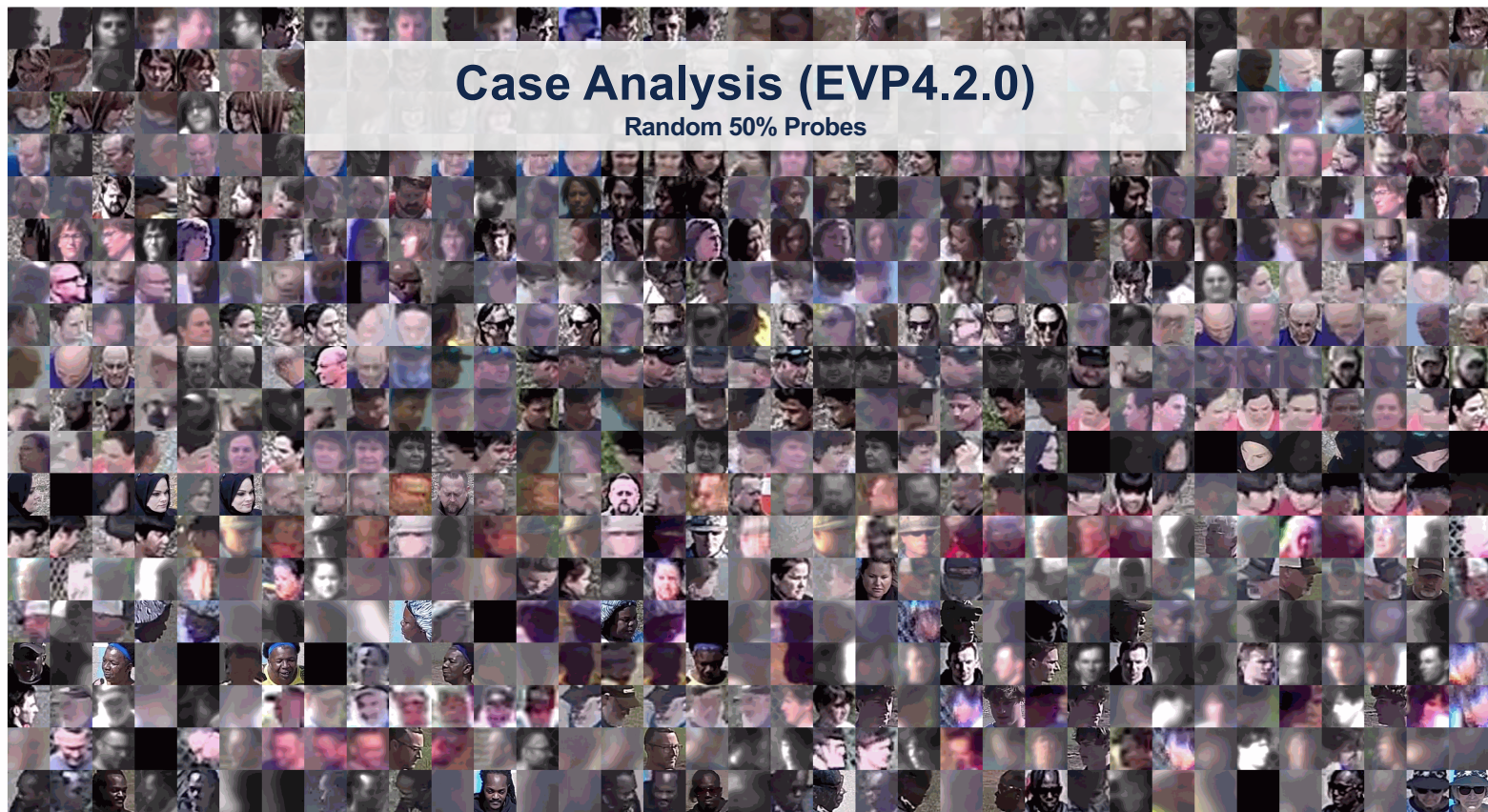


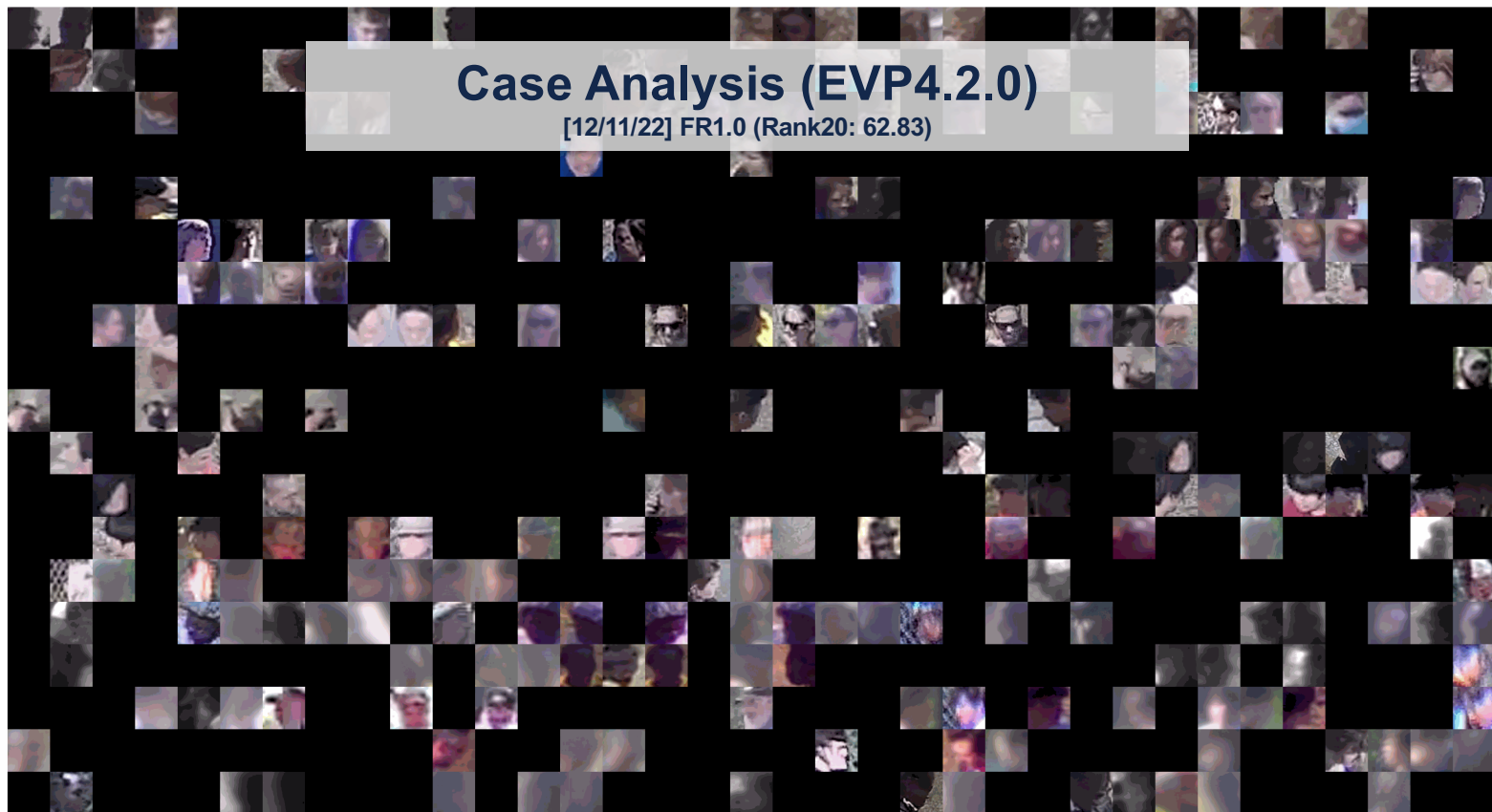
← Probe → Gallery

