Introduction to Biometric Recognition

Anil K. Jain

Michigan State University

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

The IAPR/IEEE Winter School on Biometrics, Shenzhen, January 21, 2024

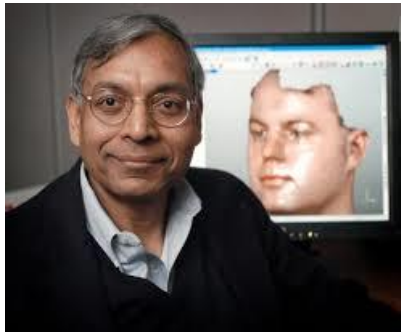
First Visit to China (1984)

Pairwise similarity

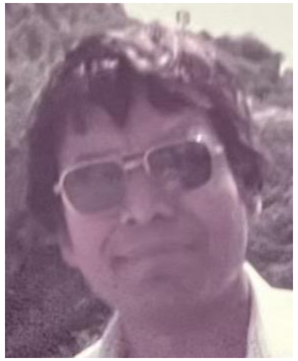
0.83

0.89

0.72



0.81

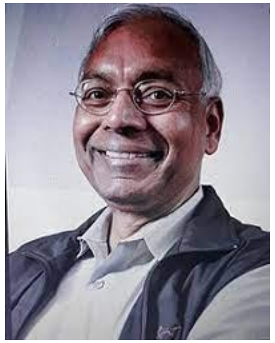


Probe

0.58

0.72

0.82



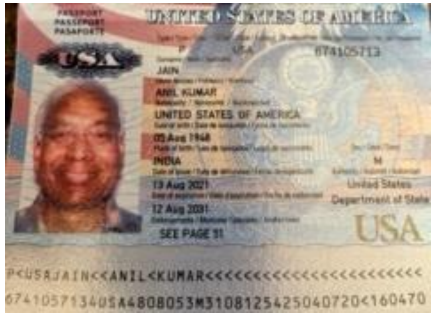
0.71

Threshold=0.54
@ FAR=1e-6

0.74

0.66

0.63



PASSPORT
PASSEPORT
PASAPORTE

UNITED STATES OF AMERICA

USA

P USA 674105713

JAIN

ANIL KUMAR

UNITED STATES OF AMERICA

05 Aug 1948

INDIA M

13 Aug 2021 United States Department of State

12 Aug 2031

SEE PAGE 51

USA

```
P<USAJAIN<<ANIL<KUMAR<<<<<<<<<<<<<<<<<<<<<<<<
6741057134USA4808053M3108125425040720<160470
```

0.49

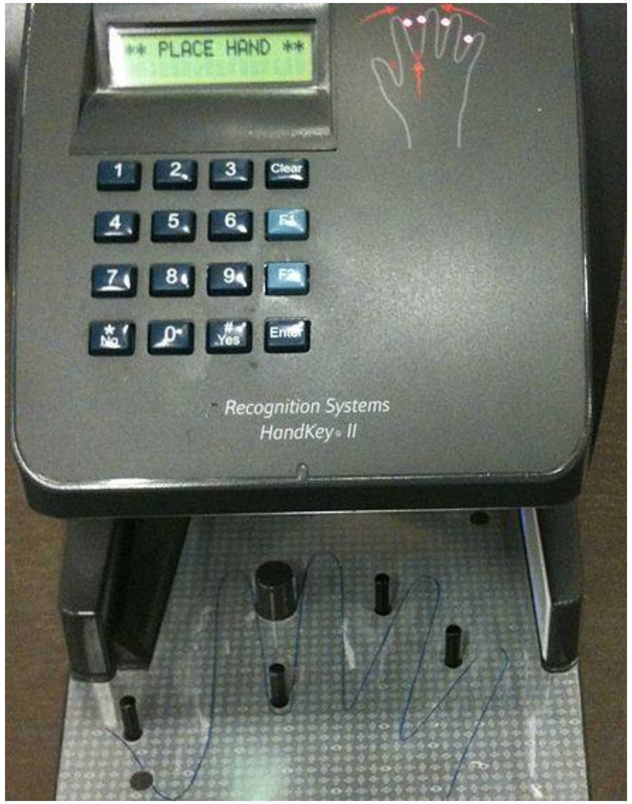
0.17

- Representation
- Similarity measure

https://roc.ai/

Gallery images

Biometric Recognition in 1980s

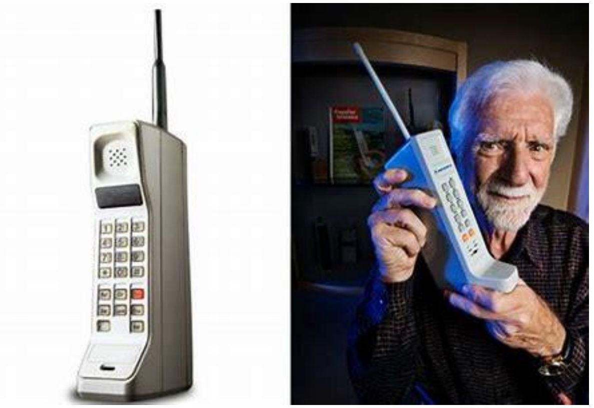


Hand geometry recognition

Manual fingerprint comparison

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

Biometrics Now!



The first mobile phone (1973)

1.4B Mobiles shipped in 2022; 1B with biometrics

Joseph Van Os / Getty Images

The Pantech GI100 (2004)

Fingerprints
Success
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

Touch ID, iPhone 5S (2013)

Apple Pay, iPhone 6 (2014)

Face ID, iPhone X (2017)

Vivo In-Display Scanner (2018)

- We check our phones, an average, 58 times each day; Touch ID offered convenience & security
- **Requirements: high accuracy, low cost, low latency, high usability, hackproof**

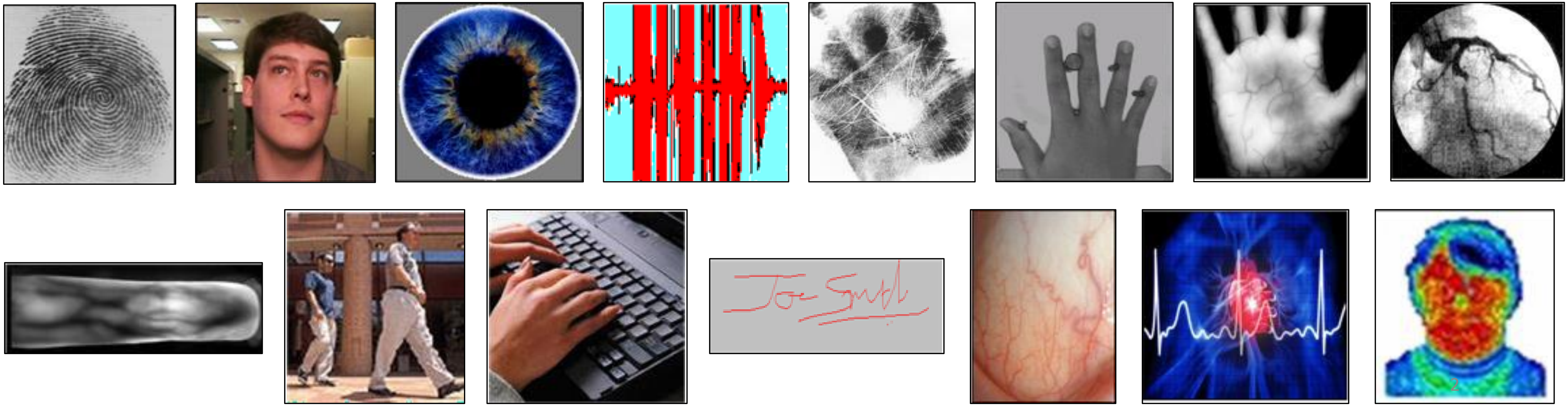
https://www.theverge.com/23868464/apple-iphone-touch-id-fingerprint-security-ten-year-anniversary

Biometric Recognition

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

Stigler, “The Problematic Unity of Biometries”, BIOMETRIC5, S6 , Sept. 2000; Pollack, “Technology: Recognizing the Real You”, NYT, Sep. 24, 1981

Biometric Traits



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

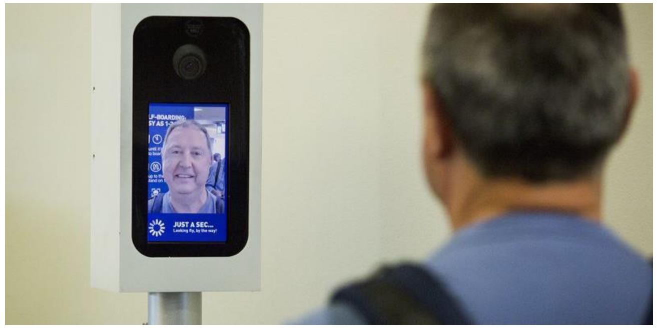
Which Biometric Trait?

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

Choice of biometric trait depends on application requirements

Most Popular Biometric Traits

Incheon, South Korea: Smart Entry

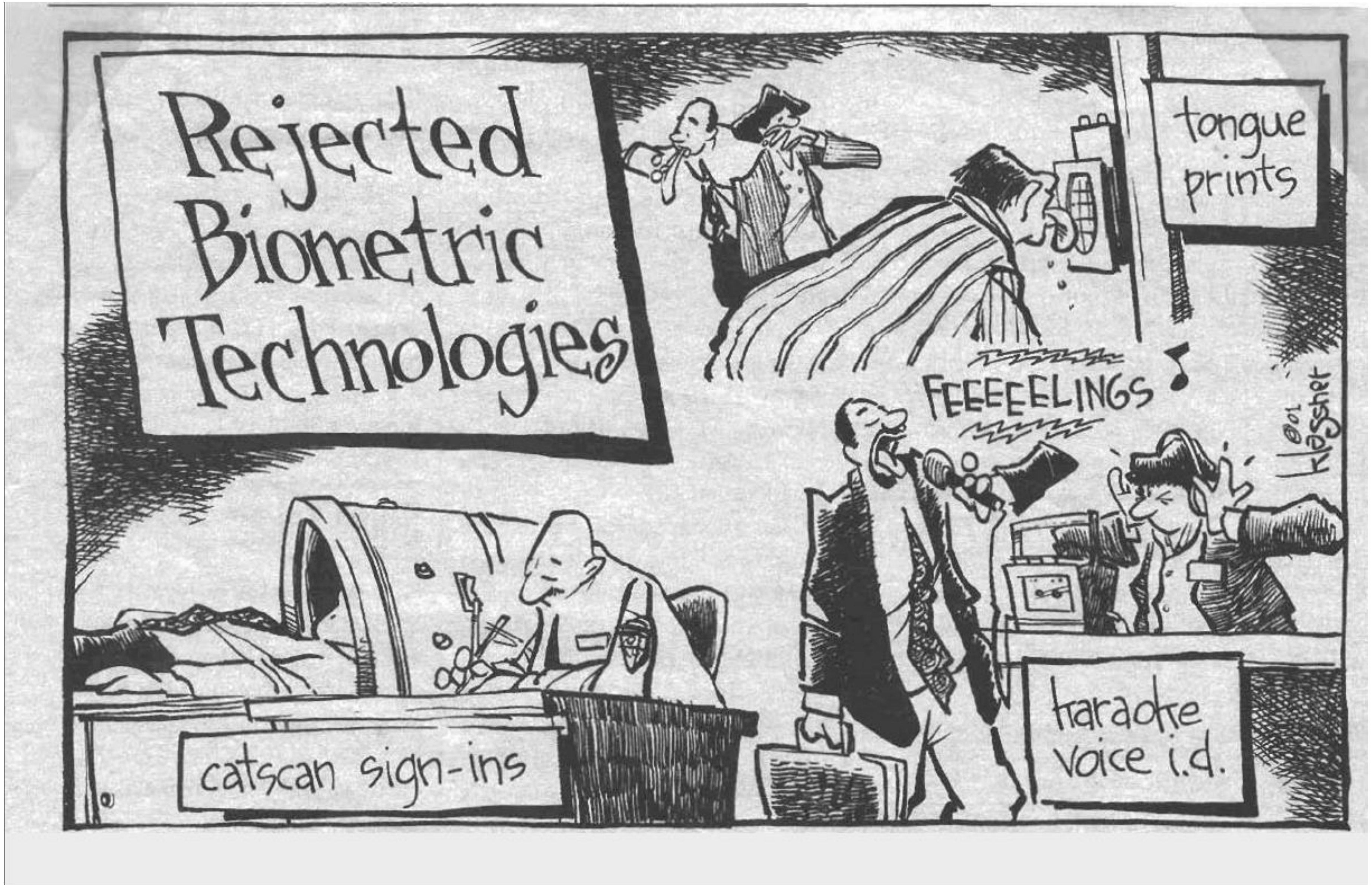

Australia: SmartGate

Amsterdam: Privium border passage

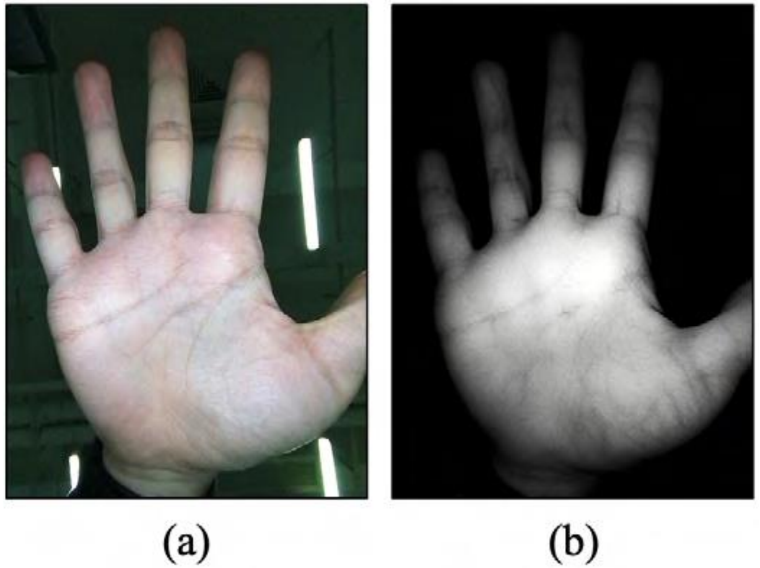
1. *Satisfy individuality* and *permanence* properties
2. Demostrate high accuracy in NIST evaluations
3. Fast search (1:N comparison) of large legacy databases (in millions)

http://www.homestaykorea.com/?document_srl=73667&mid=bbs_koreainfo_news
https://tottnews.com/tag/smart-gates/
https://www.idemia.com/news/multi-biometrics-future-border-control-2016-04-21

