

Introduction to Biometrics

Anil K. Jain

Michigan State University

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

Israeli School on Biometrics, April 21, 2025

How Do We Know Who You Are?

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



**Phishing attacks, social engineering,
incentives for personal information**

Too Many Passwords to Remember!

Copyright 1996 Randy Glasbergen. www.glasbergen.com



“Sorry about the odor. I have all my passwords tattooed between my toes.”



WILL SELL
PERSONAL
INFORMATION
FOR FOOD

KING

Fake ID Documents



[Buy Scannable Fake ID - We Make Premium Fake IDs](#)

~33% of underage college students on US campuses have a fake ID

Biometric Recognition

- Biometrics: *Bios* (life); *metron* (measure)
- Biometric Recognition: Real-time, automated person recognition based on body trait(s)

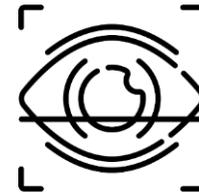
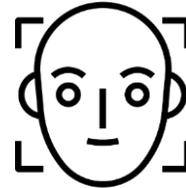


Israeli Biometric ID Card (Teudat Zehut)



The biometric Teudat Zehut contains an image of the facial features and images of the fingerprints of the ID holder. This database of identification is intended to prevent fraud and identity theft.

Most Popular Biometric Traits



Incheon, South Korea: Smart Entry



Australia: SmartGate



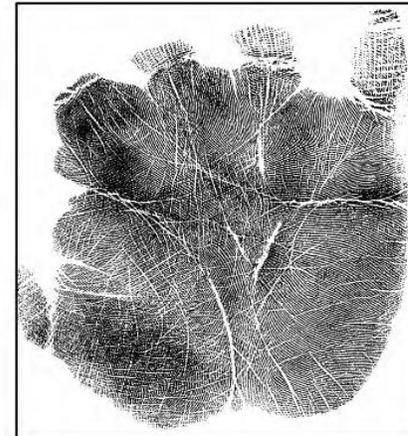
Amsterdam: Privium border passage

- *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)

Growing Interest in Palm Biometric



(a)



(b)



(c)



(a)

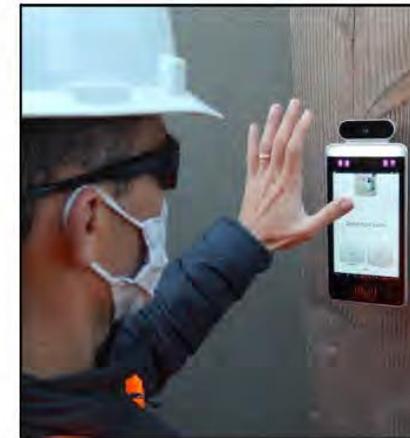


(b)

(a) Palmprint, (b) Palmvein



(d)



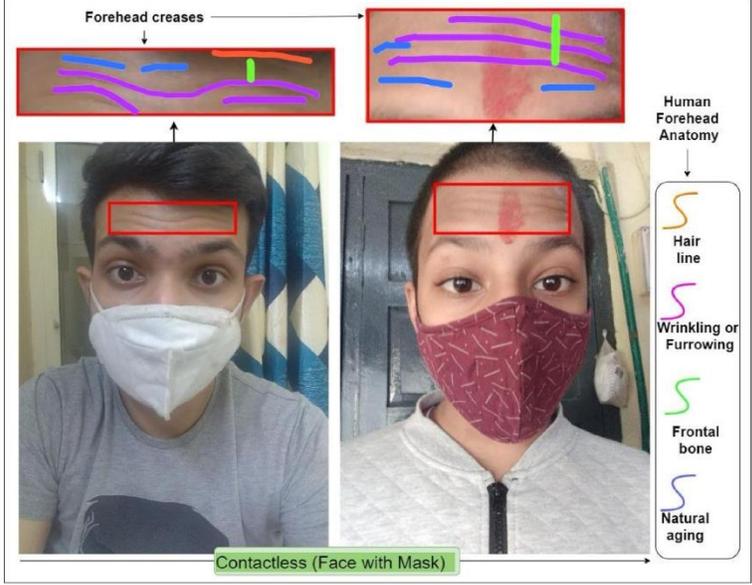
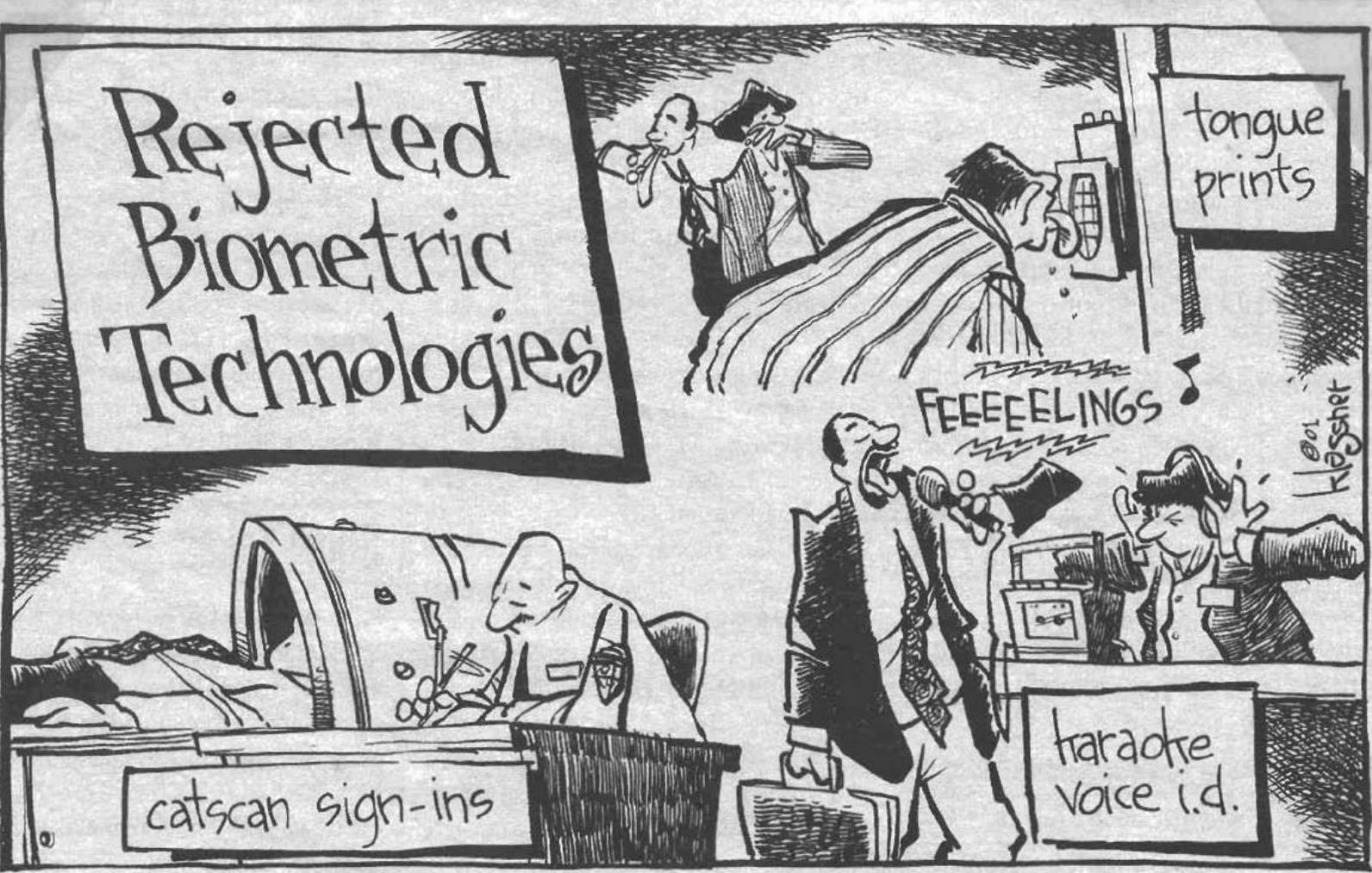
(e)



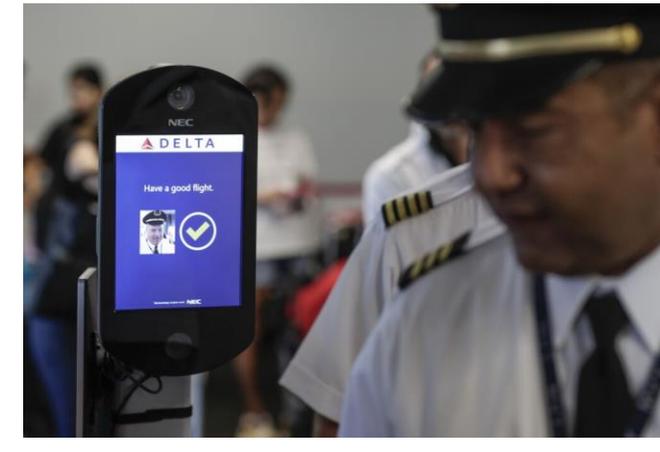
(f)

(a) Earliest use of palmprint (**Herschel ~1855**) in lieu of signature on legal contracts, (b) latent palmprint from crime scene, (c) contactless palmprint Recognition for metro systems by Tencent, (d) Amazon One for payment at PoS, (e) time and attendance system from RedRock, and (f) PalmSecure palm vein recognition system by Fujitsu.

Rejected Traits

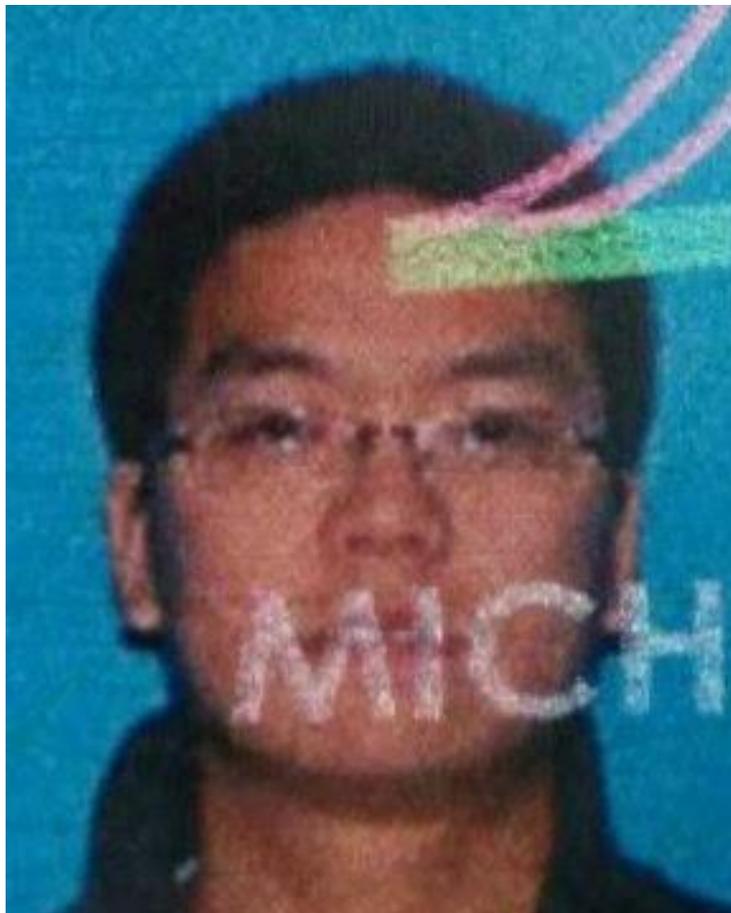


Biometrics: Here, There, Everywhere!

