

# Introduction to Biometrics

Anil K. Jain

Michigan State University

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

21st International Summer School for Advanced Studies on Biometrics and Secure Authentication, 2024

# How Do I Know Who you Are?

**Lack of Trust:** ID documents, PIN/PW can no longer be trusted; In 2021, 1 in 10 persons had been victims of identity theft <https://bjs.ojp.gov/press-release/victims-identity-theft-2021>

**Solution:** Need an authentication system that links a person to his body attributes for enhanced security and to curtail fraud



How do we know who is entering card & PIN?

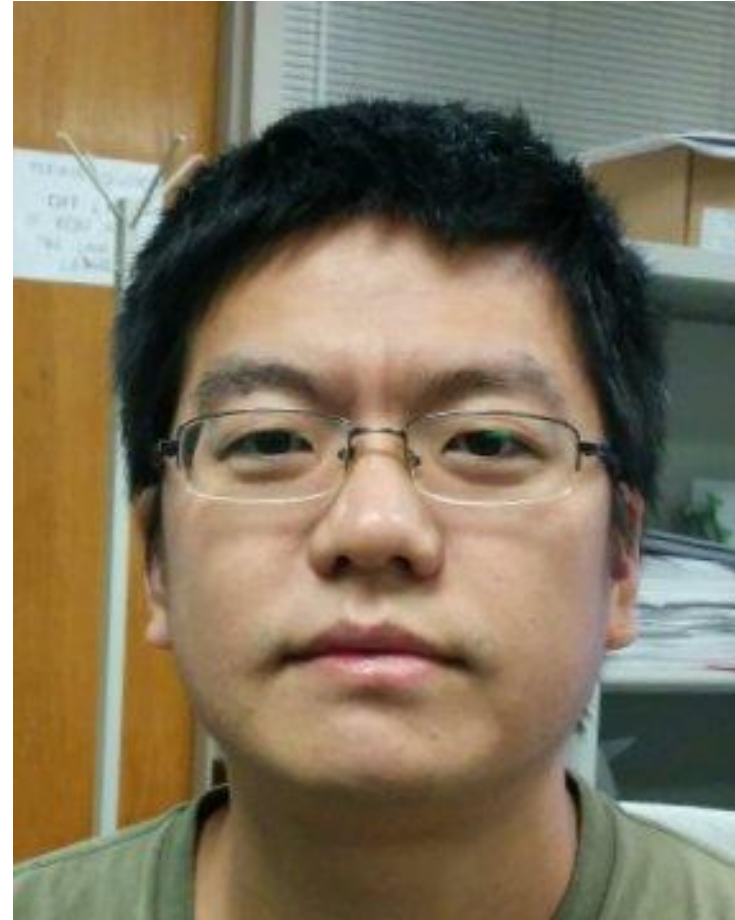
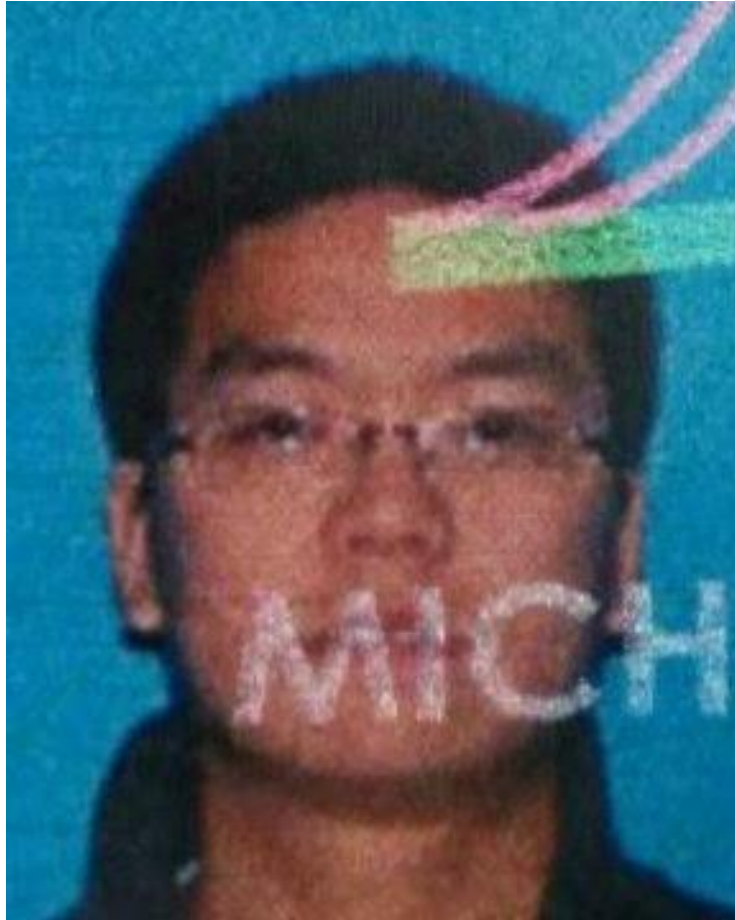


Fingerprint-enabled ATM

# Biometric Recognition

- The word biometrics is derived from two Greek words (*Morris, 1875*)
  - *Bios* means life and *Metron* means measure
  - *Statistics journal, Biometrika*
- Biometric's use for person recognition suggested by (*Pollack, 1981*)
  - What makes each person unique? *Use of biometrics for access control*
- Formal definition: (*ISO/IEC JTC1 2382-37:2012*)
  - *Automated person recognition based on behavioral & biological characteristics*

# Authentication (1 to 1 Comparison)



Same Person?

# Search (1 to N Comparison)

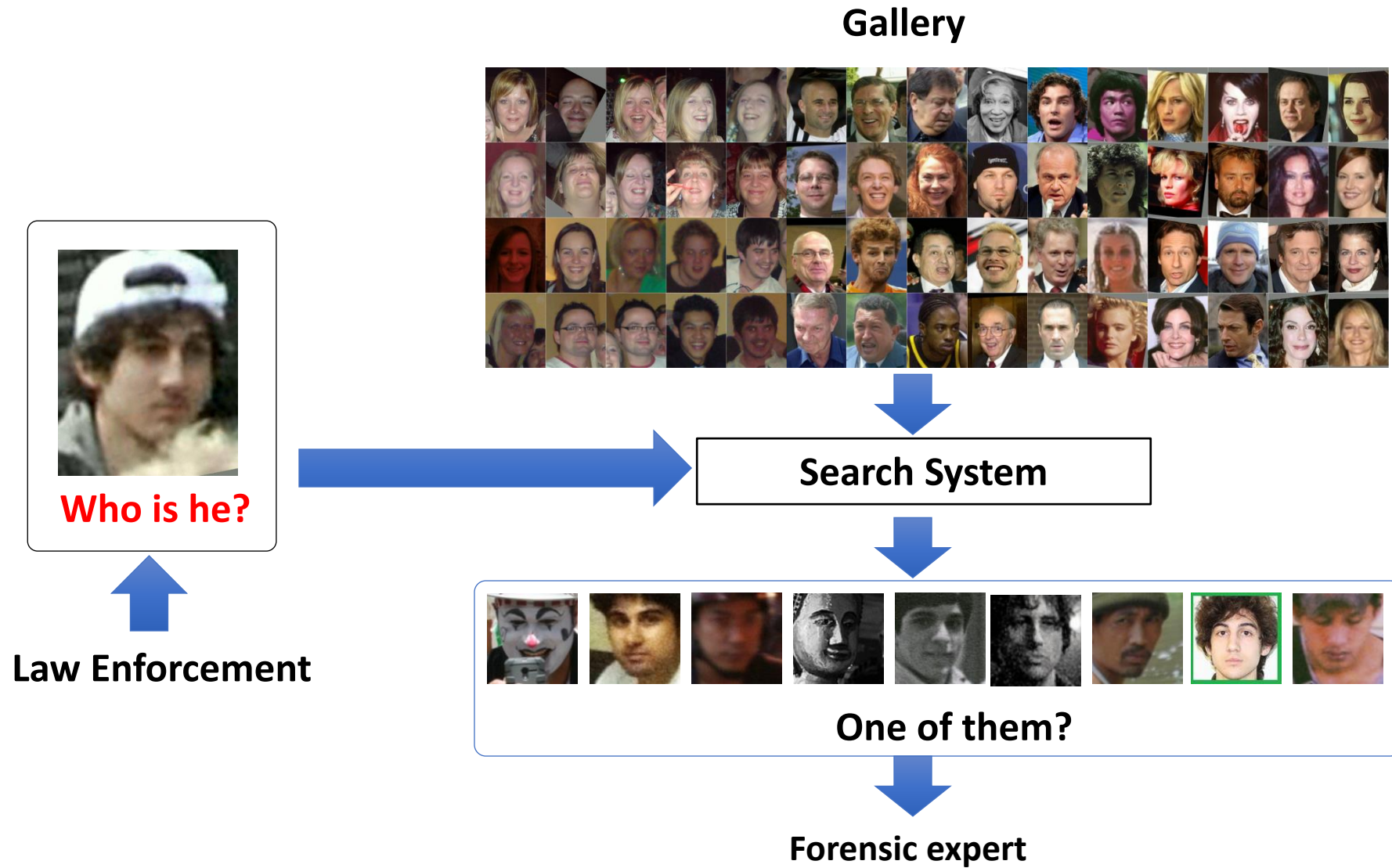
*Probe*

*Gallery*



Closed-set v. Open-set search

# Semi-automated Search



# Biometric Traits



**Multi-factor (Face +PIN) and Multi-modal (palmprint + palm vein) identification**

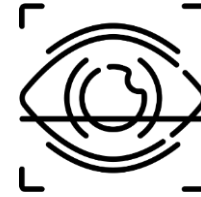
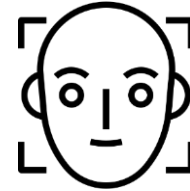
# Which Biometric Trait?

- Uniqueness and persistence
- Recognition accuracy
- User acceptance
- Ease of integration
- Resistance to spoofing
- Ease of sensing, Return on investment (RoI), robustness,.....