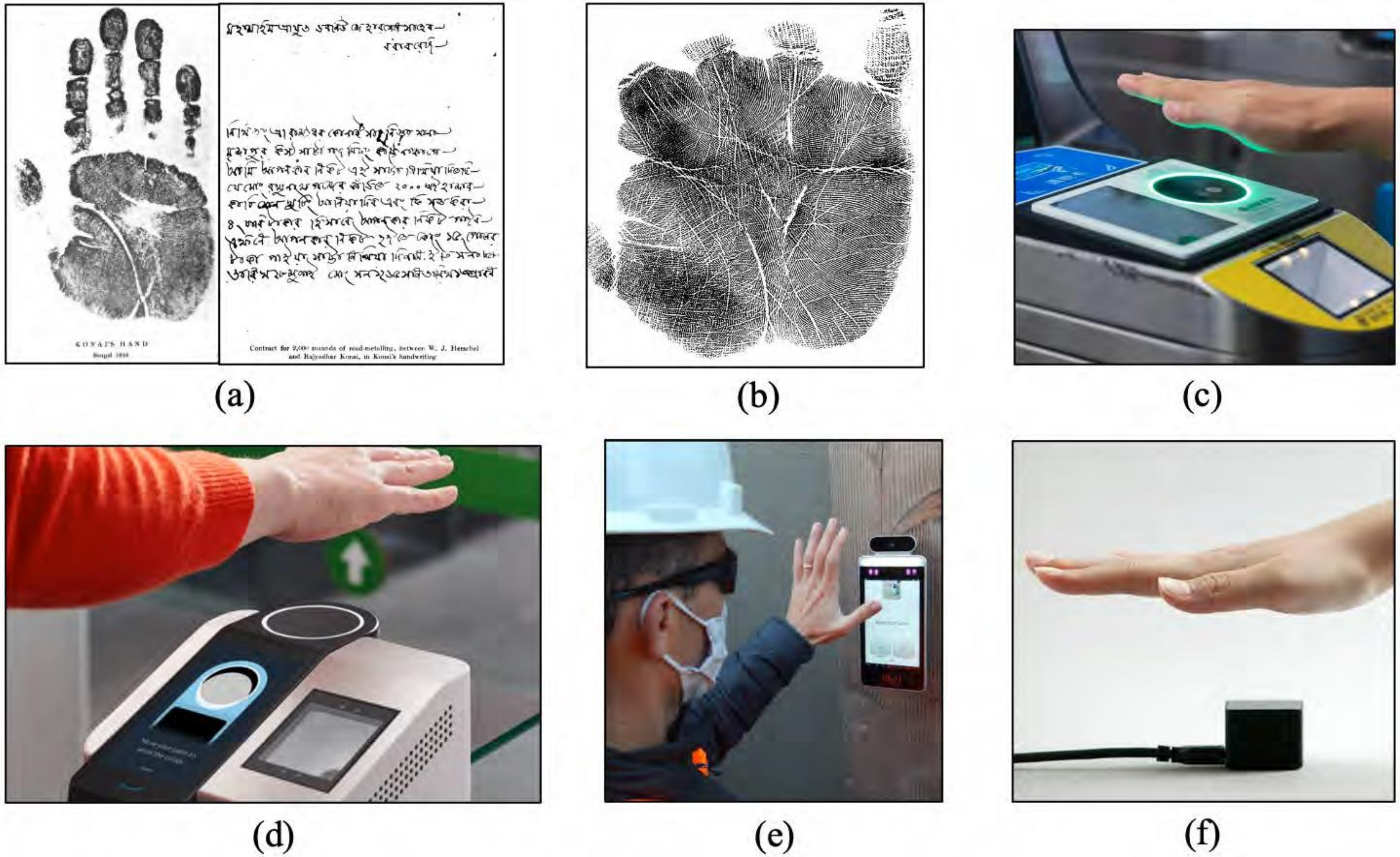
Rejected Traits



Growing Interest in Palm Biometric



(a) Palmprint, (b) Palmvein


KONAI'S HAND
Bengal 1858
Contract for 2,000 maunds of road-metalling, between W. J. Herschel and Rajyadhar Konai, in Konai's handwriting
(a)
(b)
(c)
(d)
(e)
(f)

(a) Earliest use of palmprint by Herschel ~1855 in lieu of signature on legal contracts, (b) latent palmprint from crime scene, (c) contactless palmprint Recognition for train and 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.

Drivers of Biometric Recognition

- Lack of Trust: ID documents, password/PIN can no longer be trusted
- Higher security (border crossing), higher throughput (reduce transaction time), reduce fraud (who is doing transaction), improve user experience

How do we know who is entering card & PIN?

Fingerprint enabled ATM

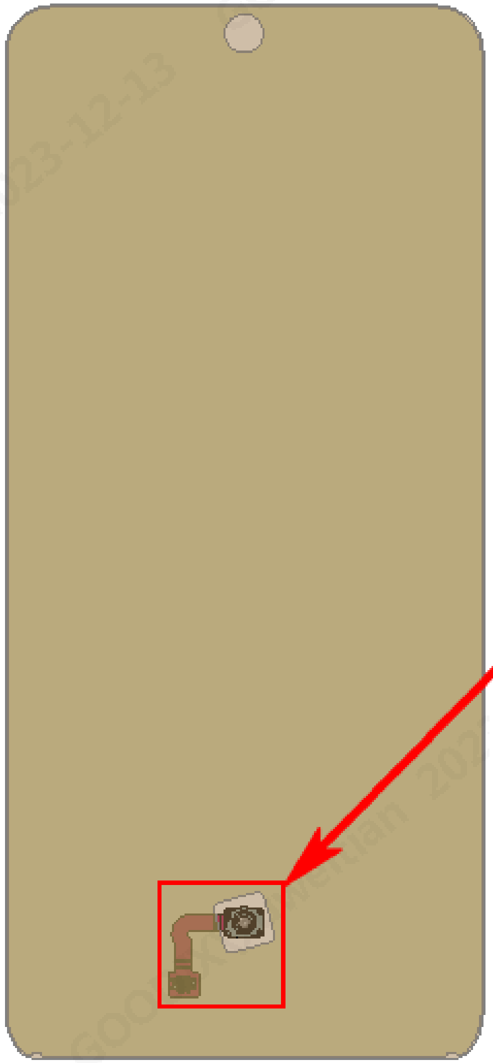
Drivers of Biometric Recognition

Requirements: Accuracy, throughput, cost, integration, usability, security, privacy

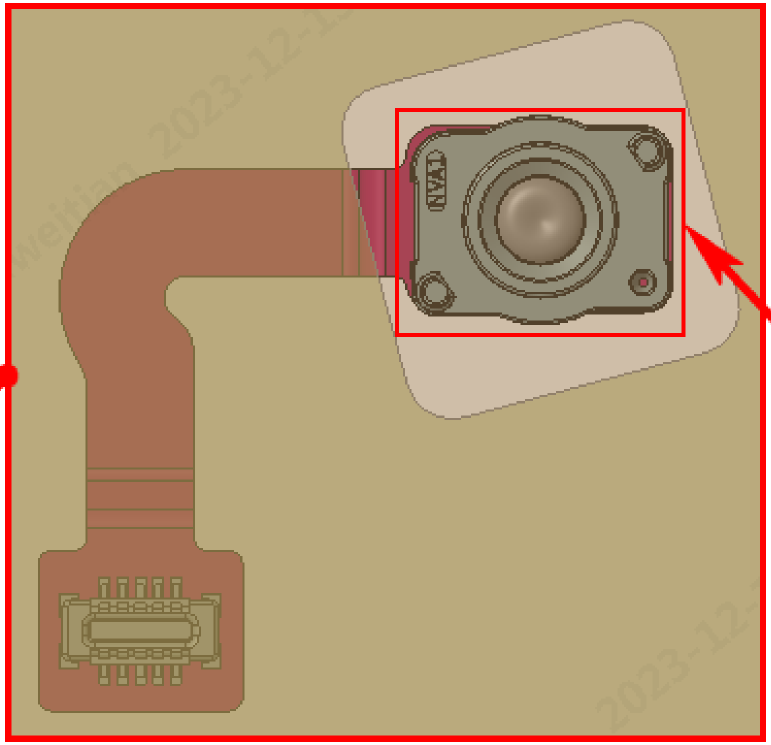
Enablers of Biometric Recognition

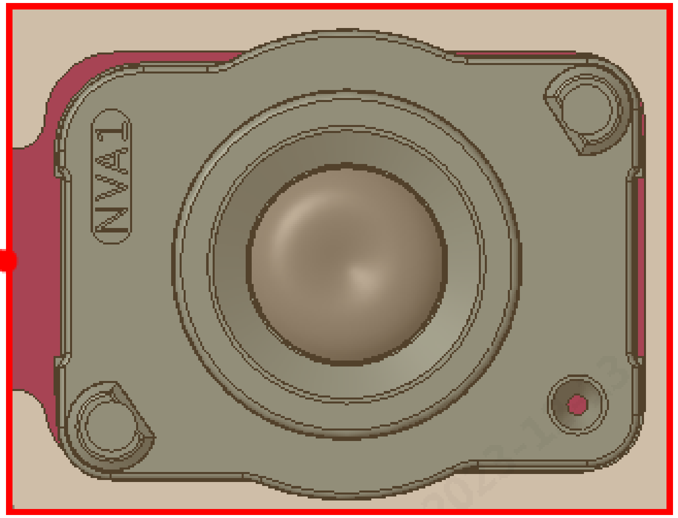
- **Advances in sensing, processing and memory technologies**
- **HCI, ergonomics, low cost (FP module costs US1$)…**

7 cm x 14 cm



FP module pasted on screen frame





Length: 5.8 mm
Width: 4.3 mm
Depth: 4.2 mm

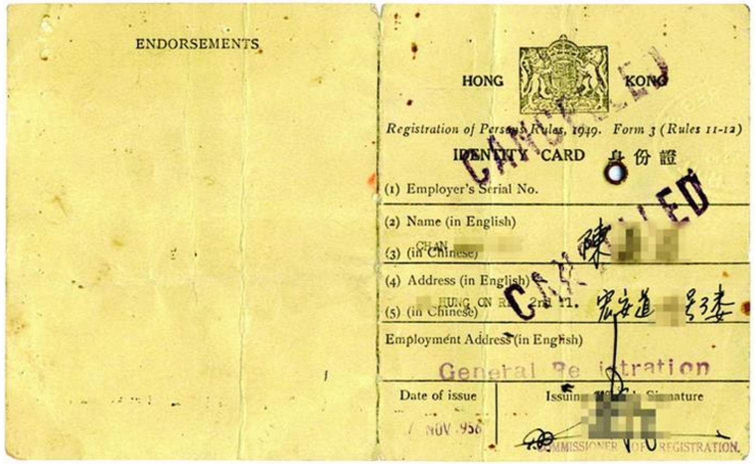
FP module (containing Sensor and FPC, courtesy Goodix))

Enablers of Biometric Recognition

1
2
6
BIOMETRICS
BY FINGERPRINTS™
1987 2654 5451 09
Expiry date:
01/23
ELIN SVENSSON
5
4
3
XXXX

Match on Card: Sensor, feature extractor & matcher all reside on the card

HK ID Cards: Paper to Smart Card



ENDORSEMENTS

HONG KONG

Registration of Persons Rules, 1949. Form 3 (Rules 11-12)

IDENTITY CARD 身份證

CANCELLED

(1) Employer's Serial No.

(2) Name (in English) CHAN [redacted]

(3) (in Chinese) 陳 [redacted]

(4) Address (in English) [redacted] HUNG ON R 2nd Fl.

(5) (in Chinese) 宏安道 [redacted] 号3楼

Employment Address (in English)

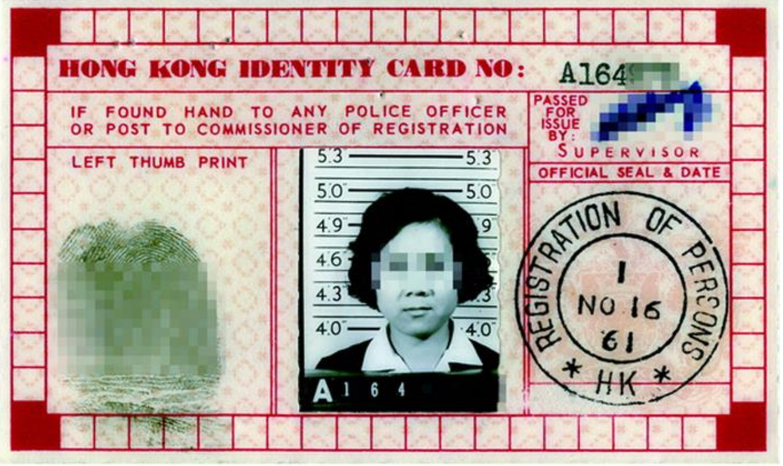
General Re istration

Date of issue / NOV 956

Issuing [redacted] Signature

COMMISSIONER OF REGISTRATION.