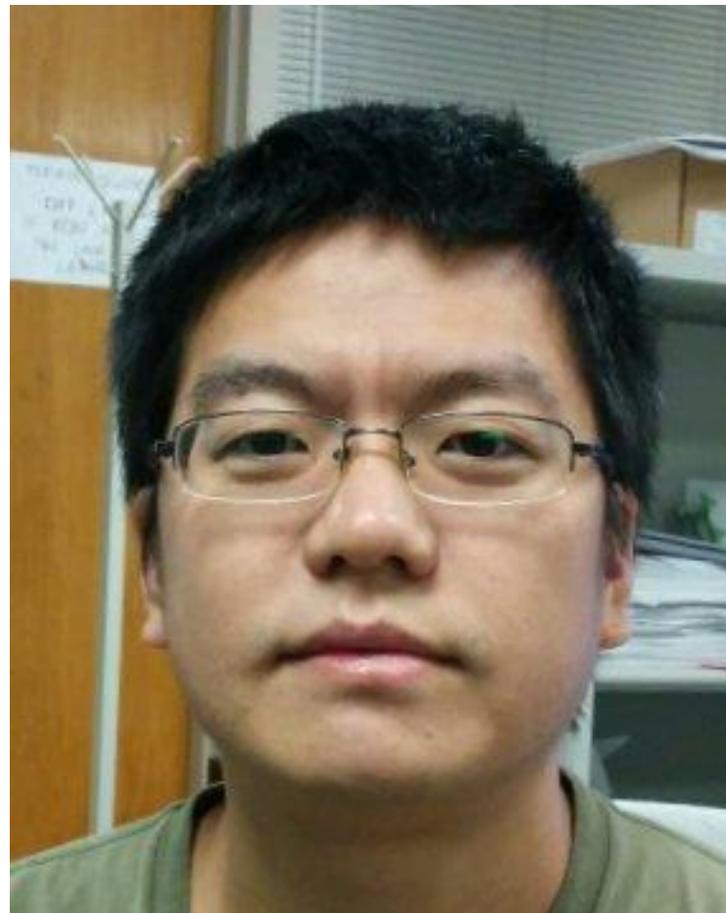


Why biometrics: Enhance security, reduce fraud, convenience
Requirements: High accuracy, large throughput, integration, usability, data privacy

Authentication: Pair-wise Comparison



Selfie + claim of "I am Kai Cao"



Enrolled face of Kai Cao

False Match Rate (FMR); False Non-Match Rate (FNMR); Failure to Acquire and Failure to Enroll

Identification (N Pair-wise Comparisons)

Probe

Gallery

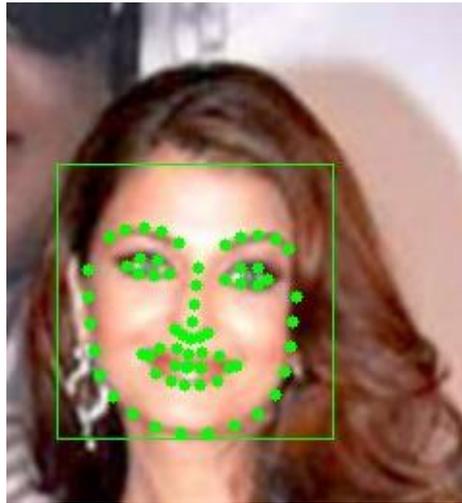


Open-set identification vs. Closed-set identification

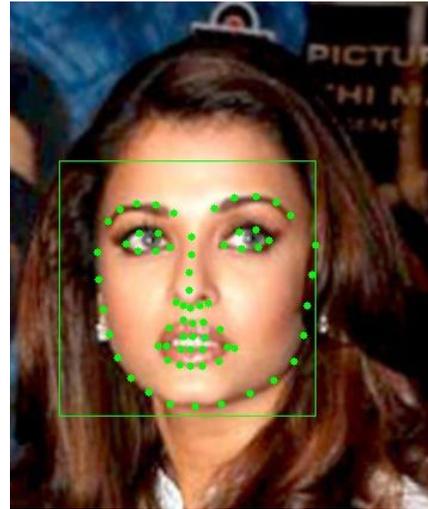
Why is Biometrics so Difficult?

- Intra-class variability and inter-class similarity
- Fireground/background separation
- Noisy input (intrinsic or extrinsic factors)
- Individuality and persistence of biometric traits
- Scalability
- Template aging and update

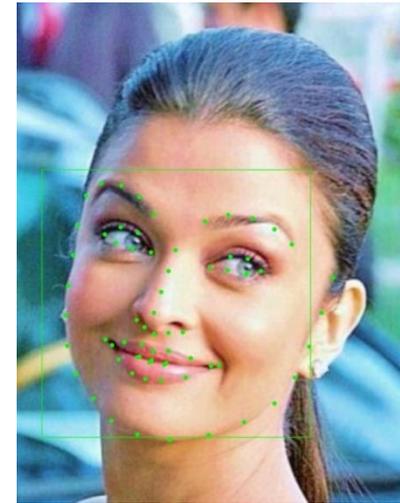
Intra-Class Variability



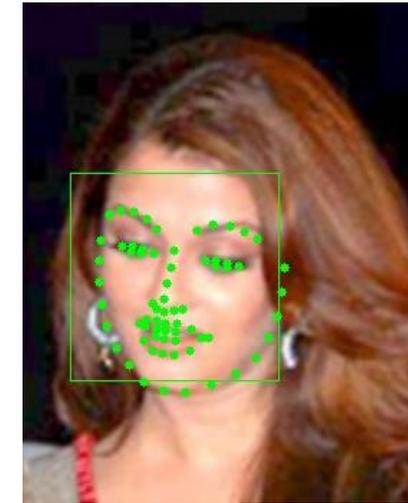
Source Image



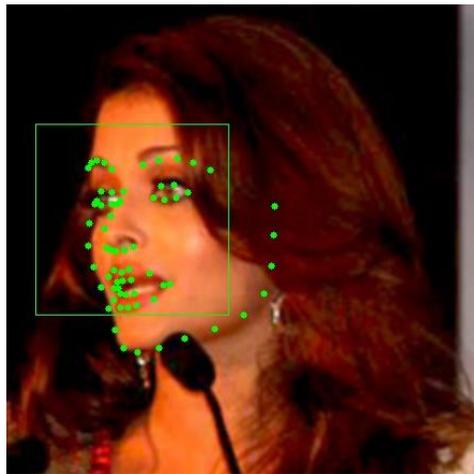
0.5959



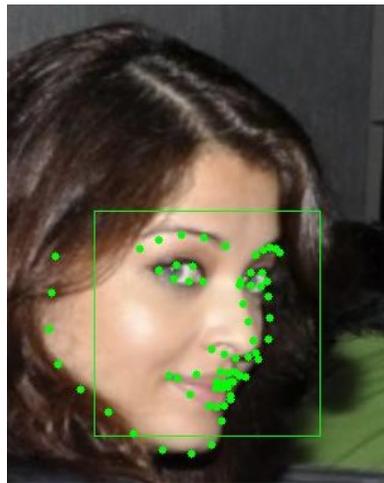
0.4605



0.4796



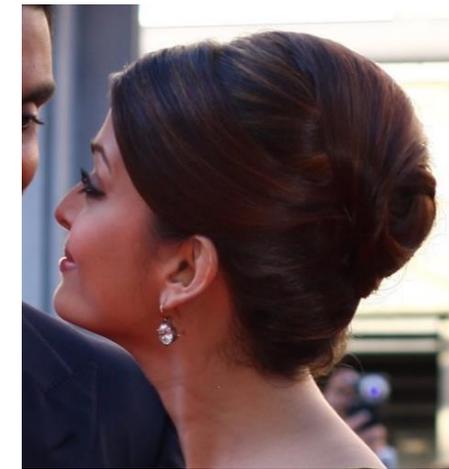
0.4682



0.4318



0.4652



0.1357

Matcher is ViT KP-RPE[1] trained on WebFace4M dataset

[1] Kim, Minchul, et al. "Keypoint relative position encoding for face recognition." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2024.

Intra-Class Variability



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

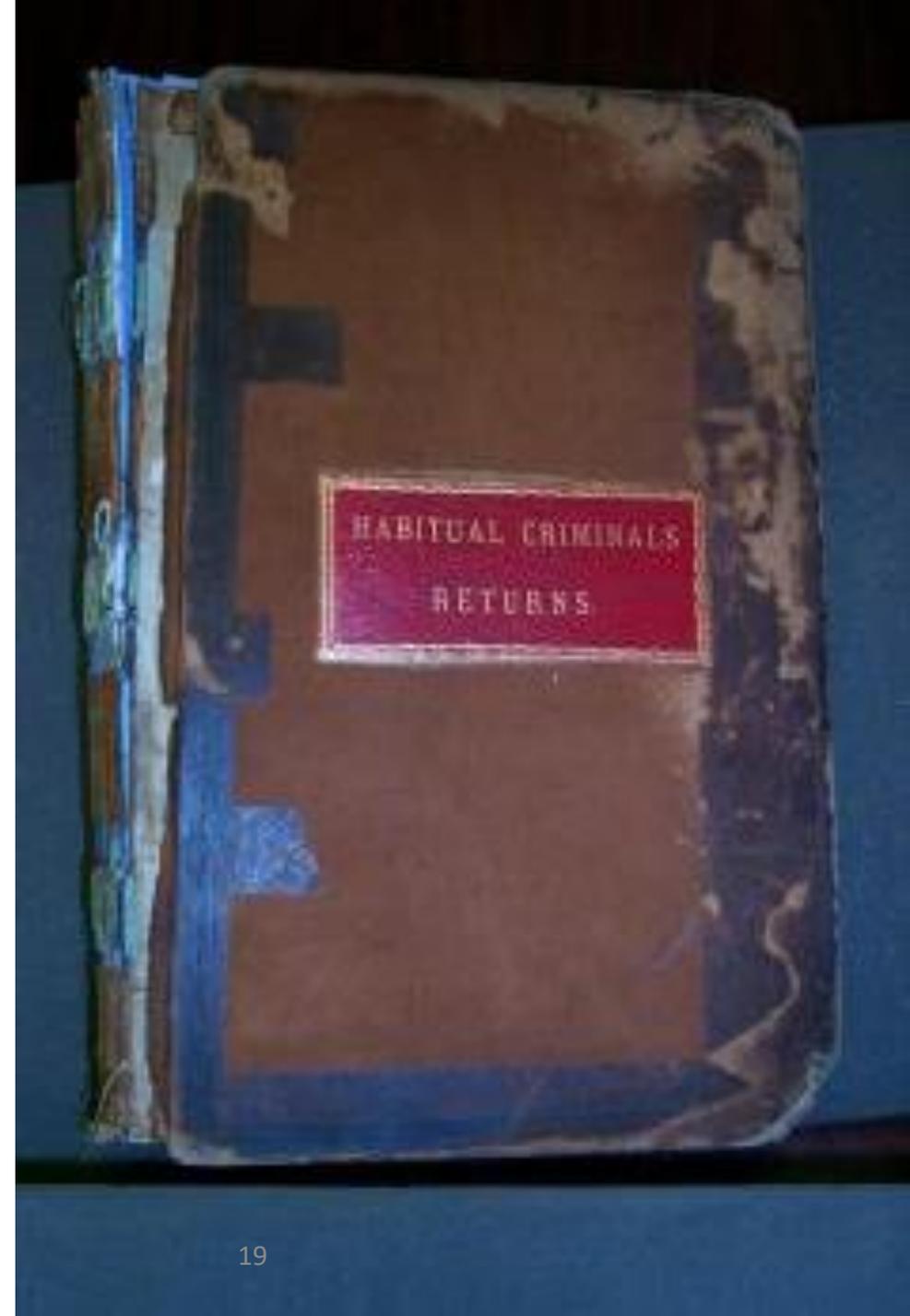
Inter-Person Similarity



Biometric Recognition is Not New

Habitual Criminal Act (1869)