**Choice of biometric trait depends on application requirements**



# Most Popular Biometric Traits



Incheon, South Korea: Smart Entry



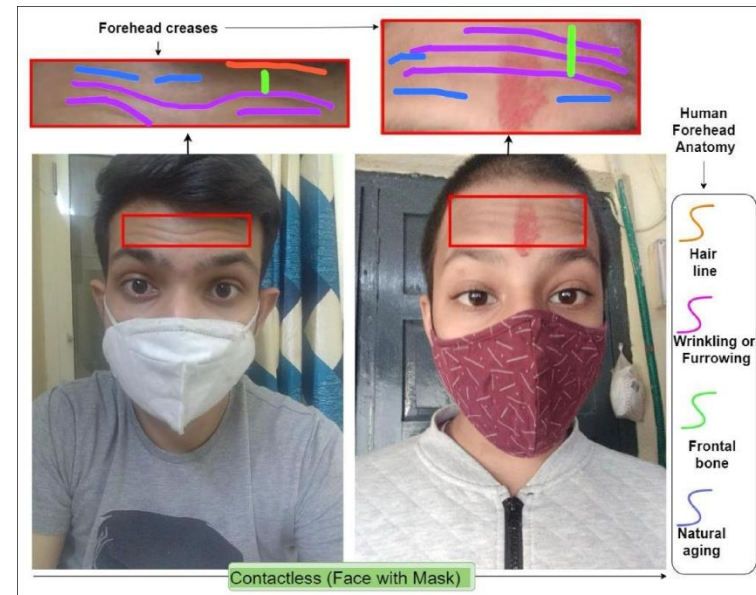
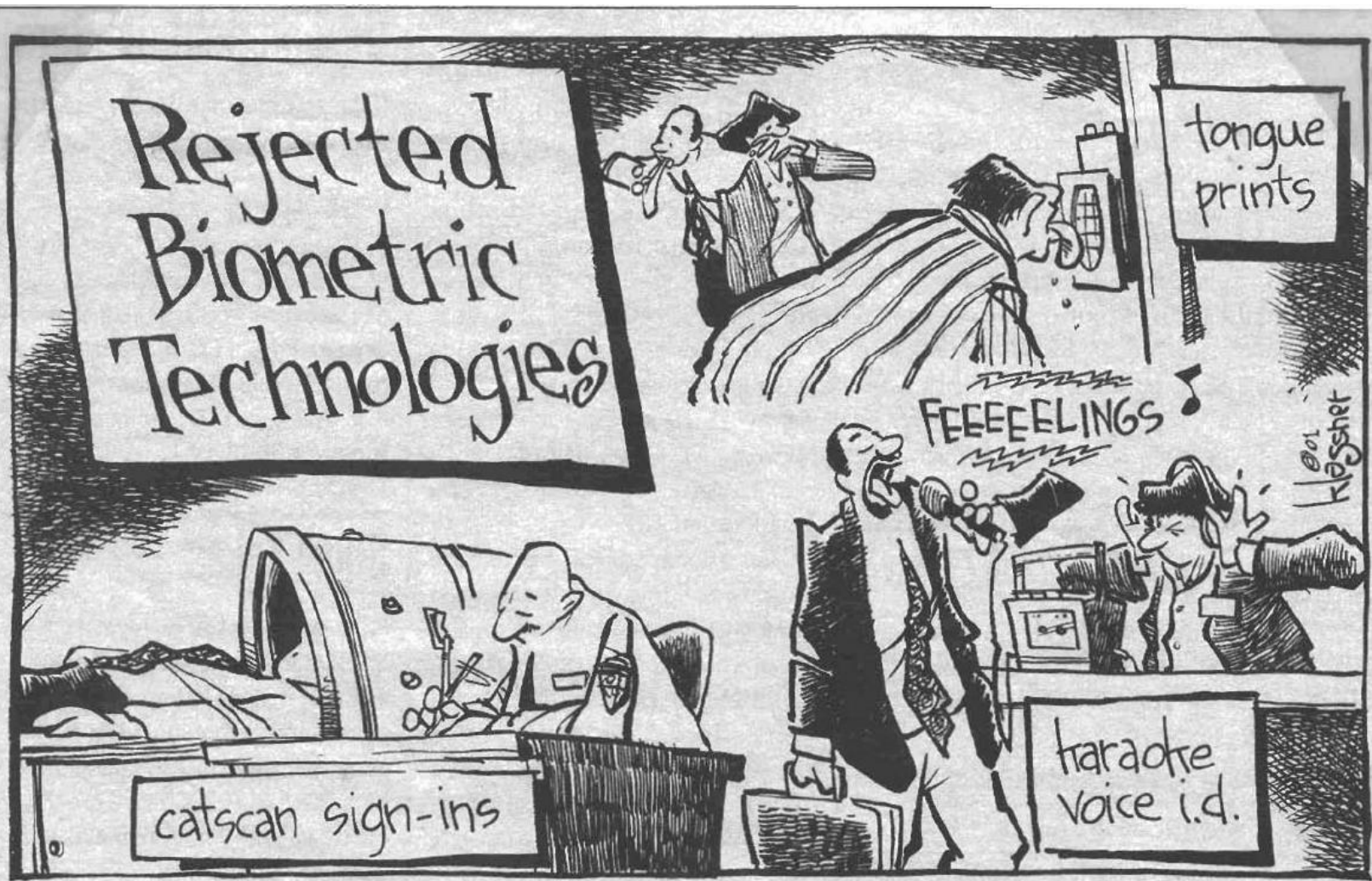
Australia: SmartGate



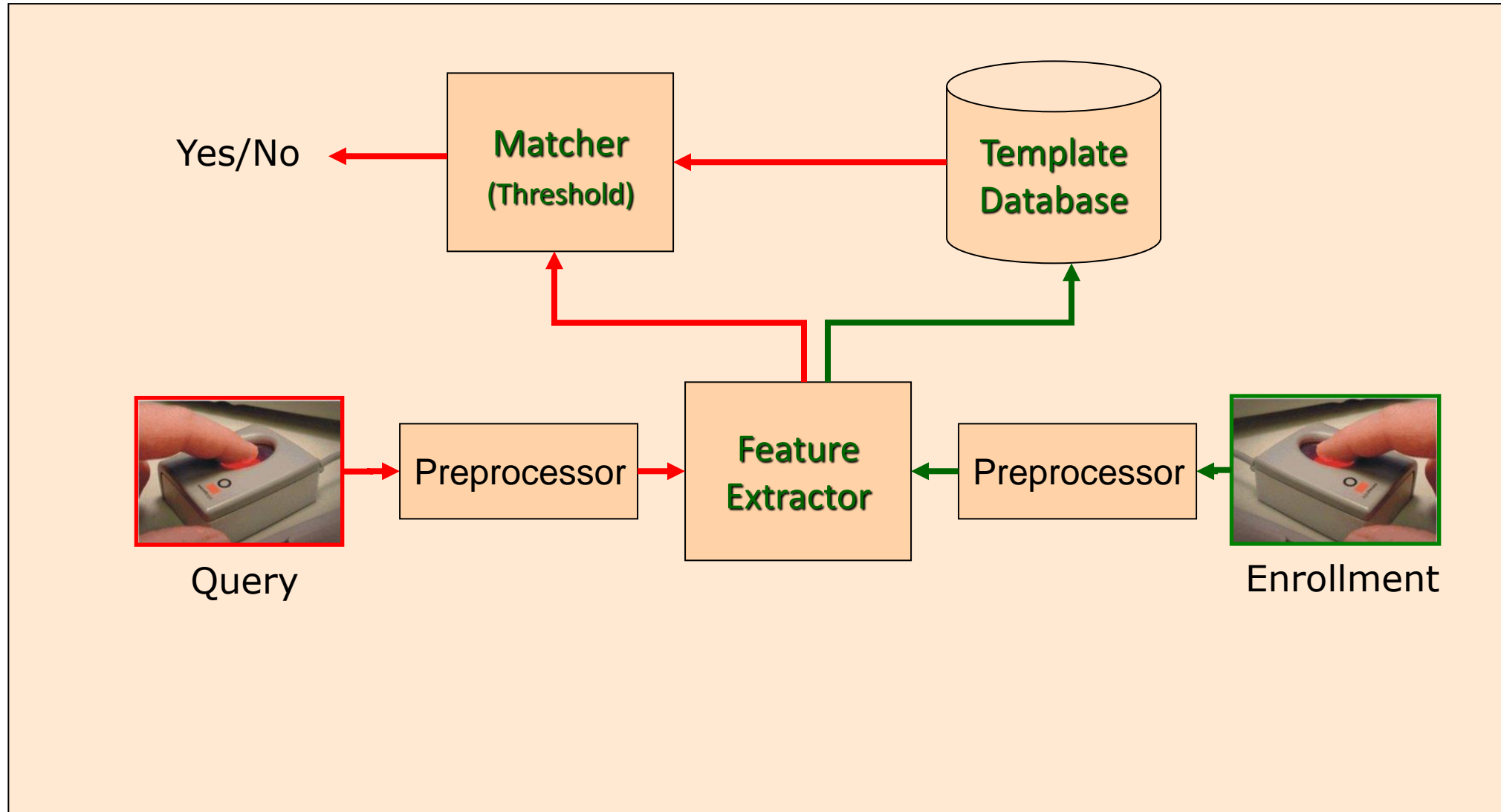
Amsterdam: Privium border passage

1. Satisfy individuality and permanence properties
2. Demonstrate high accuracy (NIST evaluations)
3. Fast search (1:N comparison) for large legacy databases