Paper Identity Card (1949)



HONG KONG IDENTITY CARD NO: A164[redacted]

IF FOUND HAND TO ANY POLICE OFFICER OR POST TO COMMISSIONER OF REGISTRATION

PASSED FOR ISSUE BY: [redacted]

SUPERVISOR

OFFICIAL SEAL & DATE

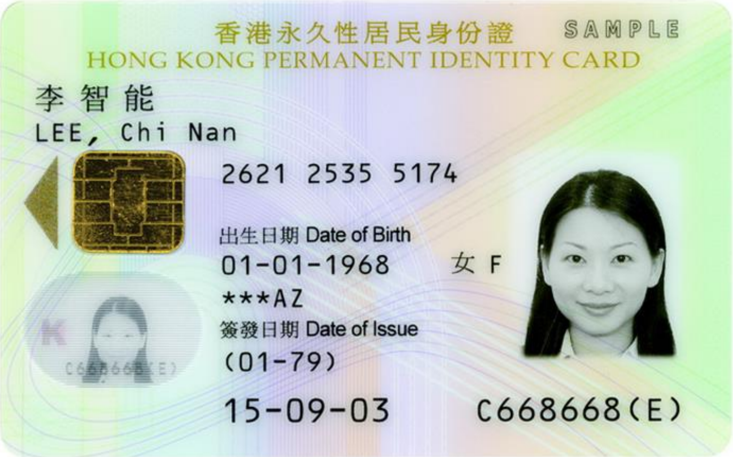
LEFT THUMB PRINT

[redacted]

[redacted]

REGISTRATION OF PERSONS 1 NO 16 61 * HK *

Laminated Identity Card (1960)



香港永久性居民身份證 SAMPLE

HONG KONG PERMANENT IDENTITY CARD

李 智 能

LEE, Chi Nan

2621 2535 5174

出生日期 Date of Birth

01-01-1968 女 F

***AZ

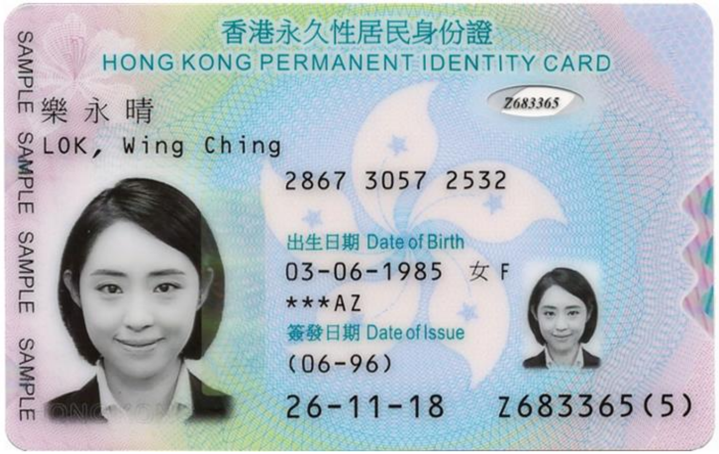
簽發日期 Date of Issue

(01-79)

15-09-03 C668668(E)

C668668(E)

Smart Identity Card (2003)



SAMPLE SAMPLE SAMPLE SAMPLE

香港永久性居民身份證

HONG KONG PERMANENT IDENTITY CARD

Z683365

樂 永 晴

LOK, Wing Ching

2867 3057 2532

出生日期 Date of Birth

03-06-1985 女 F

***AZ

簽發日期 Date of Issue

(06-96)

26-11-18 Z683365(5)

New Smart Identity Card (2018)

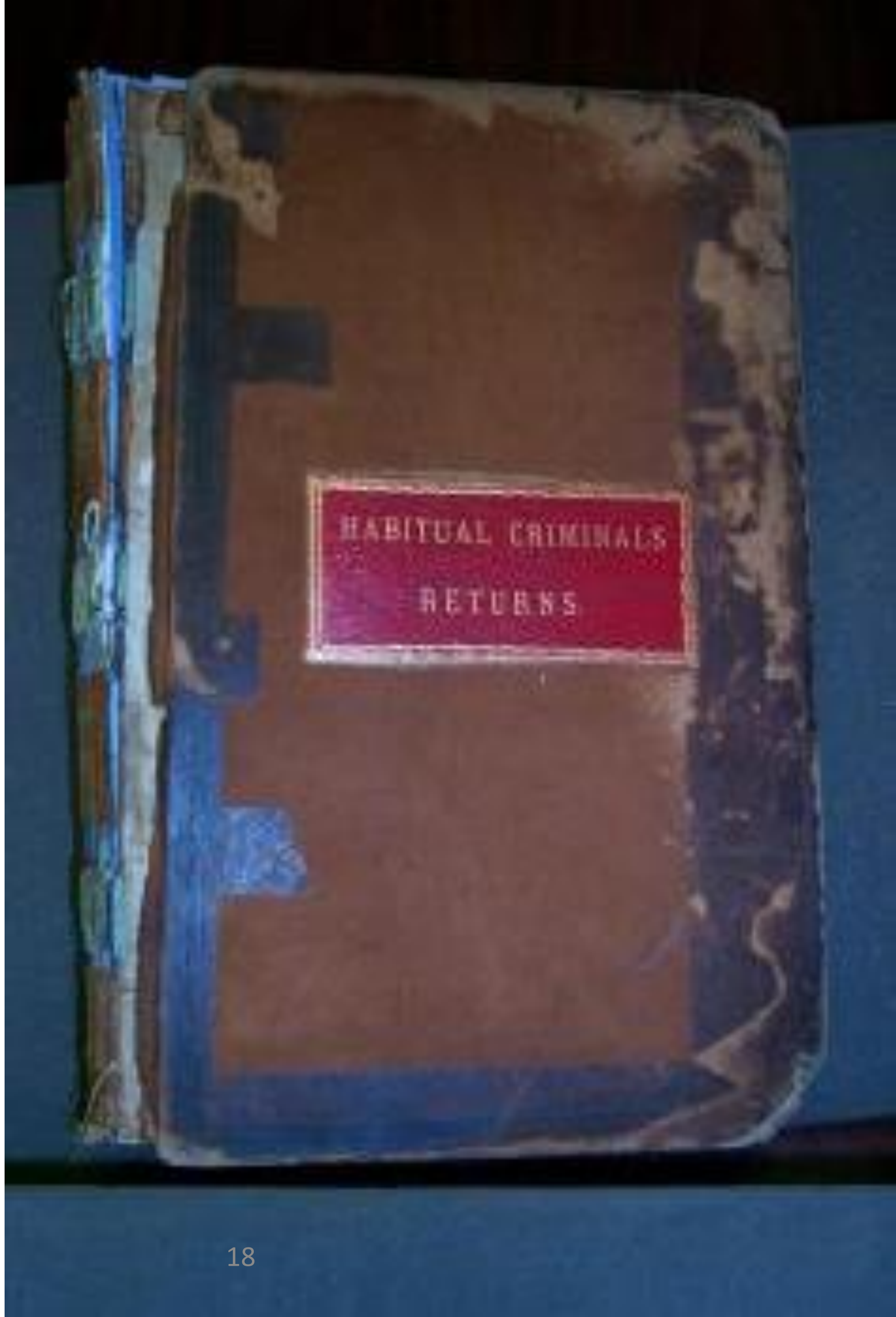
Better durability, security features for protection of personal data.

Biometric Recognition is Not New

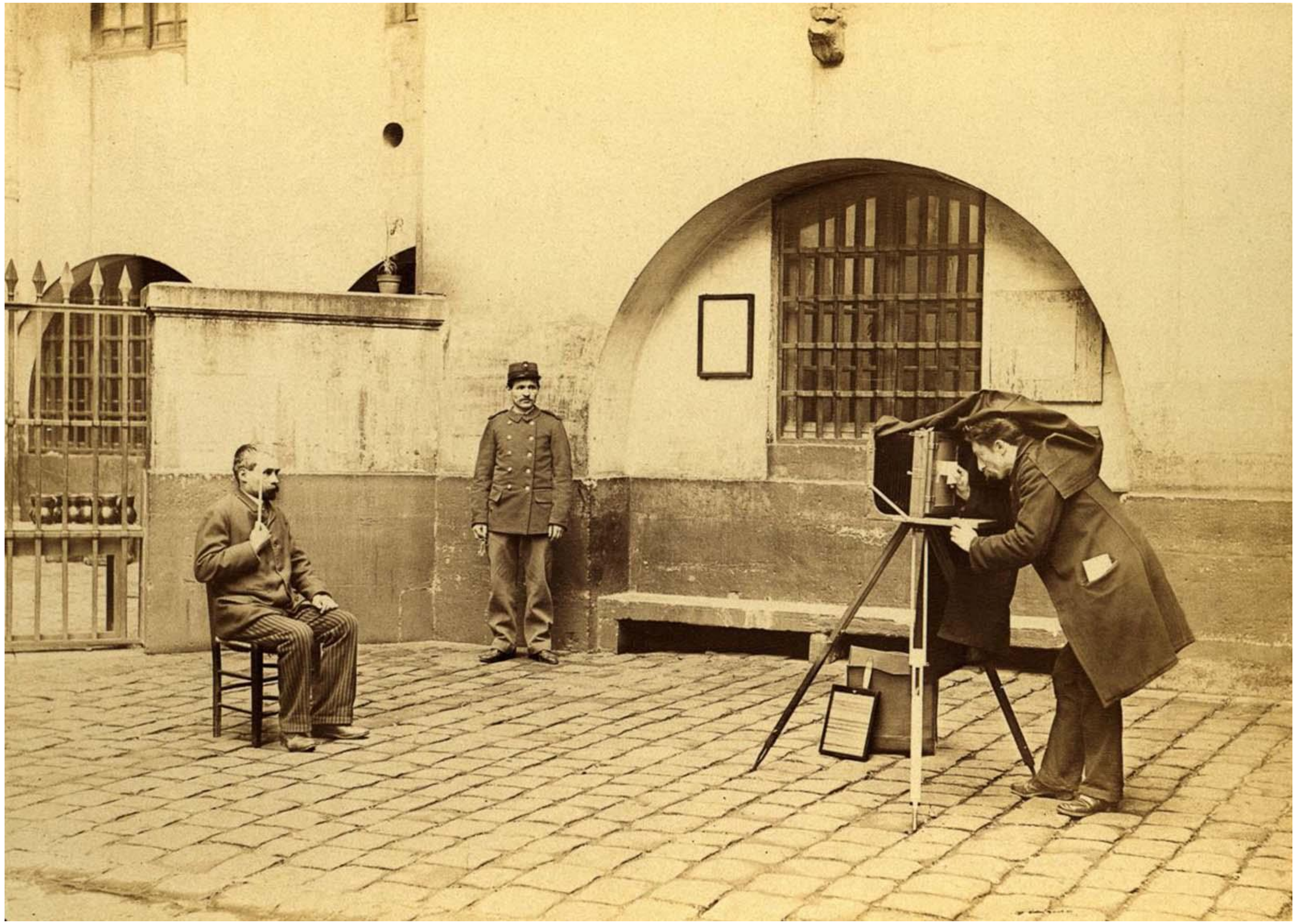
Habitual Criminal Act (1869)

"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"

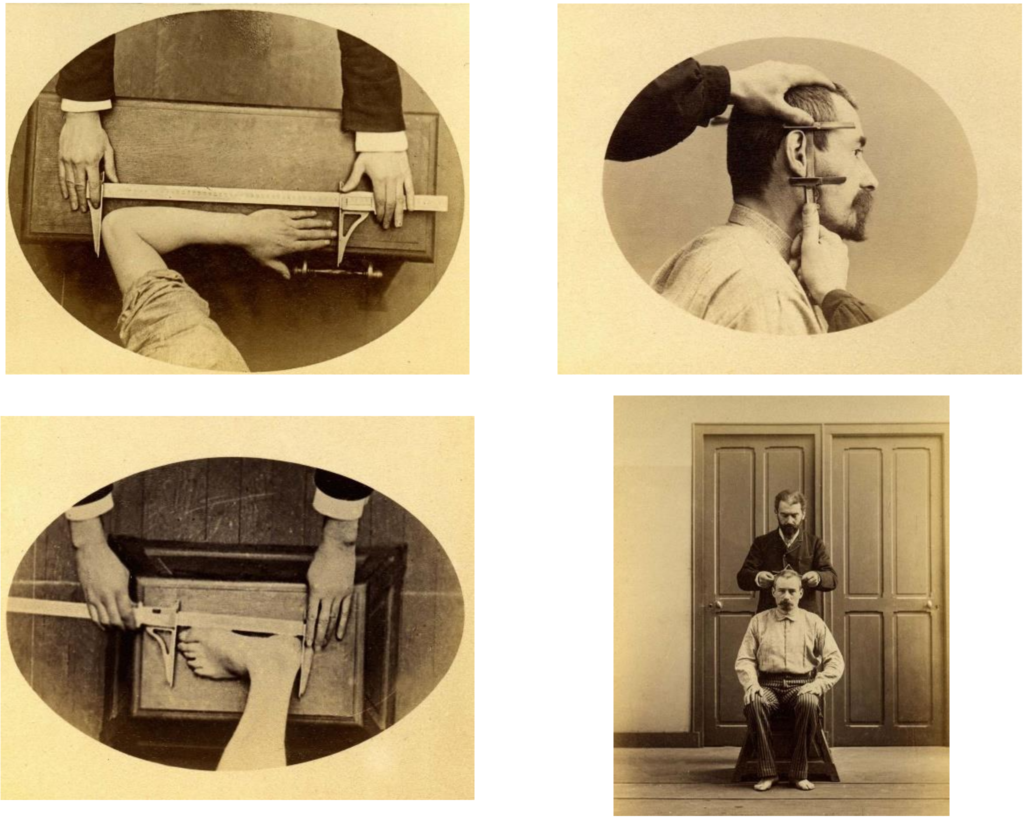
https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1968&context=ohlj