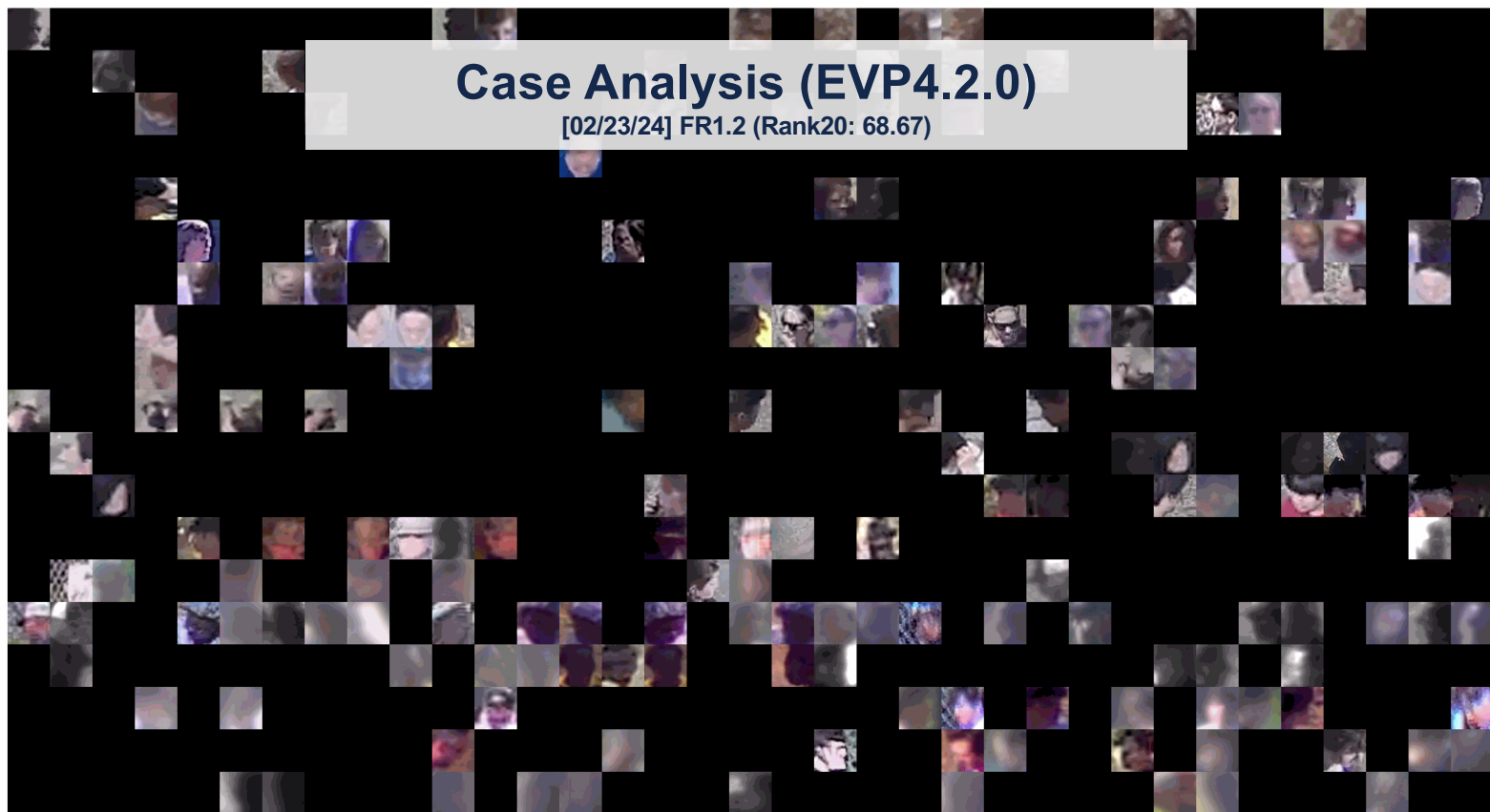
Y-axis: Similarity – Threshold

- Predict match
- Predict no match





