Biometrics
Successes, Innovations and Challenges

Anil K. Jain

Michigan State University

http://biometrics.cse.msu.edu/

ELECOM, Mauritius, November 20, 2024

Mauritius Wallet
Digital ID Wallet for Govt Service Access

Implementation of the Mobile ID in the MWA digital wallet app, Mauritius will become the first African country to bring in a digital ID wallet based on ISO standards.

Users will need to complete a native device unlock authentication method like face or fingerprint biometrics to activate their digital wallet. **Users upload photos of both sides of their ID card as well as a photo of themselves. The digital version of their ID card will then be created, along with a QR code that can be used for verification.**

Outline

- Biometric recognition
- Success stories
  - Law enforcement
  - India's national ID, Aadhaar
  - Mobile phone unlock & payment
  - Airport entry/exit
- State-of-the-art accuracy
- Challenges & path forward

Biometric Recognition

- **Lack of Trust:** We now live in a society where people can no longer be trusted based on keys, access cards, PIN and even government issued ID. Smartphone security

- **Digital safety:** Are you using one of the world's most popular passwords? 123456, admin

- **ID/Travel document fraud:** False (counterfeits, forgeries) and modified genuine documents

- **Biometrics:** Automated recognition of a person based on their body trait(s)

Which Biometric Trait?
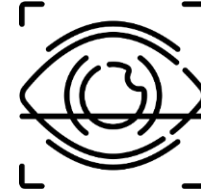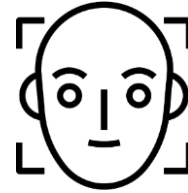
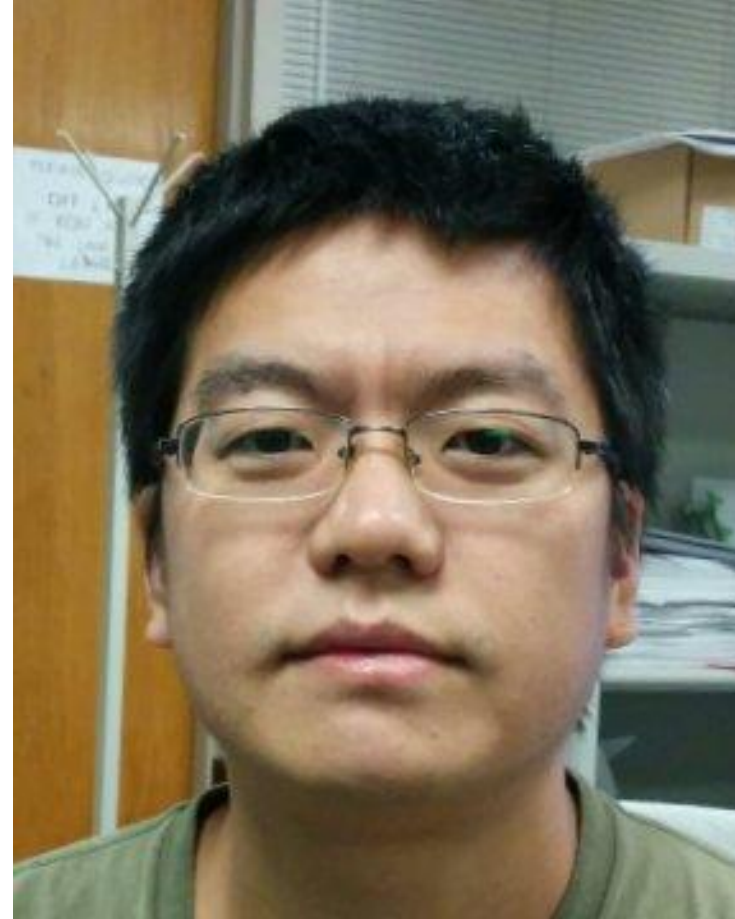Incheon, South Korea: Smart Entry

Australia: SmartGate

Amsterdam: Privium border passage

- *Satisfy Individuality* and *permanence* properties
- Legacy databases
- Extremely high search (1:N) accuracy in NIST evaluations
- Representation/matching: Fingerprints (Trauring, 1963); Face (Bledsoe,1966); Iris (Daugman, 1993)

Central Problem: Pair-wise similarity

Selfie + Kai Cao

Enrolled face of Kai Cao

Claim of identity is made; system decides if it is the same person?
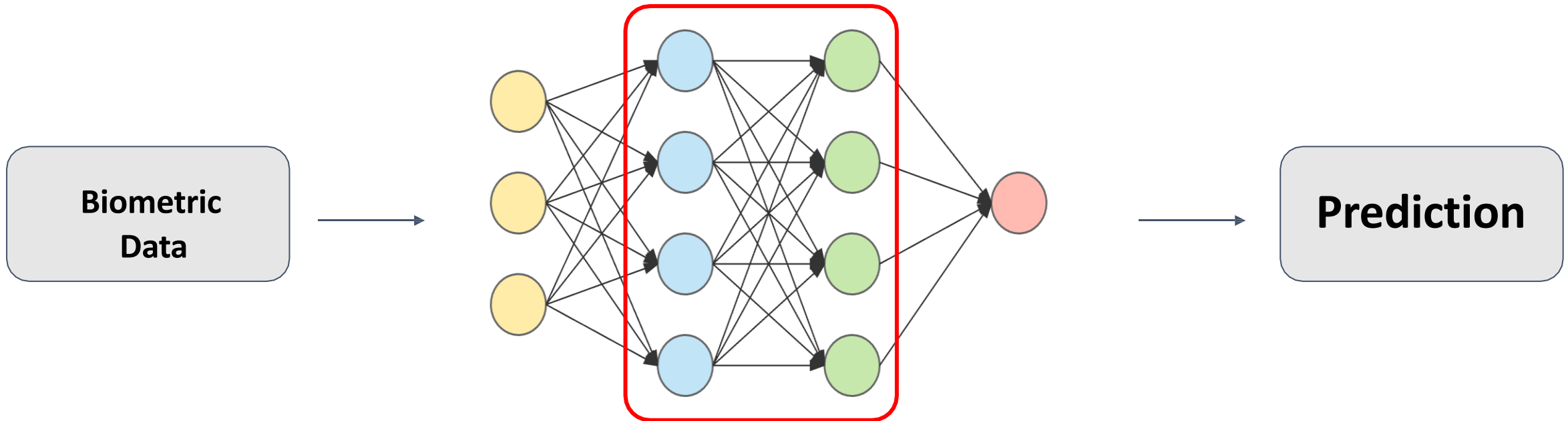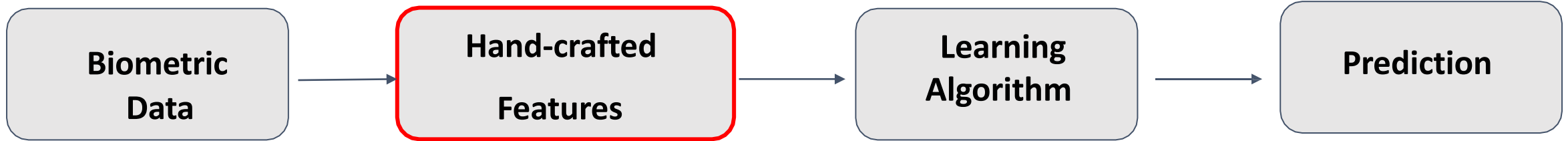
Search (N Pair-wise Comparisons)