# Rejected Traits



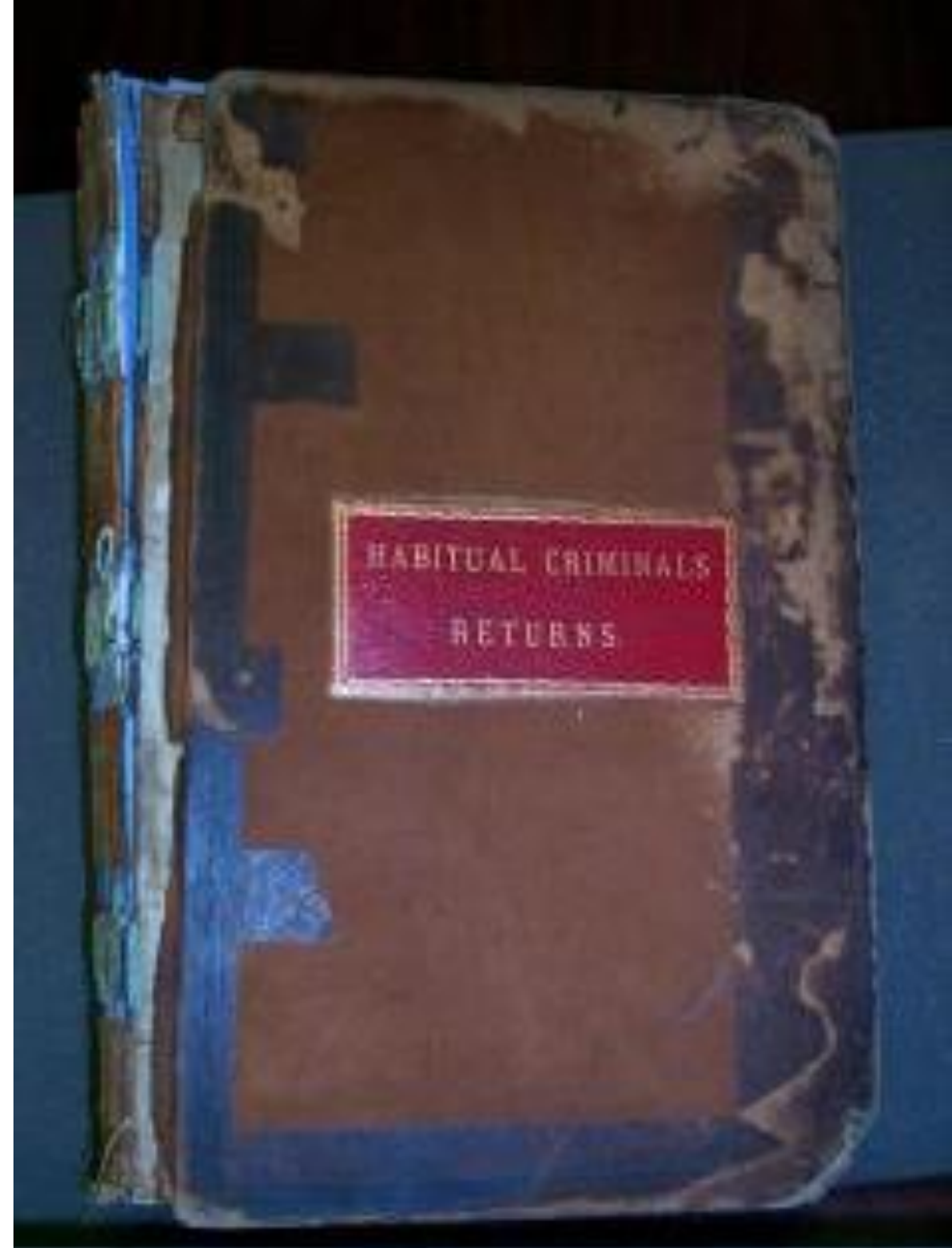
# Biometric Recognition Pipeline



# Biometric Milestones

# Habitual Criminal Act (1869)

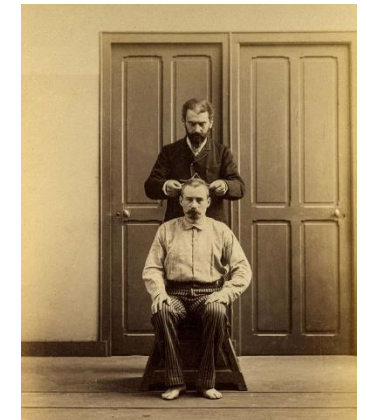
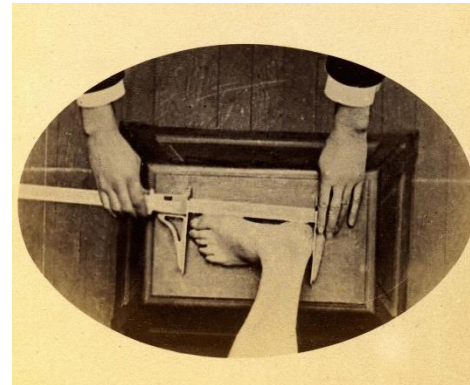
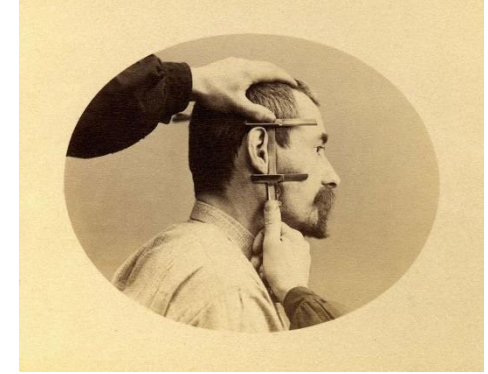
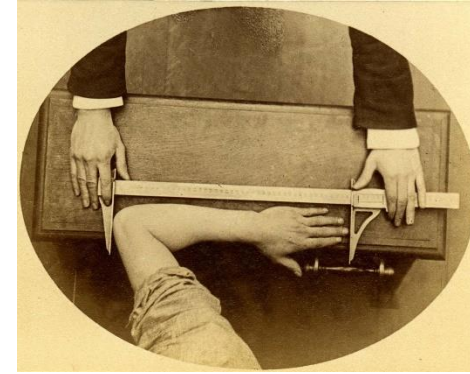
*“What is wanted is a means of classifying the records of **habitual criminals**, such that as soon as the particulars of the personality of any prisoner (whether description, measurements, marks, or photographs) are received, it may be possible to ascertain readily, and with certainty, whether his case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



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

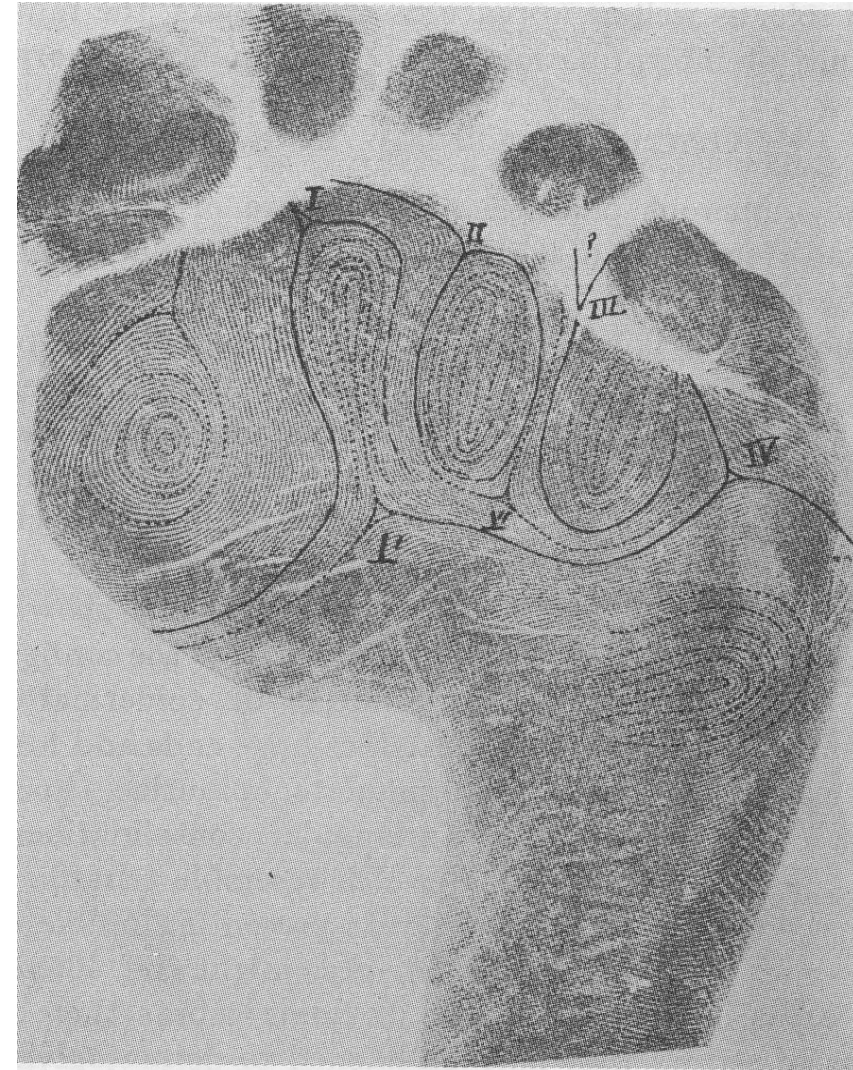


Photographing a suspect in the courtyard of a Police Prefecture in Paris



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

# Friction Ridge Patterns



Cumins and Midlo, *Finger Prints, Palms and Soles*, Dover, 1961

**Dermatoglyphics: Derma (skin) + glyphe (carve): study of ridged patterns**

# Scotland Yard (1905)



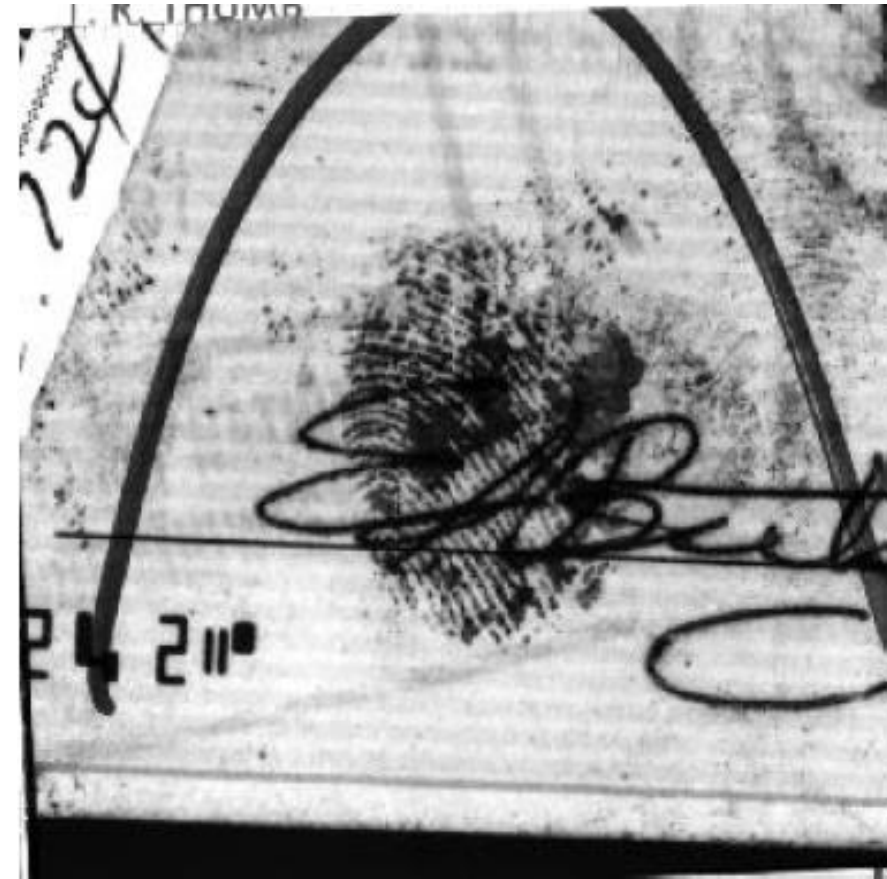


# FBI (1924)

APPLICANT		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK		FBI		LEAVE BLANK	
		Last Name <i>Teacher, Theresa C.</i>		First Name <i>Teacher, Theresa C.</i>		Middle Name <i>Teacher, Theresa C.</i>			
SIGNATURE OF PERSON FINGERPRINTED		ALIASES AKA		O R I		NY921940Z		DATE OF BIRTH DOB	
		<i>Formerly: Theresa Smith</i>				NYSTED Dept-FPU ALBANY, NY		<i>12/31/70</i>	
RESIDENCE OF PERSON FINGERPRINTED		CITY/TOWNSHIP PCT		SEX		HAIR		PLACE OF BIRTH POB	
<i>318 School Street Hometown, NY 11111</i>		<i>US</i>		<i>F</i>		<i>W</i>		<i>Ohio</i>	
DATE		SIGNATURE OF OFFICIAL TAKING FINGERPRINTS		WEIGHT		HEIGHT		EYES	
<i>5/02/02</i>				<i>155</i>		<i>5'7"</i>		<i>Gr</i>	
EMPLOYER AND ADDRESS		MARRIAGE		CLASS		REF		LEAVE BLANK	
<i>(if applicable) Smart Falls Central School Dist Smart Falls, NY 11111</i>		<i>Leave Blank</i>		<i>Leave Blank</i>		<i>Leave Blank</i>			
REASON FINGERPRINTED		SOCIAL SECURITY NO.		MARRIAGE		MARRIAGE			
<i>Leave Blank</i>		<i>000-10-1111</i>		<i>Leave Blank</i>		<i>Leave Blank</i>			