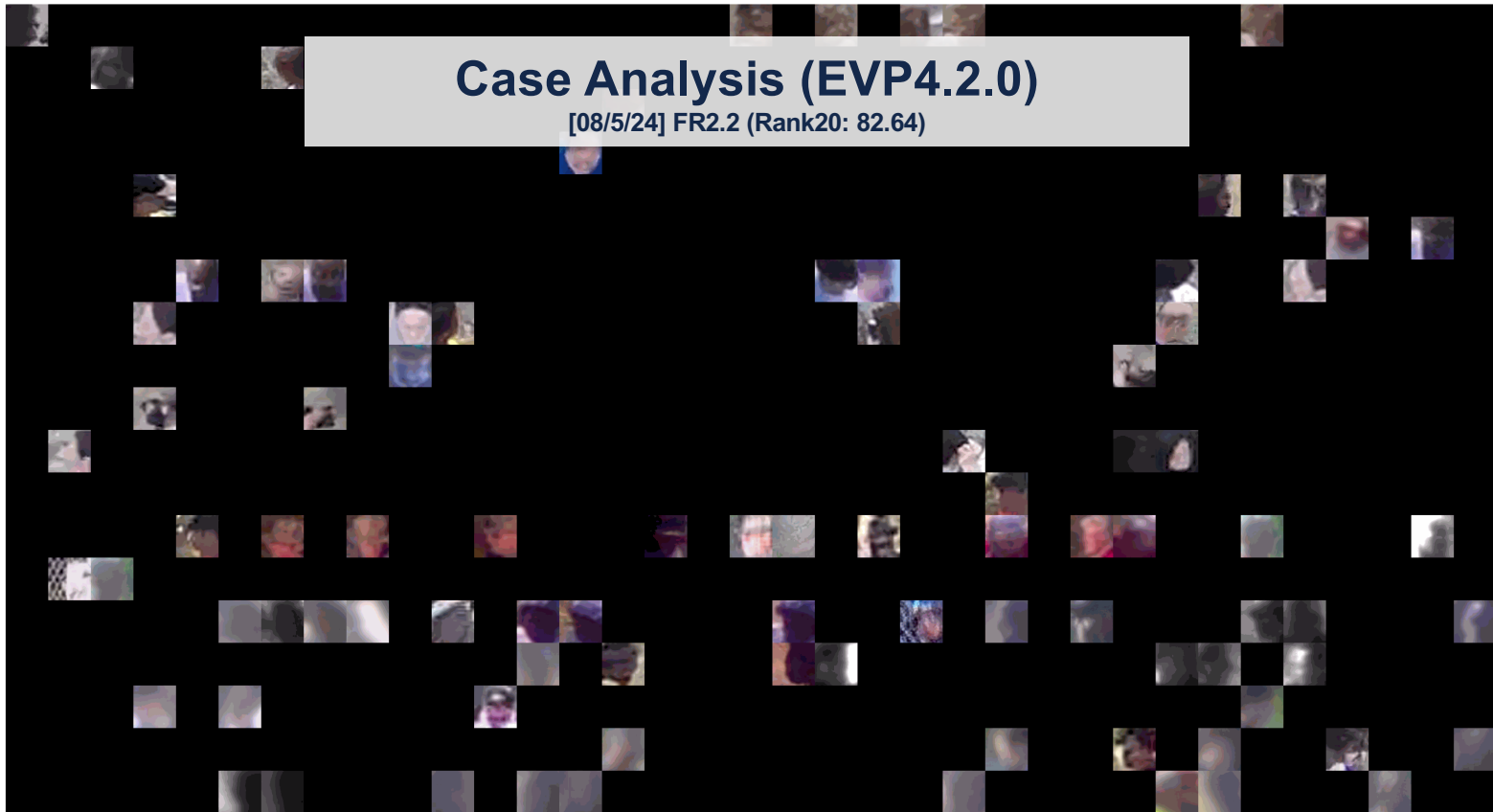






Case Analysis (EVP4.2.0)

[08/5/24] FR2.2 (Rank20: 82.64)



