Biometrics
Successes, Innovations and Challenges

Anil K. Jain
Michigan State University
http://biometrics.cse.msu.edu/

Thales ID eXperience, Madrid, October 2, 2024

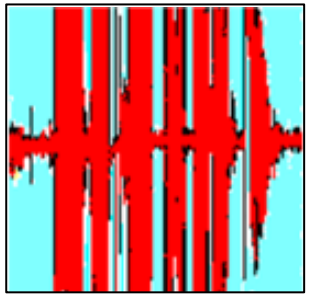
Outline

- Biometric recognition
- Success stories
- State-of-the-art accuracy
- Challenges & path forward

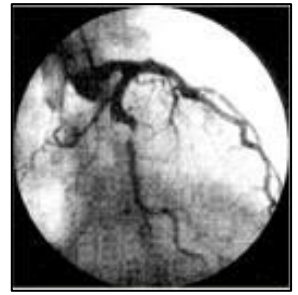
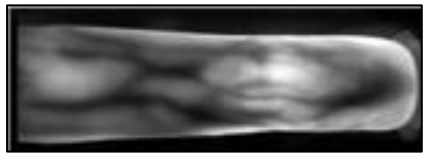
Biometric Recognition

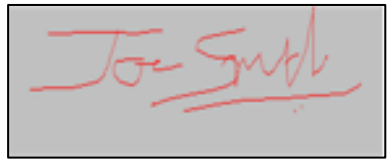
- People can no longer be trusted based on keys, access cards, PIN and even government issued ID.
- Biometrics refers to automated recognition of a person based on their body trait(s).

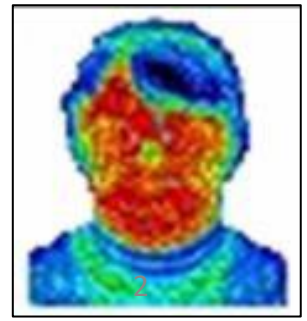




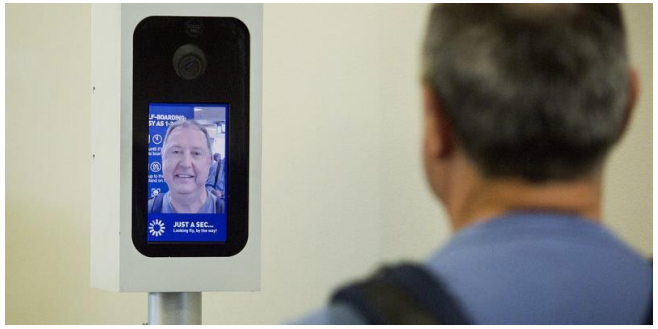



Which Biometric Trait?

Incheon, South Korea: Smart Entry



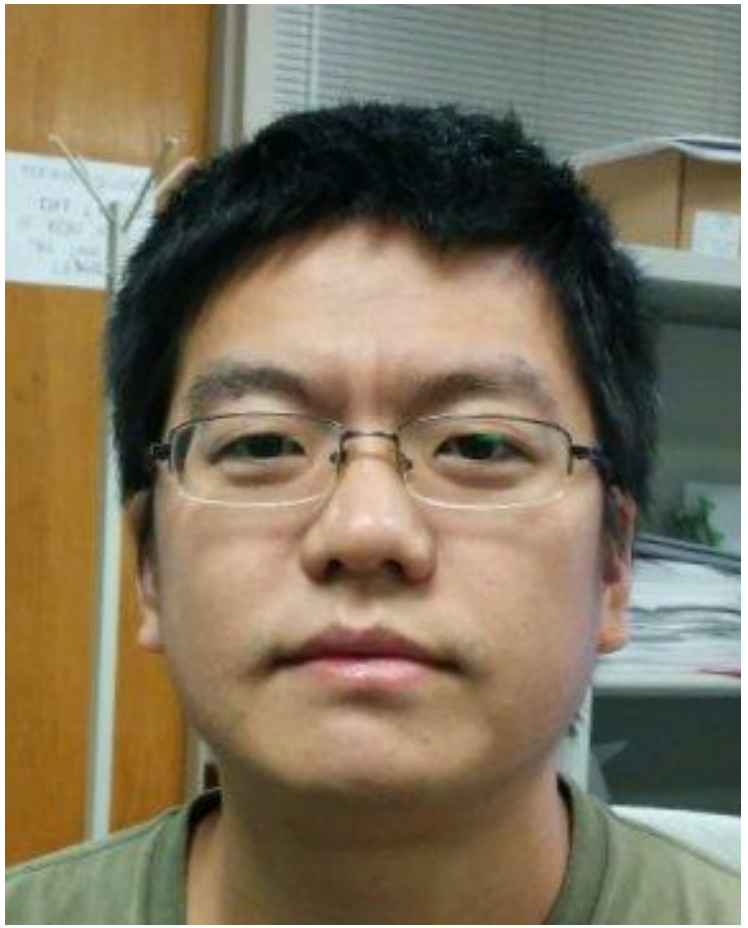
Australia: SmartGate

Amsterdam: Privium border passage

- *Satisfy Individuality* and *permanence* properties
- Large legacy databases
- High search (1:N) accuracy in NIST evaluations
- Fingerprints (Trauring, 1963); Face (Bledsoe,1966); Iris (Daugman, 1993)

Authentication: Pair-wise Comparison

Driver license photo of Kai Cao)

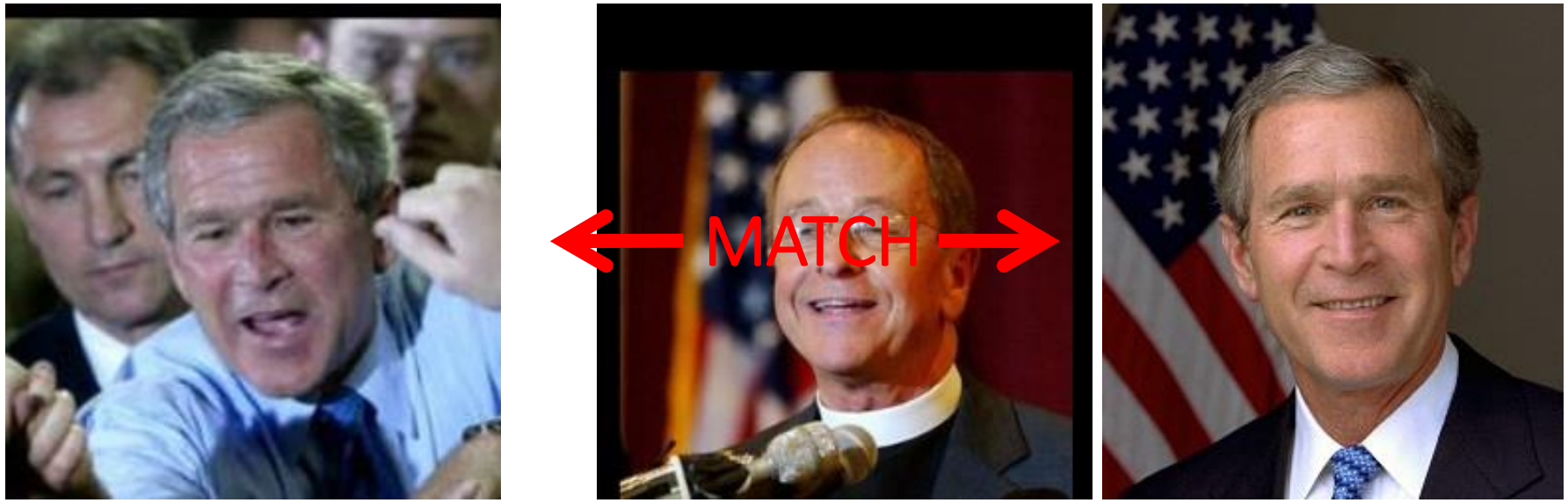


Enrolled face of Kai Cao

Claim of identity is made; system decides if it is the same person based on similarity?