Probe   *Gallery*

MATCH

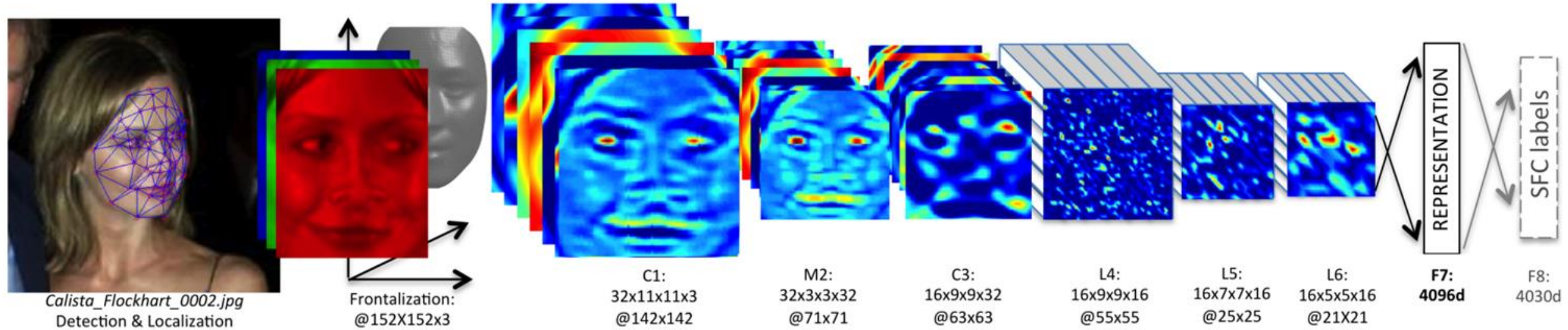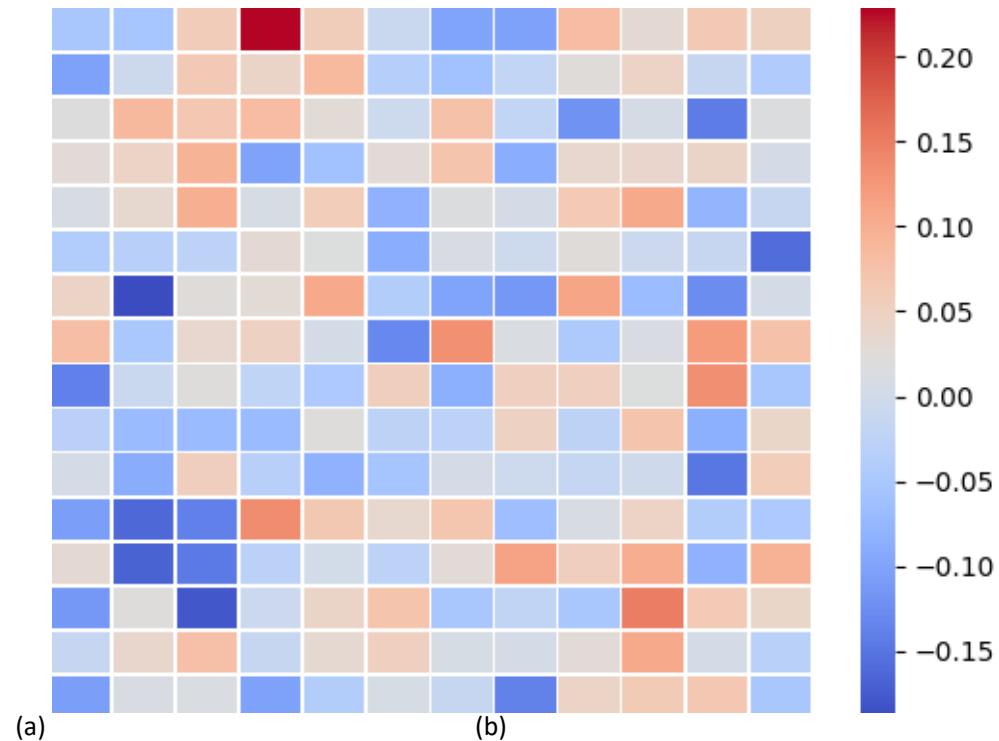No claim of identity is made; Is the probe (query) in the gallery?

How to Compute Pair-wise Similarity?

Select a feature vector (representation, embeddings) and a measure to compare two vectors

Deep Networks: Deepface (2014)

Calista_Flockhart_0002.jpg
Detection & Localization

Frontalization:
@152X152x3

C1:
32x11x11x3
@142x142

M2:
32x3x3x32
@71x71

C3:
16x9x9x32
@63x63

L4:
16x9x9x16
@55x55

L5:
16x7x7x16
@25x25

L6:
16x5x5x16
@21X21

F7:
4096d

F8:
4030d

REPRESENTATION

SFC labels

- 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 representation & 192-dim (192 bytes) embedding
- Comparing embeddings is ~3 times faster than minutiae comparison
- The two representations are complimentary; their fusion 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

FBI Tenprint card (TP), 1924

Latent print from a crime scene (LP)

- 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: ~180 million tenprints (civil + criminal + govt/military)**
- **#Criminal tenprint submissions = 700K; avg. response time = 3 Minutes**

Forensic Science Lab, Mauritius was established in the 1950's; an autonomous body under the Prime Minister's Office.
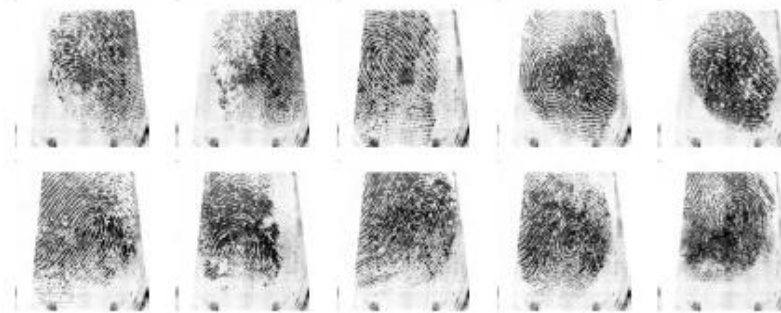
Success Story #2: Aadhaar (2008)