IDENTIX TP600 1259		ALS004228 LEX004229		
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L. THUMB	R. THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY



Partial fingerprint from a crime scene

Tenprint card

# 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.”*

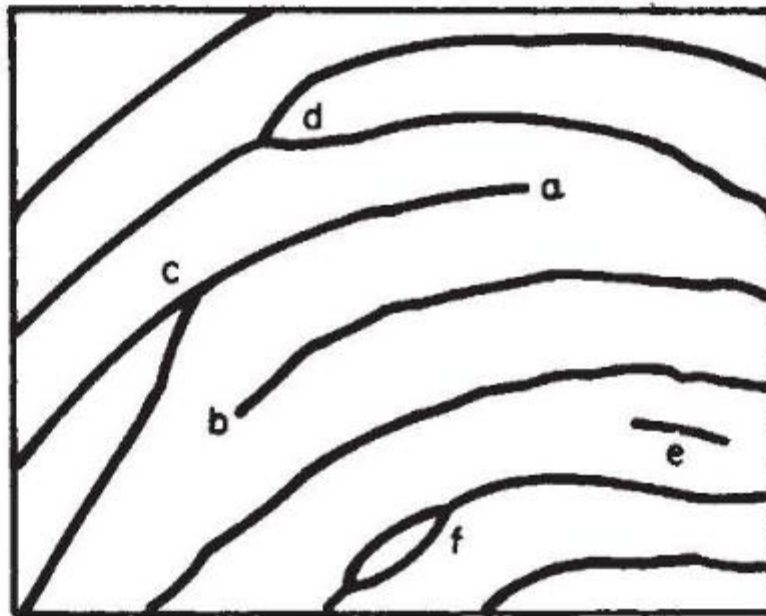
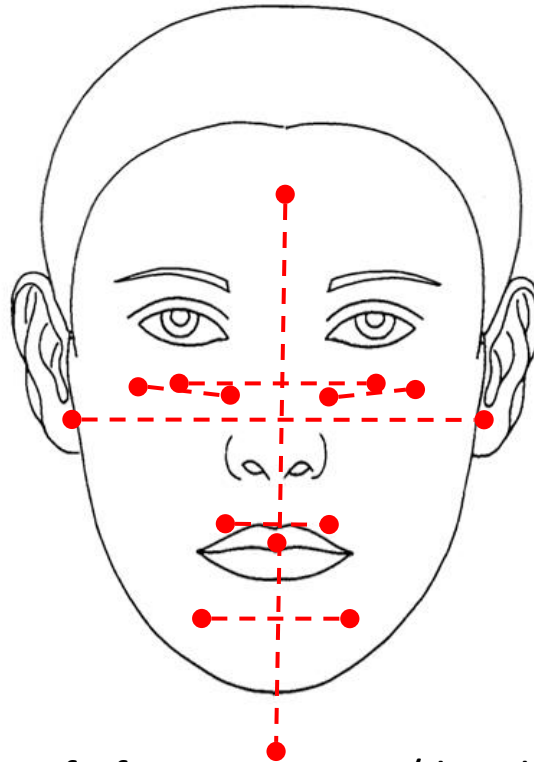


Fig. 1. Portion of fingerprint pattern (diagrammatic, enlarged) after Galton, showing minutiae. *a* and *b* are ridge ends, *c* and *d* are ridge branchings or valley ends, *e* is an island, and *f* is an enclosure. The ridge end and valley end are the principal minutia types, accounting for almost all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

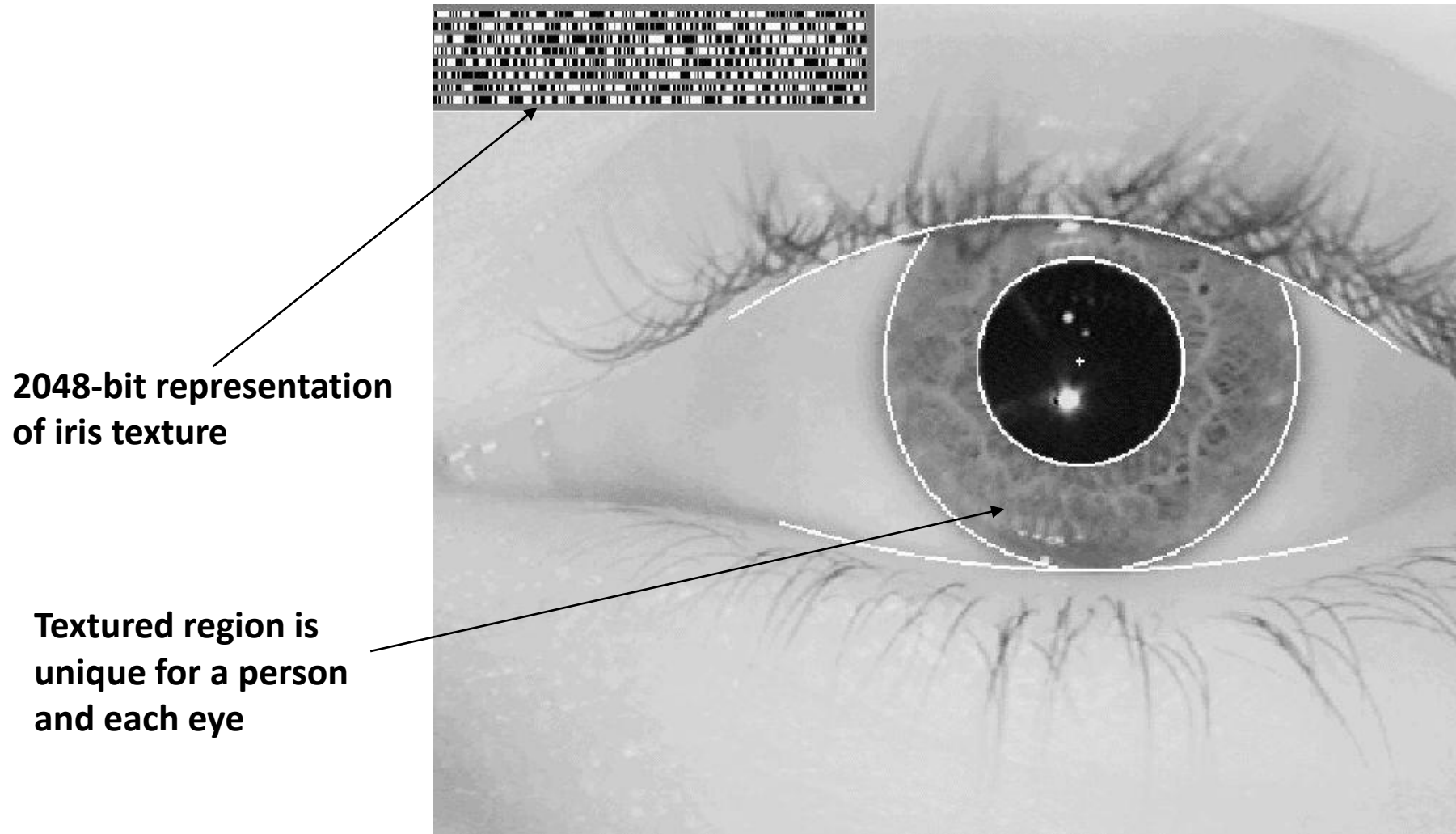
# Face Recognition (Bledsoe, 1966)

"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**

# Iris Recognition (Daugman, 1993)



**Ophthalmologists Frank Burch (1936) and Leonard Flam and Aran Safir (1985) suggested use of iris pattern**

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

# Biometric Recognition Before 1990



Hand geometry recognition



Manual fingerprint comparison

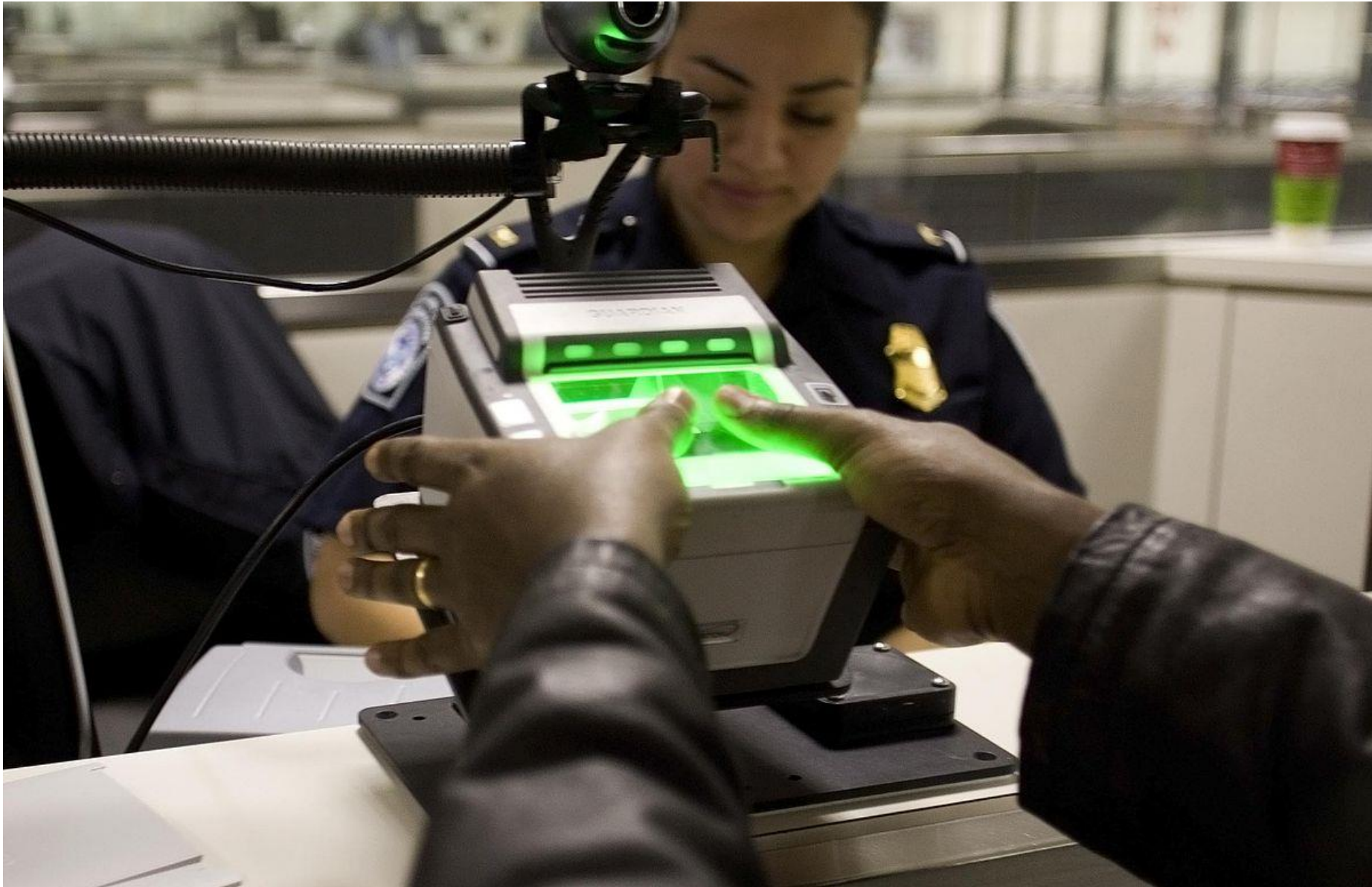


MSP AFIS (1989): 700K tenprints in database; 5K rolled print searches; no latent search; 15K comparisons/sec.