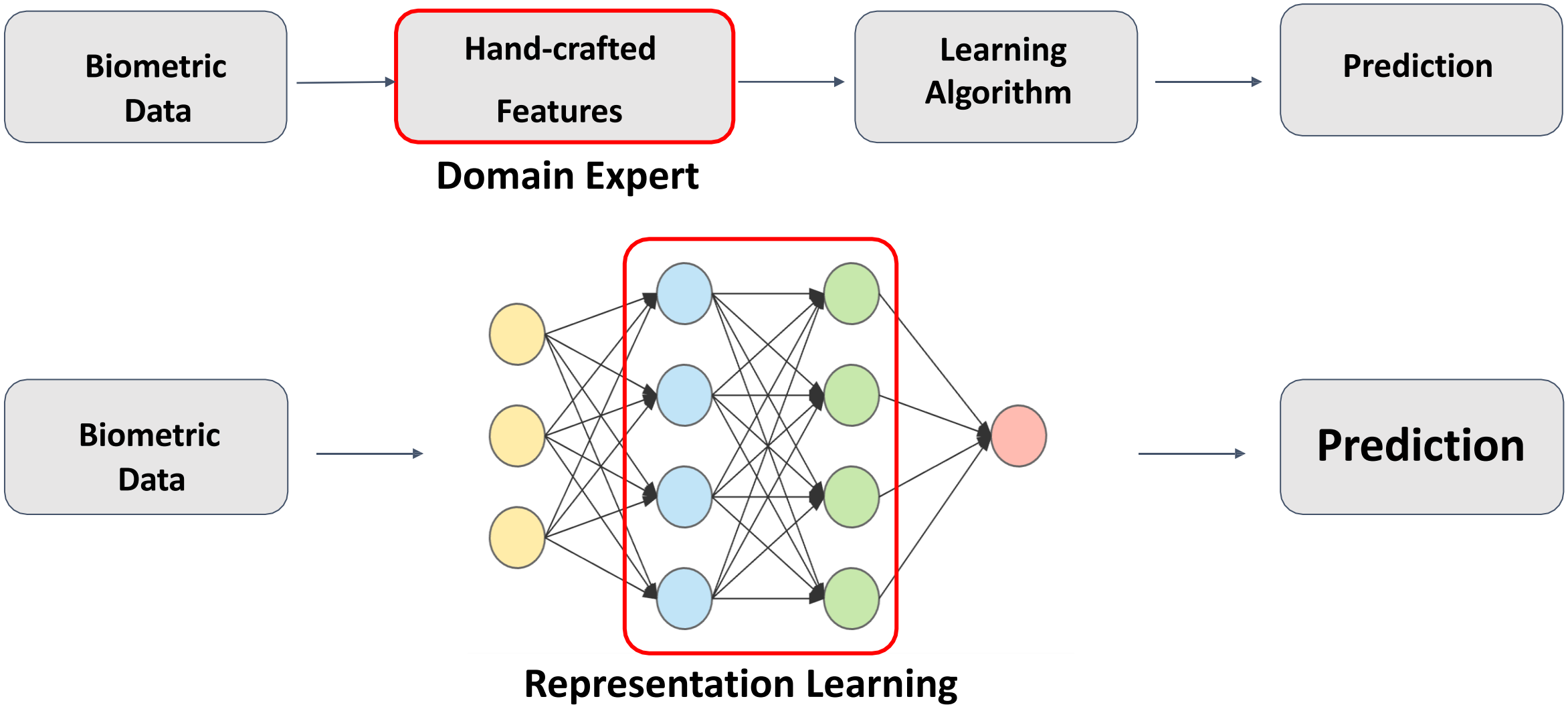
Search (N Pair-wise Comparisons)

Query *Database*



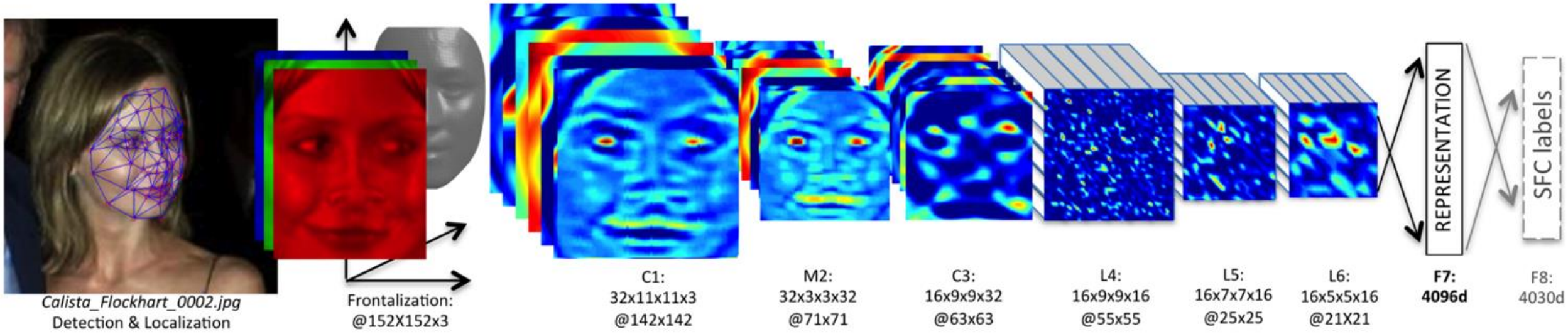
- Find the face in the database which is most similar to the query
- What if the query face is not in the database? Open-set recognition

How to Compute Pair-wise Similarity?



Need to select feature vector (representation, embeddings) and similarity measure

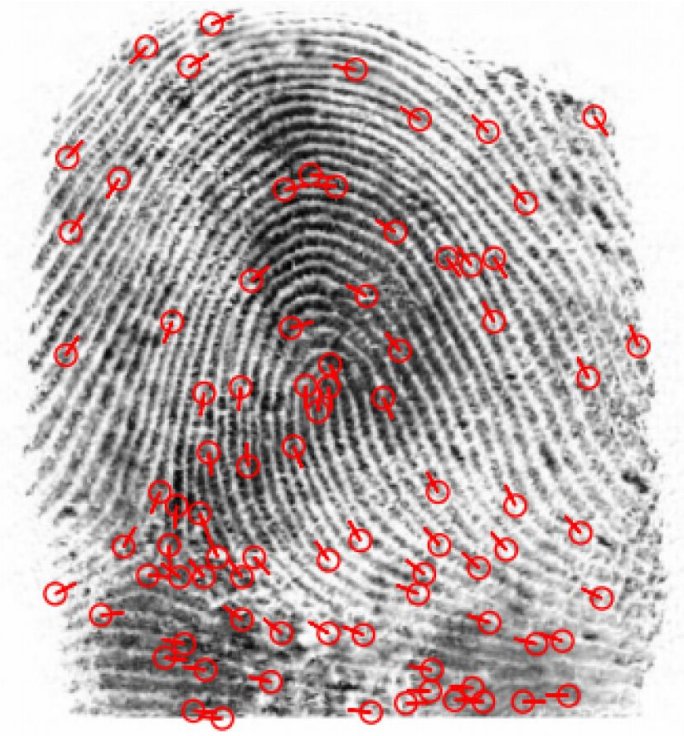
Deep Networks: Deepface (2014)

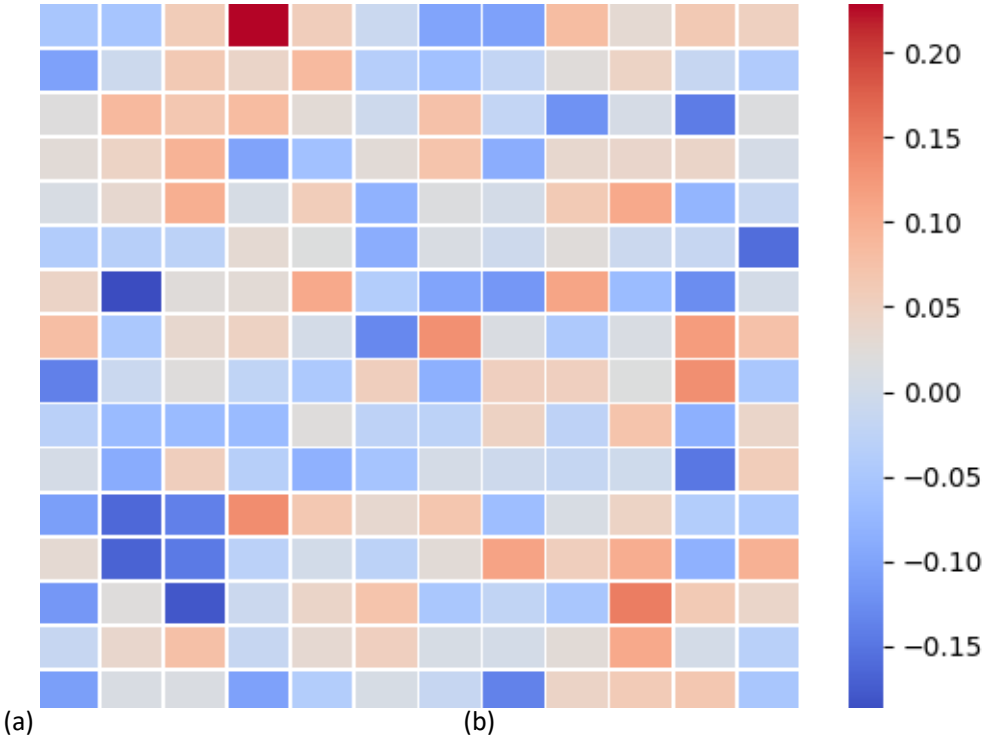


- Multiple layers of neurons connected to a small area in previous layer (120M parameters)
- Deep networks are responsible for progress in face recognition
- **Black Box: no interpretability of features and no ability to explain the decision**

Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. "Deepface: Closing the gap to human-level performance in face verification." CVPR, 2014