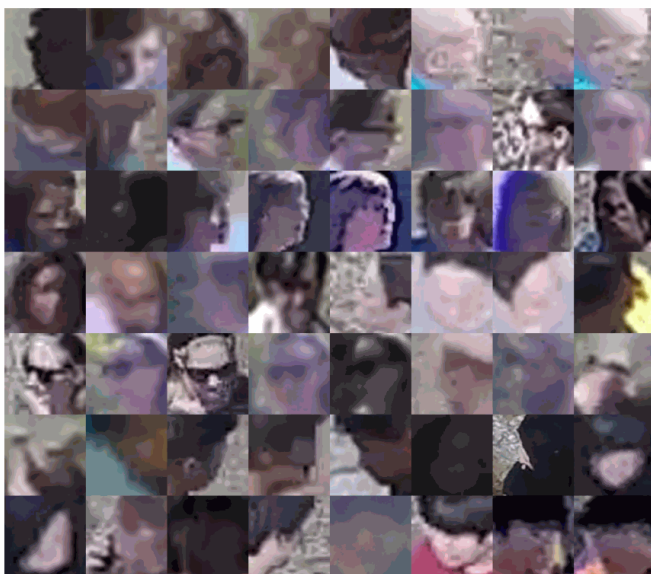
Failure Cases



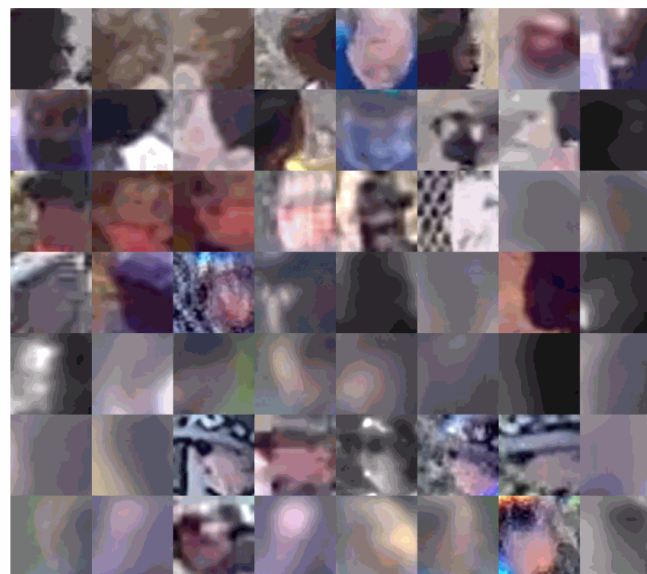
Case Analysis

[08/5/24] FR2.2 (Rank20: 82.64)