# 9/11 Terrorist Attacks (2001)



# US-VISIT (2003)

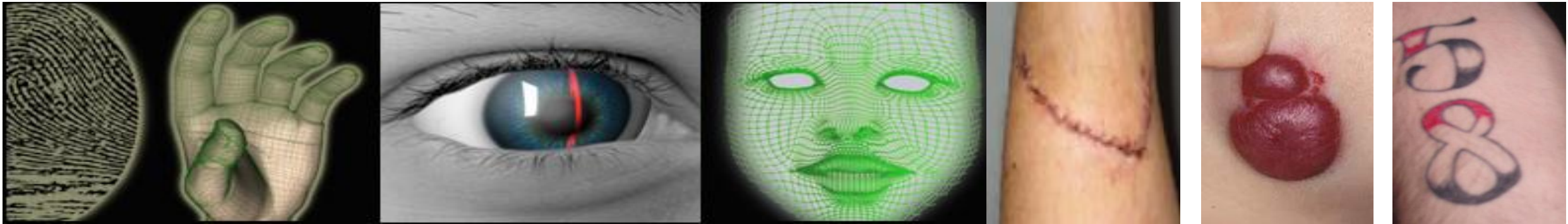


# Walt Disney Theme Park (2005)





# FBI Next Generation Identification (2008)

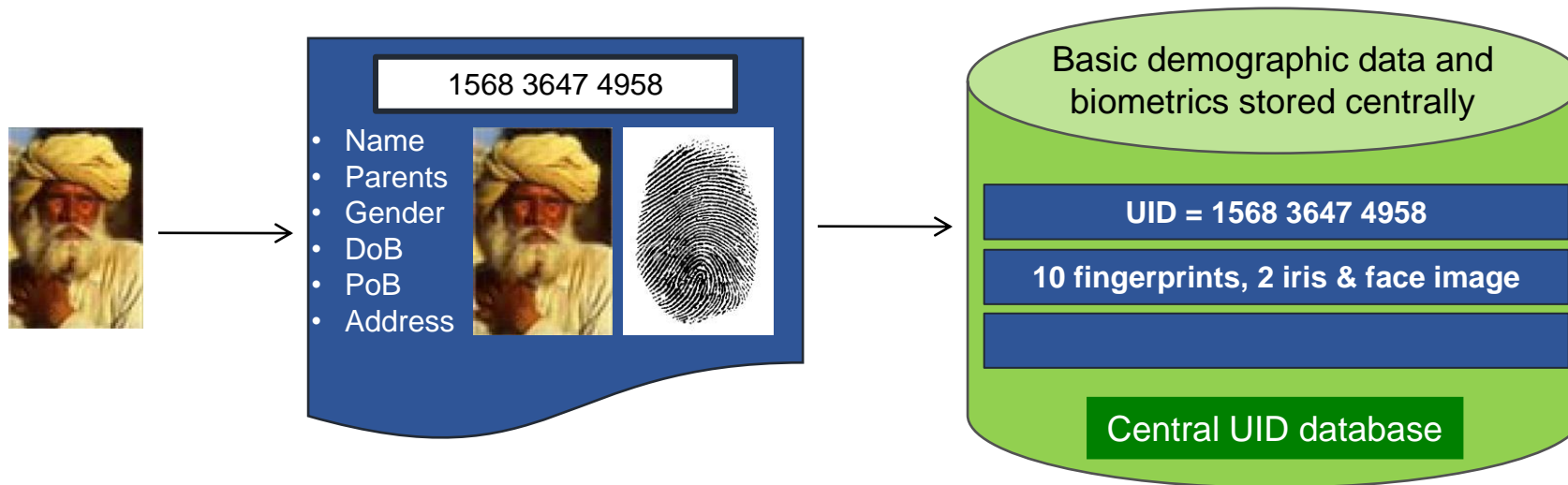


First AFIS in 1980s; IAFIS launched in 1999; use of **soft biometrics** (SMT)

[http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/ngi/ngi2/](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2/)

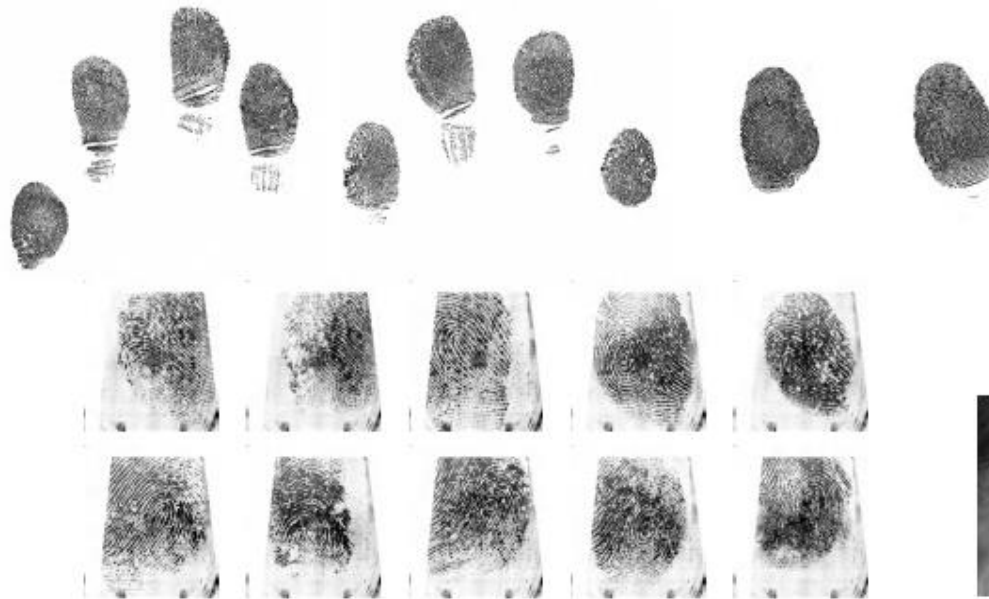
# Aadhaar: World's Largest Biometrics System (2009)

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



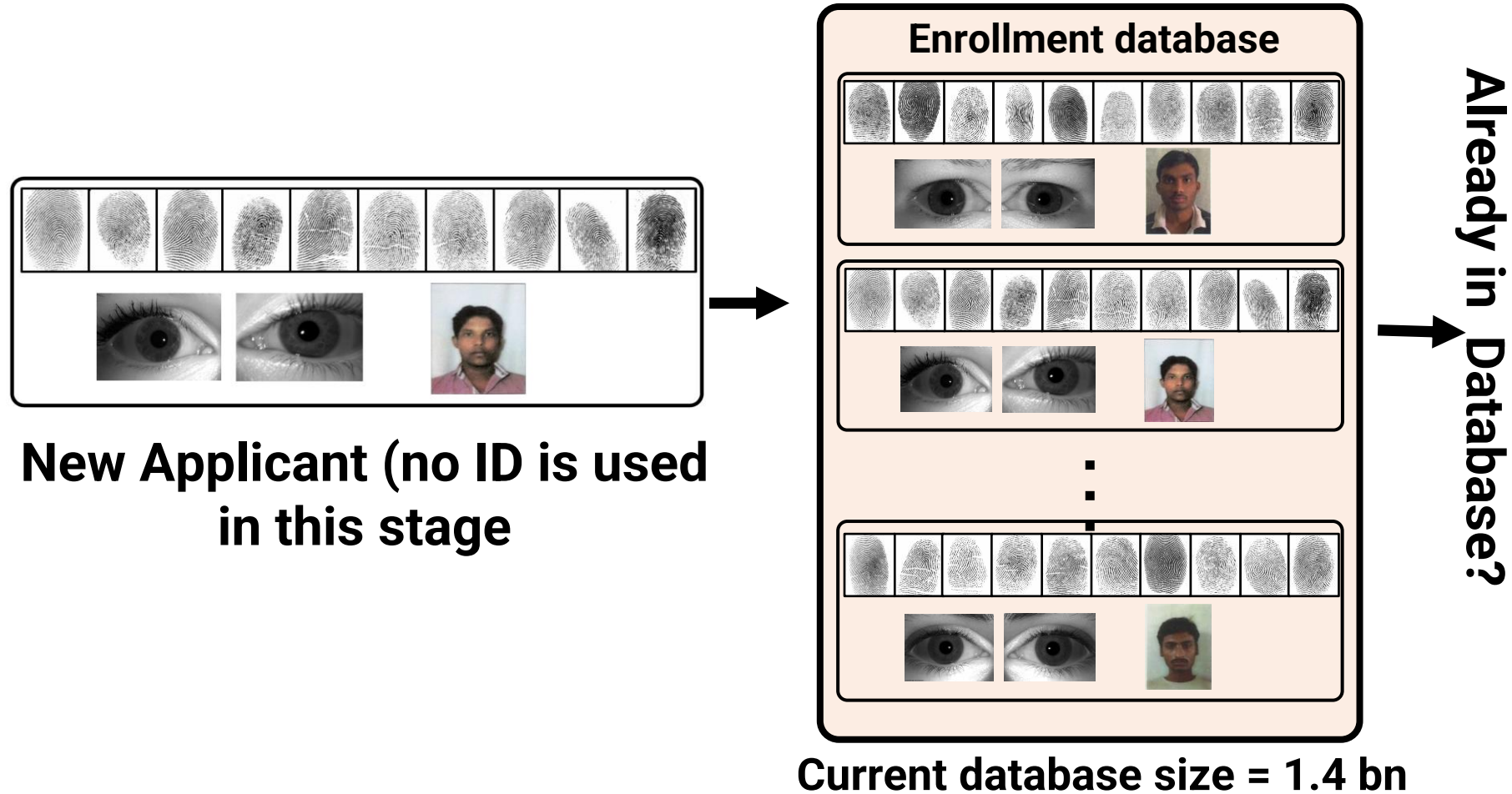
**Enrollment (1.4 billion), de-duplication, authentication (~70 million/day)**