Two Representations for Fingerprints



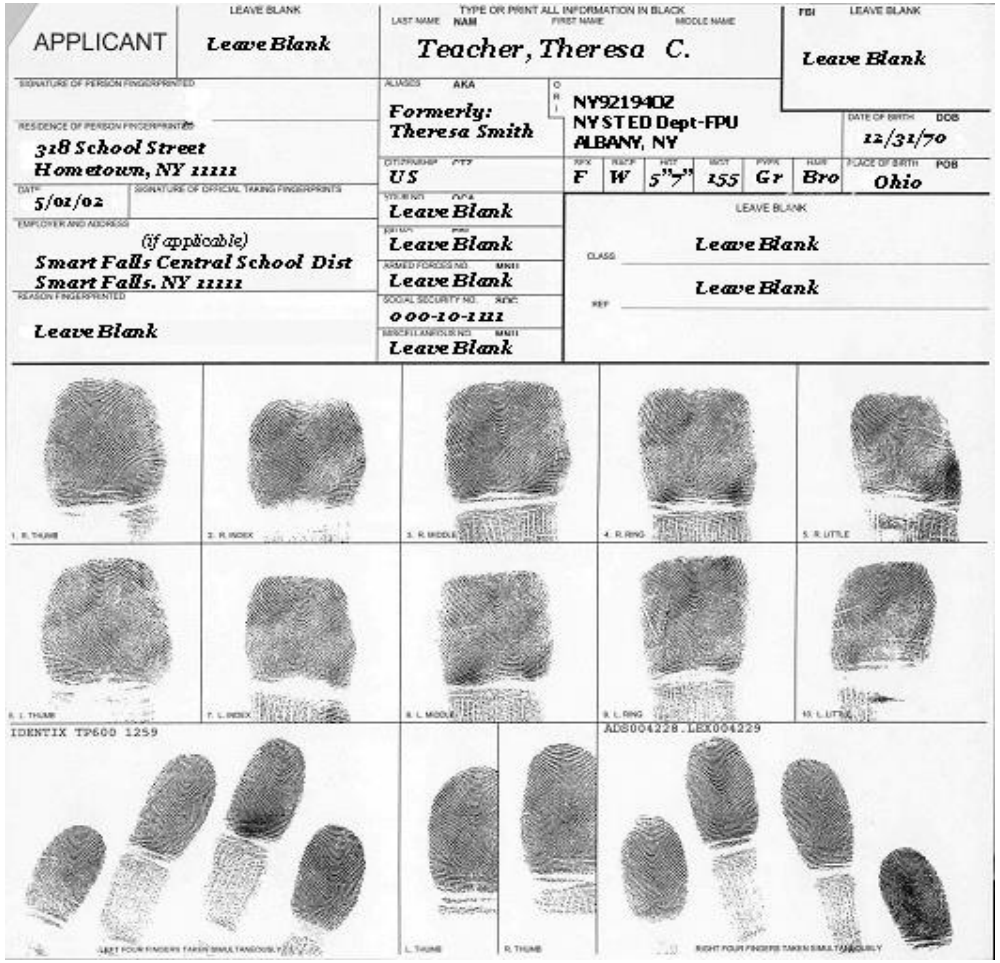


(a) (b)

- Minutiae set & 192-dim (192 bytes) embedding
- Three times faster to compare embeddings than minutiae comparison
- Fusion of the two representations improves accuracy

Engelsma, Cao and Jain, "Learning a Fixed-Length Fingerprint Representation", IEEE Trans. on Pattern Analysis and Machine Intelligence, 2019

Success Story #1: Law Enforcement & Forensics


APPLICANT

Leave Blank

Teacher, Theresa C.

Leave Blank

Formerly: Theresa Smith

NY9219402
NYSTED Dept-FPU
ALBANY, NY

318 School Street
Hometown, NY 11111

5/01/02

12/31/70

F W 5'7" 155 Gr Bro

Ohio

(if applicable)
Smart Falls Central School Dist
Smart Falls, NY 11111

000-10-1111

IDENTIX TP600 1259

FBI Tenprint card (TP), **1924**

Latent print from a crime scene (LP)

100 years of fingerprint collection at FBI

- TP to TP comparison: Have we encountered this person before?
- LP to TP comparison: who left the impression at the crime scene?

From Manual Fingerprint Comparison to AFIS

1960

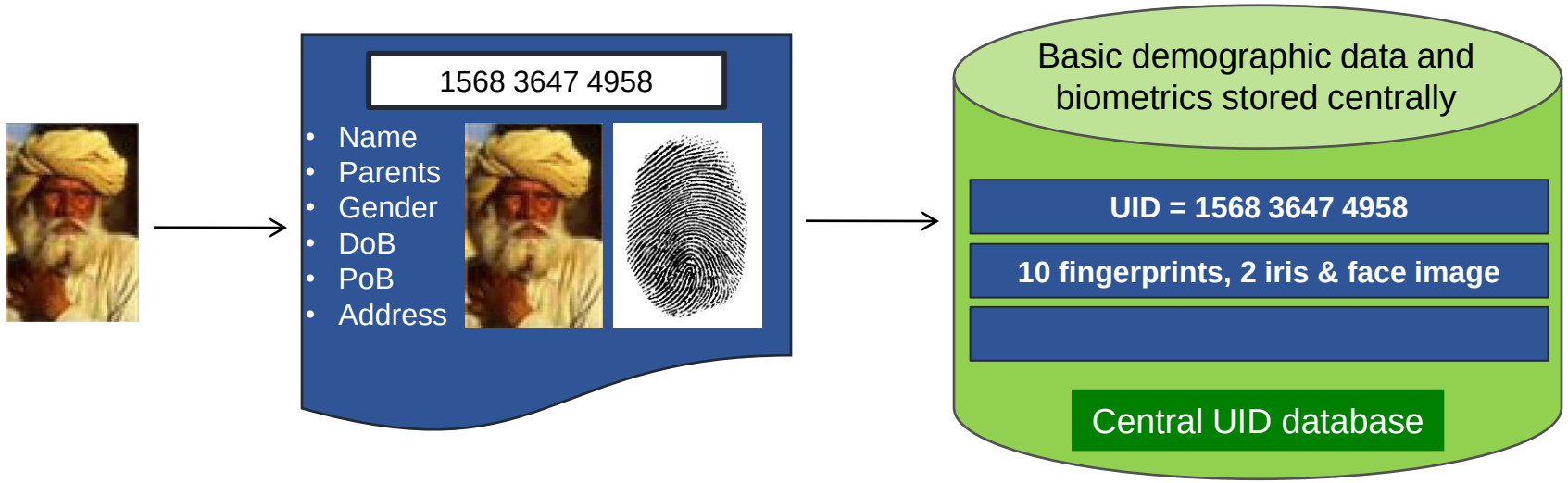
1989 (725K TPs; 15K comparisons/sec

2017 (4M TPs;1M comparisons/sec)

- FBI NGI system repository: ~180M tenprints (civil + criminal + govt/military)
- #Criminal tenprint submissions = 700K; avg. response time = 3 Minutes

Success Story #2: Aadhaar (2008)

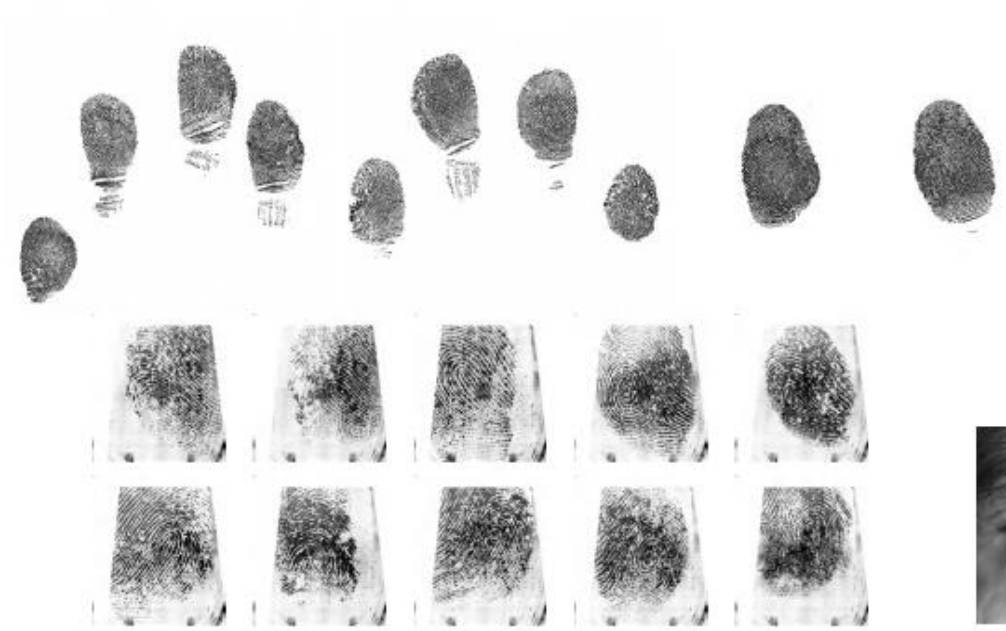
"Issue a 12-digit unique identification number (UID) to Indian residents that can be used to eliminate duplicate and fake identities."



- Efficient, transparent, and targeted delivery of subsidies.
- World's largest biometric system with approx. 1.5 billion enrollment.

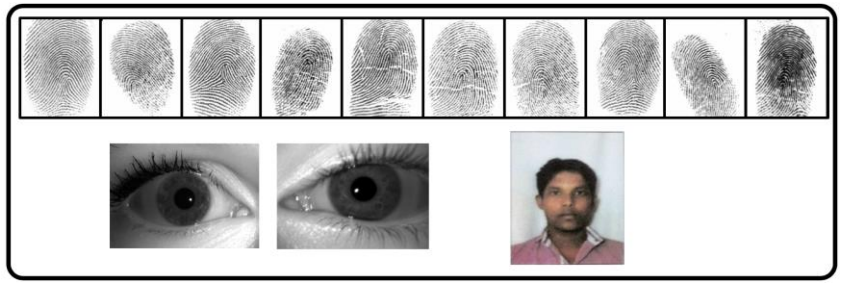
https://uidai.gov.in/

Enrollment

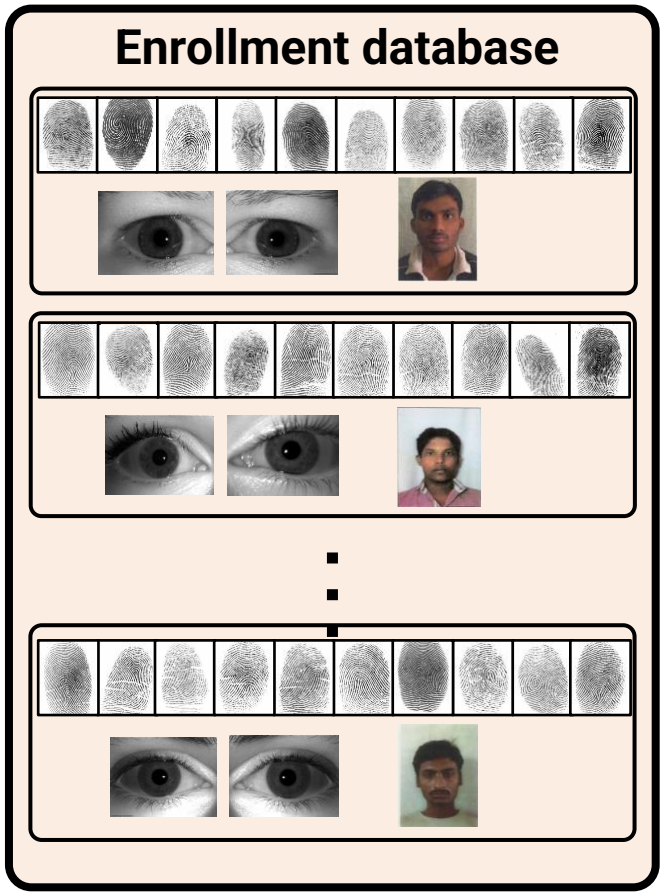


Face, slap fingerprints (4-4-2) and 2 iris images are captured; minimal biographic data collected.