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”

https://rarehistoricalphotos.com/bertillon-system-rare-photographs/

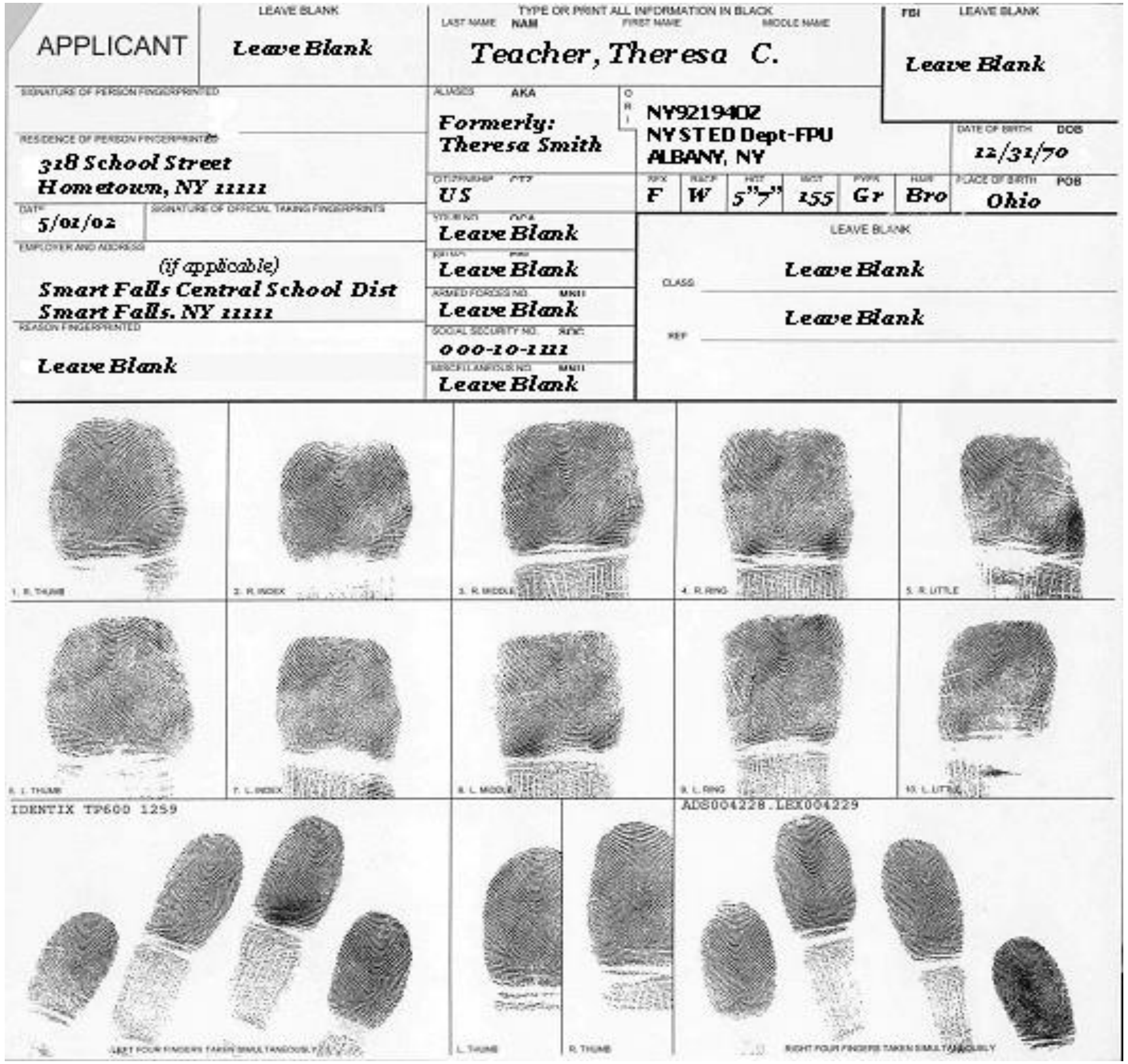
Fingerprints (1880)

“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)

FBI (1924)



APPLICANT

LEAVE BLANK: *Leave Blank*

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM FIRST NAME MIDDLE NAME: Teacher, Theresa C.

FBI LEAVE BLANK: *Leave Blank*

SIGNATURE OF PERSON FINGERPRINTED

ALIASES AKA: *Formerly: Theresa Smith*

ORI: NY9219402Z
NYSTED Dept-FPU
ALBANY, NY

DATE OF BIRTH DOB: *12/31/70*

RESIDENCE OF PERSON FINGERPRINTED:
318 School Street
Hometown, NY 11111

CITIZENSHIP CTZ: *US*

SEX	RACE	HGT	WGT	EYES	HAIR	PLACE OF BIRTH POB
F	*W*	*5"7"*	*155*	*Gr*	*Bro*	*Ohio*

DATE: *5/01/02*

SIGNATURE OF OFFICIAL TAKING FINGERPRINTS

YOUR NO. OCA: *Leave Blank*

FBI NO. FBI: *Leave Blank*

LEAVE BLANK

CLASS: *Leave Blank*

REF: *Leave Blank*

EMPLOYER AND ADDRESS
(if applicable)
Smart Falls Central School Dist
Smart Falls. NY 11111

ARMED FORCES NO. MNU: *Leave Blank*

SOCIAL SECURITY NO. SOC: *000-10-1111*

REASON FINGERPRINTED: *Leave Blank*

MISCELLANEOUS NO. MNU: *Leave Blank*

1. R. THUMB
2. R. INDEX
3. R. MIDDLE
4. R. RING
5. R. LITTLE
6. L. THUMB
7. L. INDEX
8. L. MIDDLE
9. L. RING
10. L. LITTLE

IDENTIX TP600 1259

ADS004228.LBX004229

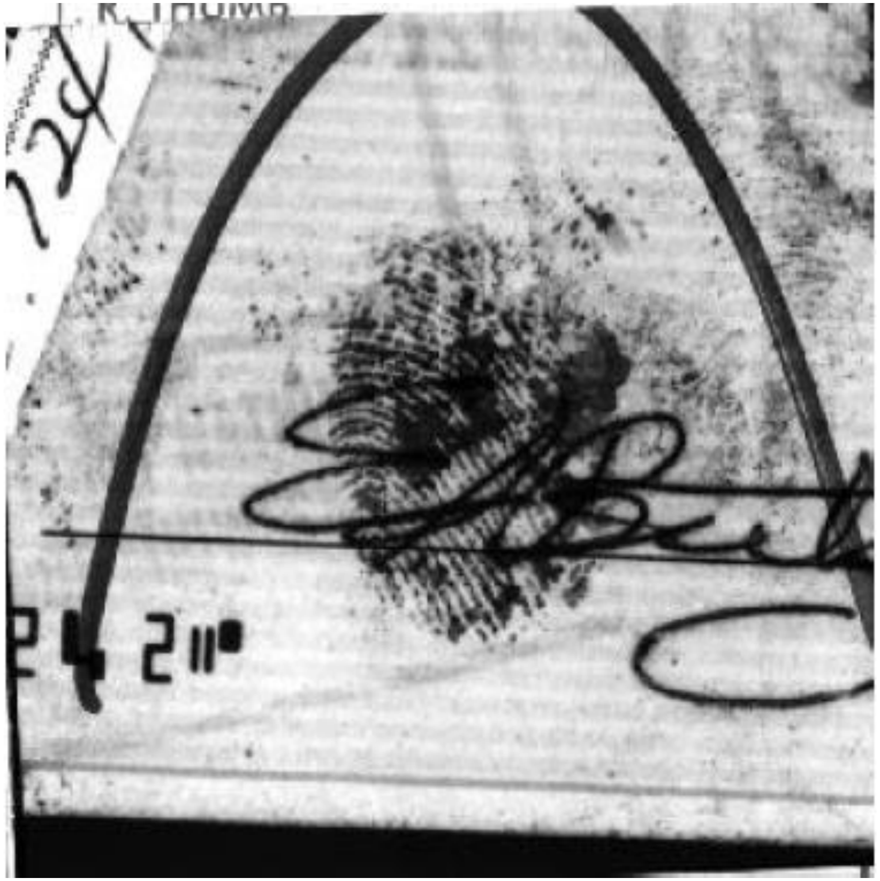
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY

L. THUMB

R. THUMB

RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

Tenprint card



Partial fingerprint from a crime scene

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.”*

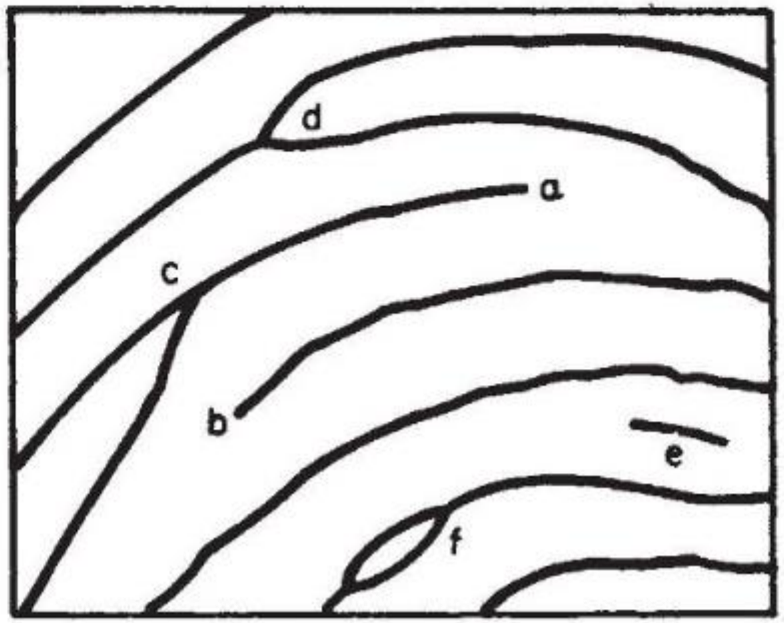
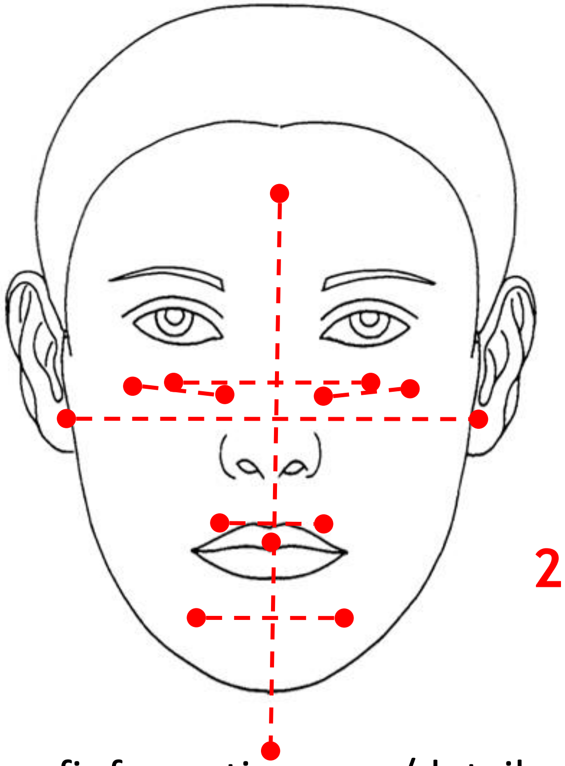


Fig. 1. Portion of fingerprint pattern (diagrammatic, enlarged) after Galton, showing minutiæ. *a* and *b* are ridge ends, *c* and *d* are ridge branchings or valley ends, *e* is an island, and *f* is an enclosure. The ridge end and valley end are the principal minutia types, accounting for almost all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

Face Recognition (Bledsoe,1966)

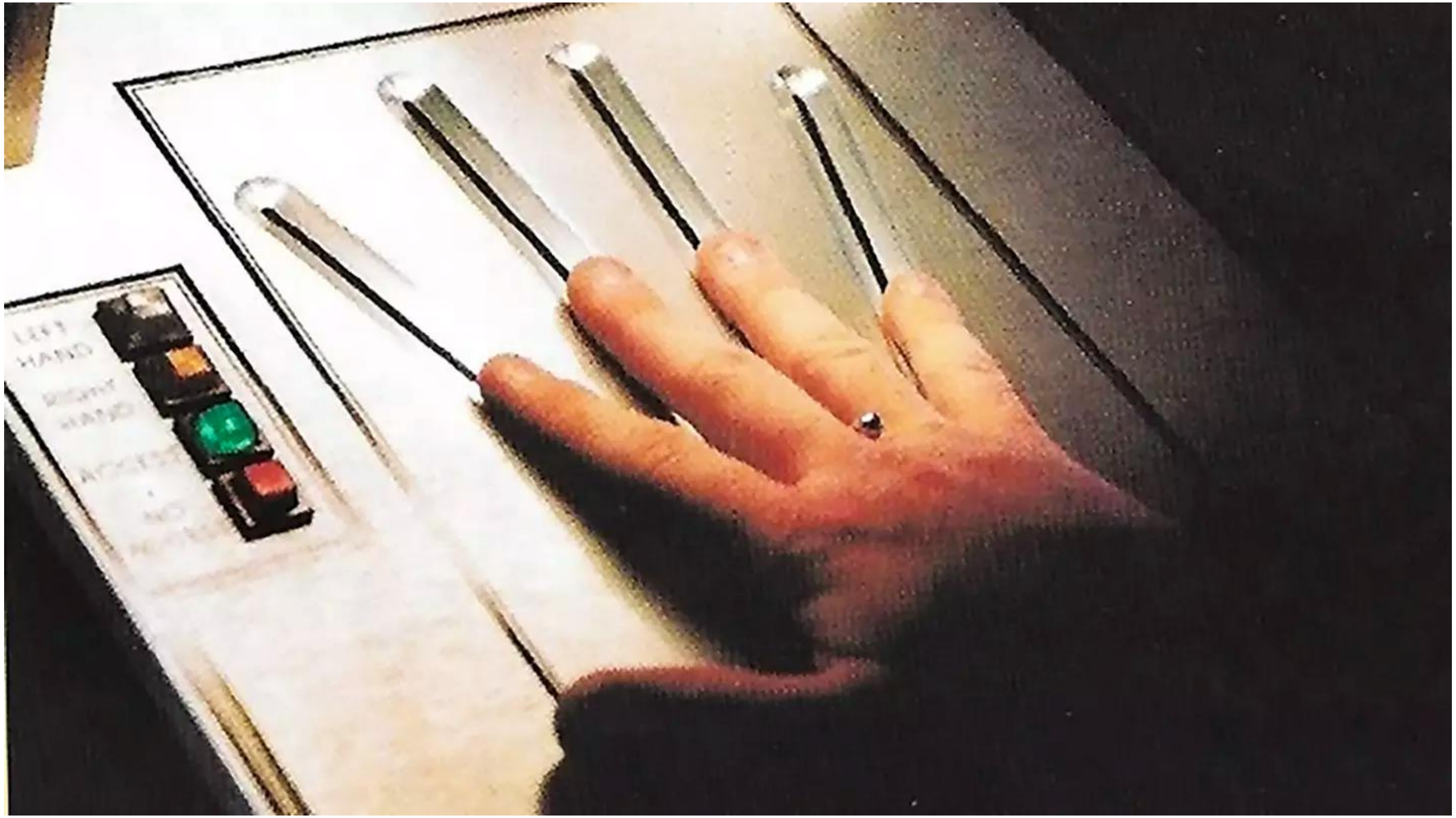
"This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc." *Bledsoe, Chan and Bisson (1966)*