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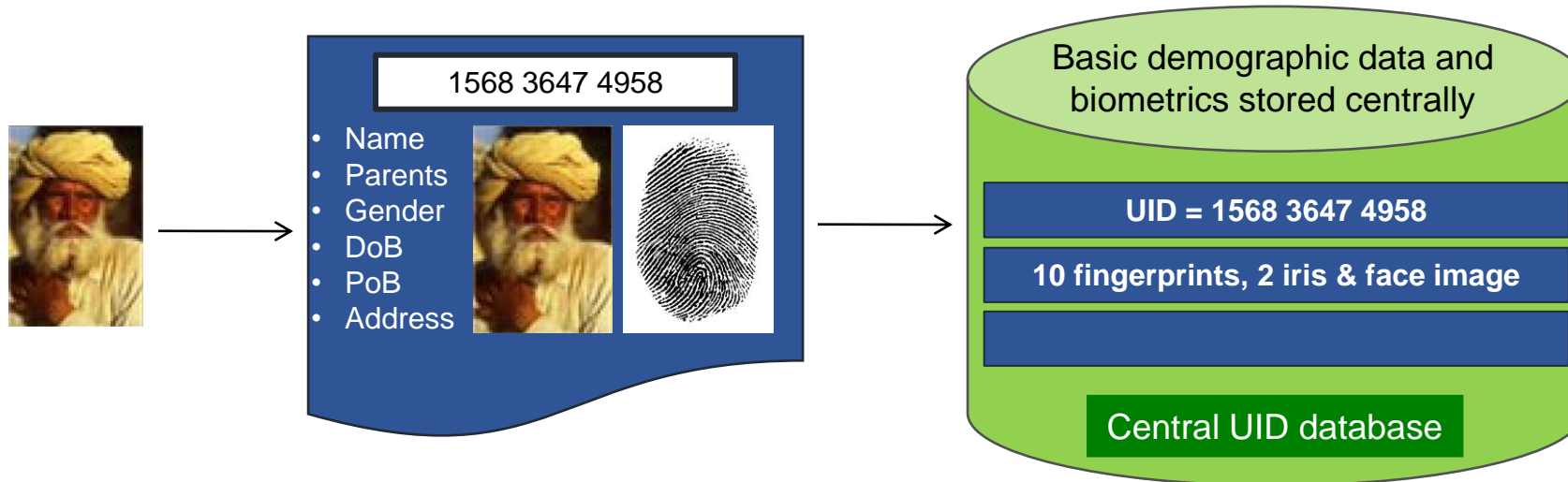

- Efficient, transparent, and targeted delivery of subsidies.
- World's largest biometric system with over 1.5 billion enrollment.

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)

Enrollment database

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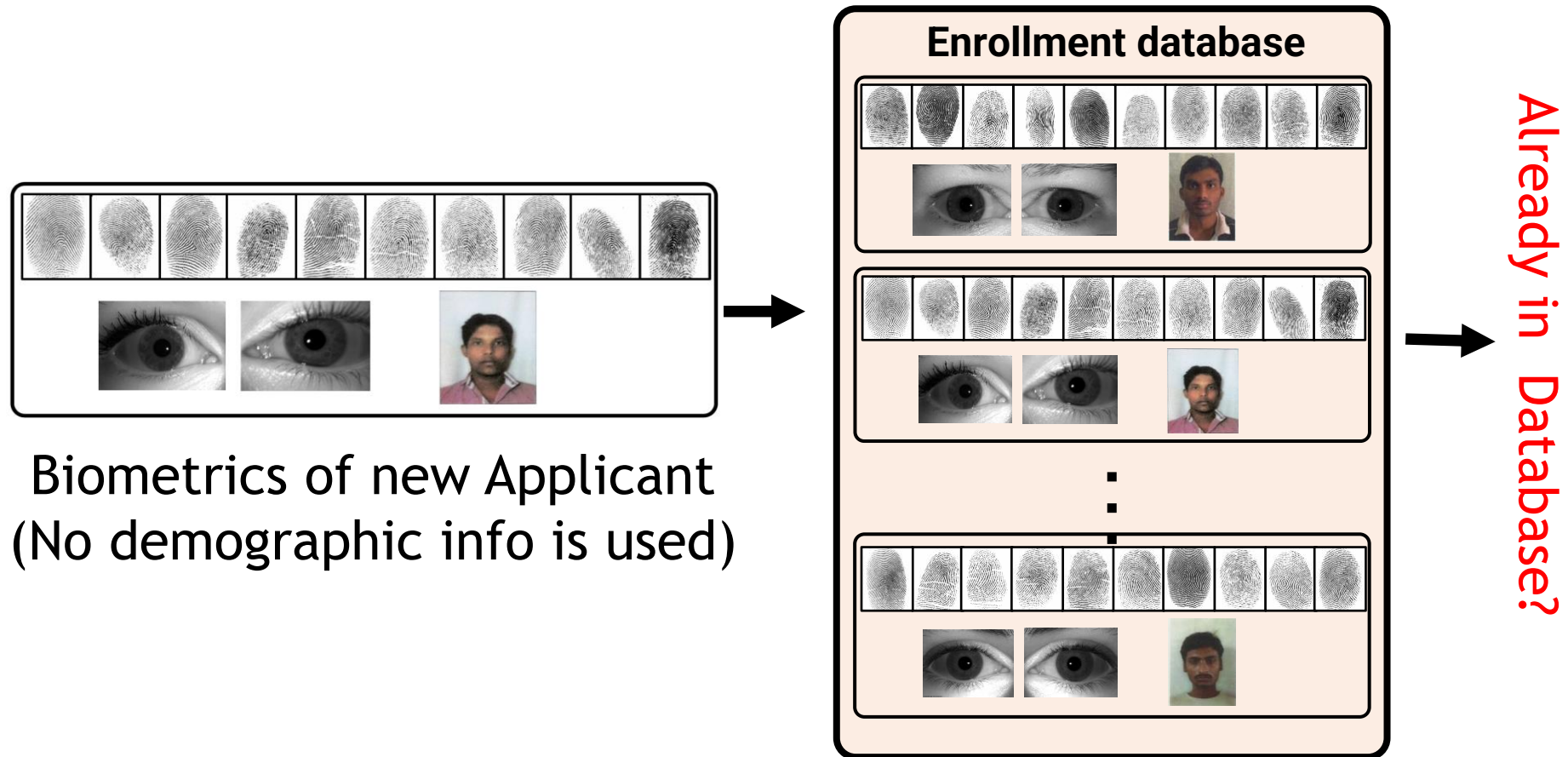
Fusion of 10 prints, two irises and face is necessary to distinguish among 1.5 billion individuals

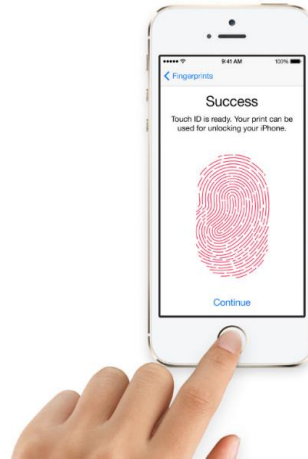# Authentication (12-digit ID + fingerprint)

~70 million authentications/day (total130 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

17

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

Mauritius Wallet
Digital ID Wallet for Govt Service Access

Implementation of the Mobile ID in the MWA digital wallet app, Mauritius will become the first African country to bring in a digital ID wallet based on ISO standards.