De-duplication (1 to 1.5 billion comparison)



Biometrics of new Applicant
(No demographic info is used)



Already in Database?

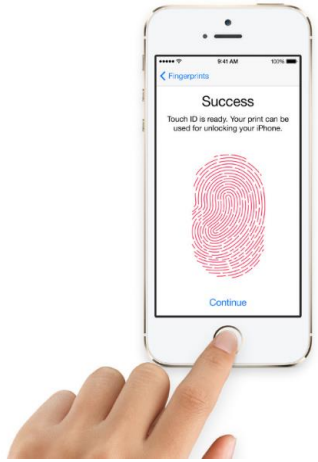
Fusion of 10 prints, two irises and face is necessary to distinguish among 1.5 billion individuals

Authentication (12-digit ID + fingerprint)

Approximately 70 million authentications/day (total of 130 billion to date)

Success Story #3: Mobile Phone Unlock & Payment

The Pantech GI100 (2004)



Touch ID, iPhone 5S (2013)

Apple Pay, iPhone 6 (2014)

Face ID, iPhone X (2017)

Delta ID, phone with iris

Vivo In-Display Scanner (2018)

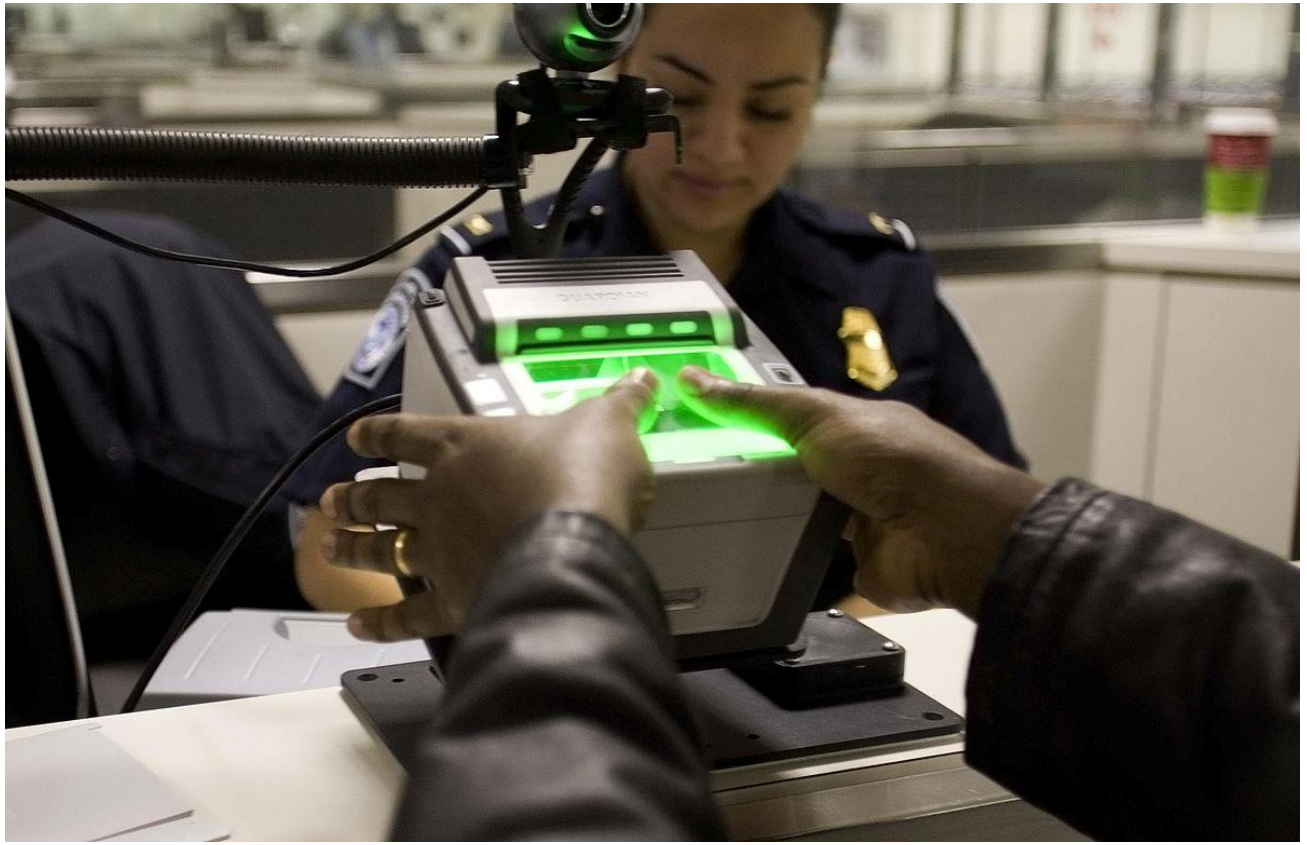
Galaxy S10's in-screen ultrasonic fingerprint scanner

Touch ID was revolutionary: convenience, accuracy, security, cost (1 US$) & latency

https://www.theverge.com/23868464/apple-iphone-touch-id-fingerprint-security-ten-year-anniversary

Success Story #4: Who is Entering/Leaving the Country?

Twin tower attack, NYC (9/11, 2021)



US-VISIT (2003)

In response to the attacks, U.S. Congress enacted the Patriot Act, to dramatically strengthen national security.

Entry/Exit Systems

- Airport entrance, baggage dropoff & flight boarding use face recognition.
- Passenger photo is compared with DHS database (passport,flight manifest.

NIST Evaluations (Constrained Acquisition)

1:1 comparison (authentication); FAR = 0.001%

Fingerprint: TAR = 99.56% (Verifinger V12.3)

Iris: TAR = 99.43% (NIST IREX IX)

Face: TAR = 99.83% (NIST FRVT 2022)

1:N Comparison (Identification); FPIR = 0.001

Fingerprint (10 fingers): FNIR = 0.001 (5M gallery)

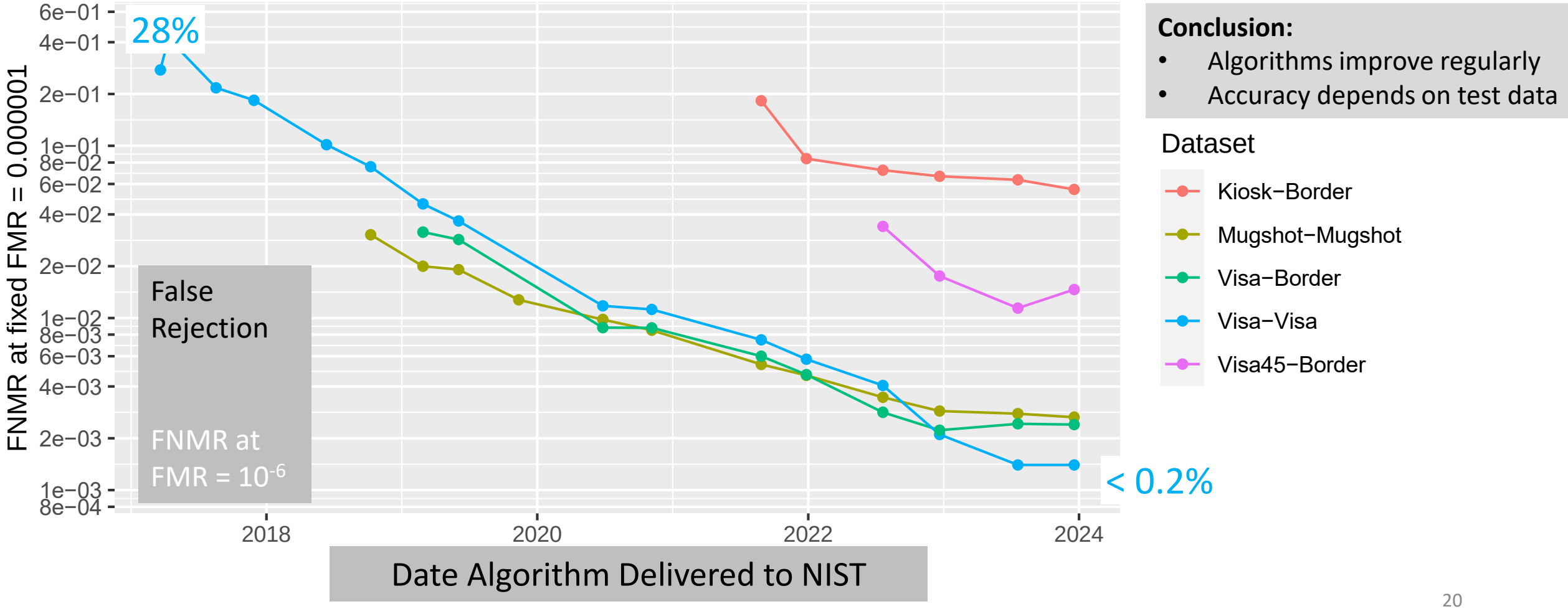
Fingerprint (1 finger): FNIR = 0.019 @ (100K gallery)