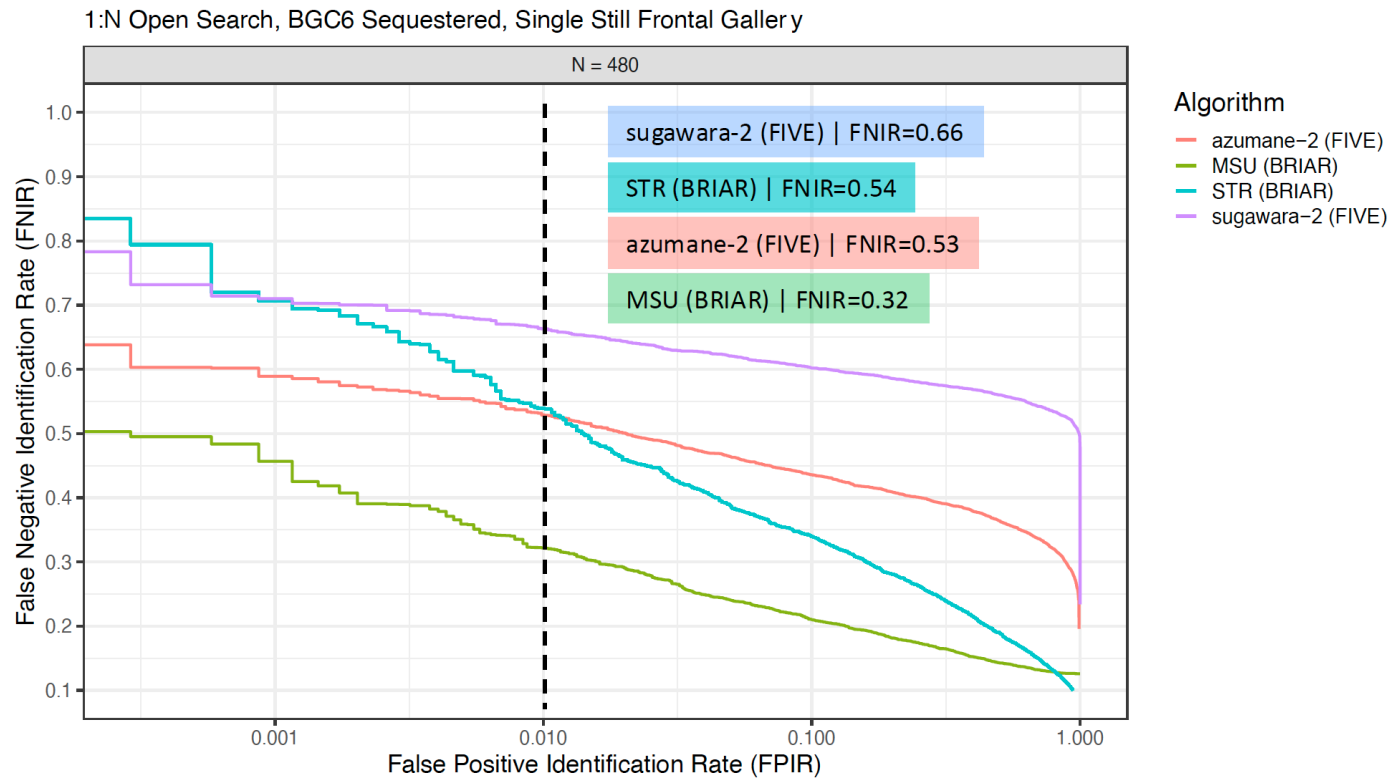
wrong $\mapsto$ correct



wrong $\mapsto$ wrong



NIST Evaluation on Sequestered Partition





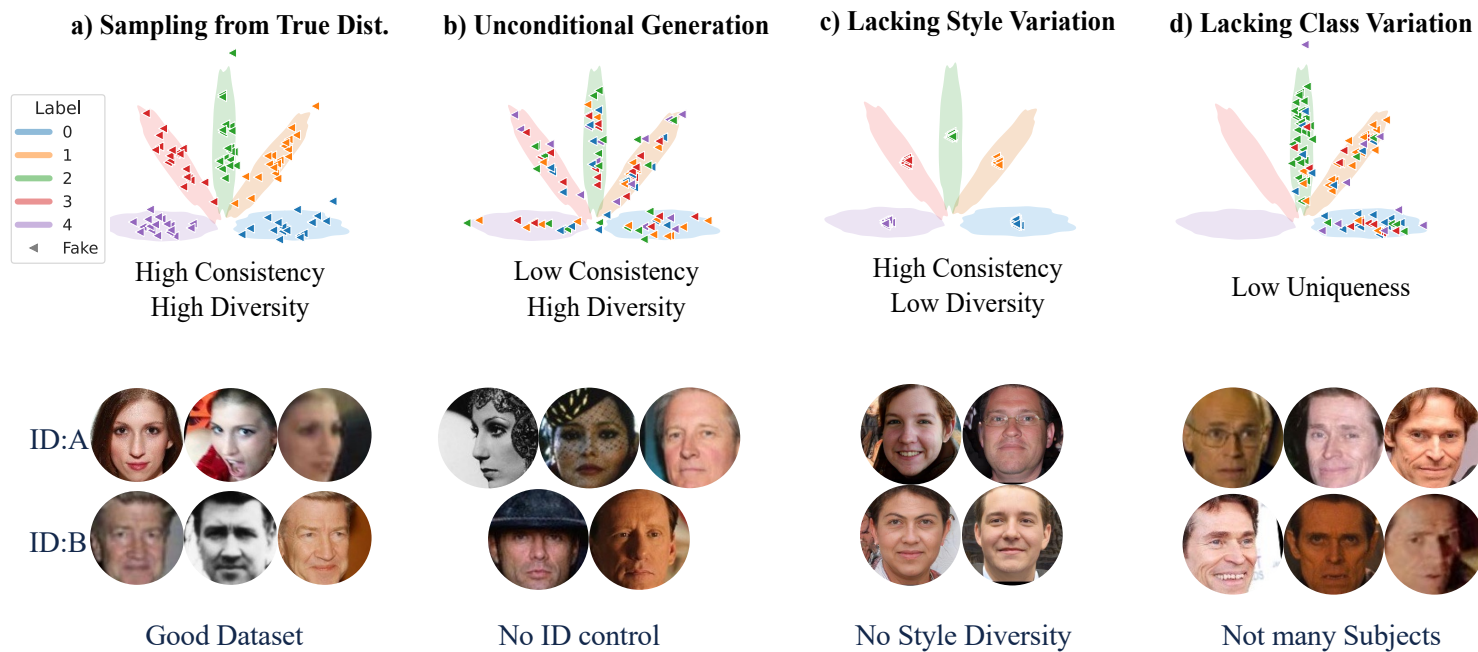
Privacy Challenge

- There are always privacy concerns when using real faces for training FR models.
- Can we leverage GenAI to synthesize a database of fake subjects as the training set?

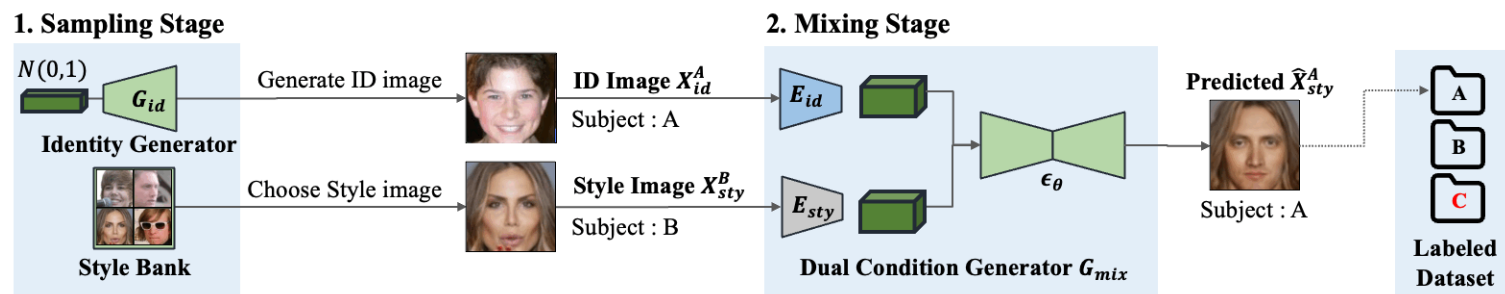
Synthetic training dataset
(CVPR'23)