# Enrollment



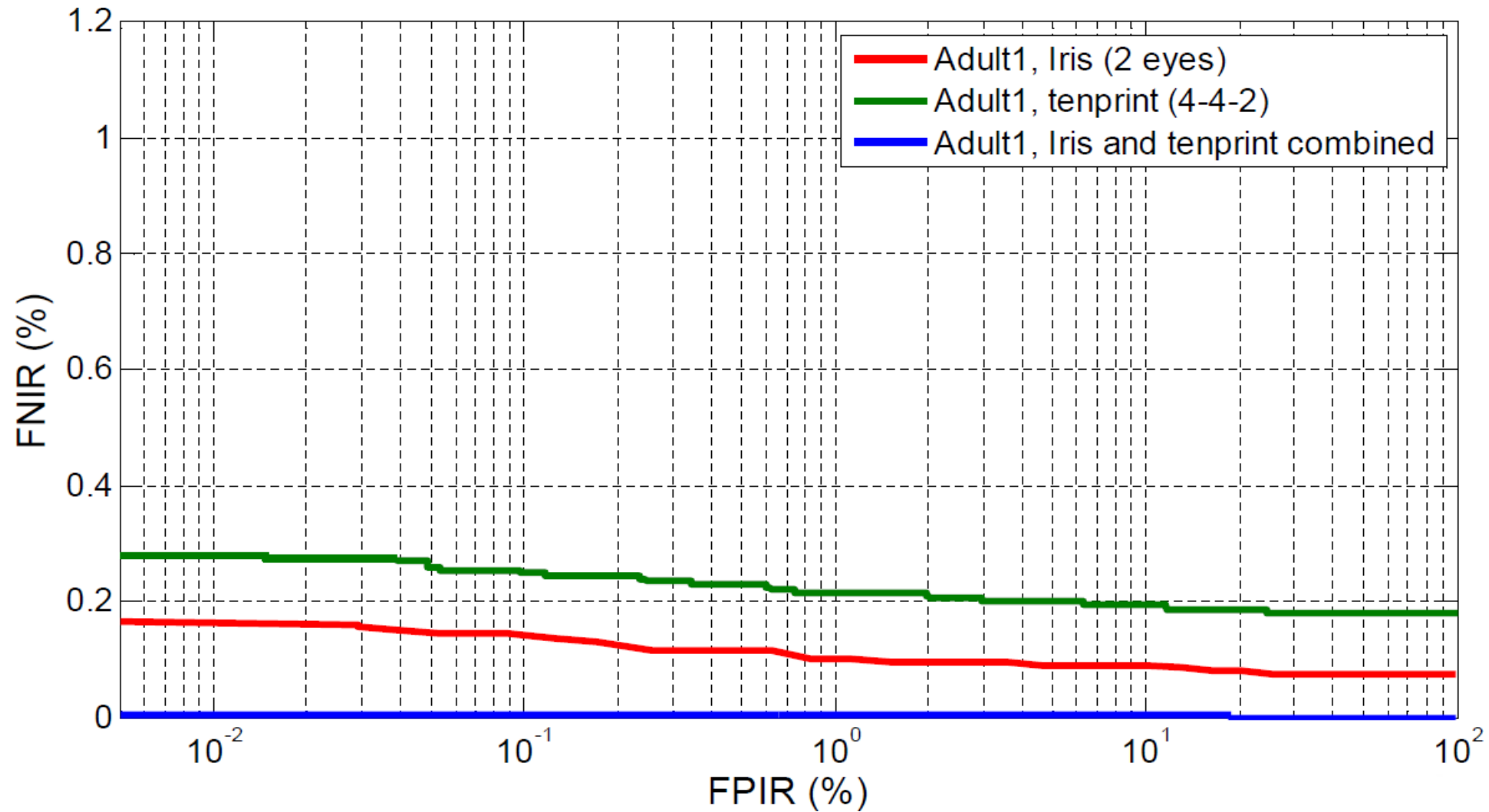
- 10 slap (4-4-2) fingerprints, 2 irises & face image are captured along with minimal demographic information
- Minimum age of enrollment is 5 years; re-enrollment at age 15;

# De-duplication (1:N Comparison)



- Is the person already enrolled?
- No single biometric trait can distinguish among 1.4 billion individuals

# Multimodal Biometrics



- **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) biometric authentications/day; 12-digit Aadhaar + fingerprint

[https://uidai.gov.in/aadhaar\\_dashboard/auth\\_trend.php](https://uidai.gov.in/aadhaar_dashboard/auth_trend.php)

# Smart Phones and Biometrics



**The first mobile phone (1973)**  
(Joseph Van Os / Getty Images)



**Touch ID, iPhone 5S (2013)**



**Face ID, iPhone X (2017)**



**The Pantech G100 (2004)**



**Apple Pay, iPhone 6 (2014)**



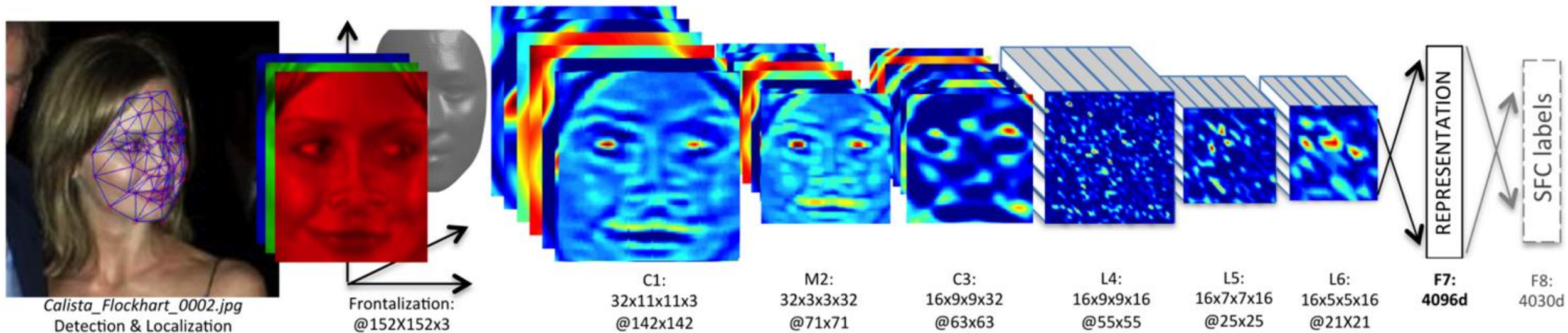
**Vivo In-Display Scanner (2018)**



**~1.4B Mobiles shipped in 2022;  
1B with biometrics**

- **We check our phones, an average, 58 times each day; Touch ID offered convenience & security**
- **Smartphone camera is now being used to capture selfie, contactless fingerprints and palmprints!!**

# DeepFace (2014)



- Multiple layers of neurons stacked together and connected to a small area in previous layer (120M parameters)
- Progress in face recognition: deep features, web crawled data, processing power
- **What about network design, loss function, embedding domain knowledge..?**

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



# SOTA Performance (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)

# Authentication



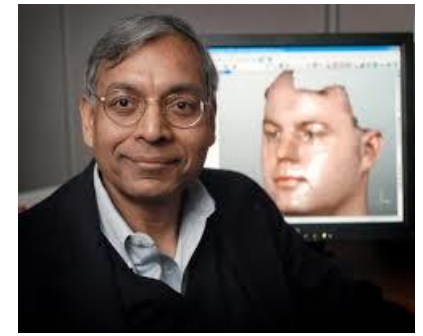
0.83



0.89



0.72



0.81



Probe (1984)