Users will need to complete a native device unlock authentication method like face or fingerprint biometrics to activate their digital wallet. **Users upload photos of both sides of their ID card as well as a photo of themselves. The digital version of their ID card will then be created, along with a QR code that can be used for verification.**

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

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

US-VISIT (2003)

In response to the 9/11 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)

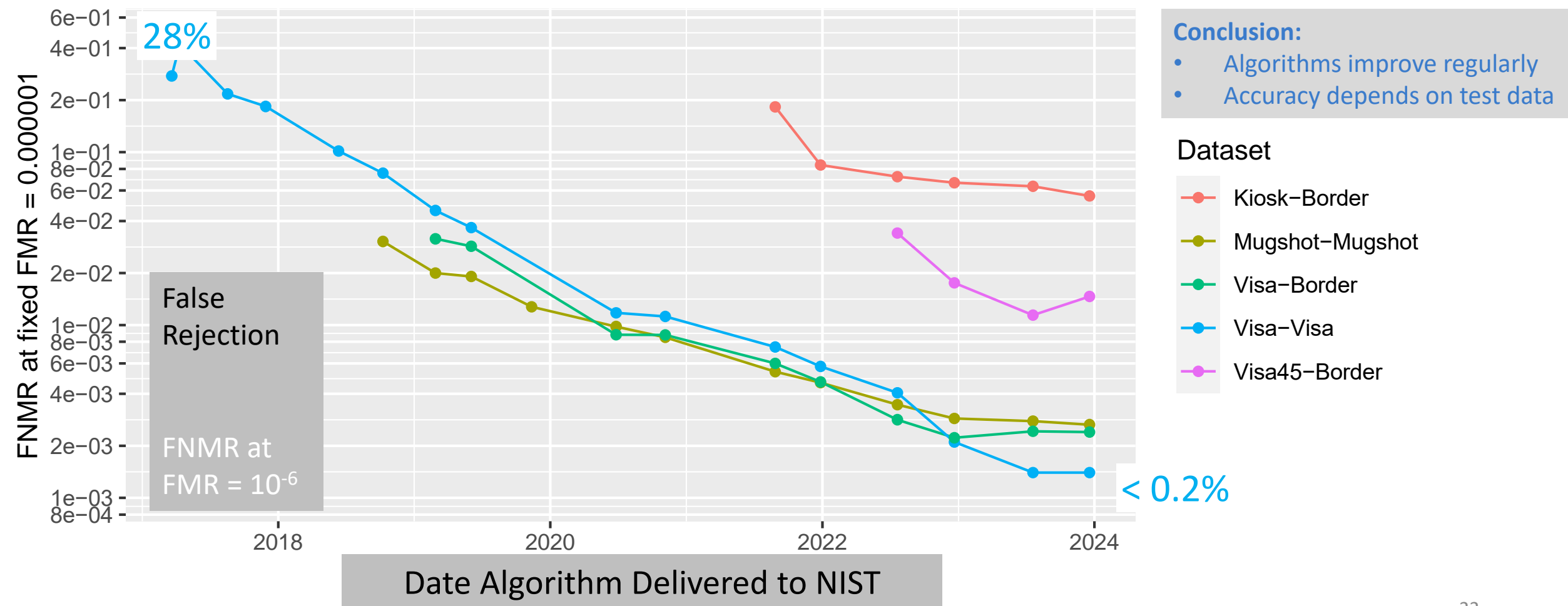**1:N Comparison (Identification); FPIR = 0.001**

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

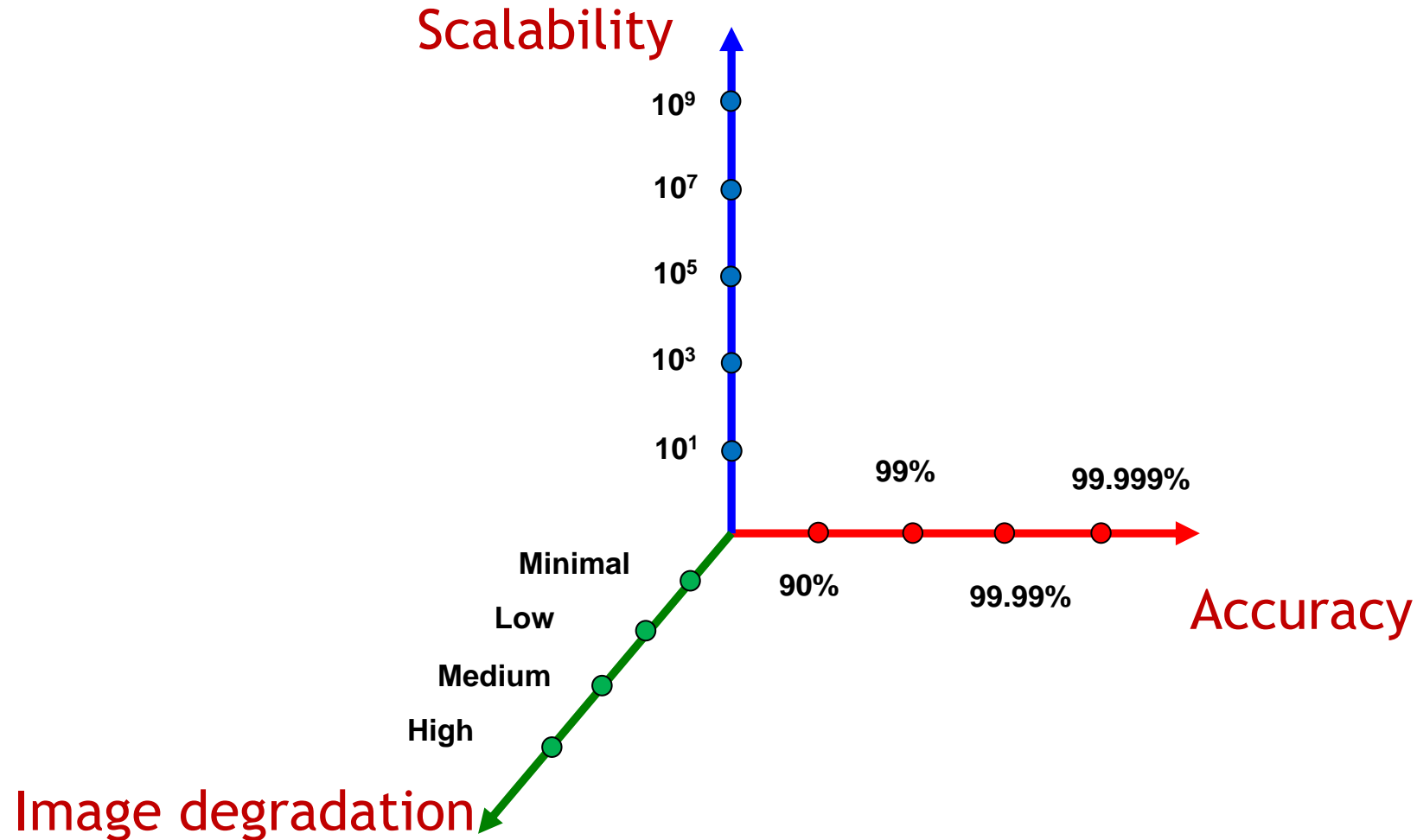Fingerprint (1 finger): FNIR = 0.019 @ (100K gallery)

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

Dataset
- Kiosk–Border
- Mugshot–Mugshot
- Visa–Border
- Visa–Visa
- Visa45–Border