20 inter-point distances for matching

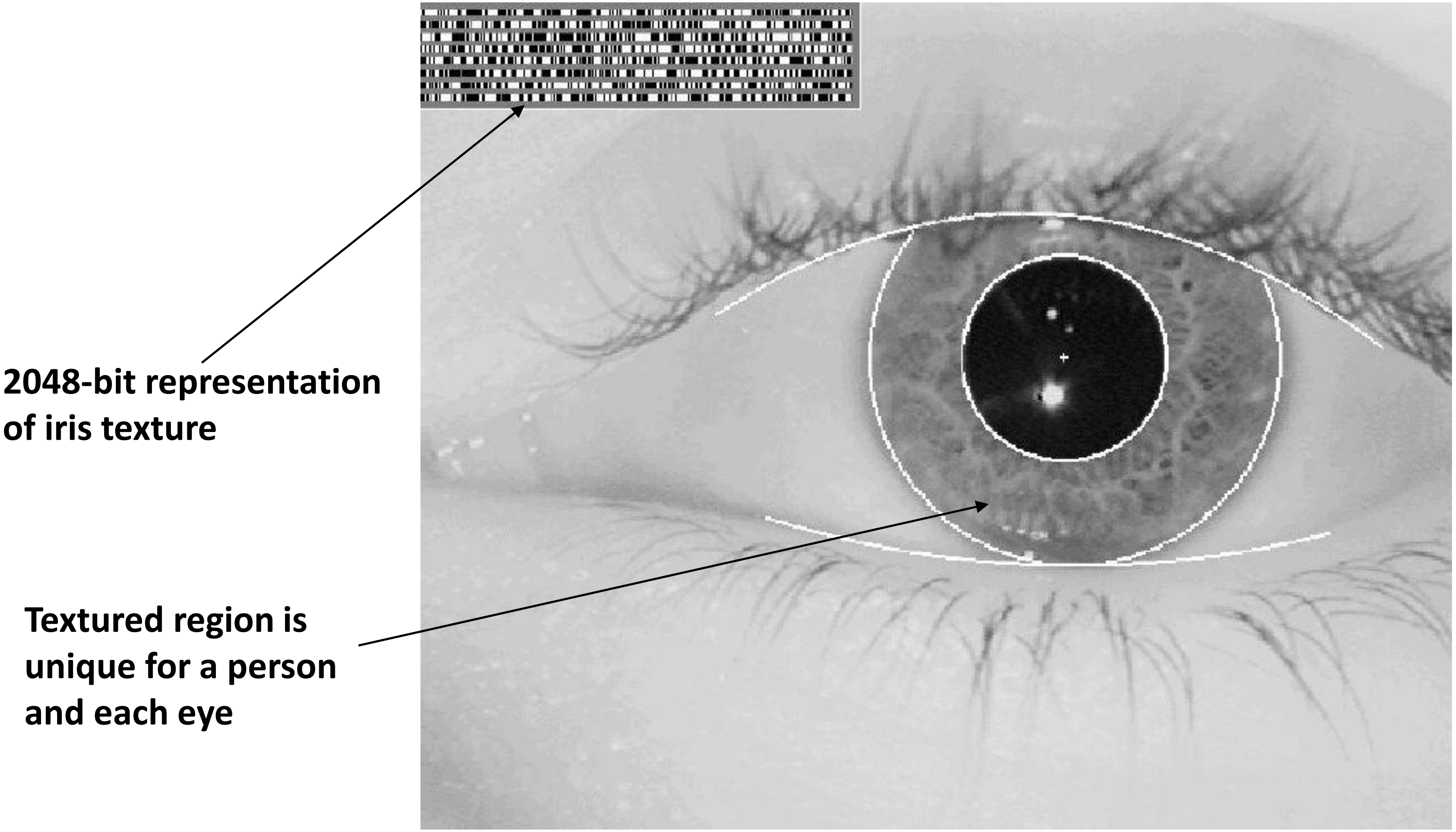
https://www.historyofinformation.com/detail.php?entryid=2495

Identimate (1972)



First commercial use of biometrics

Iris Recognition (Daugman,1993)



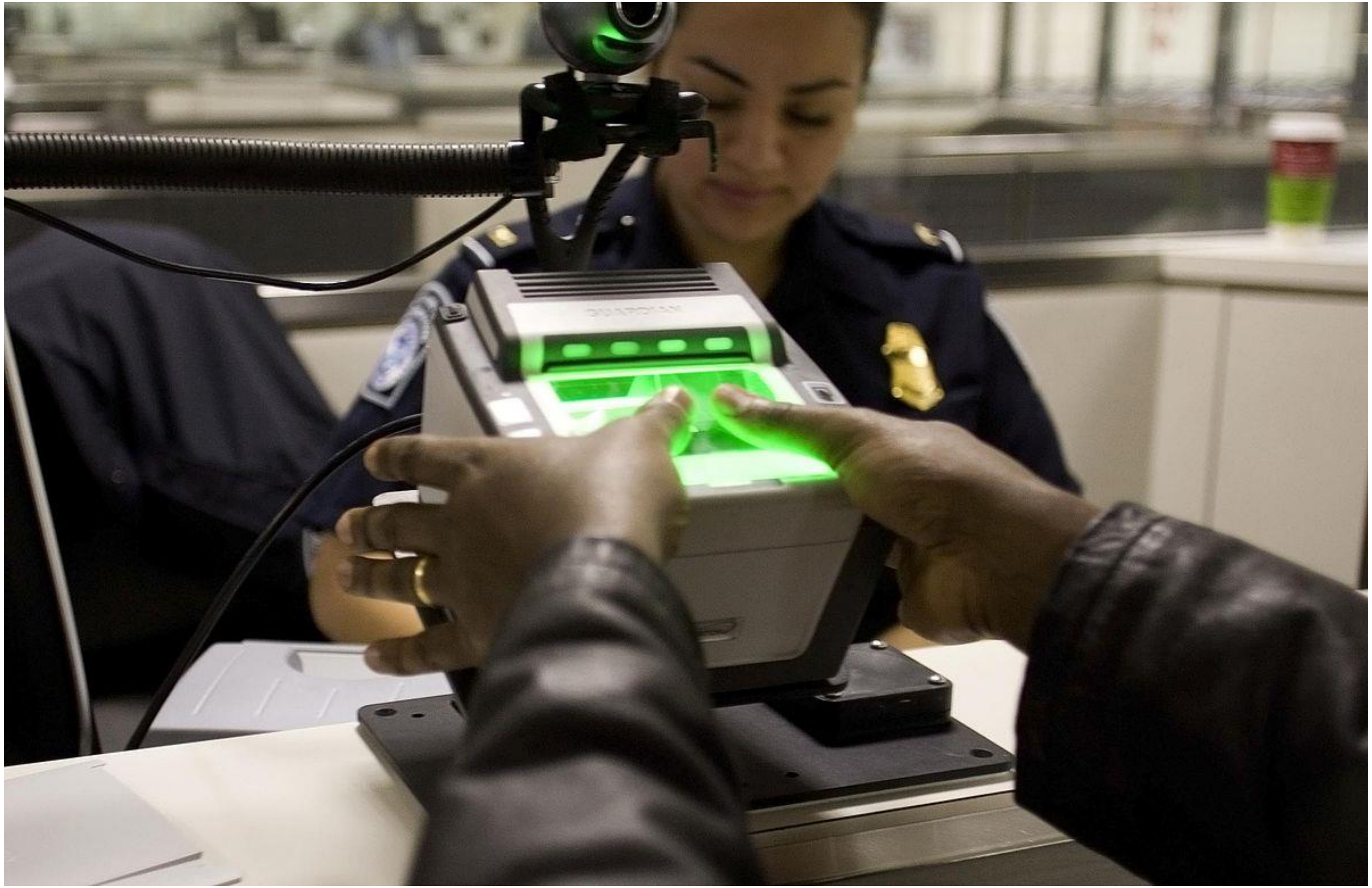
2048-bit representation of iris texture

Textured region is unique for a person and each eye

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

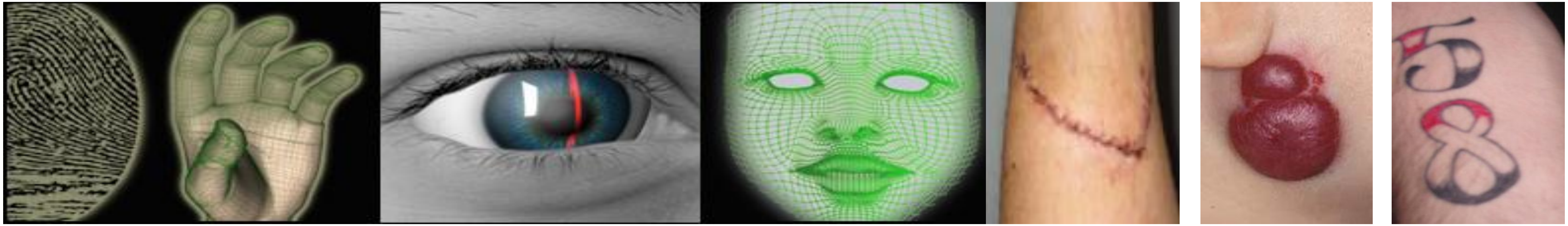
9/11 Terrorist Attacks (2001)

US-VISIT (2003)



Walt Disney Theme Park (2005)

FBI Next Generation Identification (2008)

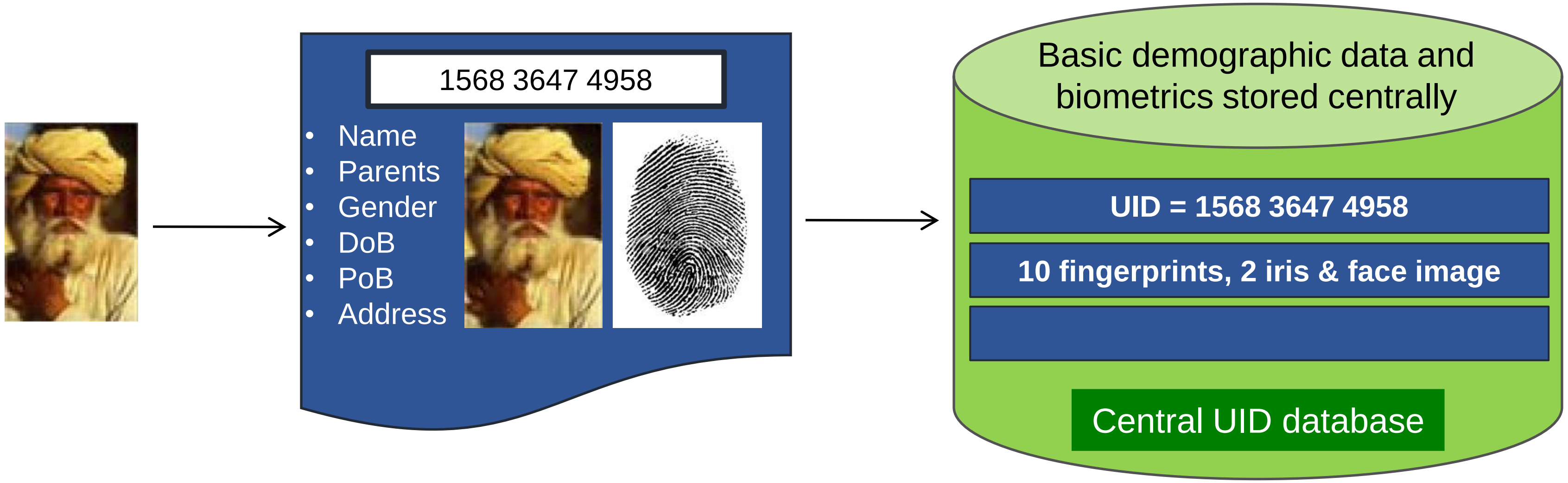


First AFIS in1980s; IAFIS launched in 1999; use of **soft biometrics** (SMT)

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."