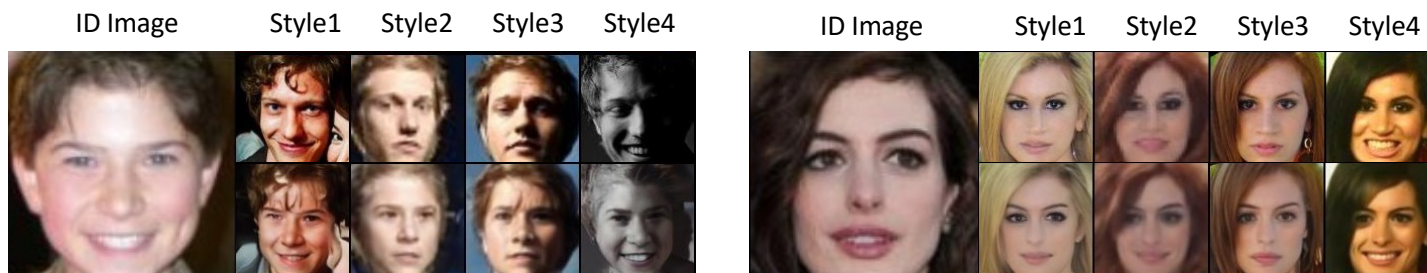
Characteristics of Labeled Faces



Our Method



5. Repeat this procedure to generate a dataset.



Performance



Face Recognition Performance

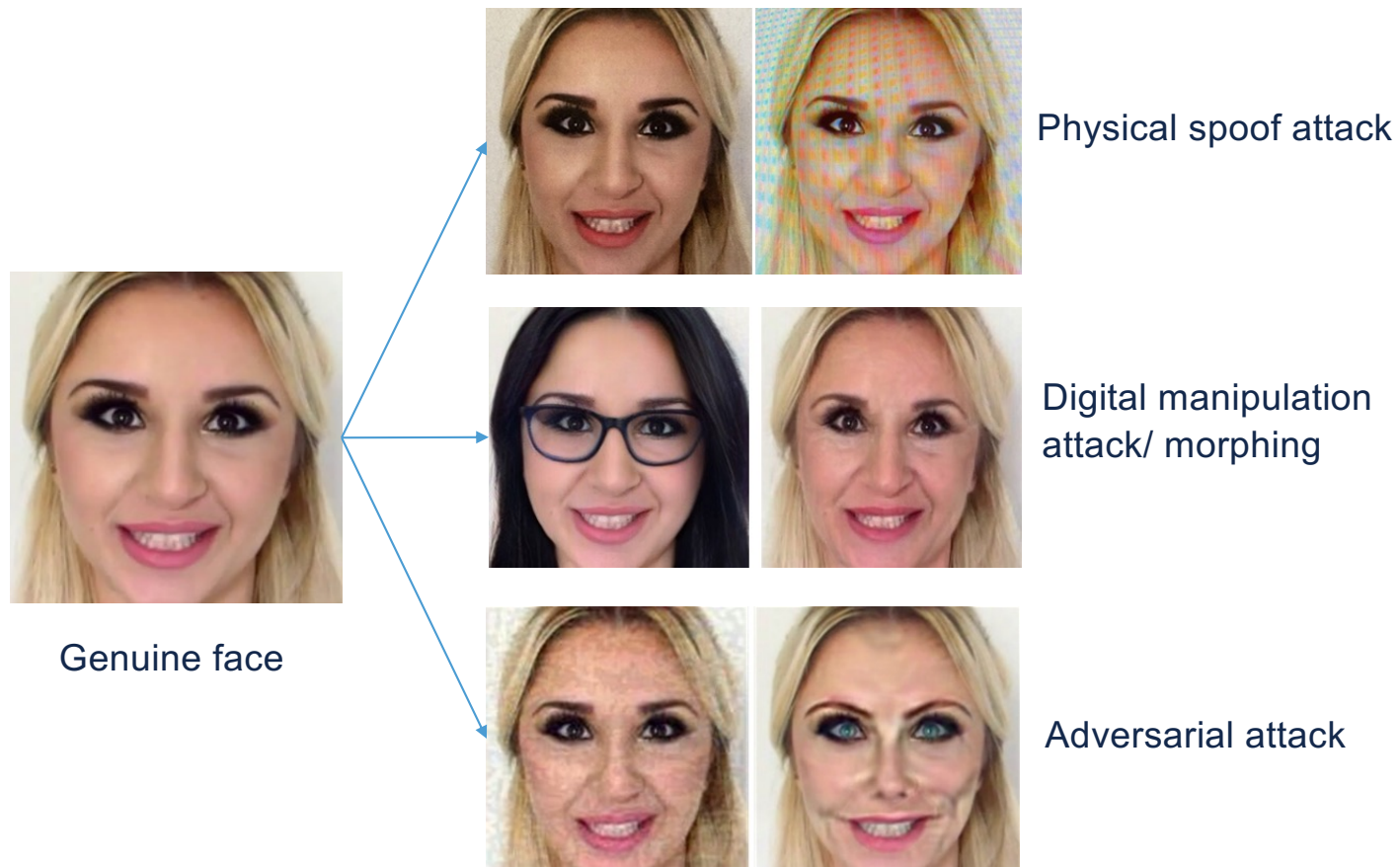
	# Synthetic Imgs	# Real Imgs	LFW	CFPFP	CPLFW	AGEDB	CALFW	AVG	Gap to Real
DigiFace	1.2M (10K × 72 + 100K × 5)	0	96.17	89.81	82.23	81.10	82.55	86.37	8.72
DigiFace	1.2M (10K × 72 + 100K × 5)	2K × 20	99.17	94.63	88.1	90.5	90.97	92.67	2.06
DCFace	1.2M (20K × 50 + 40K × 5)	0	98.58	88.61	85.07	90.97	92.82	91.21	3.61
DCFace	1.2M (20K × 50 + 40K × 5)	2K × 20	98.97	94.01	86.78	91.80	92.95	92.90	1.82
DCFace+DigiFace (2.4M)		0	99.20	93.63	87.25	92.25	92.95	93.06	1.65
CASIA	0	0.5M	99.42	96.56	89.73	94.08	93.32	94.62	0