28%

< 0.2%

False Rejection

FNMR at FMR = 10^{-6}

FNMR at fixed FMR = 0.000001

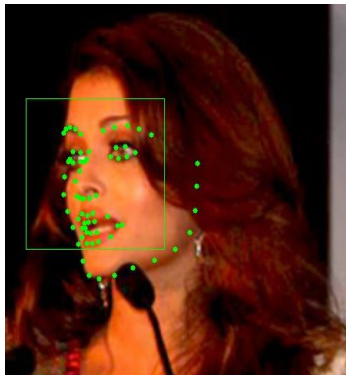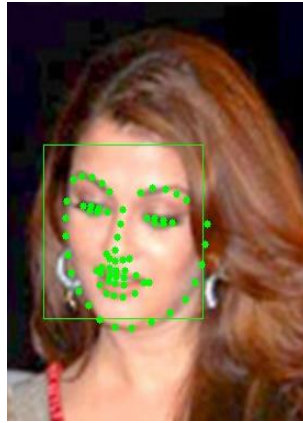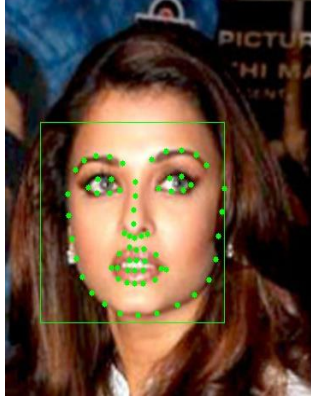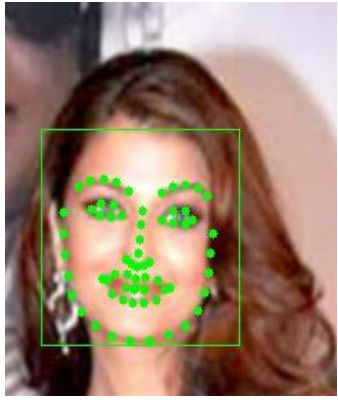Date Algorithm Delivered to NIST

Biometric Challenges

Throughput, spoof attacks, template security, usability, acceptability

Sources of Error in Biometrics
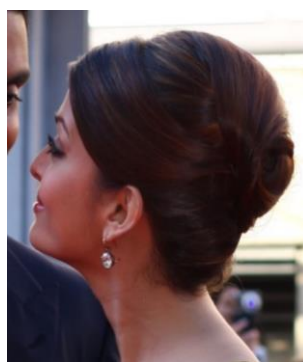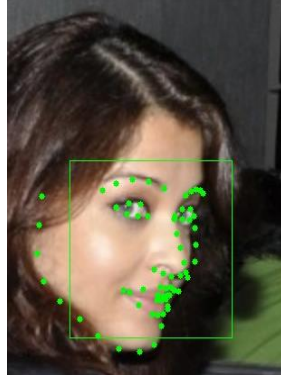
Intra-person variations (PIE, aging, occlusion)

Inter-person similarity

Semi-constrained Face Recognition

Probe (1984)

Threshold=0.54 @ FAR=0.01%
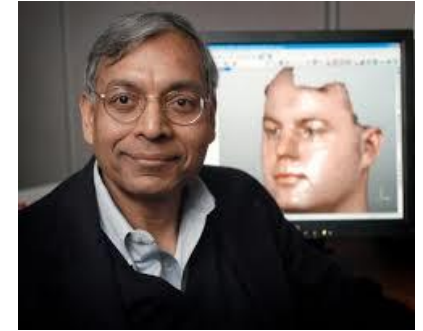
0.83   0.89   0.72   0.81

0.58   0.72   0.82   0.71

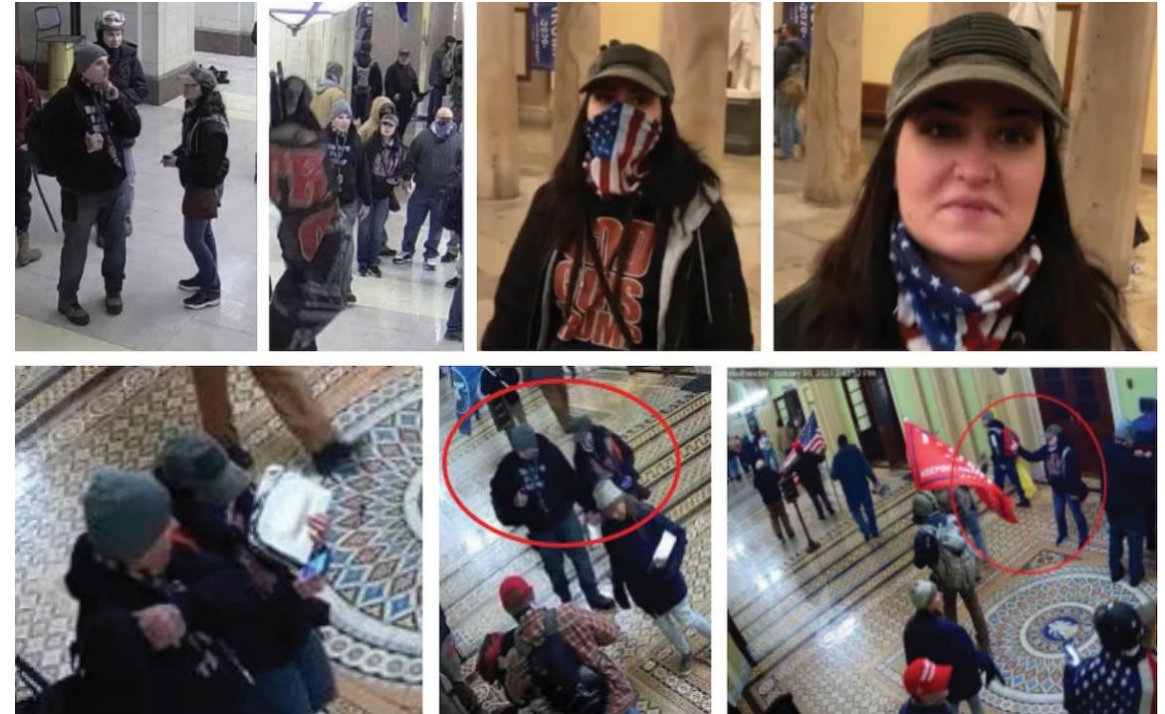0.74   0.66   0.63   0.49   0.17

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

- In Oct 2018, a store in Detroit was robbed; Michigan State Police searched a low-quality CCTV frame against 49M face database. It matched with Williams photo.
- "This is not me. You think all Black men look alike?" Williams told investigators.
- What went wrong? FR system will always return a non-zero score for every pair