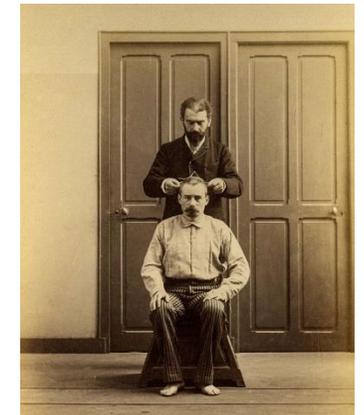
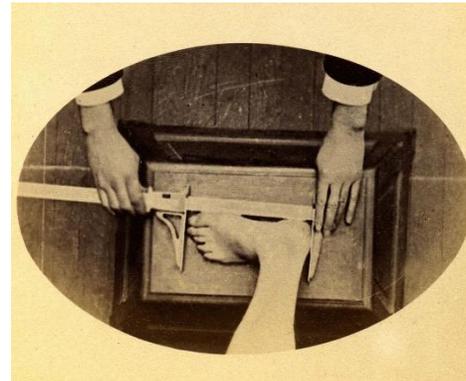
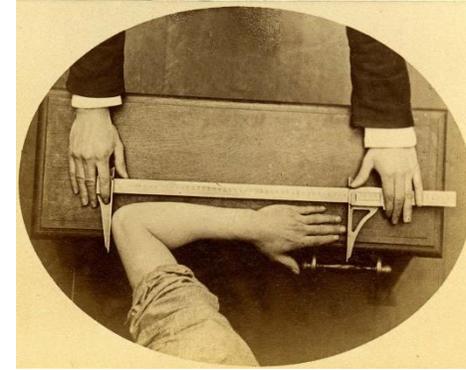
*“What is wanted is a means of classifying the records of **habitual criminals**, such that as soon as the **particulars of the personality of any prisoner (whether description, measurements, marks, or photographs)** are received, it may be possible to ascertain readily, and with certainty, whether his case is in the register, and if so, who he is”*



The Bertillon System that Cataloged Criminals by their Physical Measurements (1879)



Photographing a suspect in the courtyard of a Police Prefecture in Paris



Measurement of *unique features* of suspects; each coded as "small", "medium", "large"

Fingerprints (1880)

“Perhaps the most beautiful and characteristic of all superficial marks (on human body) are the small furrows with the intervening ridges and their pores that are disposed in a singularly complex yet even order on the under surfaces of the hands and feet.”

Francis Galton, Nature, June 28, 1888

Scotland Yard (1905)



AUTOMATIC COMPARISON OF FINGER-RIDGE PATTERNS

(Trauring, Nature, 1963)

*“It is the purpose of this article to present, together with some evidence of its feasibility, a method by which decentralized automatic identity verification, **such as might be desired for credit, banking or security purposes**, can be accomplished through automatic comparison of the minutiae in finger-ridge patterns.”*

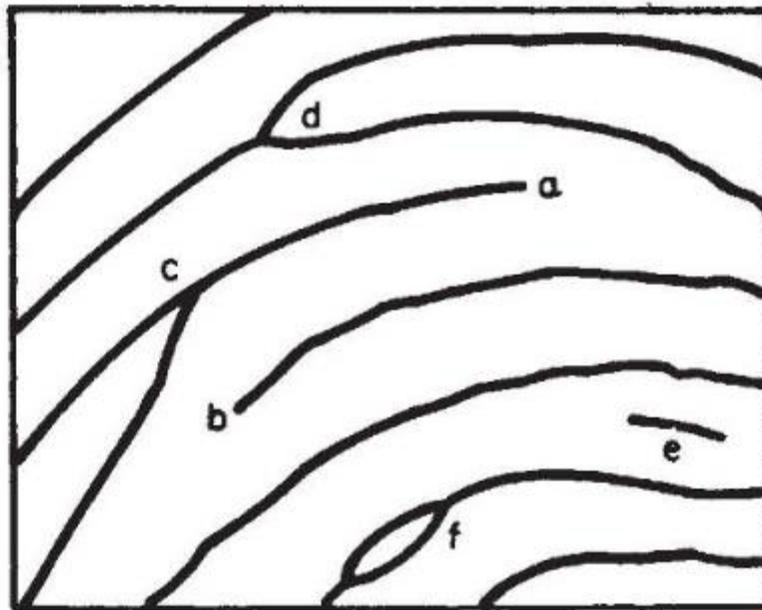
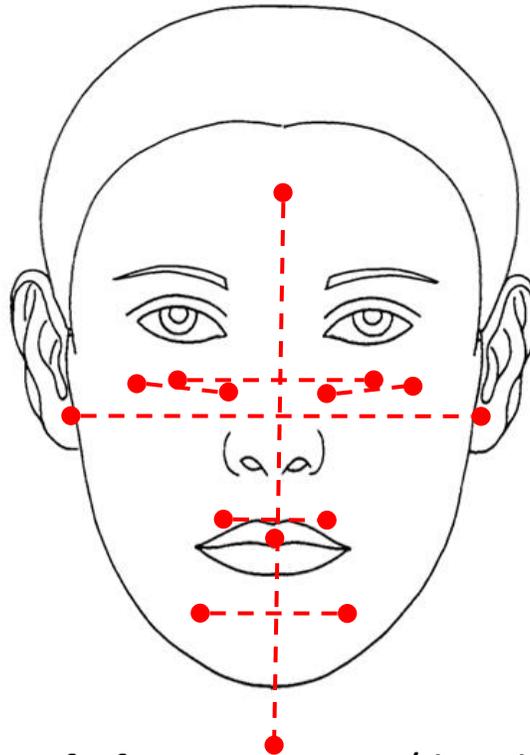


Fig. 1. Portion of fingerprint pattern (diagrammatic, enlarged) after Galton, showing minutiae. *a* and *b* are ridge ends, *c* and *d* are ridge branchings or valley ends, *e* is an island, and *f* is an enclosure. The ridge end and valley end are the principal minutia types, accounting for almost all minutia occurrences

Face Recognition (Bledsoe, 1966)

"This recognition problem is made difficult by the **great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc.**" *Bledsoe, Chan and Bisson (1966)*



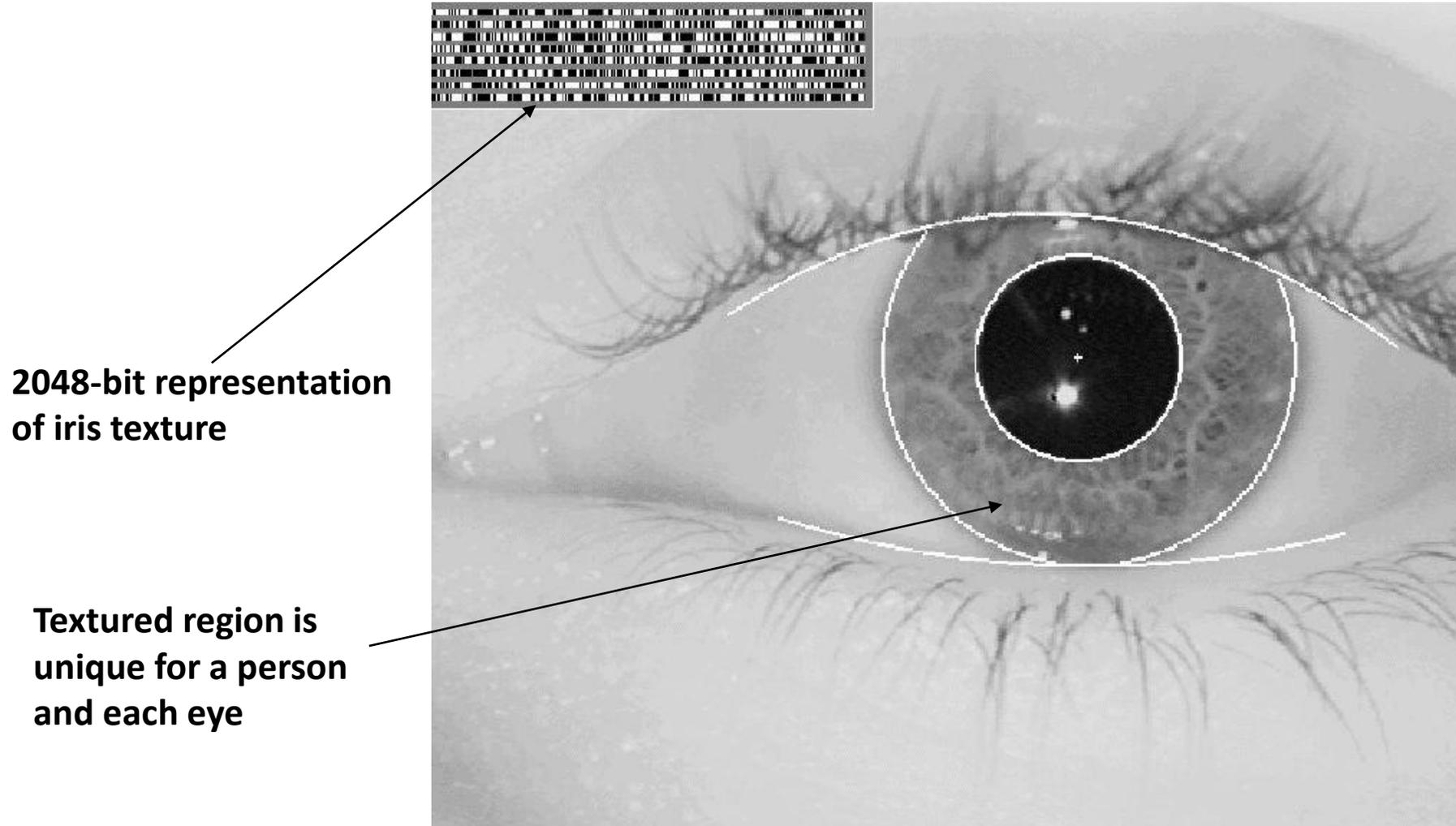
20 inter-point distances for matching

Identimate (1972)



First commercial use of biometrics based on “finger geometry”

Iris Recognition (Daugman, 1993)



J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE Trans. PAMI, 1993.