1568 3647 4958
Name
Parents
Gender
DoB
PoB
Address
Basic demographic data and biometrics stored centrally
UID = 1568 3647 4958
10 fingerprints, 2 iris & face image
Central UID database

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

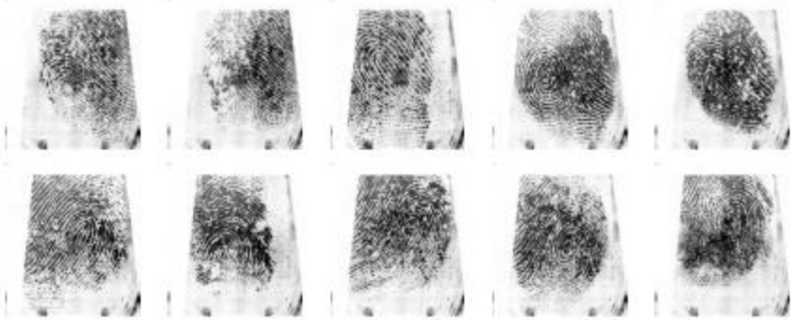
https://uidai.gov.in/

Social Good vs. Privacy

- *“Aadhaar gives dignity to the marginalized. Dignity to the marginalized outweighs privacy”* - Justice Sikri, Indian Supreme Court (Sept 2018)
- Enrolled biometric data never leaves Aadhaar server and is never shared with any entity

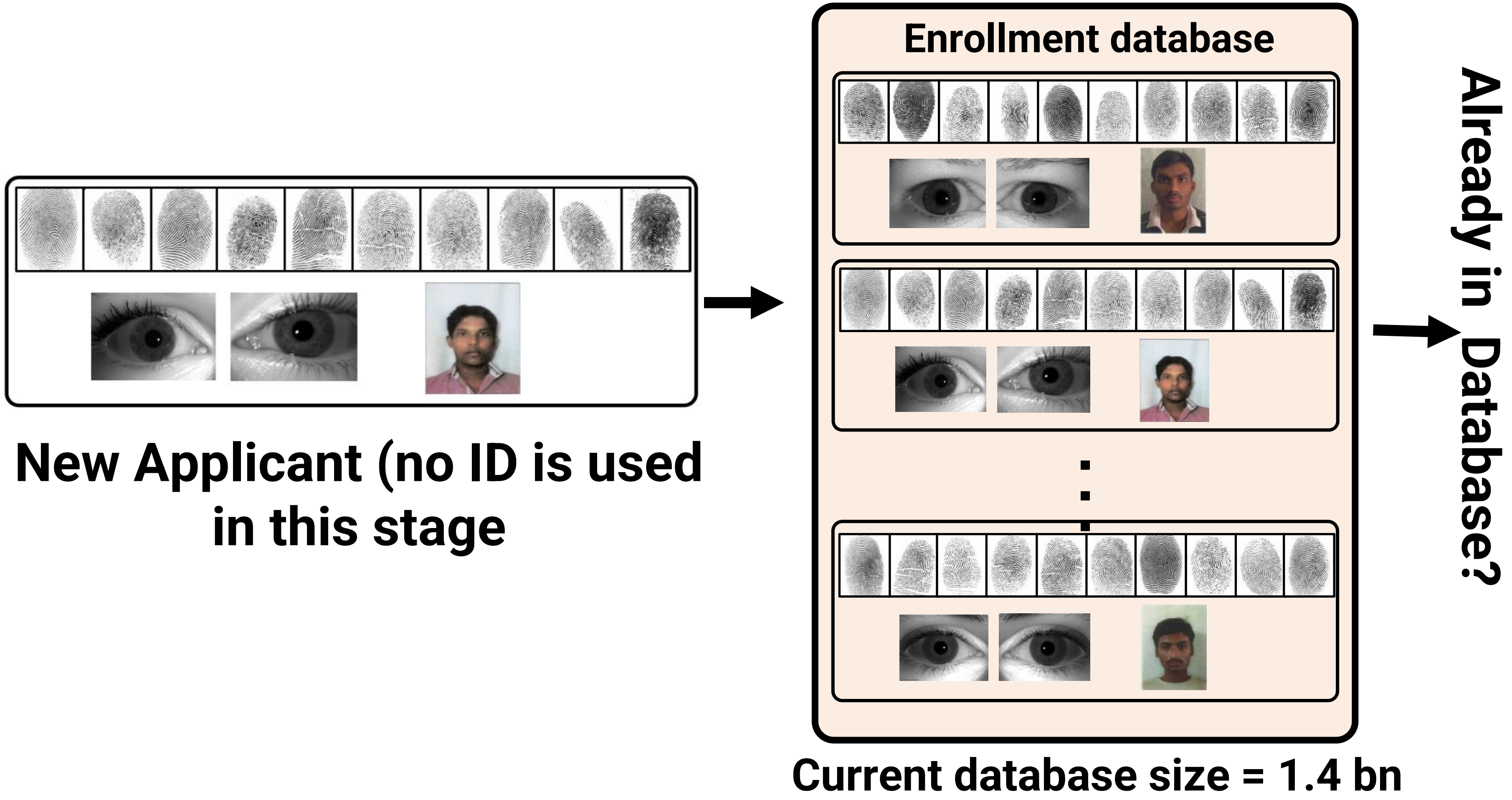
How Does Aadhaar Work?

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)

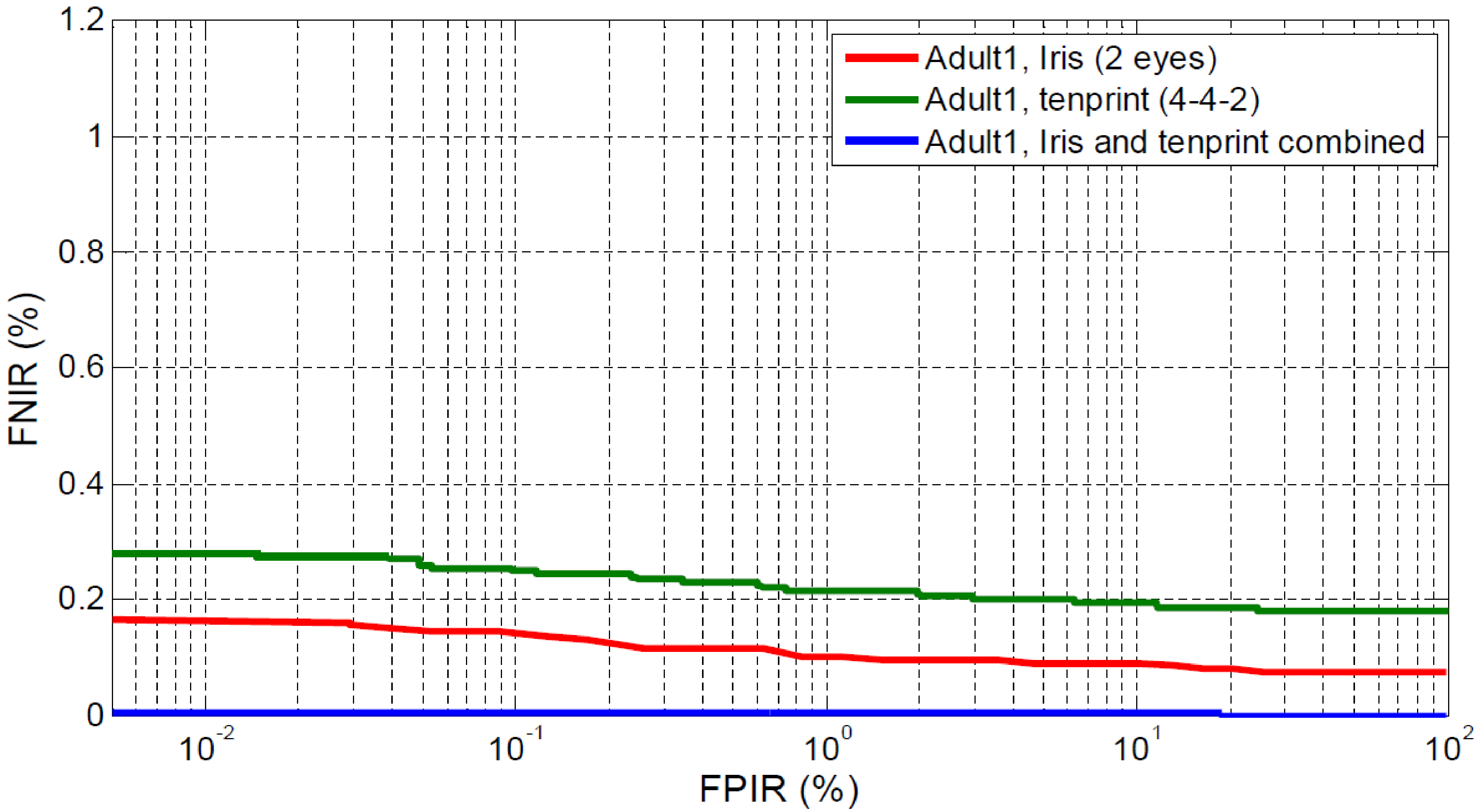


New Applicant (no ID is used in this stage

Current database size = 1.4 bn

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

~70 million (2-factor) authentications/day; 12-digit Aadhaar + fingerprint

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

Biometric Matching Algorithm

Compute Pairwise Similarity

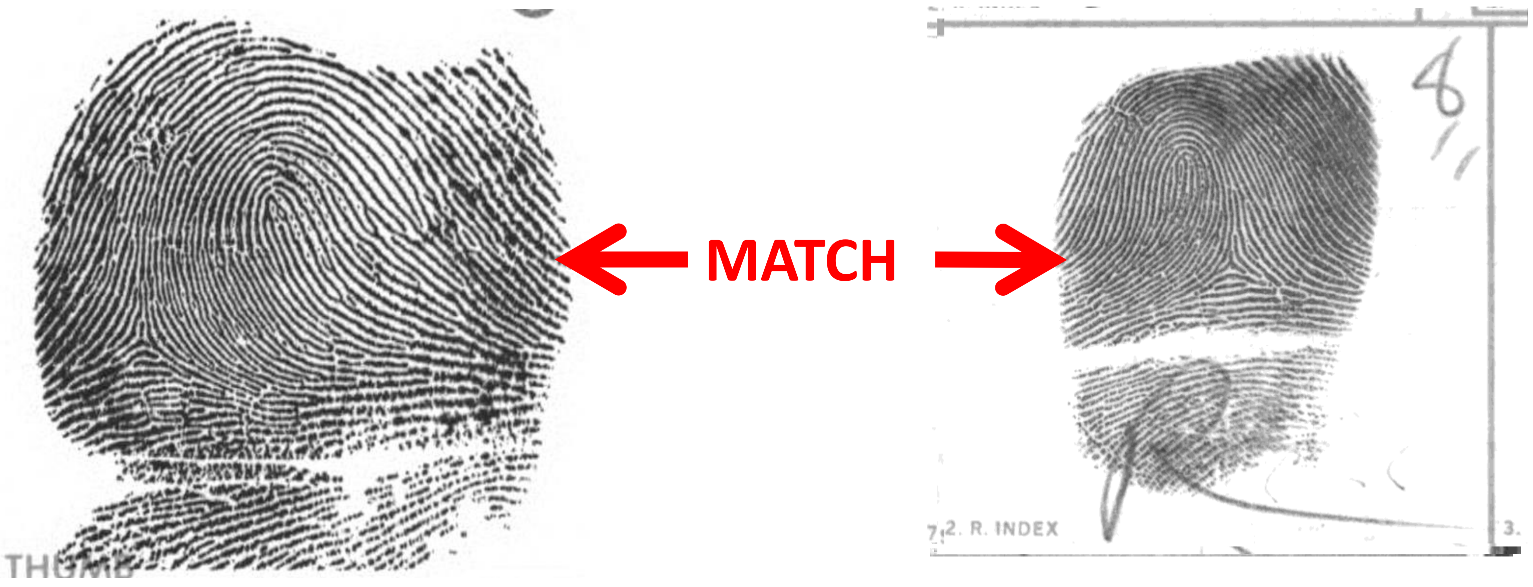
Person claims he is John

John’s enrolled fingerprint

Representation (set of features) and similarity measure

Fingerprint Identification

Query *Database*

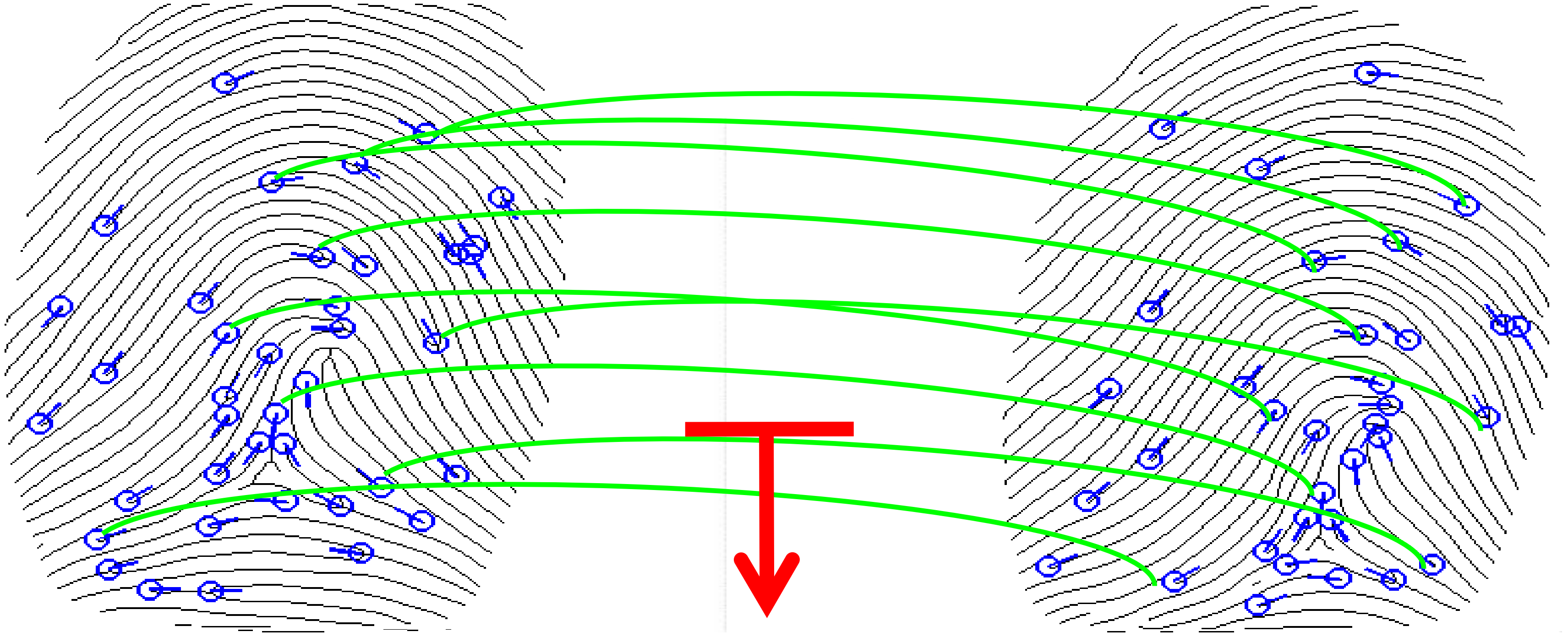


MATCH

No claim of identity made

- Who Does this fingerprint belong to?
- Query may or may not be present in the database (gallery)