Iris (Both eyes): FNIR = 0.0035 (500K gallery)

Face: FNIR = 0.03 (12M gallery)

[1] NIST FRVT 1:N Identification: *https://pages.nist.gov/frvt/html/frvt1N.html*; [2] NIST FpVTE: *https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf*
[3] NIST IREX 10 Identification Track: *https://pages.nist.gov/IREX10/*

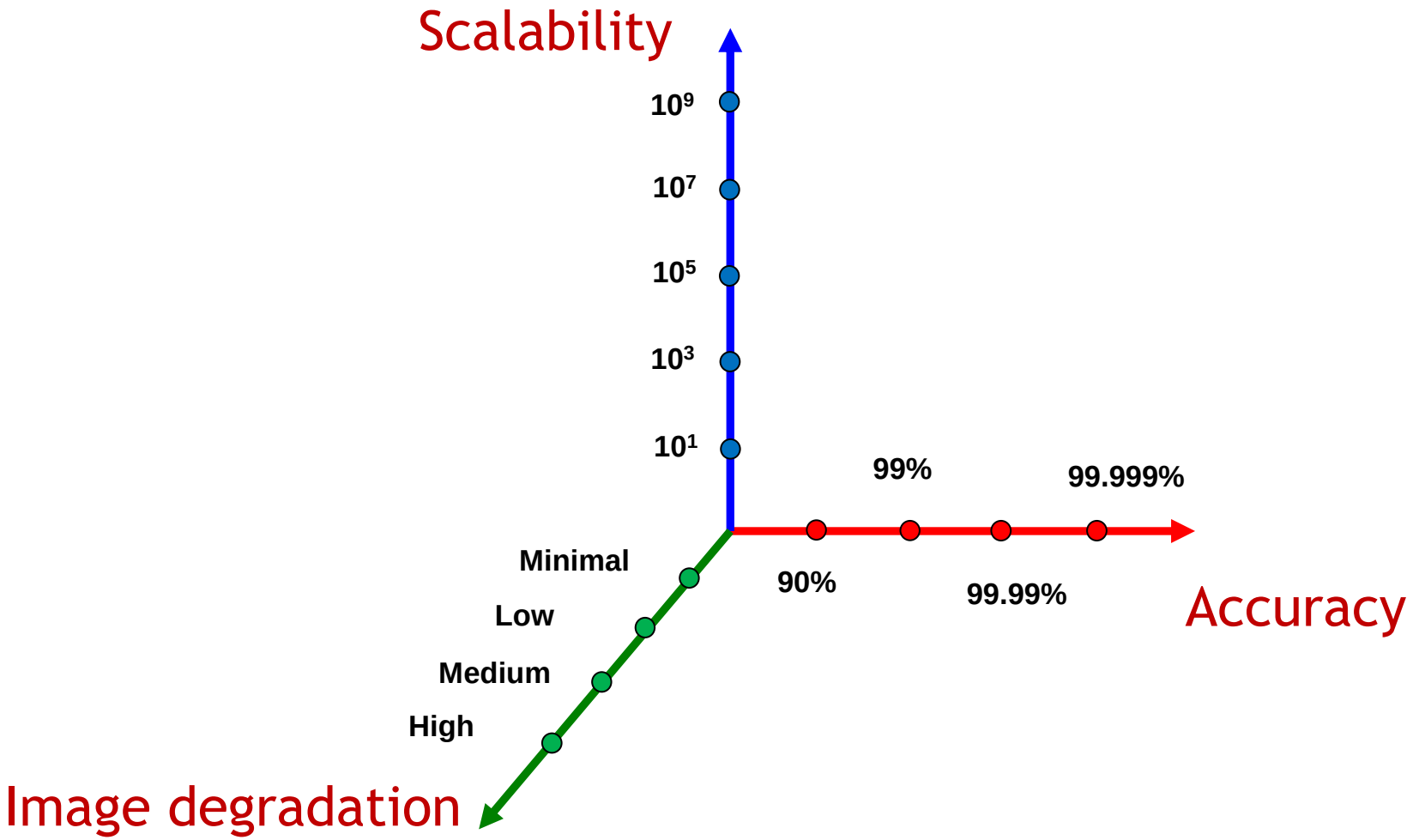
1:1 Face Accuracy Gains Continue



Conclusion:

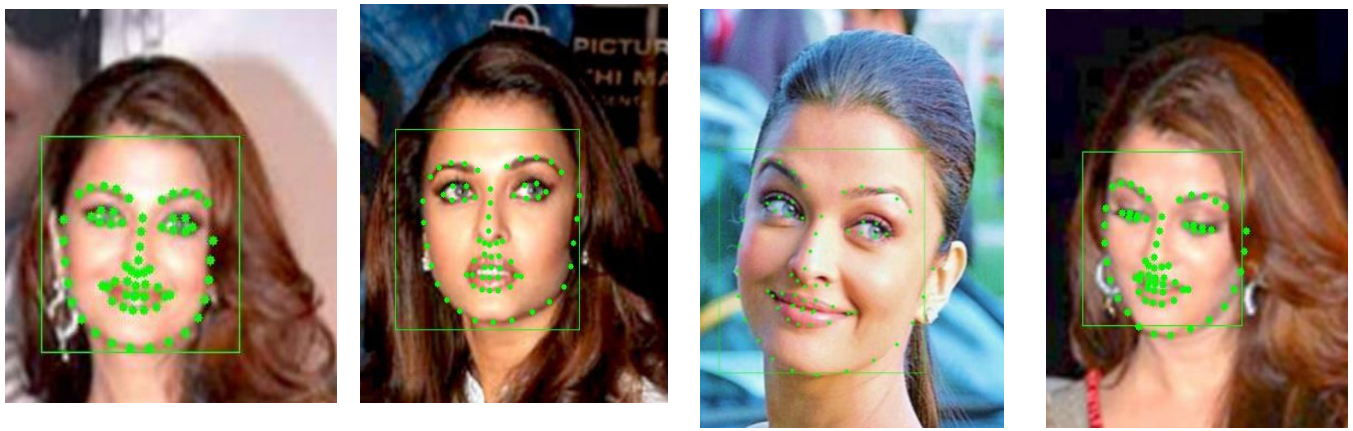
- Algorithms improve regularly
- Accuracy depends on test data

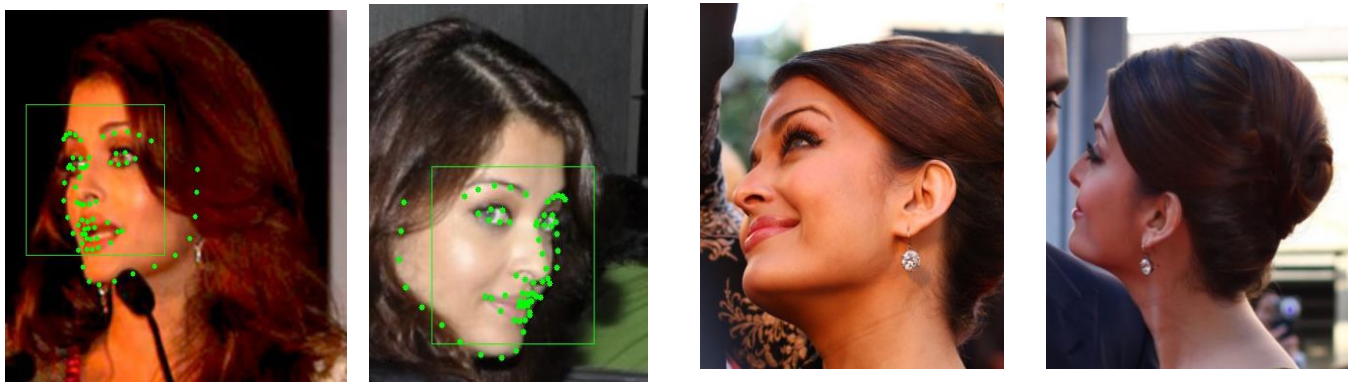
Challenges



Speed (template size), spoof attacks, template security, usability

Sources of Error in Biometrics





Intra-person variations (PIE, aging, occlusion)

Inter-person similarity

Semi-constrained Face Recognition

Probe (1984)

Threshold=0.54 @ FAR=0.01%

0.83

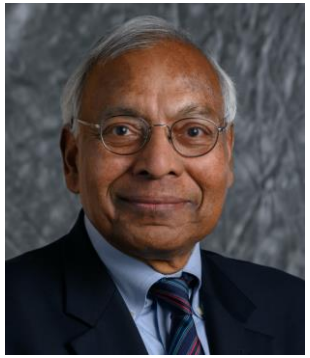
0.89

0.72

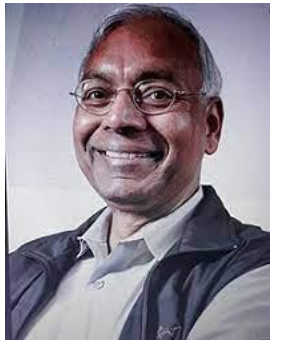
0.81

0.58

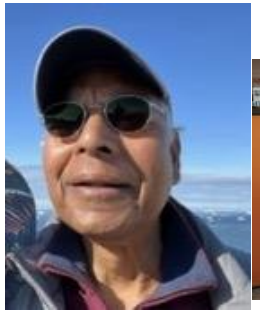
0.72



0.82



0.71



0.74

0.66

0.63

0.49

0.17

Unconstrained Face Recognition

Composite image of evidence pulled by the U.S. District Court for the District of Columbia against Debra Maimone. (U.S. District Court D.C.)