9/11 Terrorist Attacks (2001)



US-VISIT (2003)



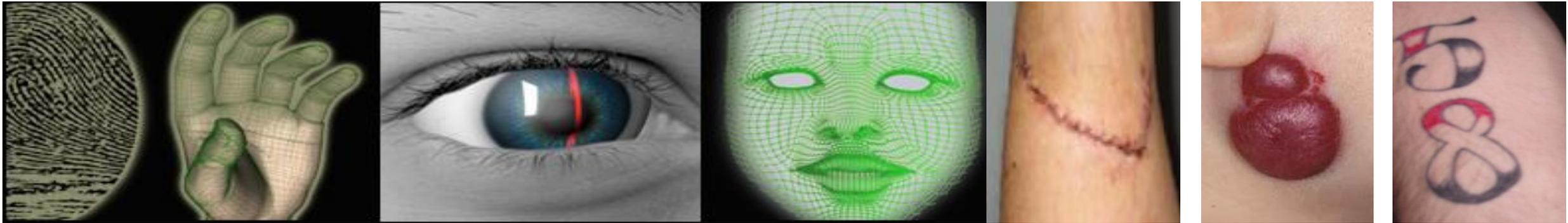
- USA Patriot Act enacted to enhance national security by tracking terrorists and preventing money laundering
- Enhanced Border Security and Visa Entry Reform Act of 2002 allowed the use of biometrics for entry/exit²⁹

Walt Disney Theme Park (2005)



Prevent sharing of tickets

FBI Next Generation Identification (2008)

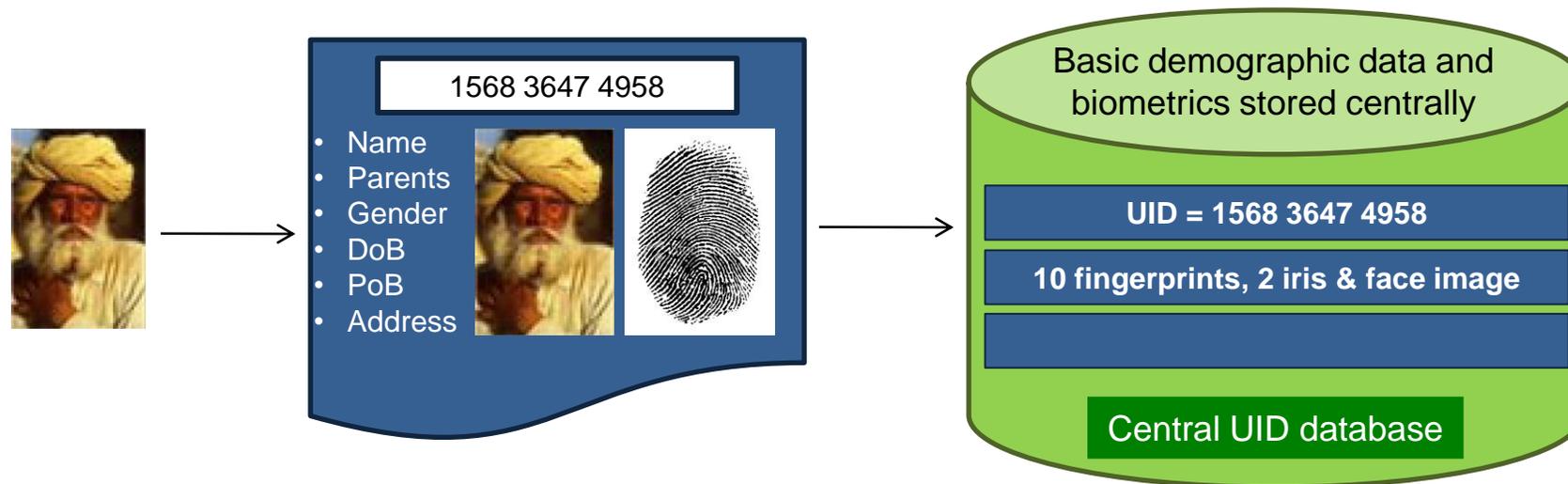


First AFIS in 1980s; IAFIS launched in 1999; use of **soft biometrics** (SMT)

http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2/

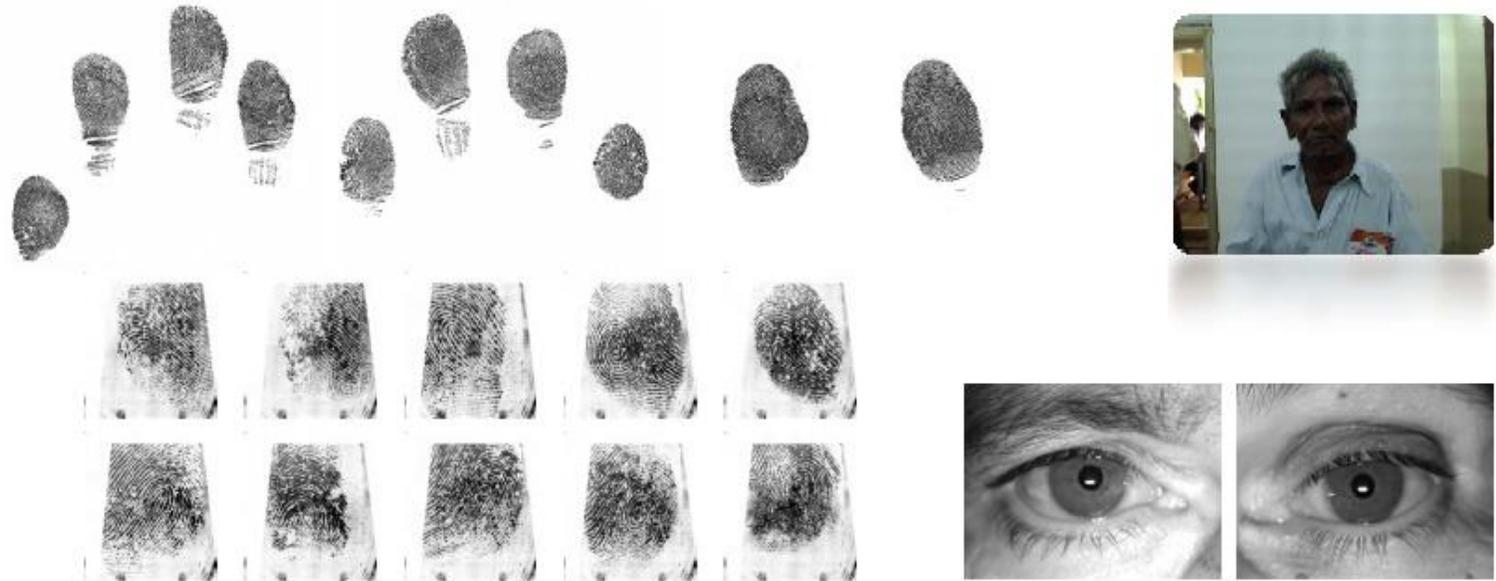
Aadhaar: Billion-Scale Biometric ID System (2009)

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



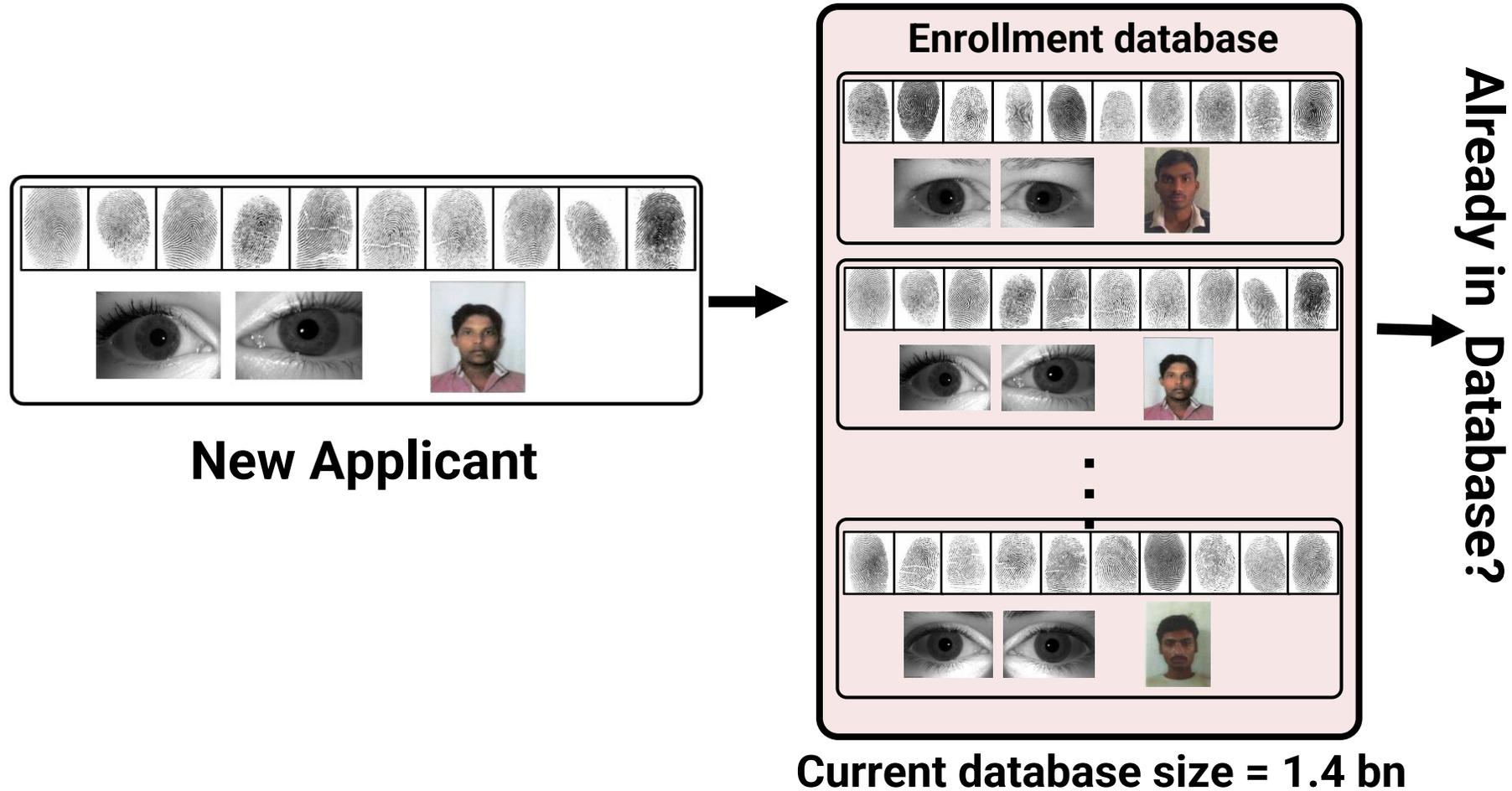
- Enrollment (1.5 billion), de-duplication & authentication (~80 million/day)
- Approx, 25 million babies born per year in India (Israel population ~10M)