Fingerprint Authentication (1:1 comparison)



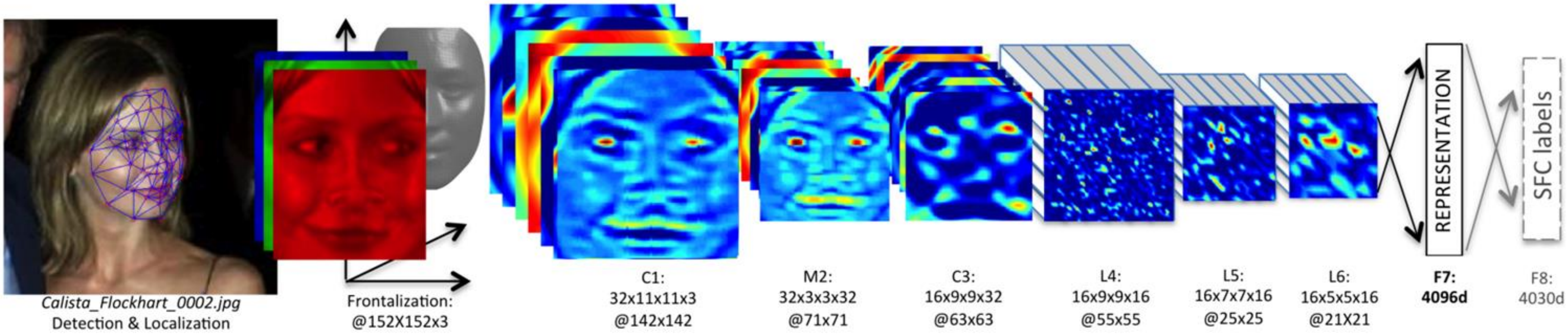
Query fingerprint

Similarity = 0.9

Enrolled fingerprint

- For over 100 years, minutiae correspondence has been used for similarity
- If the similarity value > T the two images come from the same finger

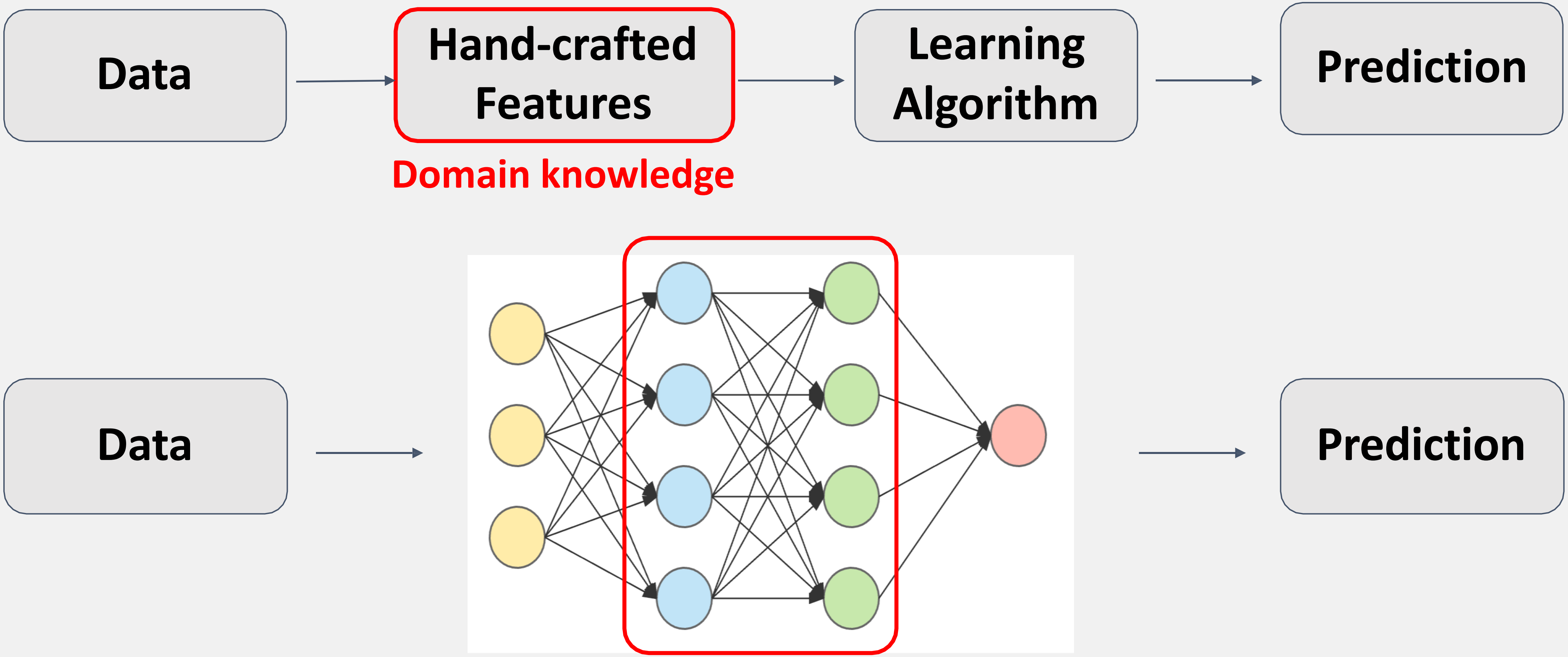
Deep Networks in Biometrics
Deepface (2014)



- 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

Representation



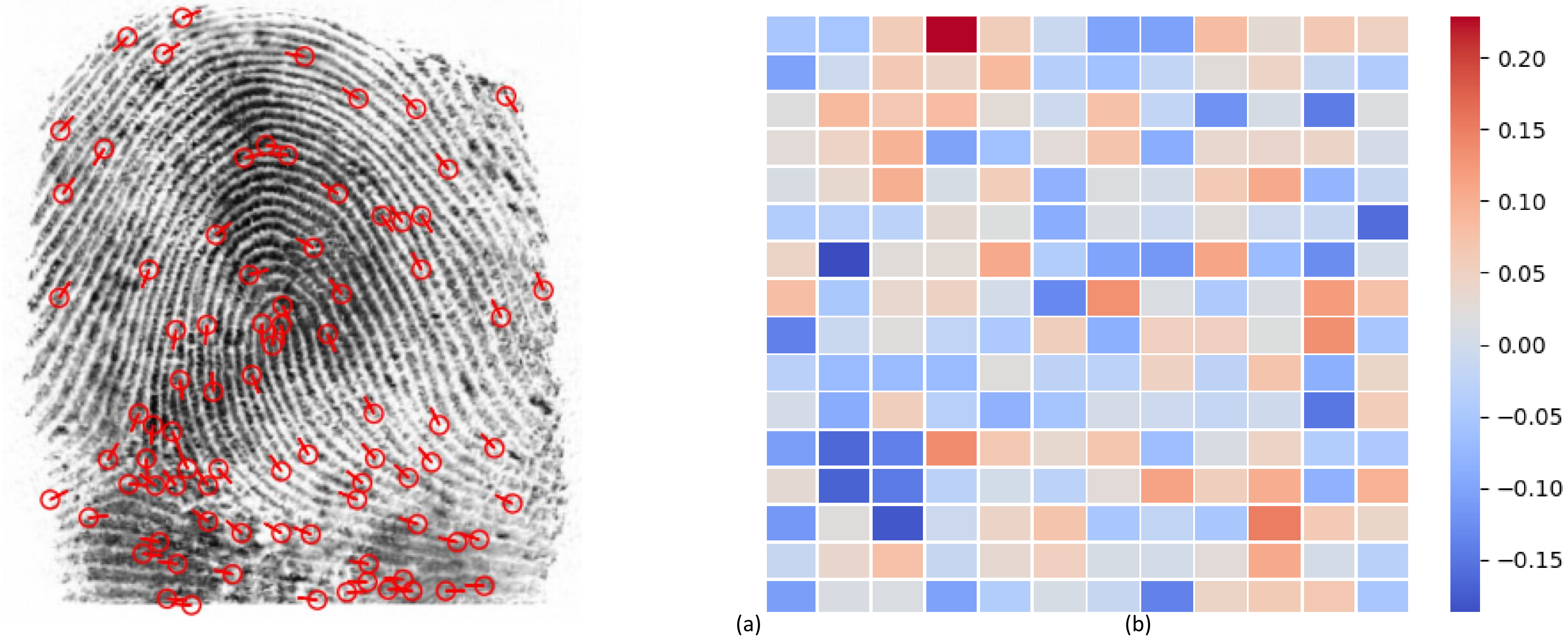
Data → Hand-crafted Features → Learning Algorithm → Prediction

Domain knowledge

Data → → Prediction

Representation Learning

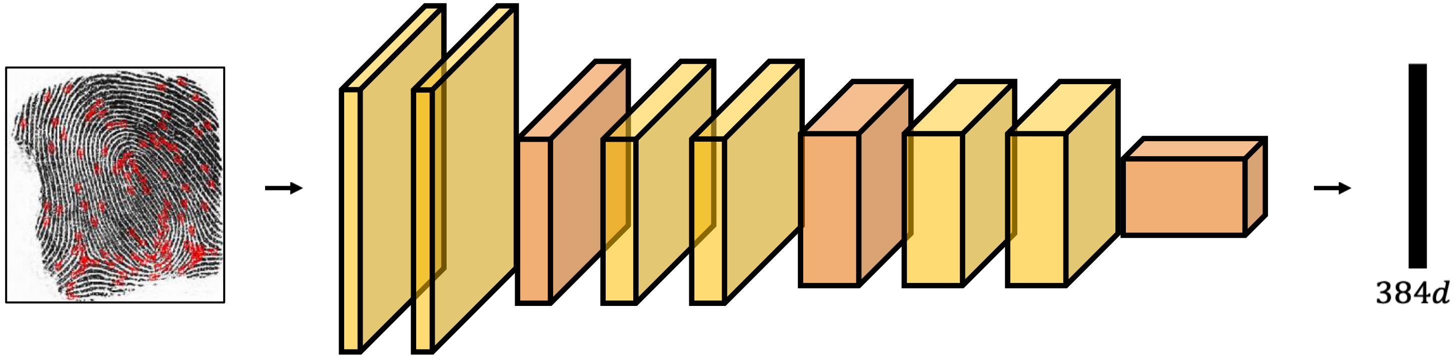
Two Representations for Fingerprints



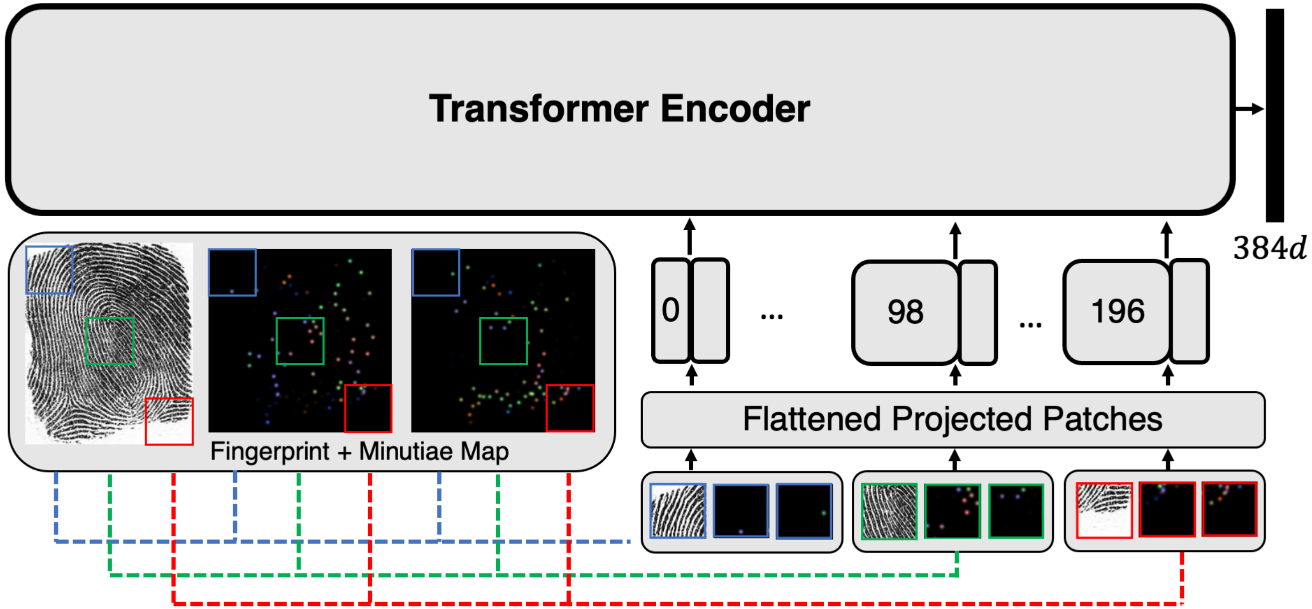
- Minutiae representation vs. 192-dim (192 bytes) embeddings
- Comparing embeddings is 3-times faster than minutiae comparison