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?
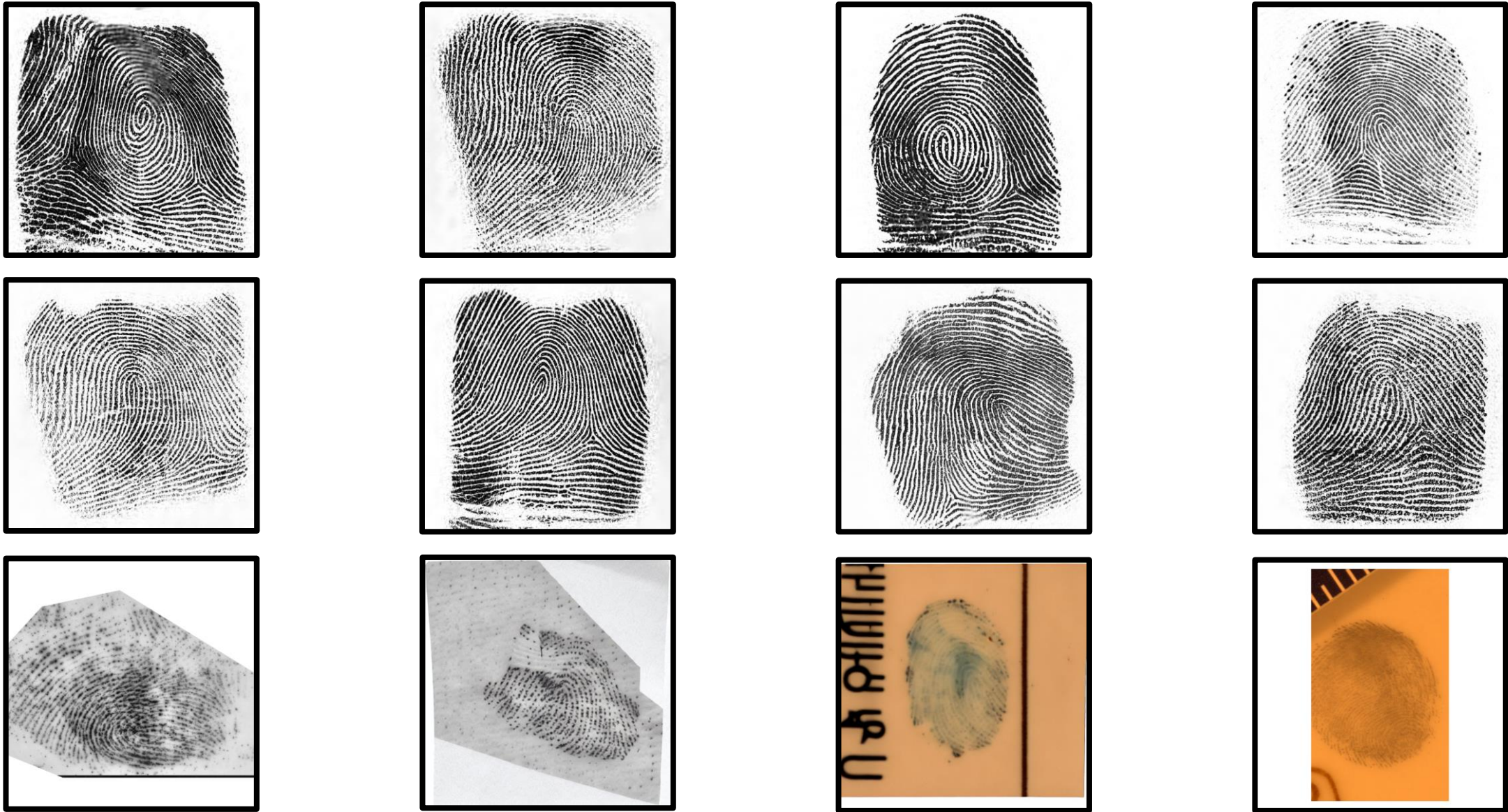
https://gdpr.eu/