Enrollment



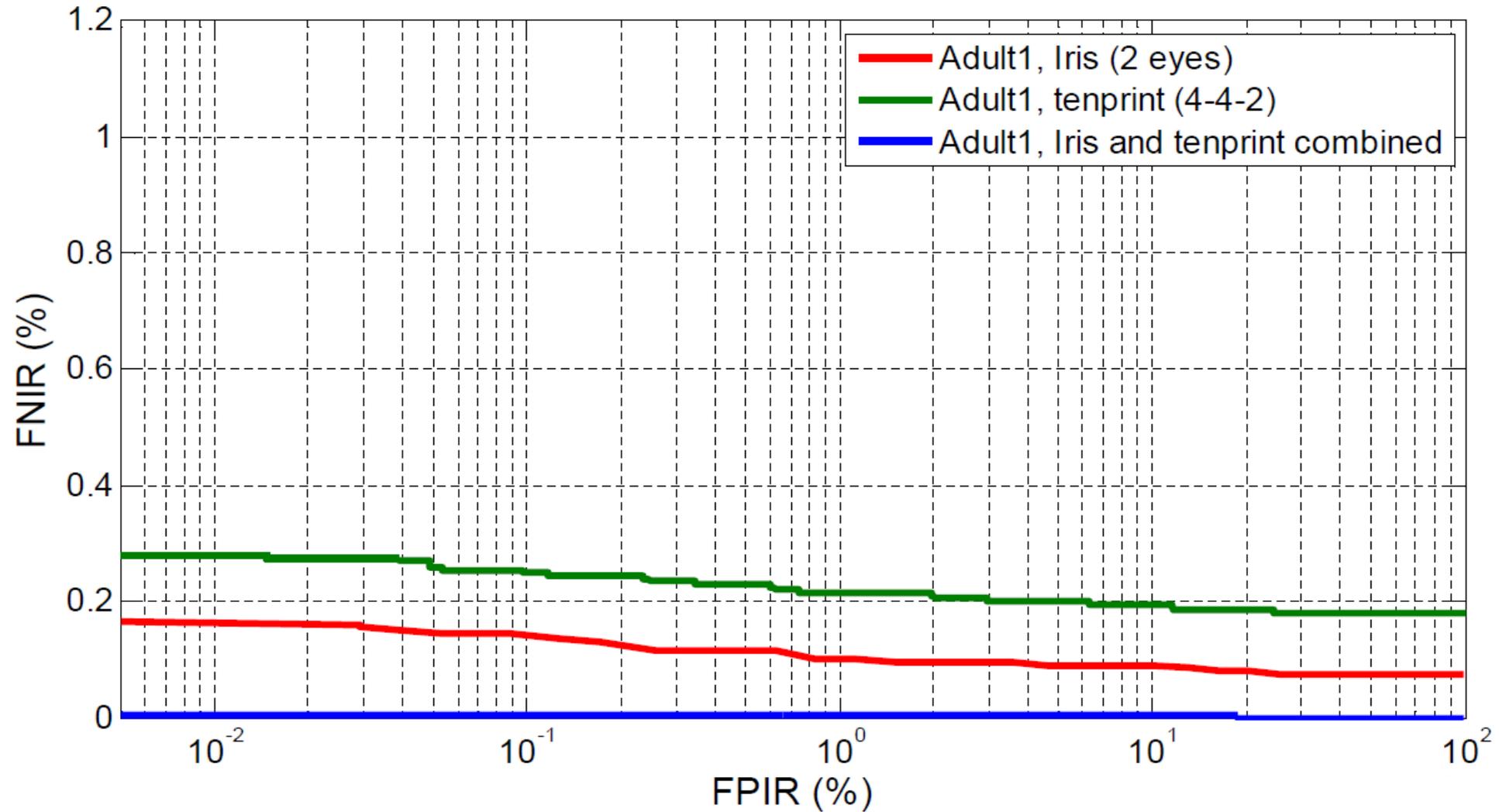
Face, slap fingerprints (4-4-2) and 2 iris images are captured; minimal biographic data collected.

De-duplication (1:N Comparison)



- Is the applicant already enrolled?
- No single biometric trait can distinguish among ~1.5 billion individuals

Benefit of Biometric Fusion



- **FPIR: Fraction of non-mated searches where one or more enrolled identities are returned at or above the threshold**
- **FNIR: Fraction of mated searches where the enrolled mate is outside the top R rank or comparison score is below the threshold**

Authentication (1:1 Comparison)



~80 million (2-factor) authentications/day; 12-digit Aadhaar + fingerprint

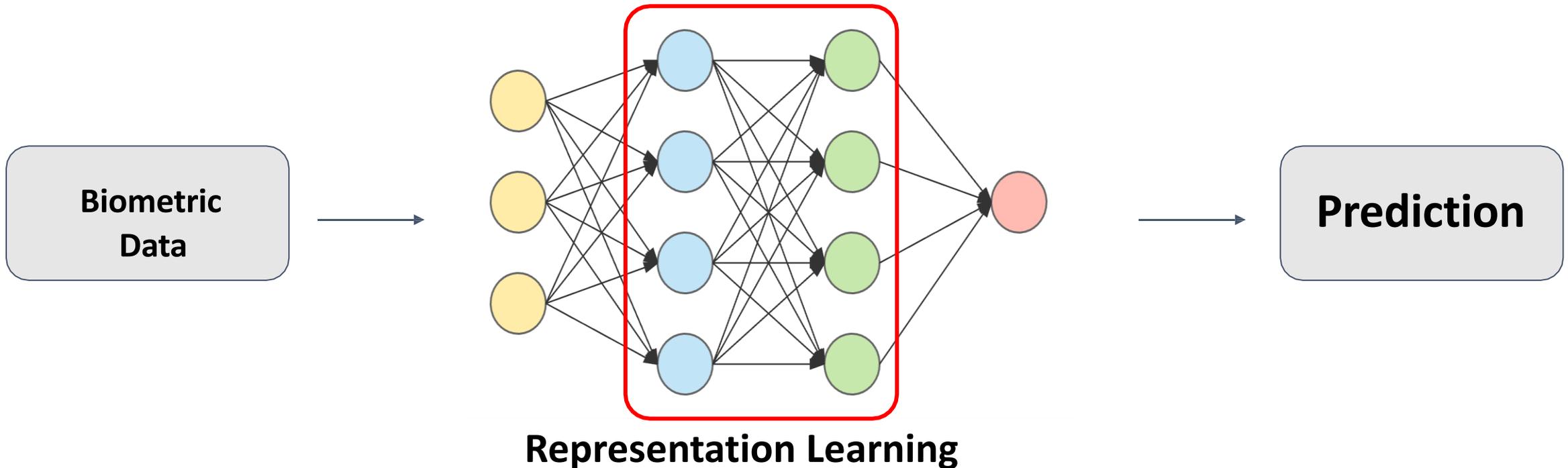
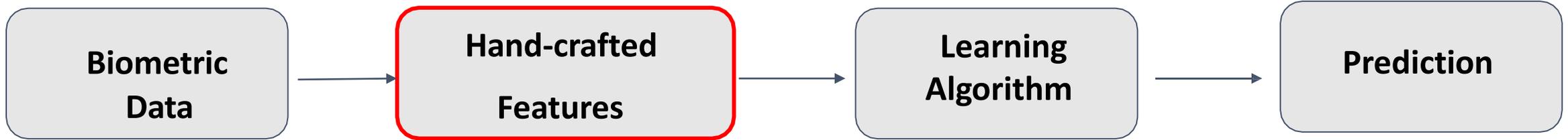
https://uidai.gov.in/aadhaar_dashboard/auth_trend.php

Social Good vs. Privacy



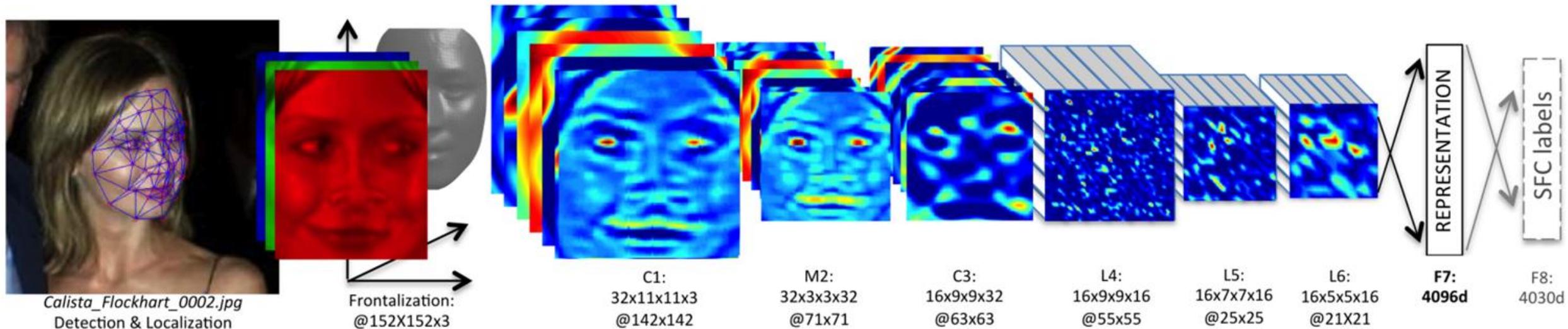
“Aadhaar gives dignity to the marginalized. Dignity to the marginalized outweighs privacy” - Justice Sikri, Indian Supreme Court (Sept 2018)

Biometric Representation



Face matching has benefitted the most from deep networks

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**

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

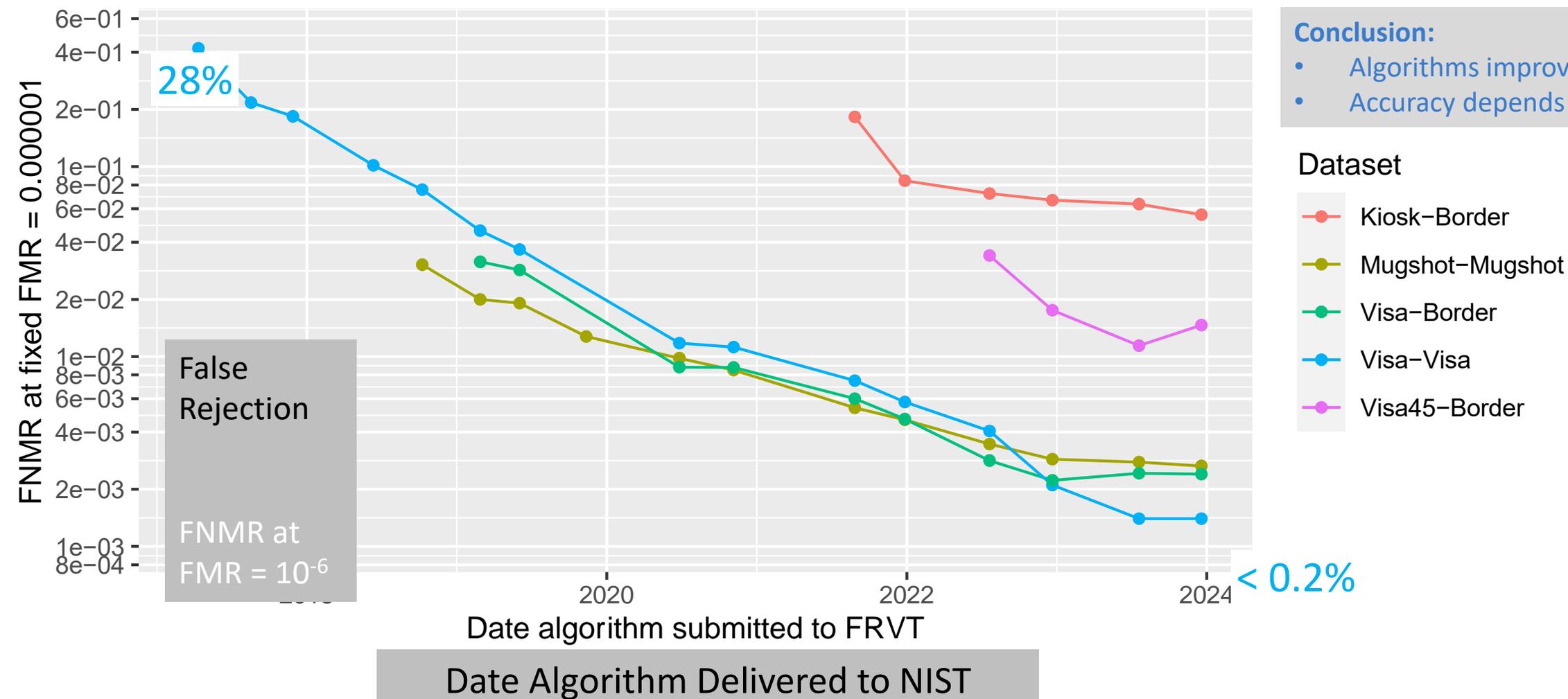
Fingerprint (10 fingers): FNIR = 0.001 (5M gallery)

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

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

Face: FNIR = 0.03 (12M gallery)

1:1 Face Accuracy Gains Continue



Face Recognition at Airports (Entry/Exit)

- International traveler's entry/exit photo is compared with DHS database (e.g., photos from U.S. passports and U.S. visas, flight manifest).