FBI used license plate readers, informants & facial recognition to identify rioters

https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/

Wrongfully Accused by Algorithm

- Michigan Police searched a CCTV frame of robbery suspect against its database of 49M photos. Williams photo had the highest similarity.
- But, Williams was at his home at the time of robbery! What went wrong?

CCTV frame

Closest match in database (old driver license photo of Williams)

Photo of Williams taken by media

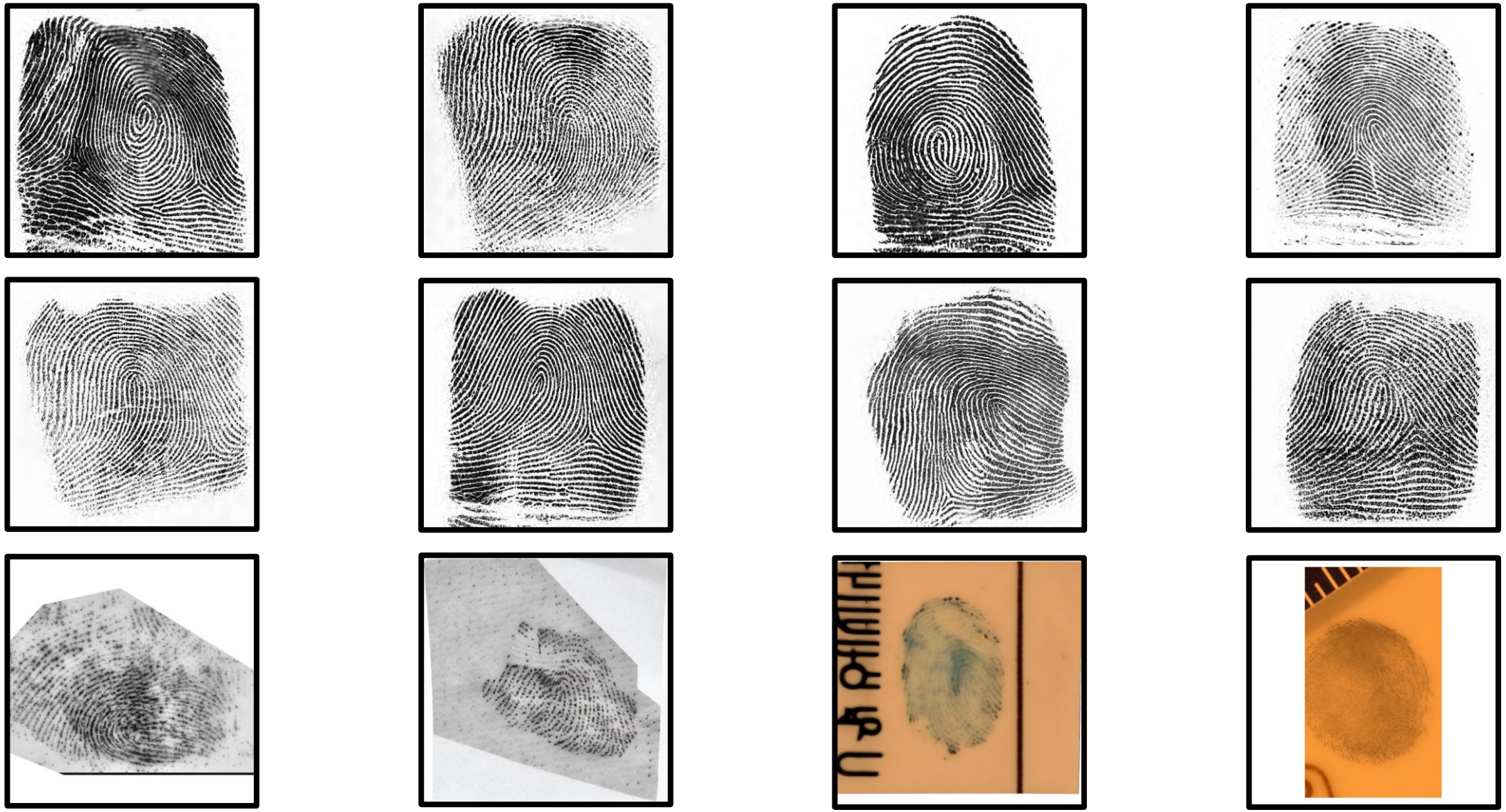
www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

User Consent and Biometric Data Privacy

- **General Data Protection Regulation (GDPR); May 25, 2018**
  - Personal Data: “any information that relates to an individual who can be directly or indirectly identified. This includes ethnicity, gender and biometric data.”
  - Seven data protection principles: (i) Lawfulness, fairness and transparency; (ii) purpose limitation; (iii) storage limitation; (iv) Integrity and confidentiality
- How do researchers get access to biometric data?

https://gdpr.eu/

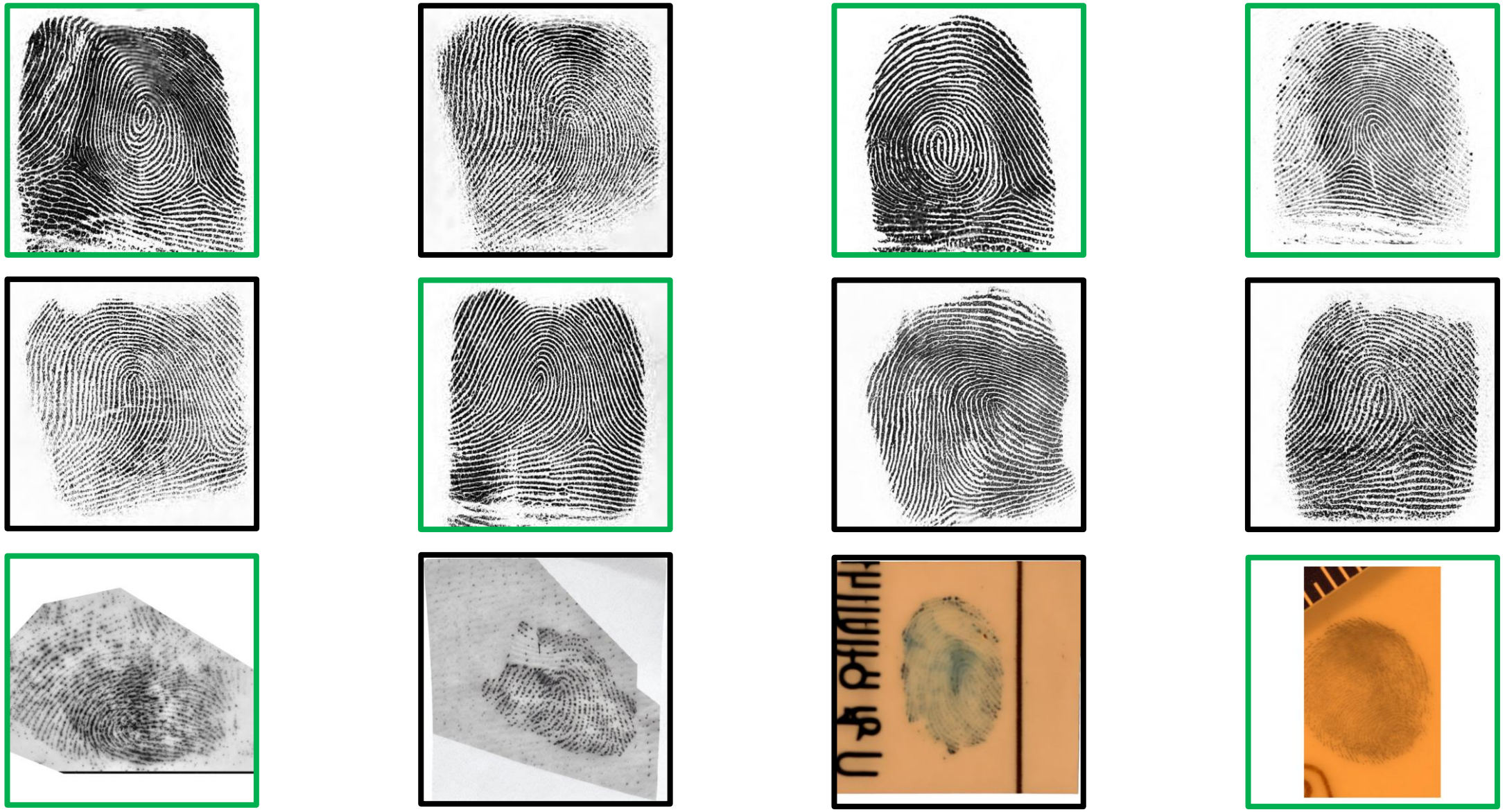
Real vs. Computer Generated Images



J. J. Engelsma, S. A. Grosz and A. K. Jain, "PrintsGAN: Synthetic Fingerprint Generator", IEEE TPAMI, 2022

S. A. Grosz and A. K. Jain, ” Universal Fingerprint Generation: Controllable Diffusion Model with Multimodal Conditions", IEEE TPAMI, 2024 (under review)