0.58



0.72



0.82



0.71

Threshold=0.54  
@ FAR=1e-6



0.74



0.66



0.63



0.49



0.17

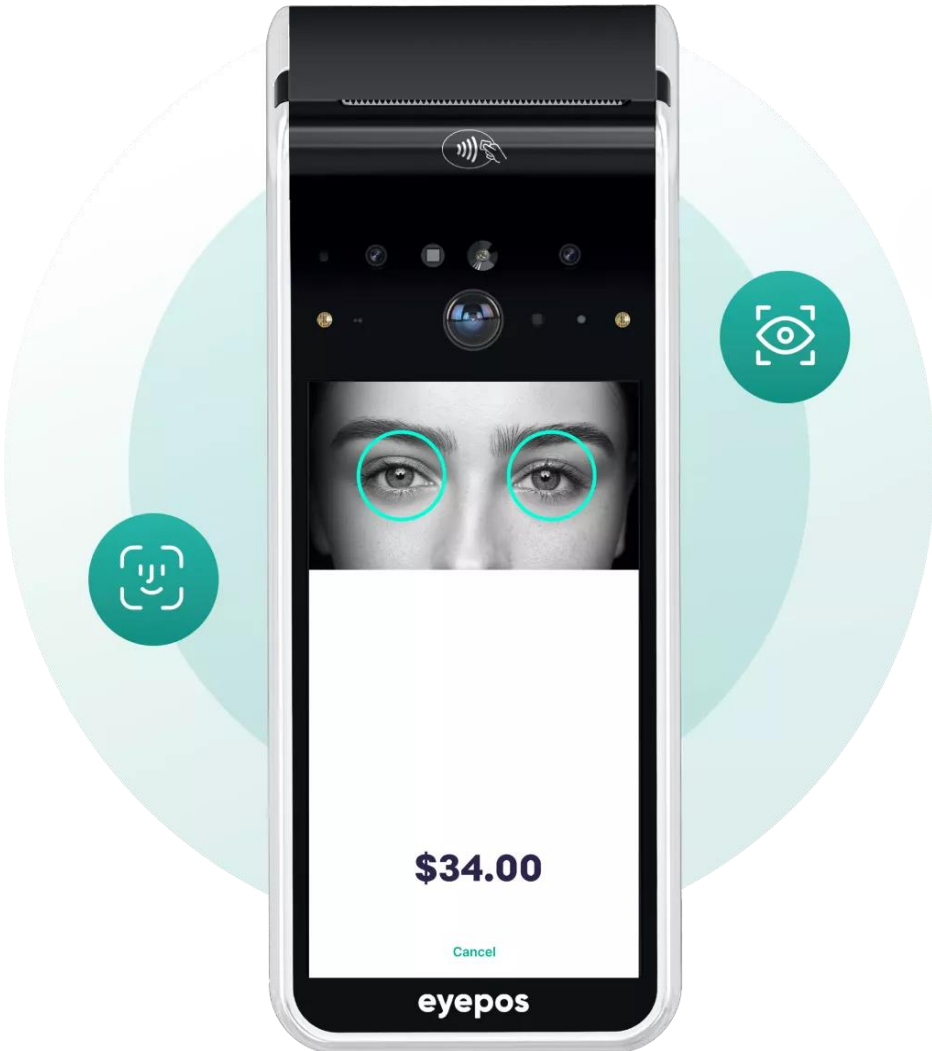
- Representation
- Similarity measure

<https://roc.ai/>

Gallery images

**Where is Biometrics Heading?**

# Biometrics in Payment



**Payment at Point of Sale**

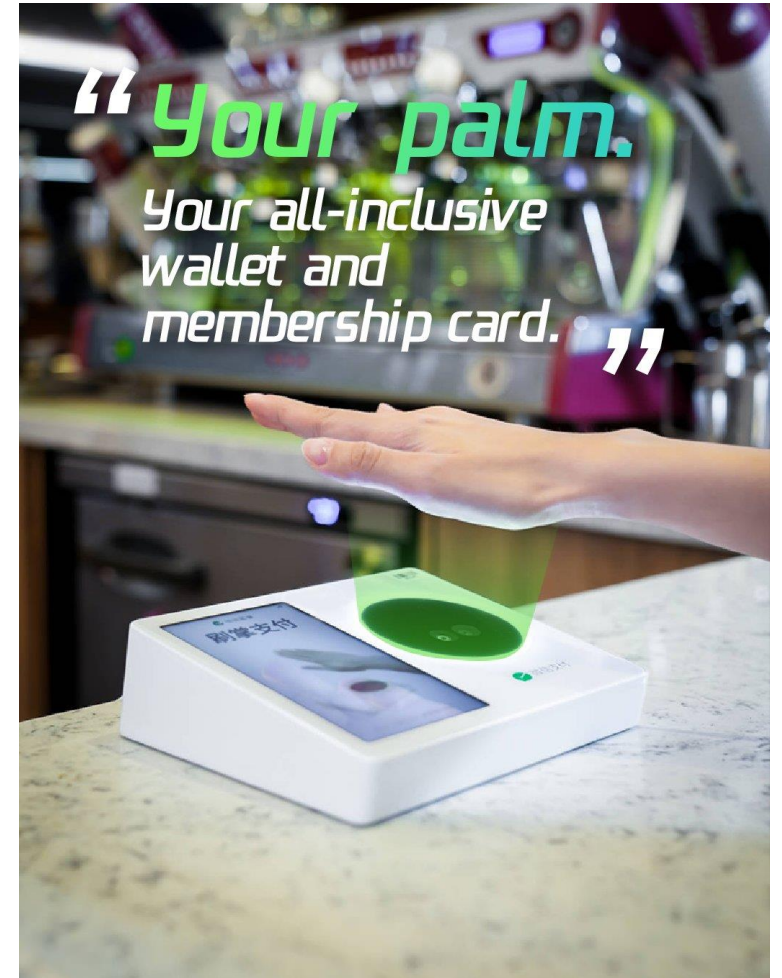
<https://payeye.com/for-business-eye-payments/>



Match on Card:



<https://one.amazon.com/how-it-works>



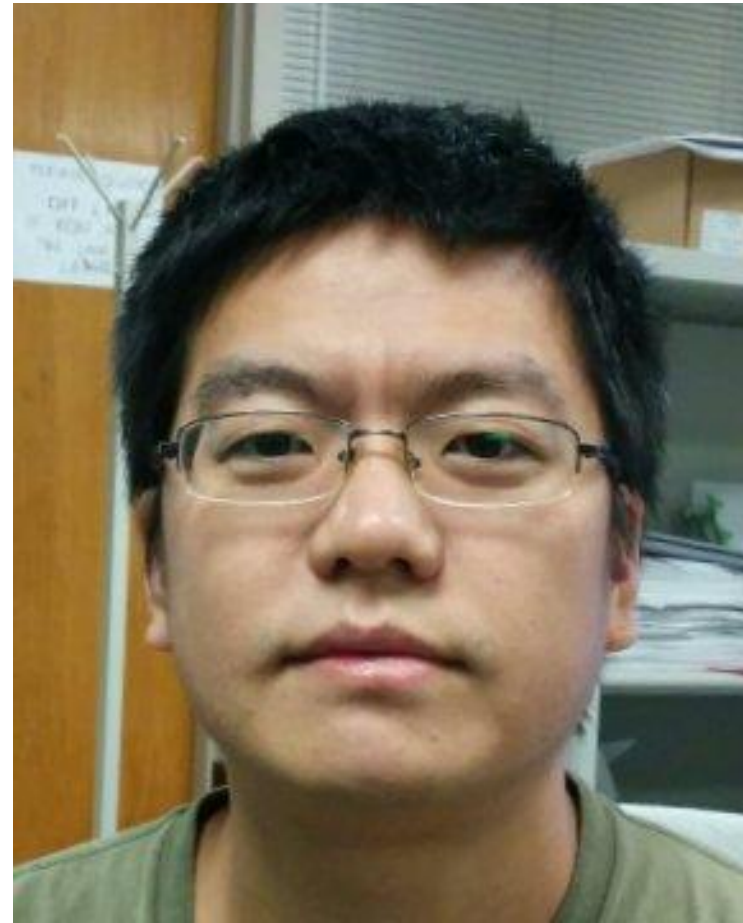
**“Your palm.**  
Your all-inclusive  
wallet and  
membership card.”

<https://x.com/WeChatApp/status/1660612850883211266/photo/2>

# Remote Authentication



Govt. issued ID



Selfie

**Matching, spoof detection, age estimation,...**

# Biometrics at Airports (Entry/Exit)

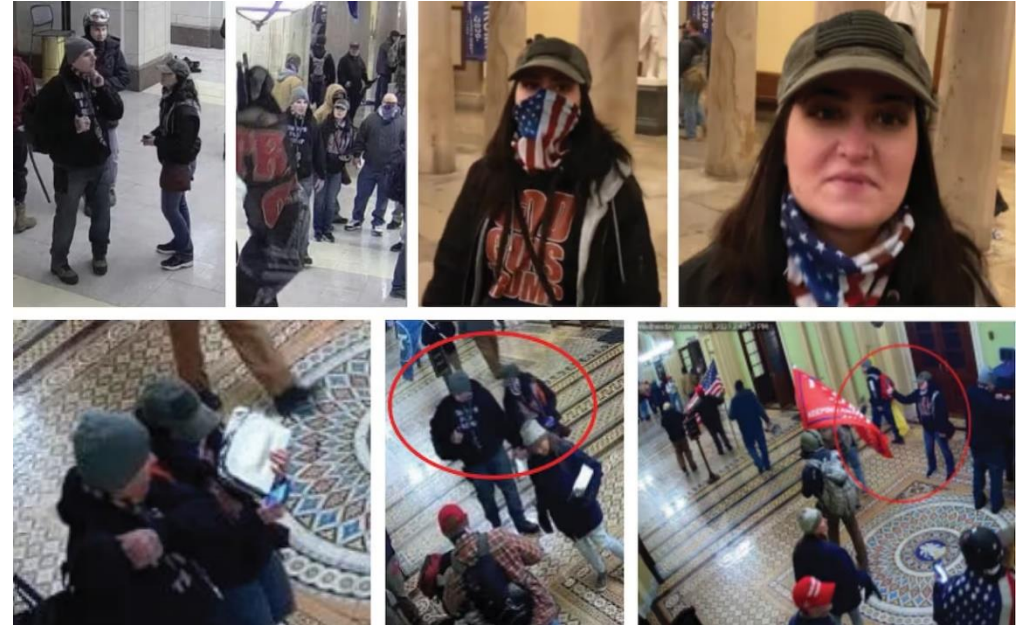
- International traveler's entry/exit photo compared with DHS database (e.g., photos from U.S. passports and U.S. visas, flight manifest).



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).

<https://www.cnn.com/travel/article/airports-facial-recognition/index.html> (8th October 2019)

# Face Recognition in Video



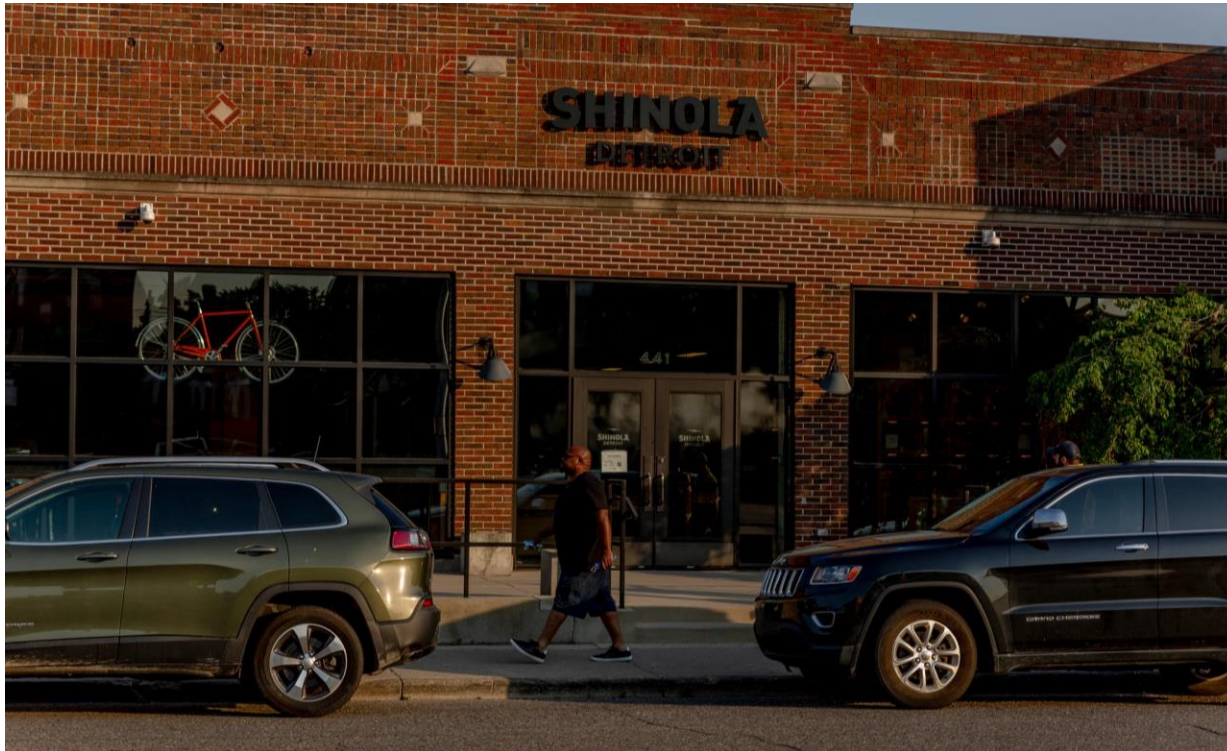
*Composite image of evidence pulled by the U.S. District Court for the District of Columbia against Debra Maimone. (U.S. District Court D.C.)*

**FBI used a mix of techniques, from license plate readers to 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, Shinola watch store in Detroit was robbed.
- Michigan Police searched a low-quality CCTV frame against 49M face database.
- *“This is not mw. You think all Black men look alike?” Robert Williams told investigators after he was arrested.*









MICHIGAN STATE POLICE  
INVESTIGATIVE LEAD REPORT

LAW ENFORCEMENT SENSITIVE

THIS DOCUMENT IS NOT A POSITIVE IDENTIFICATION. IT IS AN **INVESTIGATIVE LEAD ONLY** AND IS **NOT** PROBABLE CAUSE TO ARREST. FURTHER INVESTIGATION IS NEEDED TO DEVELOP PROBABLE CAUSE TO ARREST.

BID DIA Identifier: BID-39641-19	Requester: CA Yager, Rathe
Date Searched: 03/11/2019	Requesting Agency: Detroit Police Department
Digital Image Examiner: Jennifer Coulson	Case Number: 1810050167
	File Class/Crime Type: 3000

Probe Image	Investigative Lead
	

- A biometric matcher, as designed, returns a similarity between two images
- How to prevent different identities from having “high” similarity”?