More than 300K American passports are stolen or lost every year; Passport data sells in three formats on the darkweb, digital scans (up to \$65), templates for creating a finished passport (up to \$100) and actual physical passports (up to \$5k).

Mobile Phone Unlock & Payment



The Pantech G100 (2004)



Touch ID, iPhone 5S (2013)



Apple Pay, iPhone 6 (2014)



Face ID, iPhone X (2017)



Delta ID, phone with iris (2016)



In-Display Scanner (2018)



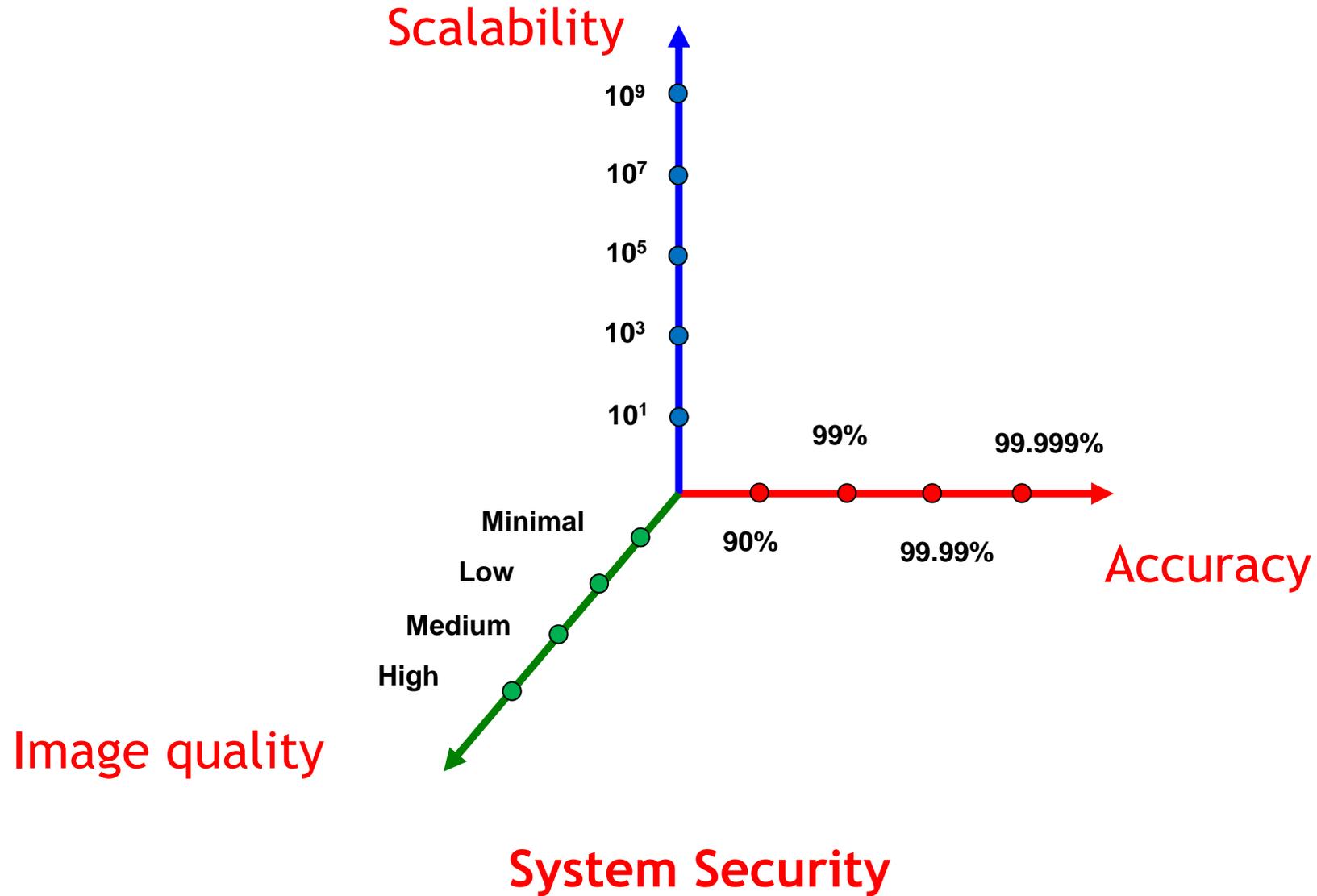
Galaxy S10's in-screen ultrasonic scanner (2019)



Under-display FaceID in iPhone 18 (2026)

Touch ID was revolutionary: convenience, accuracy, security, cost (1-5US\$) & latency

Biometric Challenges



Unconstrained Face Recognition



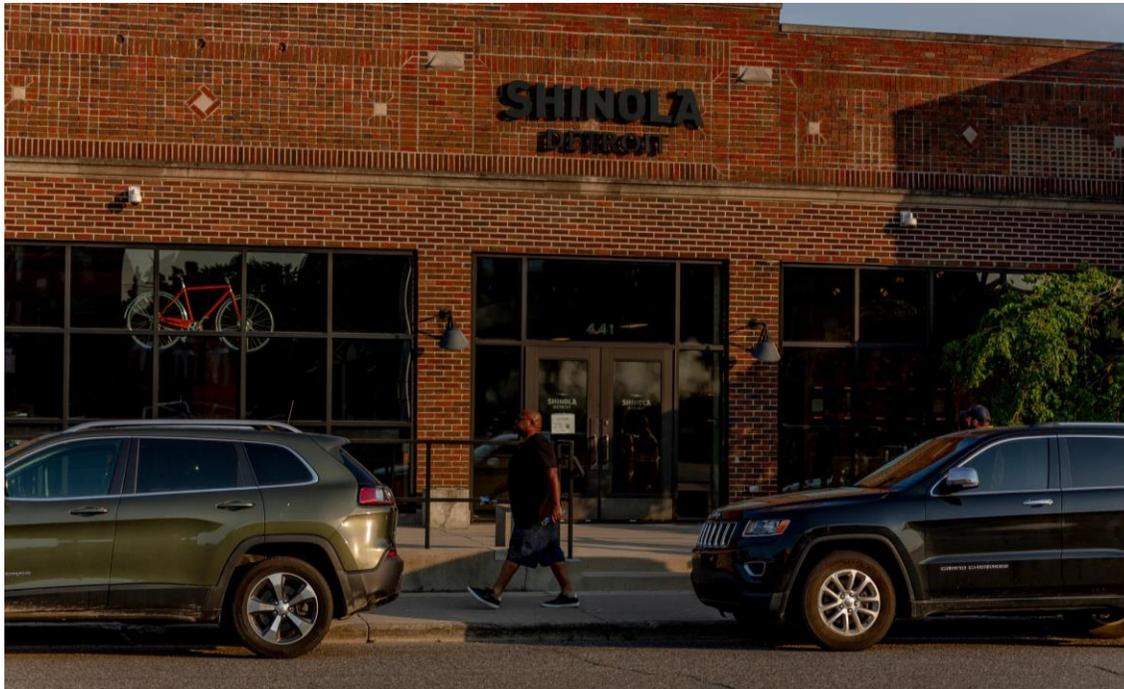
Composite image of evidence pulled by the U.S. District Court for the District of Columbia against Debra Maimone. (U.S. District Court D.C.)

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

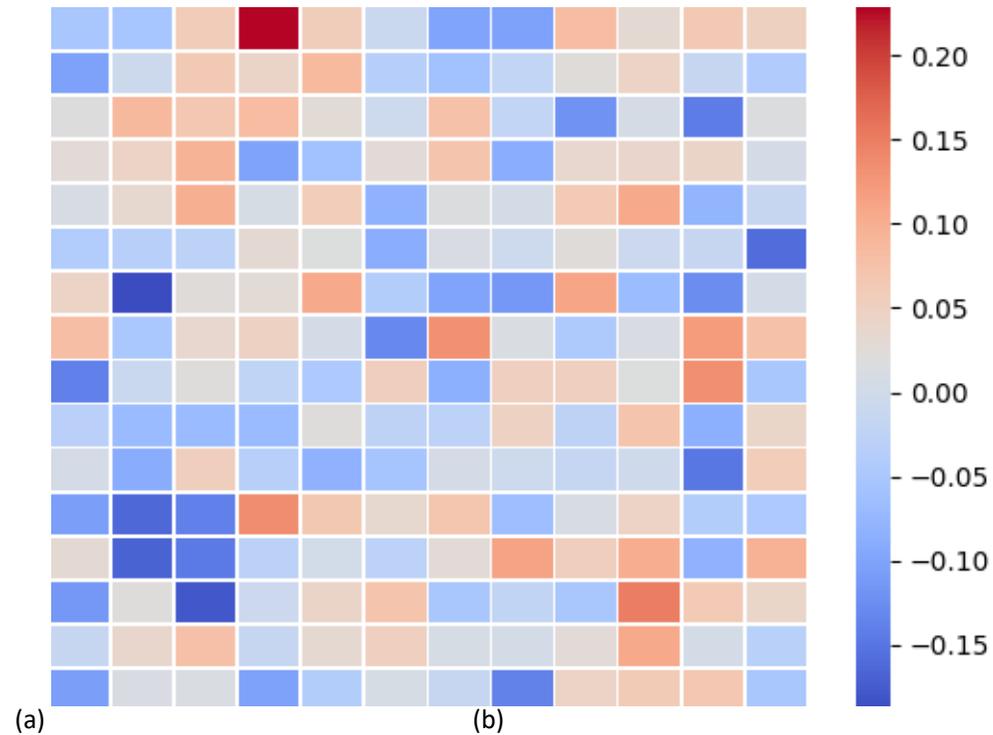
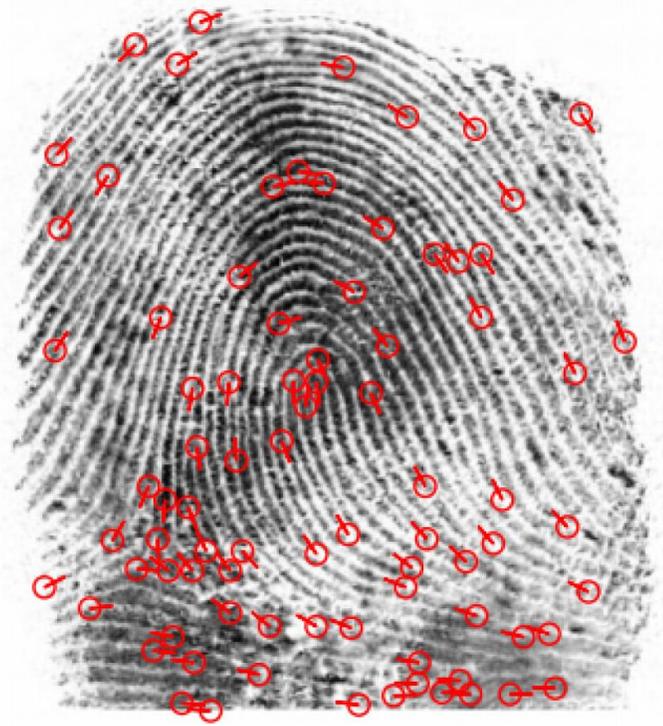
- In Oct 2018, a store in Detroit was robbed; Michigan State Police searched a low-quality CCTV frame against 49M face database. It matched with Williams photo.
- “This is not me. You think all Black men look alike?” Williams told investigators.
- **What went wrong? FR system will always return a non-zero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