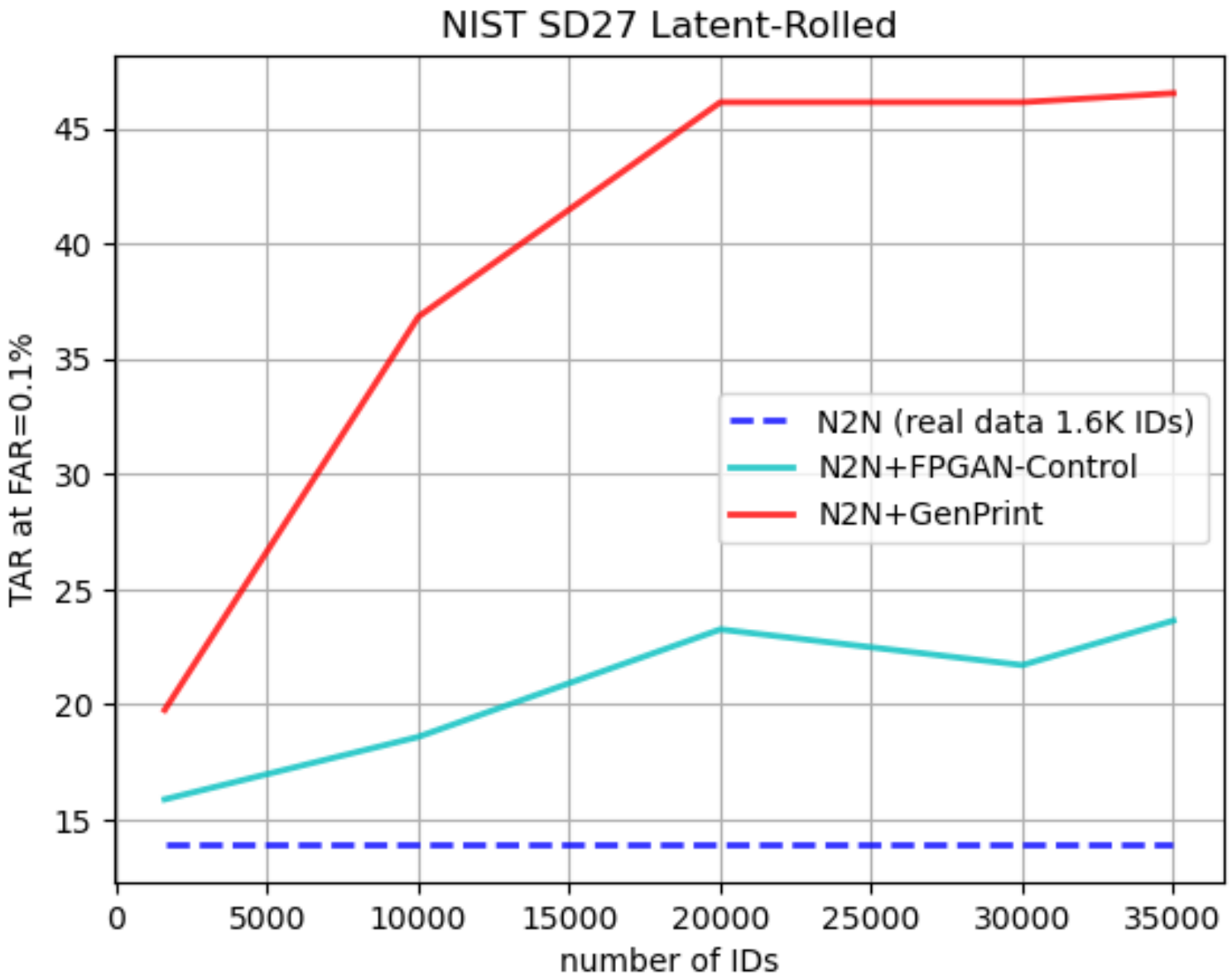
Real vs. Computer Generated Images



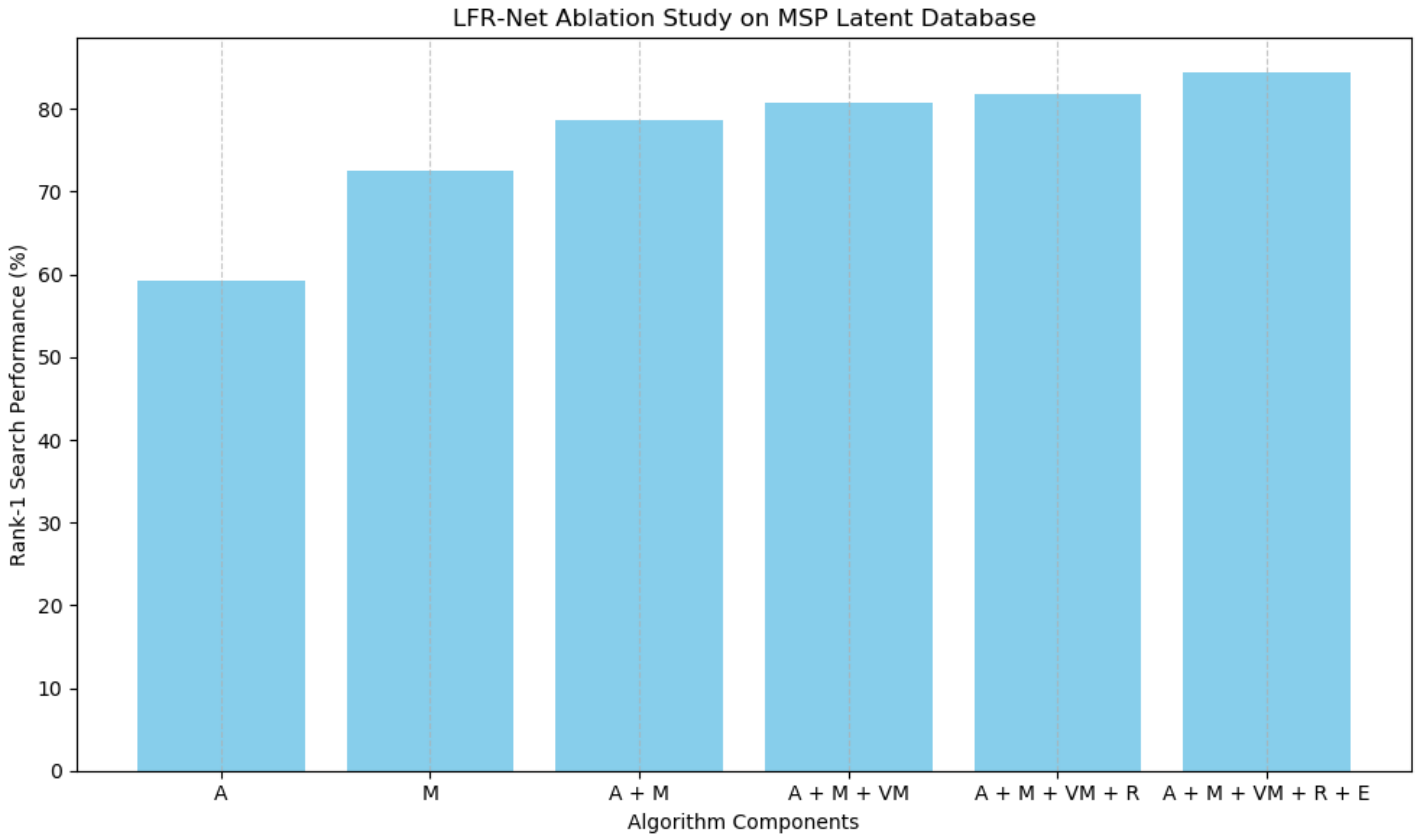
J. J. Engelsma, S. A. Grosz and A. K. Jain, "PrintsGAN: Synthetic Fingerprint Generator", IEEE TPAMI, 2022

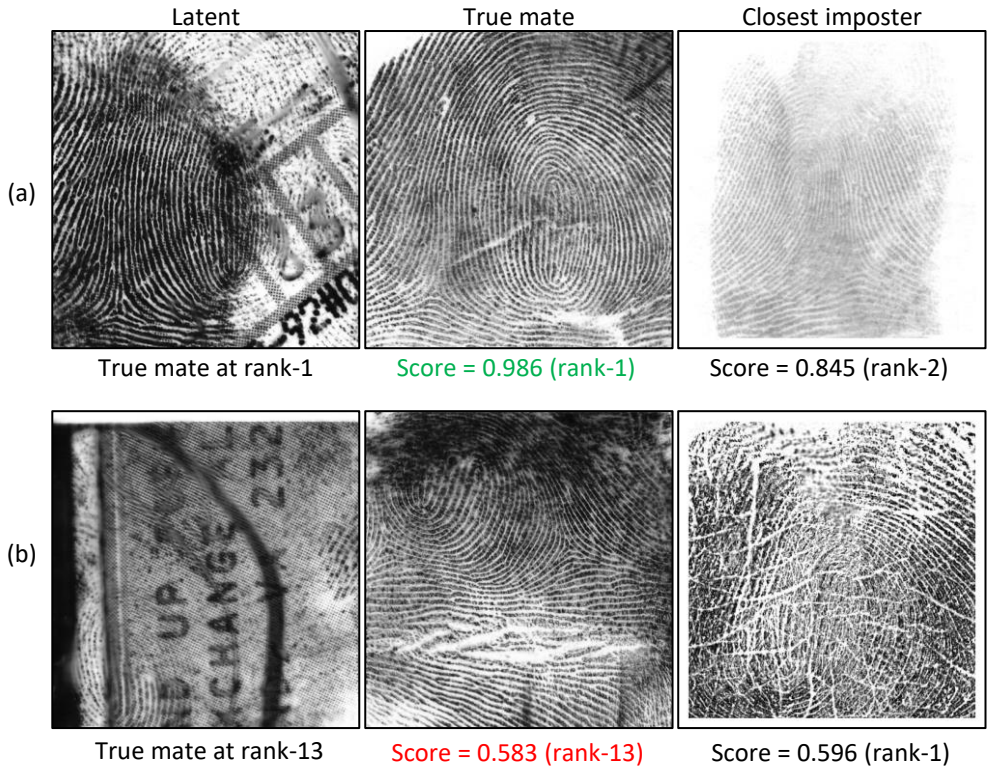
S. A. Grosz and A. K. Jain, ” Universal Fingerprint Generation: Controllable Diffusion Model with Multimodal Conditions", IEEE TPAMI, 2024 (under review)