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)
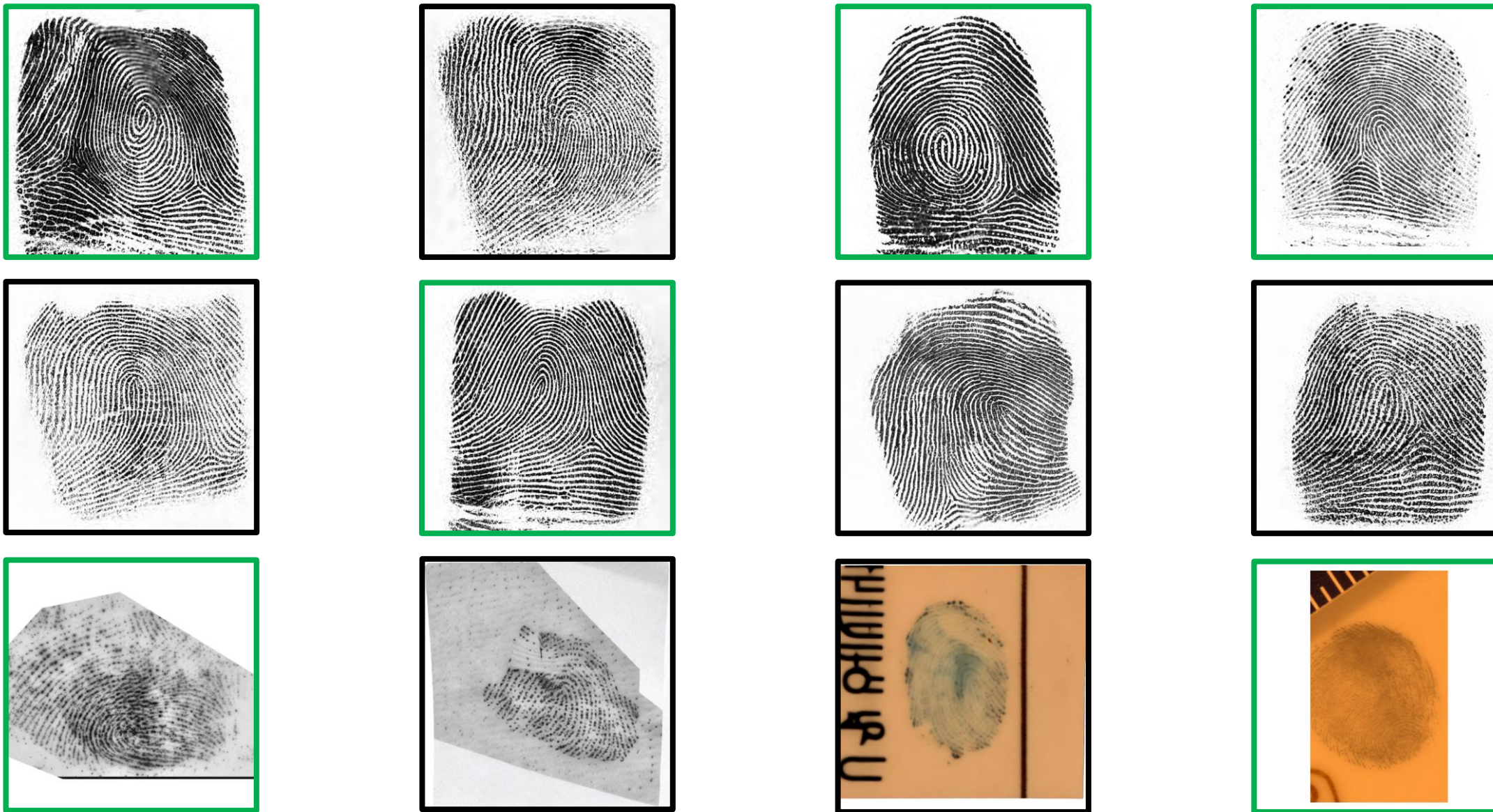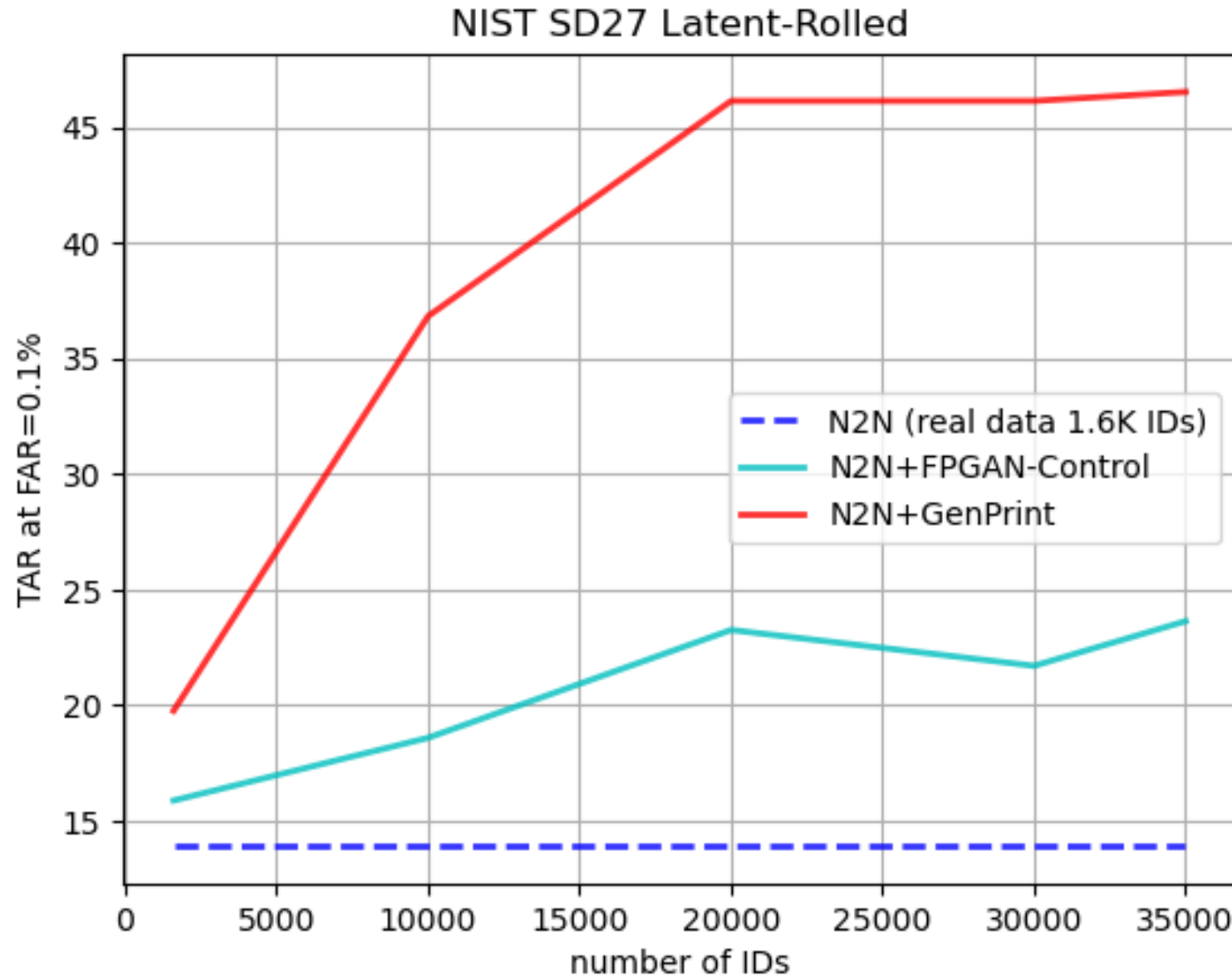
Real vs. Computer Generated Images