User Consent and Biometric Data Privacy

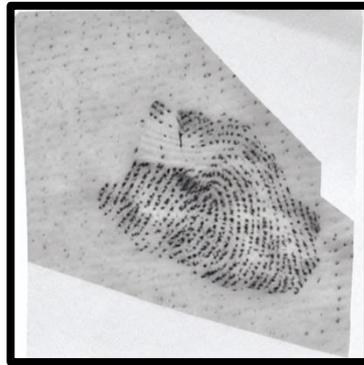
- **General Data Protection Regulation (GDPR); May 25, 2018**
 - Personal Data: “any information that relates to an individual who can be directly or indirectly identified. This includes ethnicity, gender and biometric data.”
 - Seven data protection principles: (i) Lawfulness, fairness and transparency;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

Two Representations for Fingerprints



- **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**

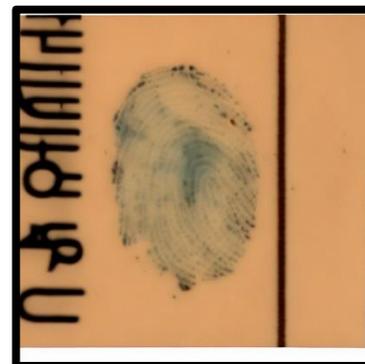
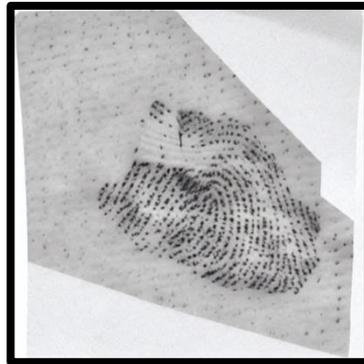
Real vs. Computer Generated Images



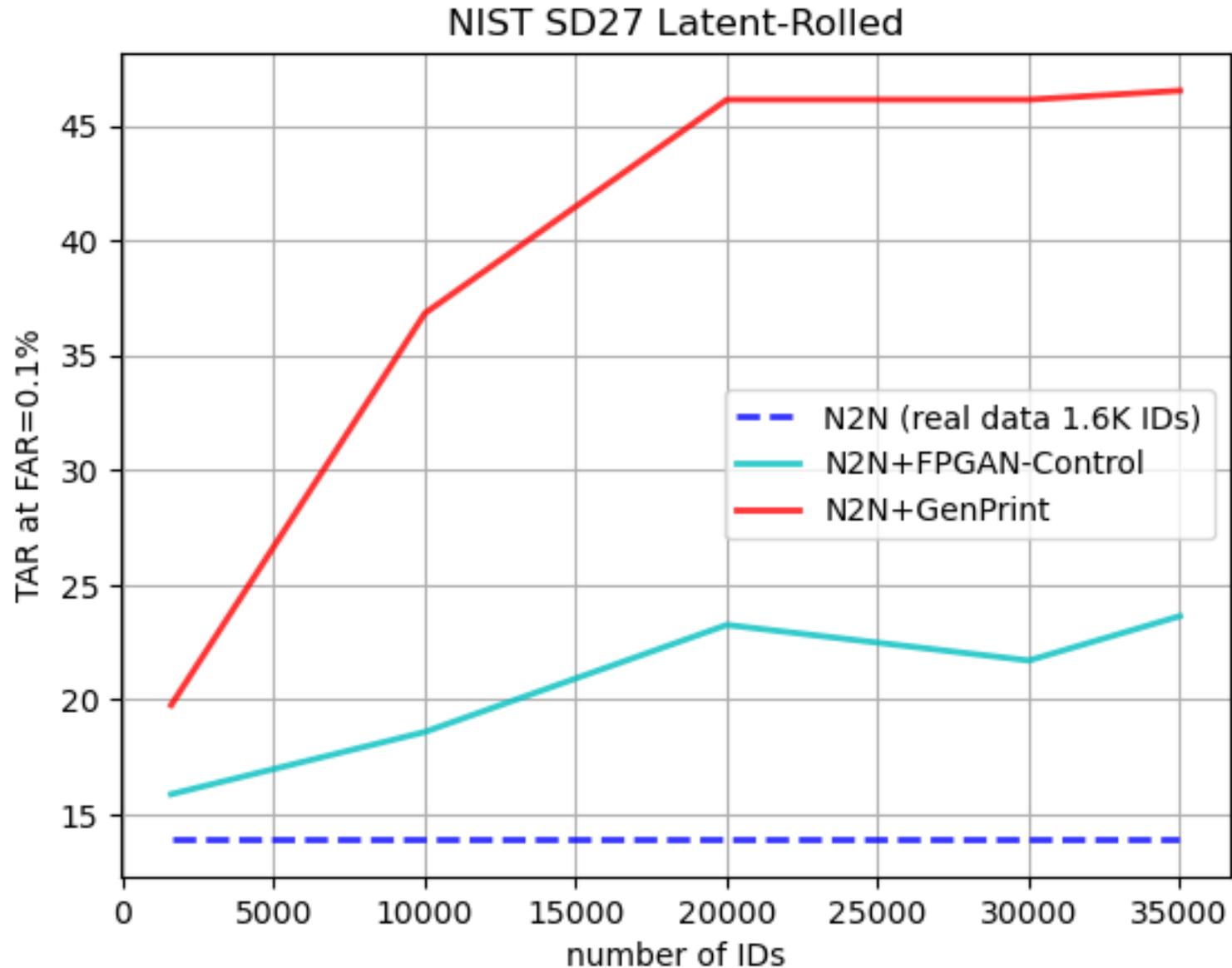
J. J. Engelsma, S. A. Grosz and A. K. Jain, "PrintsGAN: Synthetic Fingerprint Generator", IEEE TPAMI, 2022

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

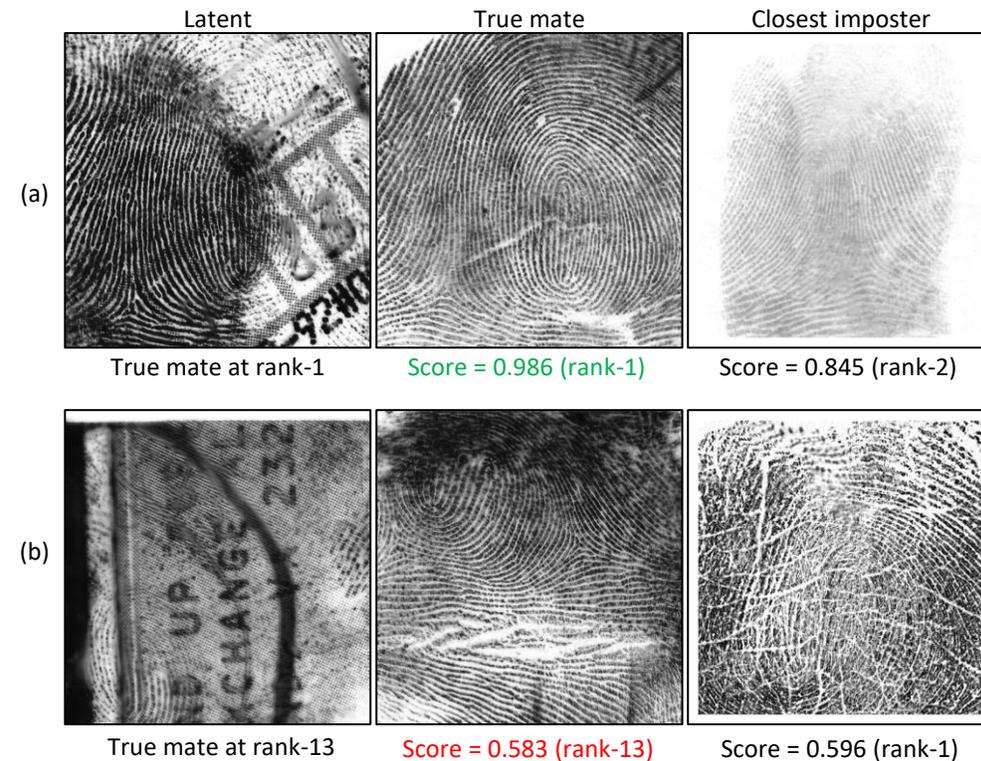
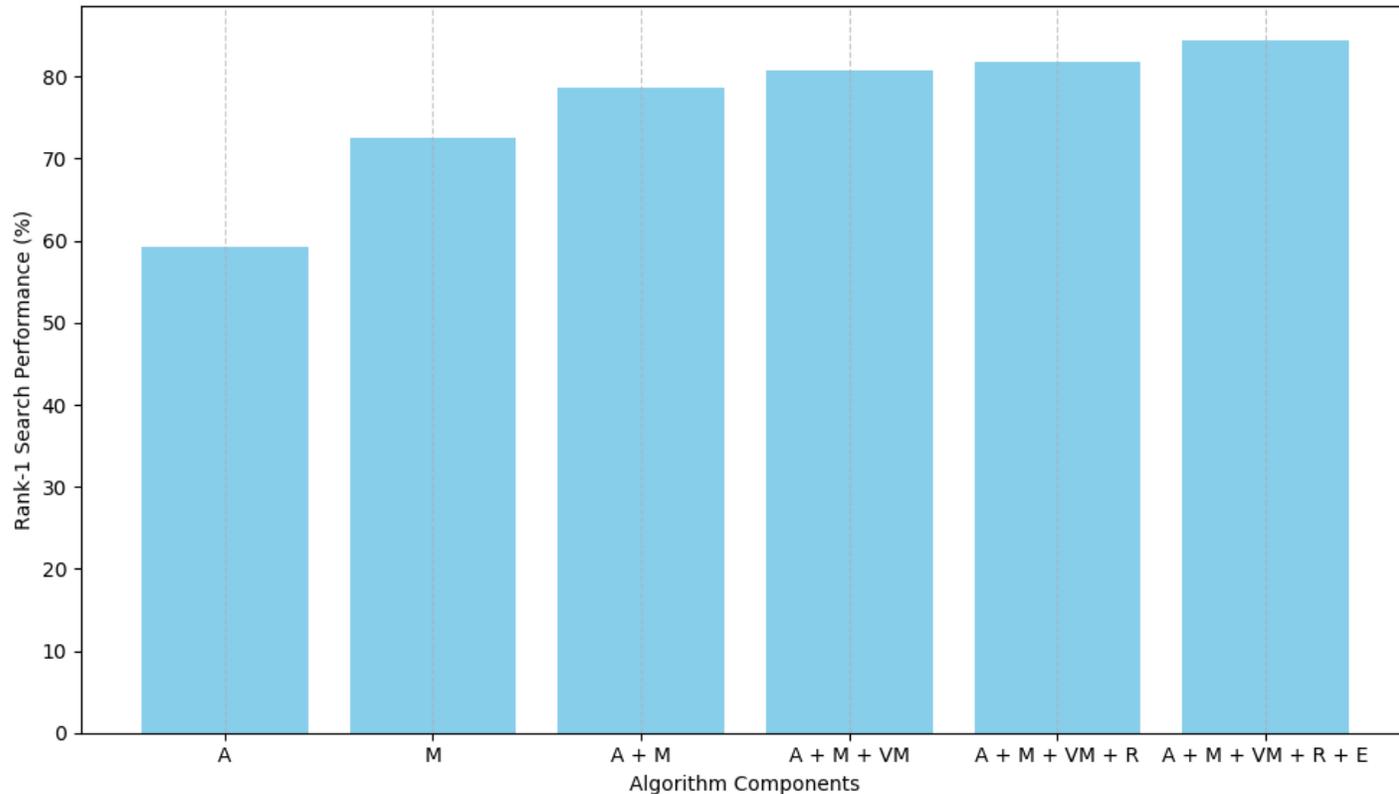