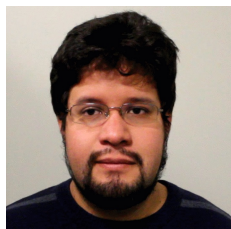
Trustworthy Biometrics

- How to defense various attacks, such as spoofing, adversarial attacks, etc.?
- How to detect media forgery?
- How to reverse engineering the attacks?

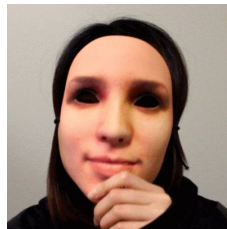
Manipulation of Faces



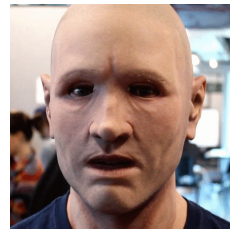
Face Anti-spoofing: IARPA 2017-2022



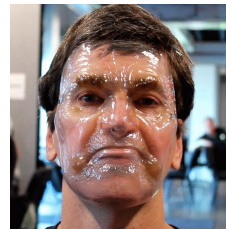
Live



Half Mask



Silicone



Transparent



Papercraft

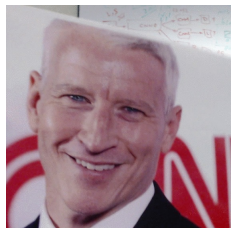


Mannequin

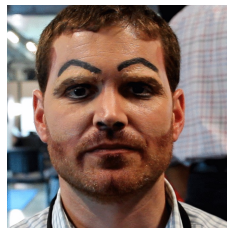


Replay

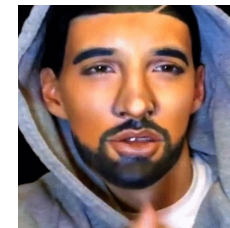
3D Mask Attacks



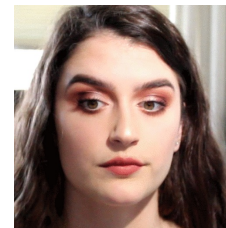
Obfuscation



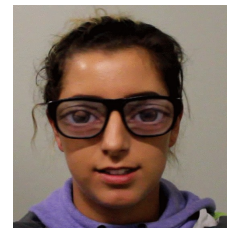
Imperson.