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
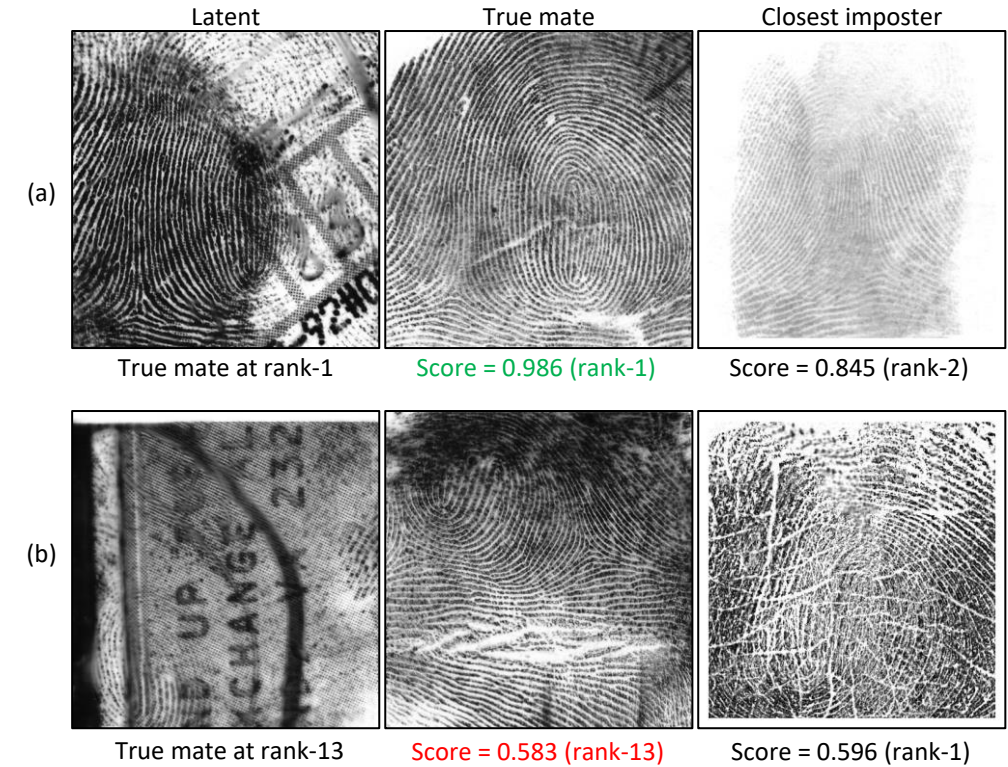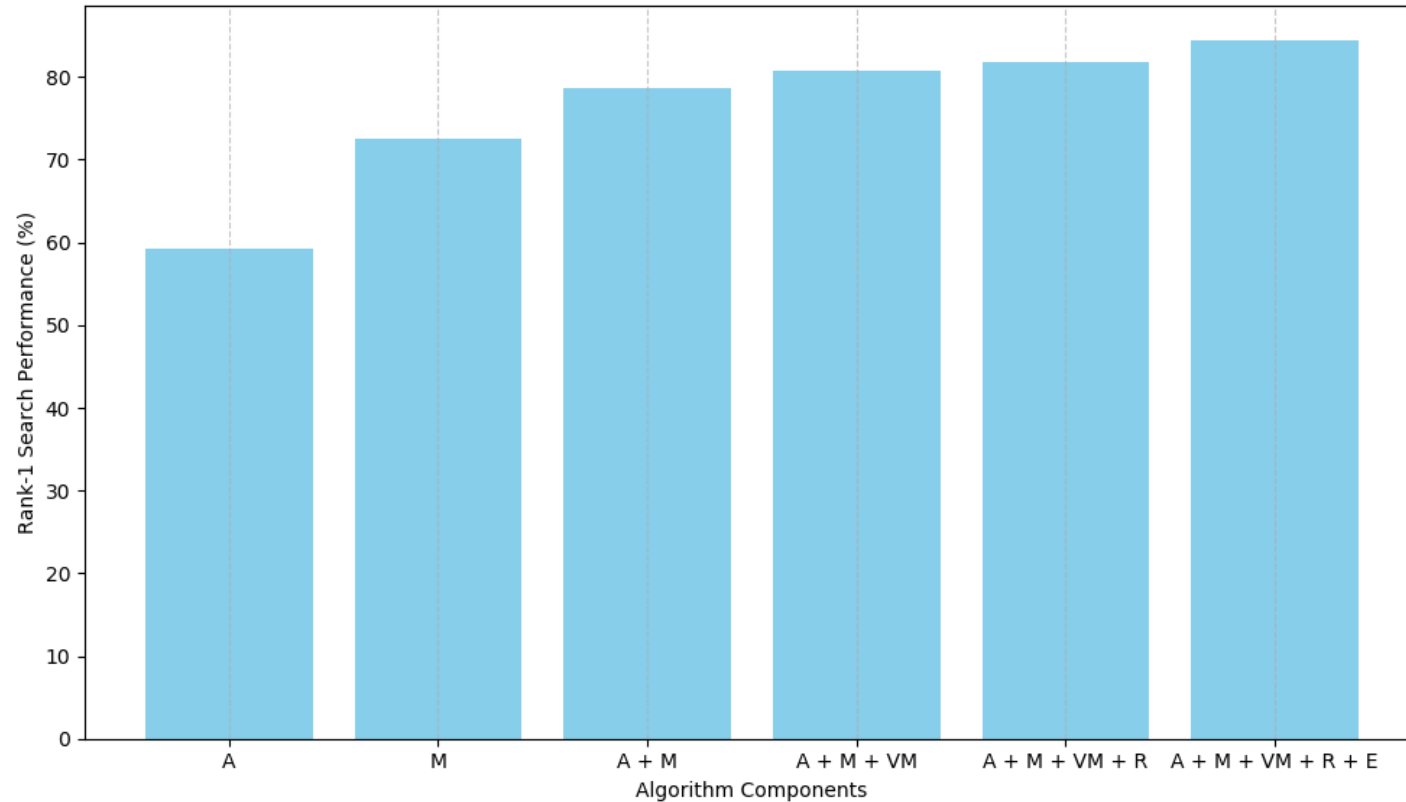

NIST SD27 Latent-Rolled

Legend:
- N2N (real data 1.6K IDs)
- N2N+FPGAN-Control
- N2N+GenPrint

X-axis: number of IDs
Y-axis: TAR at FAR=0.1%

Latent Fingerprint Matching

LFR-Net Ablation Study on MSP Latent Database

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

Fake hand

Face disguise

Fake eyeball

Silicone Mask

Print

Fingerprint alteration

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

Privacy-Preserving Authentication

Fingerprint Reader → Encrypted Query → Matching in encrypted domain → Encrypted Scores

Enrolled database
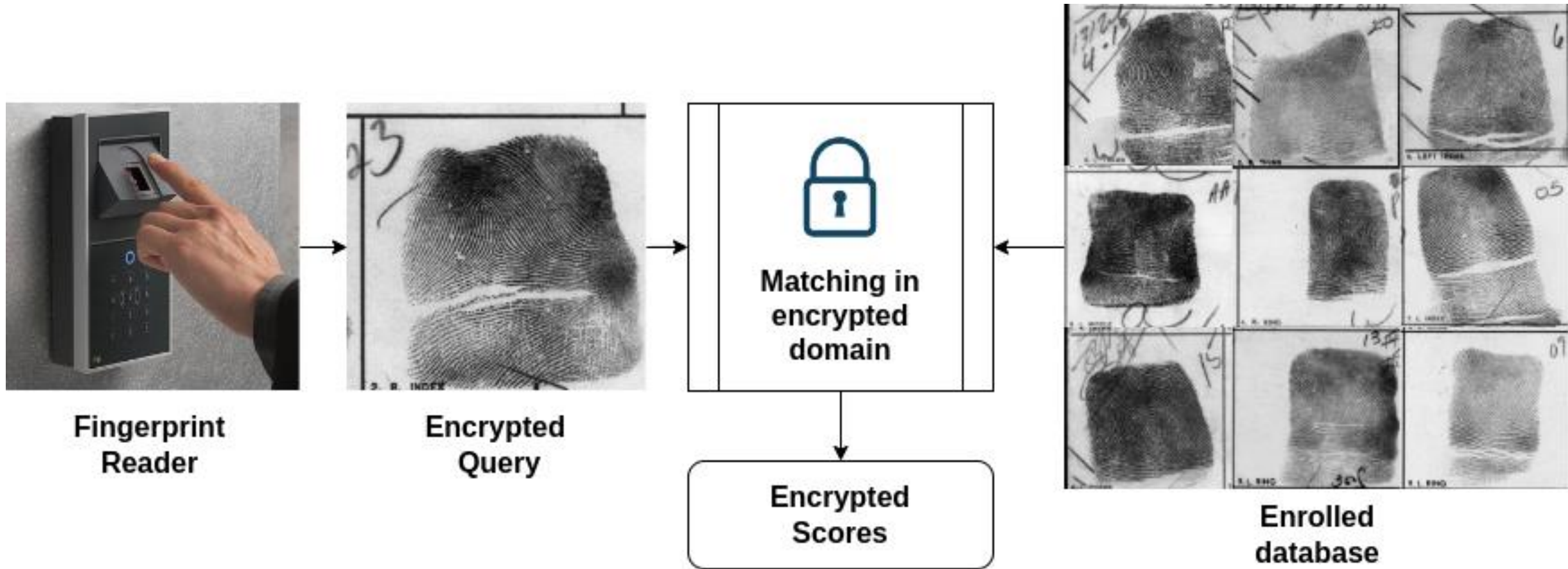
Accurate & fast image search in encrypted domain is feasible at scale (100 M gallery); no leakage of biometric

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.

- New deployments for civil registration, border crossing, banking, PoS payment, travel and immigration.

- Challenges: seamless integration in applications, recognition under non-ideal conditions, access to data, system integrity,…

- Biometrics is here to stay!!

36