Performance Gain by Data Augmentation



Latent Fingerprint Matching



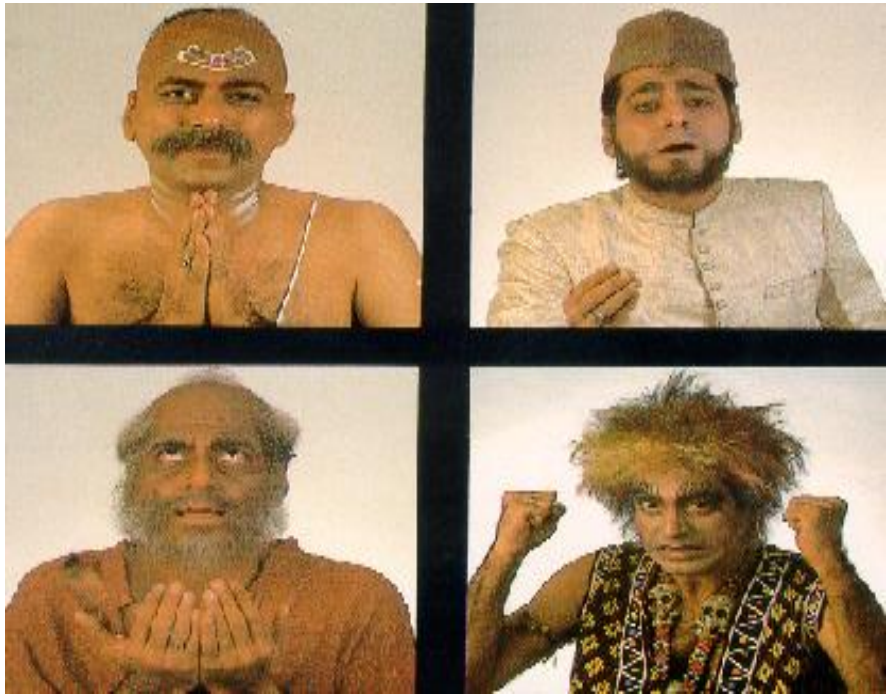


A = AFR-Net, M = Minutiae, VM = Virtual Minutiae, R = Realignment, E = Enhancement

S. A. Grosz and A. K. Jain, "Latent Fingerprint Recognition: Fusion of Local and Global Embeddings", IEEE Trans. Information Forensics and Security, 2023.

Presentation Attacks

Gummy finger



Face disguise

Silicone Mask

Print

Fake hand

Fake eyeball

Fingerprint alteration

Iarpa Odin: **TDR = 98% @FAR =0.2%**

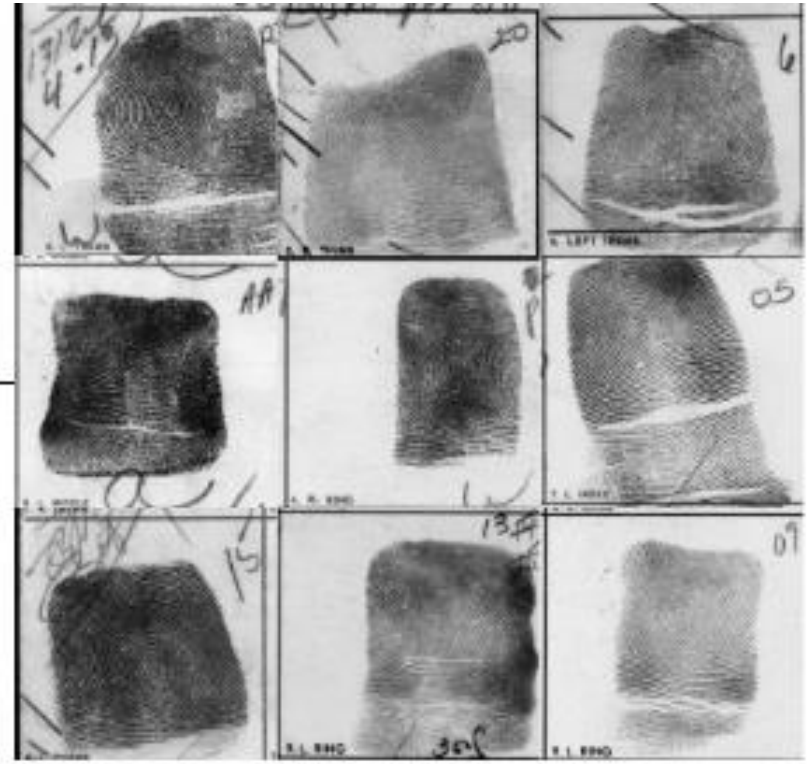
Privacy-Preserving Authentication

Fingerprint Reader

Encrypted Query

Matching in encrypted domain

Encrypted Scores



Enrolled database

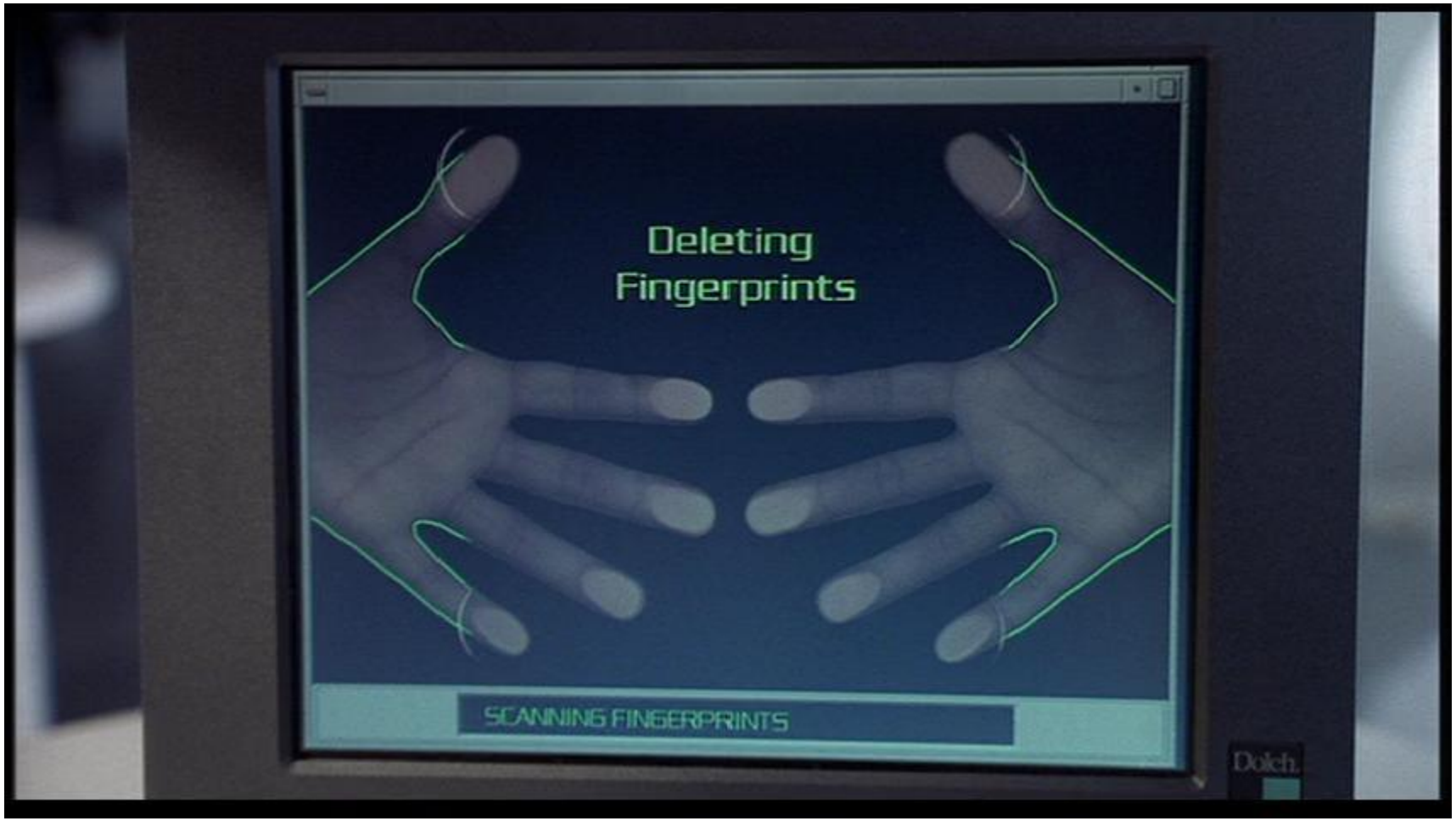
Accurate & fast image search in encrypted domain protects biometric data

Engelsma, Jain and Boddeti, "HERS: Homomorphically Encrypted Representation Search", IEEE T-BIOM, 2021.

Summary

- Biometric recognition is indispensable in growing efforts to enhance security and eliminate fraud.
- Fingerprint, face and iris will continue to dominate the market; use of face is growing (e.g., ID verification, surveillance).
- Growing deployments for civil registration, border crossing, banking, PoS payment and travel and immigration.
- Challenges: seamless integration in applications, recognition under non-ideal conditions, access to data, system integrity,…
- Biometrics is here to stay!!

Fingerprint Obfuscation



Will Smith in “Men in Black” (1997)

S. Yoon, J. Feng and A. K. Jain, "Altered Fingerprints: Analysis and Detection", *IEEE Trans. Pattern Analysis and Machine Intelligence*, 2012.