Cosmetic



Funny Eye



Paperglasses



Partial Paper

Print

Makeup Attacks

Partial Attacks

Deepfake Detection and Image Attribution



Manipulation Localization

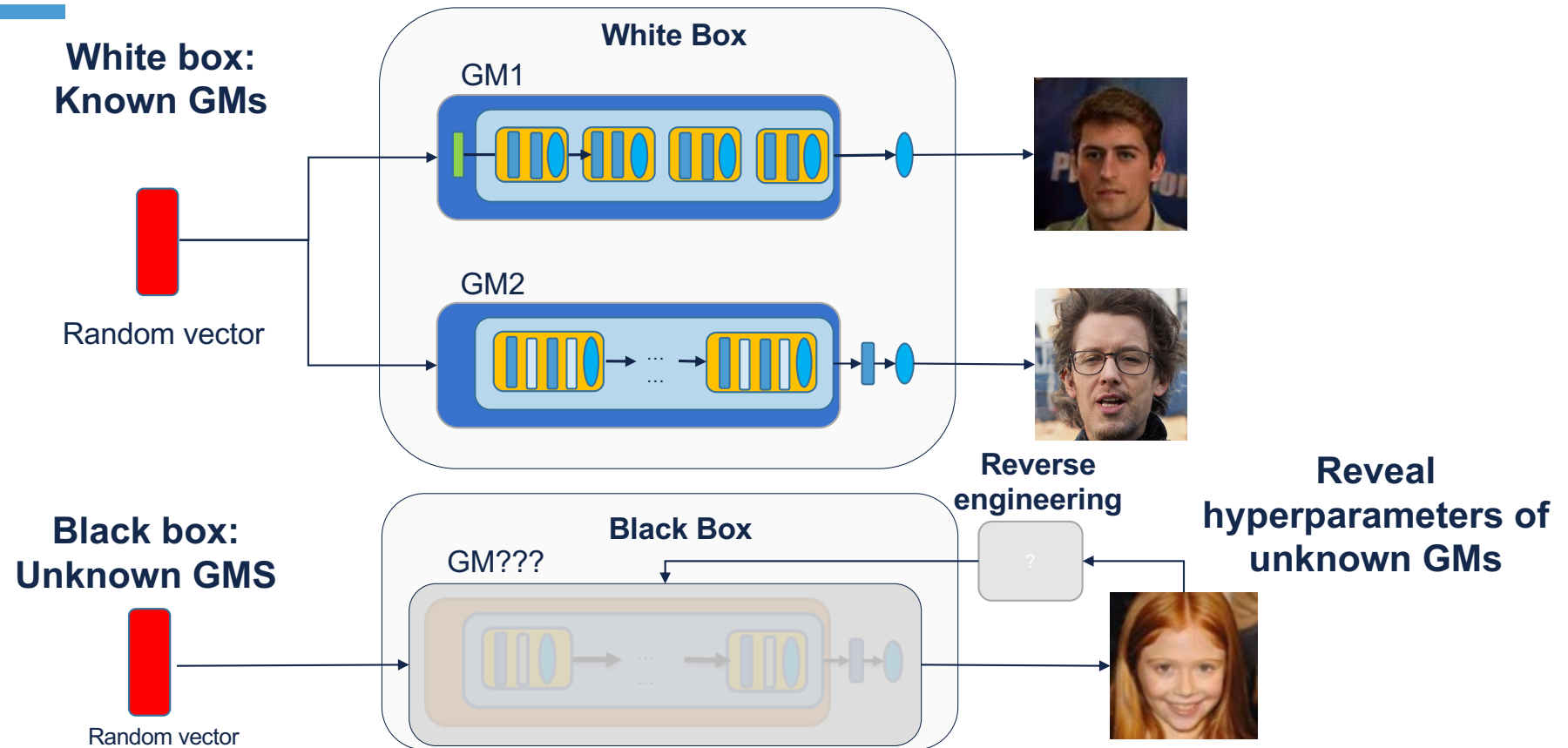


- Estimate which pixels of images are manipulated





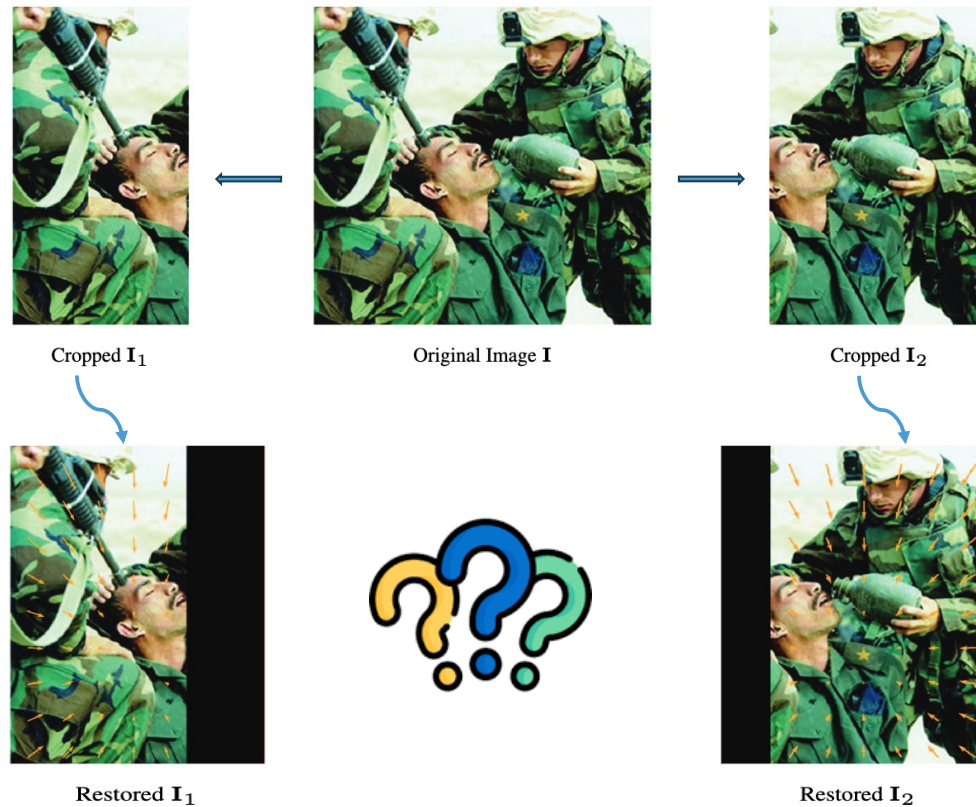
Reverse Engineering: Model Parsing



Geometric Manipulation



Geometric Manipulation



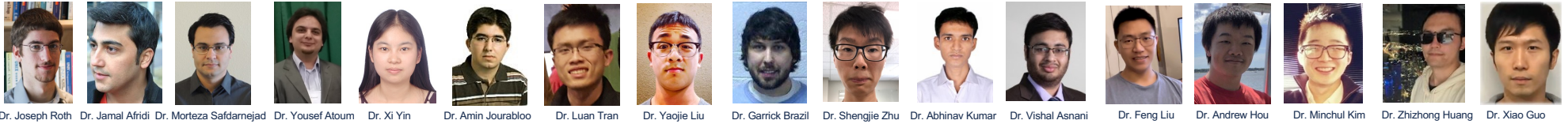
Zhu, Shengjie, et al. "Tame a Wild Camera: In-the-Wild Monocular Camera Calibration." in NeurIPS 2023.

Conclusions



- There are many new research opportunities in biometric recognition.
- Building a unified model for periocular/face/body/gait leads to a foundation model for biometrics.
- We shall strive to improve the capability in defending against attacks.

Thanks



Sponsors:





Questions?

Shooting of UnitedHealthcare CEO



<https://metro.co.uk/2024/12/08/unitedhealthcare-gunman-lookalike-contestants-gather-new-york-city-22147299/>