Performance Gain by Data Augmentation



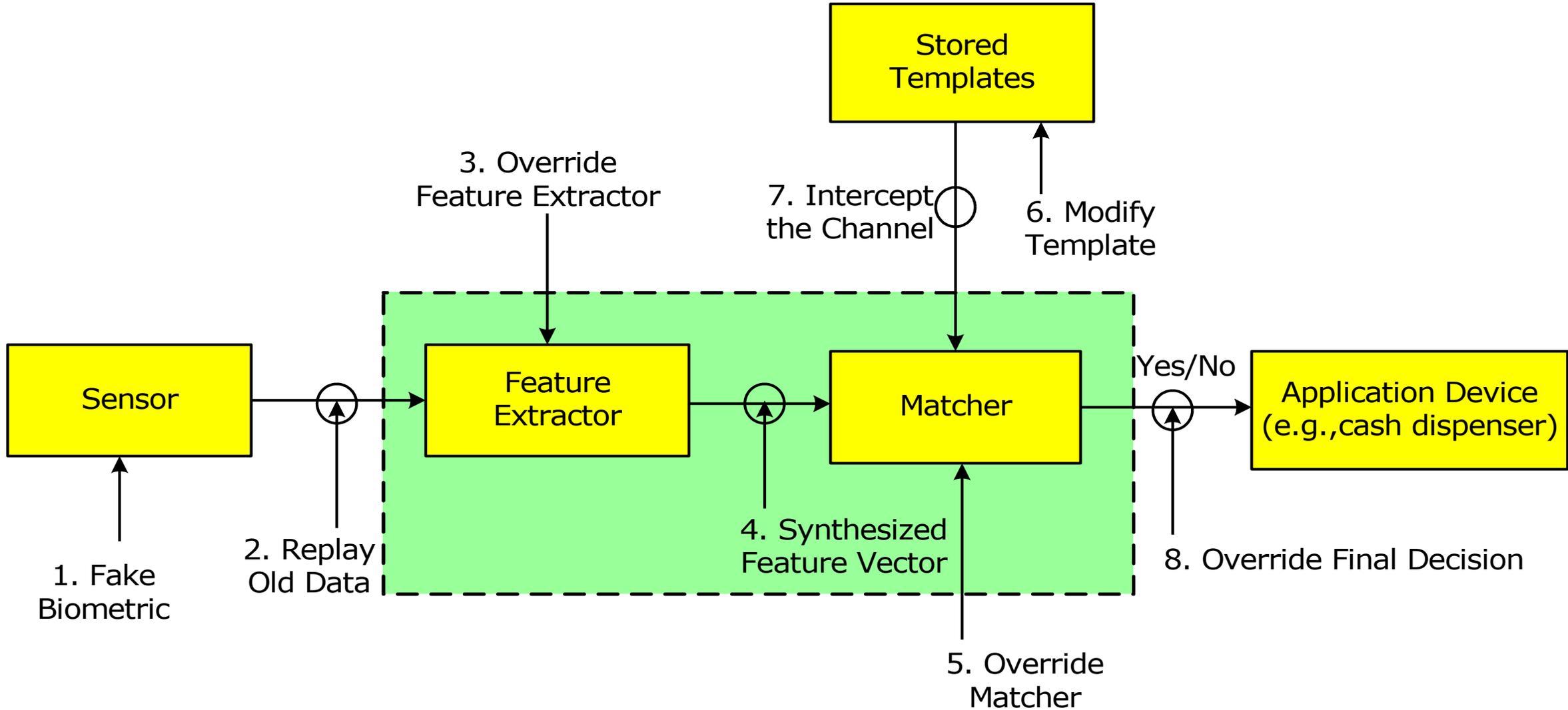
Latent Fingerprint Matching

LFR-Net Ablation Study on MSP Latent Database



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

Security of Biometric System



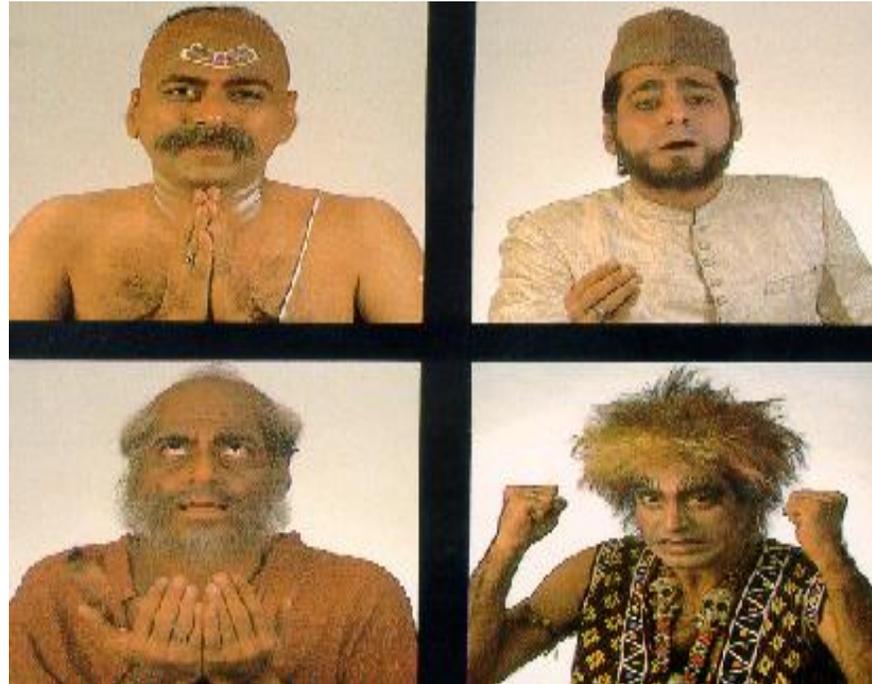
Presentation Attacks



Gummy finger



Fake hand



Face disguise



Fake eyeball



Silicone Mask



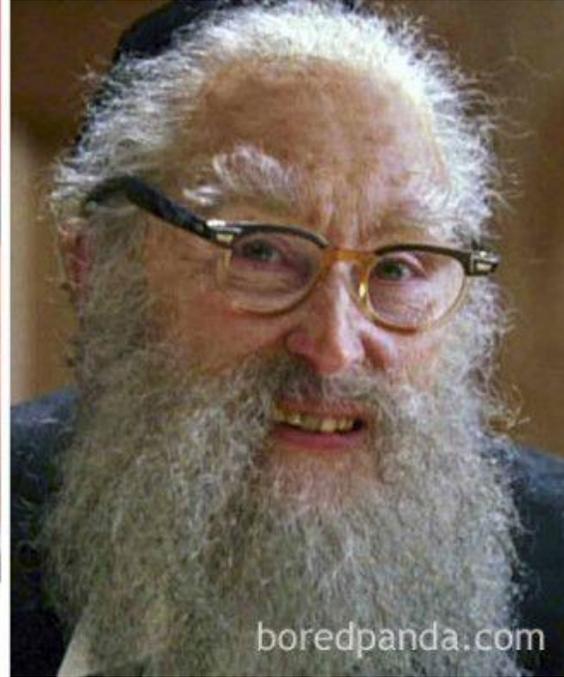
Print



Fingerprint alteration

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

Presentation Attacks

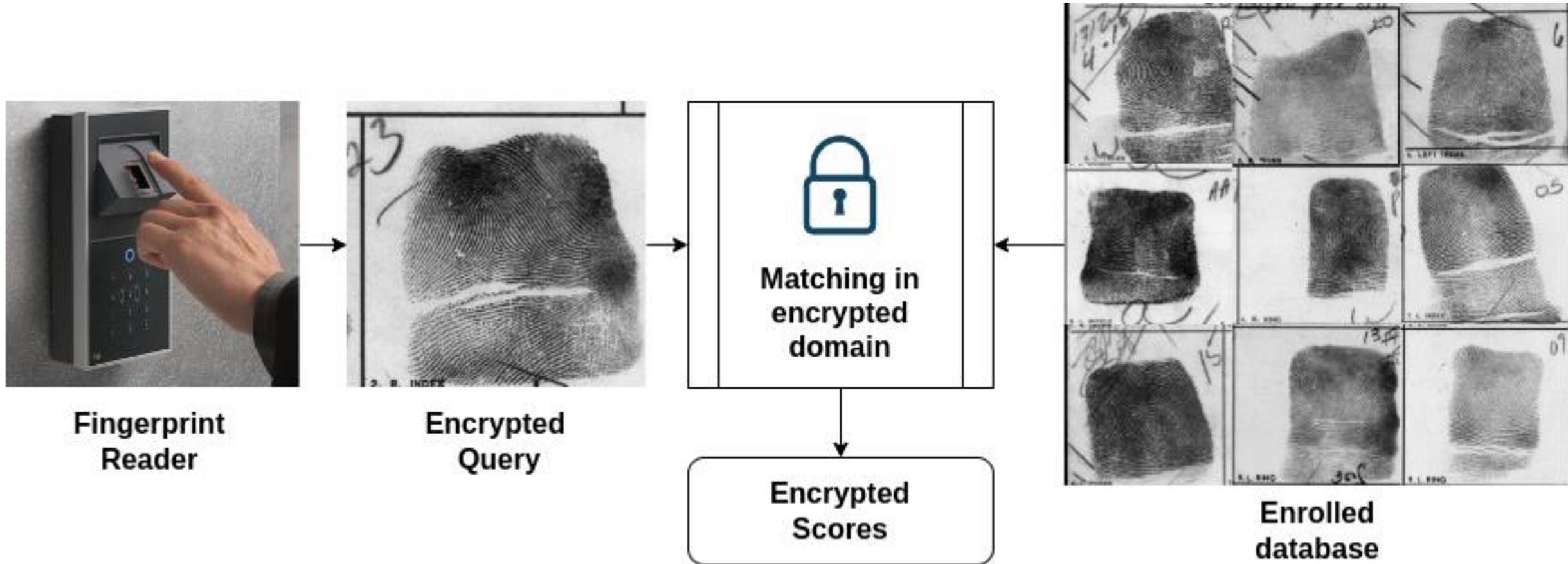


Meryl Streep - Rabbi (Angels In America, 2003)



Johnny Depp - James 'Whitey' Bulger (Black Mass, 2015)

Privacy-Preserving Authentication



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

Summary

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

Interdisciplinary Nature of Biometrics