1. A photo search outputs a sorted collection based on similarity to probe
2. A human facial examiner picks a match candidate image based on manual morphological comparison

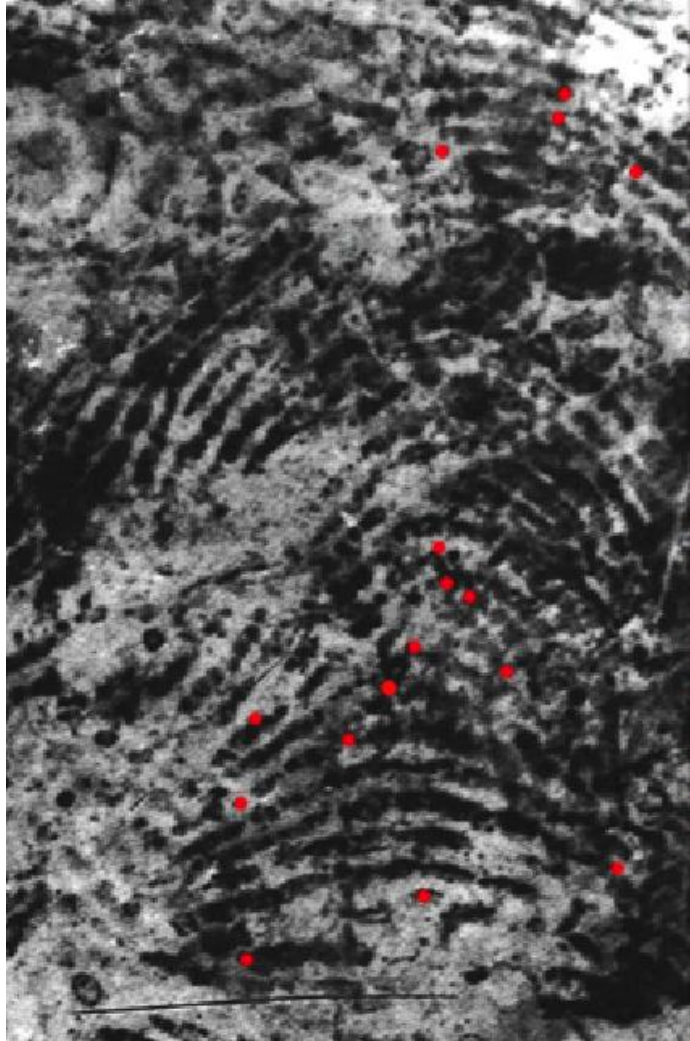


Poor quality of probe resulted in false positive



No other supporting evidence (eye witness, mobile phone GPS location, red cardinal cap), was used except for a “6-pack photo lineup”, that included Williams photo, shown to store manager

# Wrongful Apprehension of Brandon Mayfield

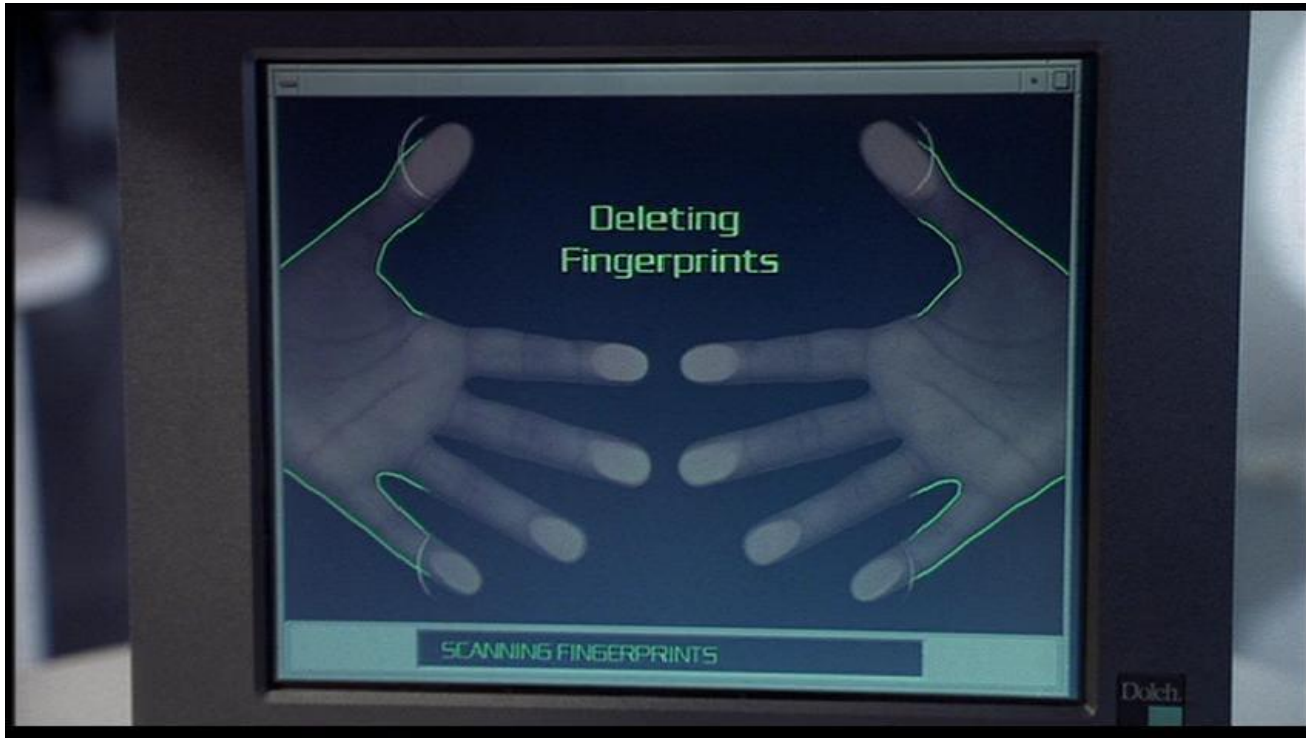


**Partial print at site of Madrid train bombing (2004)**



**AFIS incorrectly returned Brandon Mayfield's prints**

# Presentation Attacks



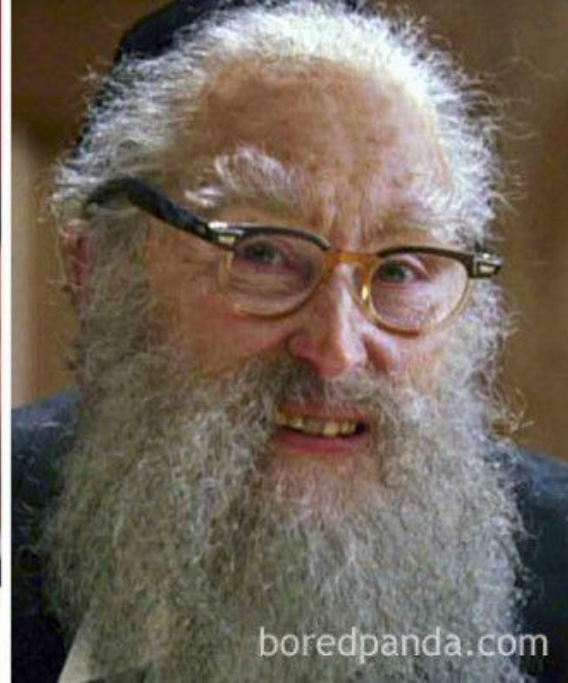
Will Smith, Men in Black (1997)



Tom Cruise, Minority Report (2002)

**Posing as another individual or hiding your identity**

# Presentation Attacks



**Meryl Streep - Rabbi (Angels In America, 2003)**



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

# 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?**

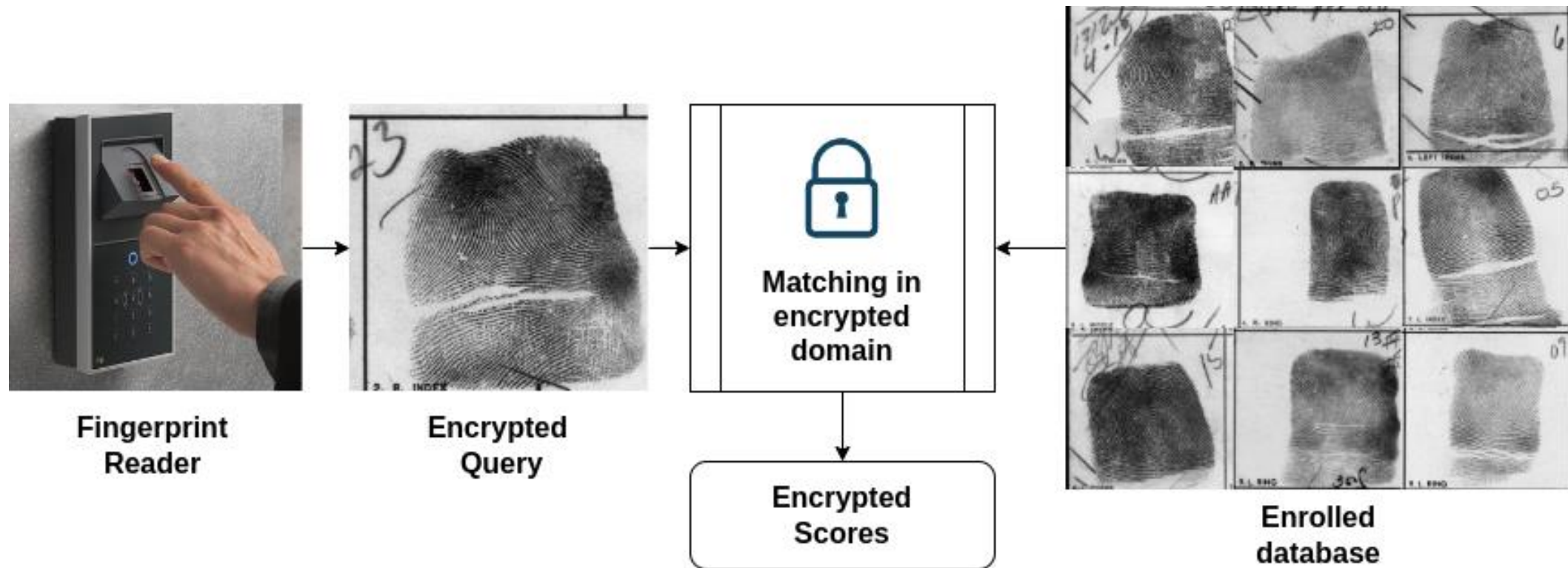
# Synthetic Biometric Images



# Synthetic Biometric Images



# Privacy Preserving Authentication



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



# Take Home Message

- Biometrics is intertwined with applications; researchers must consider application requirements (accuracy, latency, template size, user-sensor interaction, failure to acquire/enroll, presentation attack,..)
- Face, fingerprint and iris will continue to dominate biometrics market; other modalities, e.g. palmprints are finding success in specific use cases
- Need to continually improve search accuracy (FPIR, FNIR) and time, especially for unconstrained acquisitions and large-scale search
- Accuracy on lab collected datasets is not representative of actual performance on deployed systems due to “domain shift” and “user behavior”
- Deep networks are not panacea; embedding domain knowledge is important
- A system with 100% accuracy may not be enough to find a use case

# Inter-disciplinary Nature of Biometrics