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

Networks for Learned Fingerprint Features

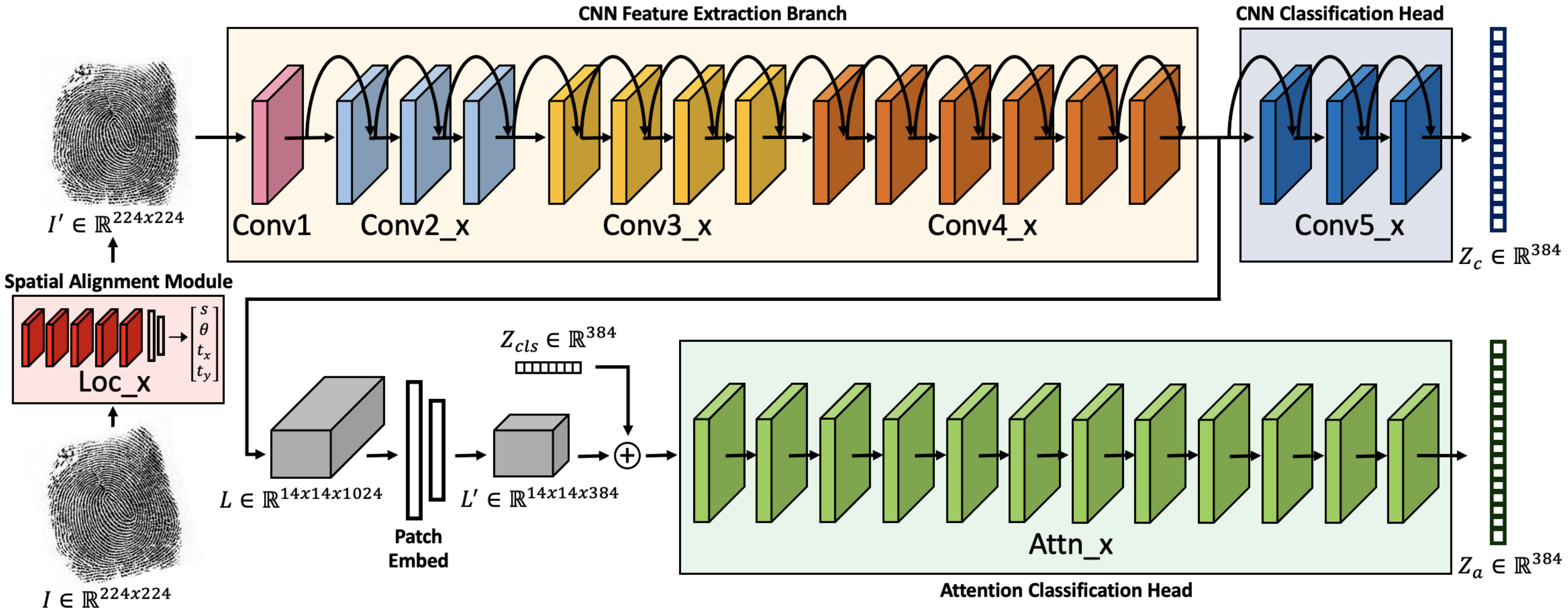


(a) CNN (ResNet-v50, Inception-V4, DeepPrint, etc.)



(b) Vision Transformer (ViT)

Fusion of Different Learned Features

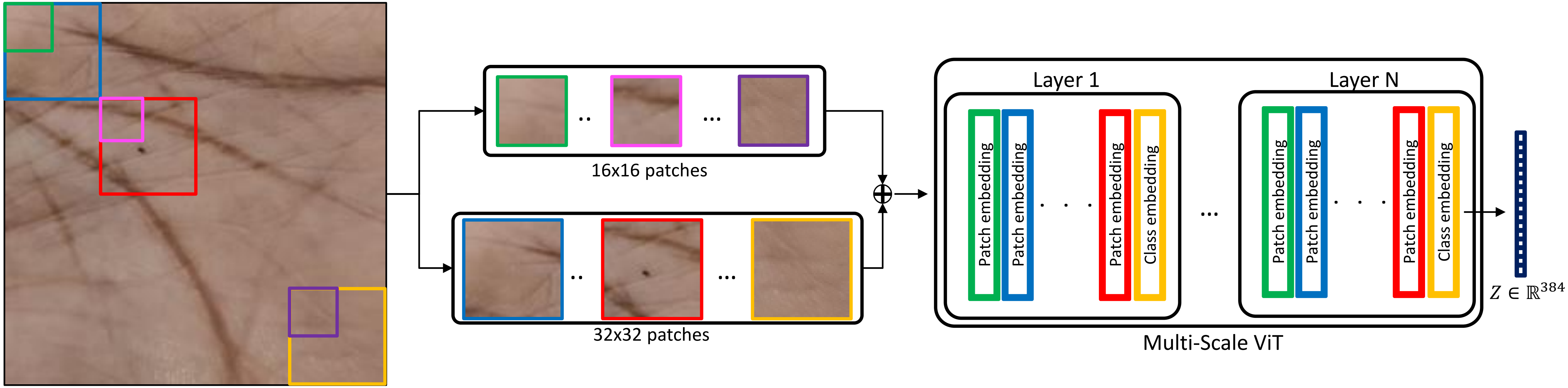


CNN Feature Extraction Branch
CNN Classification Head
Conv1
Conv2_x
Conv3_x
Conv4_x
Conv5_x
$I' \in \mathbb{R}^{224x224}$
$Z_c \in \mathbb{R}^{384}$
Spatial Alignment Module
Loc_x
s
θ
t_x
t_y
$I \in \mathbb{R}^{224x224}$
$Z_{cls} \in \mathbb{R}^{384}$
$L \in \mathbb{R}^{14x14x1024}$
Patch Embed
$L' \in \mathbb{R}^{14x14x384}$
Attn_x
$Z_a \in \mathbb{R}^{384}$
Attention Classification Head

AFR-Net: Fusion of CNN-based (e.g., ResNet-v50) and attention-based (e.g., ViT) learned features.

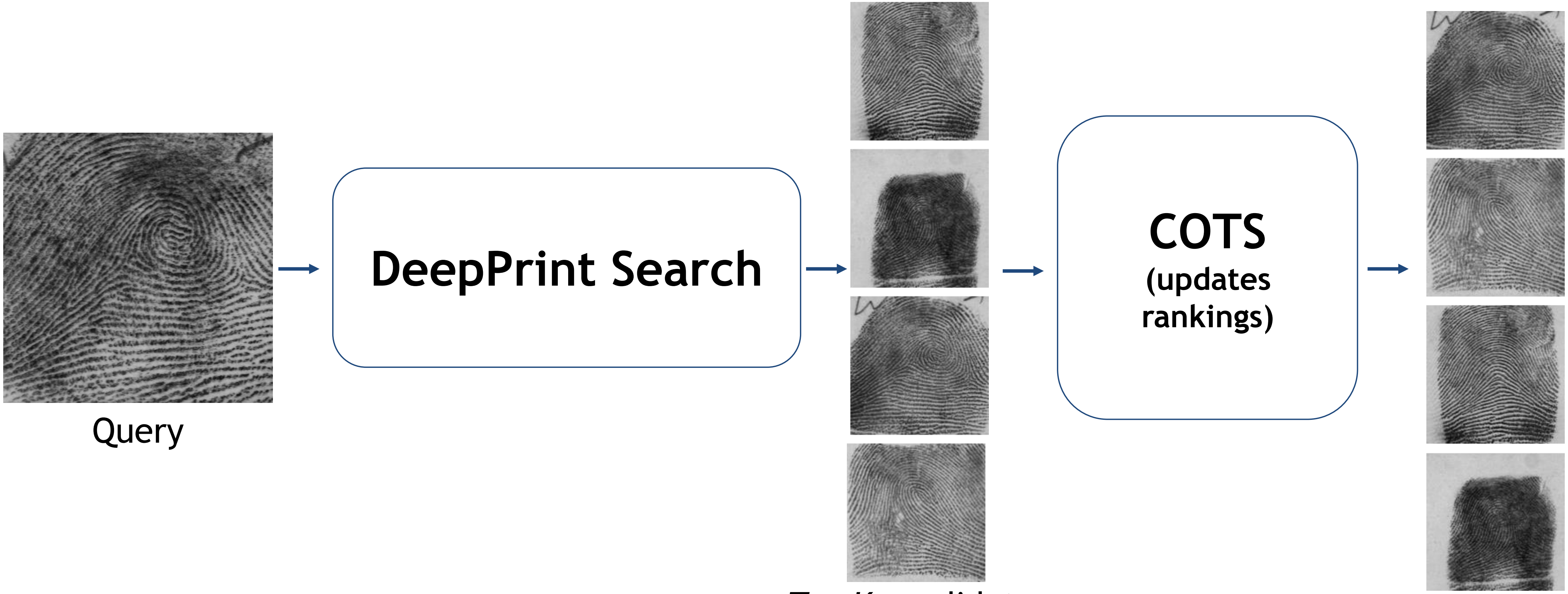
Grosz and Jain, "AFR-Net: Attention-Driven Fingerprint Recognition Network", IEEE TBIOM, 2023.

Fusion of Multiscale Features



Grosz, Godbole, and Jain, "Mobile Contactless Palmprint Recognition: Use of Multiscale, Multimodel Embeddings", https://arxiv.org/abs/2401.08111

Two-Stage Matching



Query

DeepPrint Search

Top K candidates

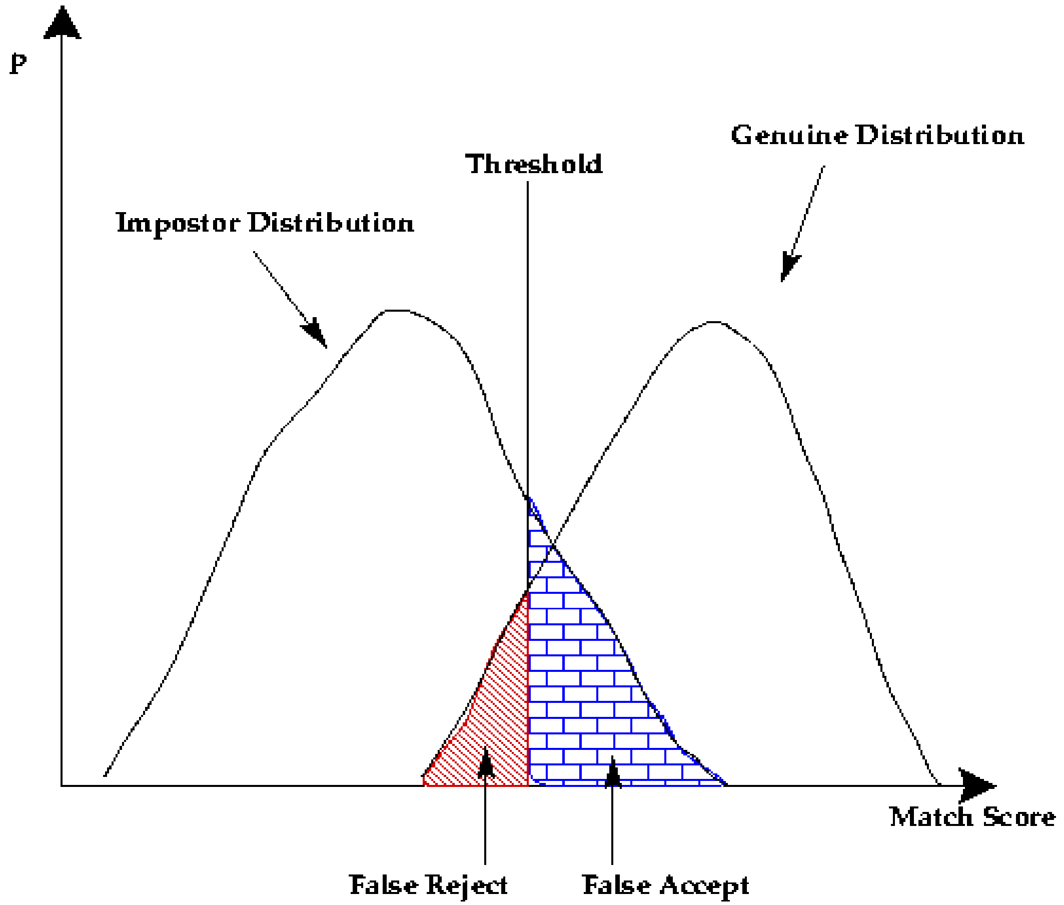
COTS
(updates rankings)

Candidates

Fusion of minutiae & CNN representations improves Rank-1 performance from 99.45% to 99.48% with speed up from 3M comparison/sec to 10M comparisons/sec

State-of-the-Art Accuracy

Similarity Score Distributions



- FAR: Proportion of fraudulent claims of identity that are incorrectly confirmed
- FRR: Proportion of transactions with truthful claims of identity that are incorrectly denied
- Threshold: A value which satisfies the specified FAR
- RoC: Plot of true positive rate (TPR) vs. false positive rate (FPR) at various threshold settings

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)

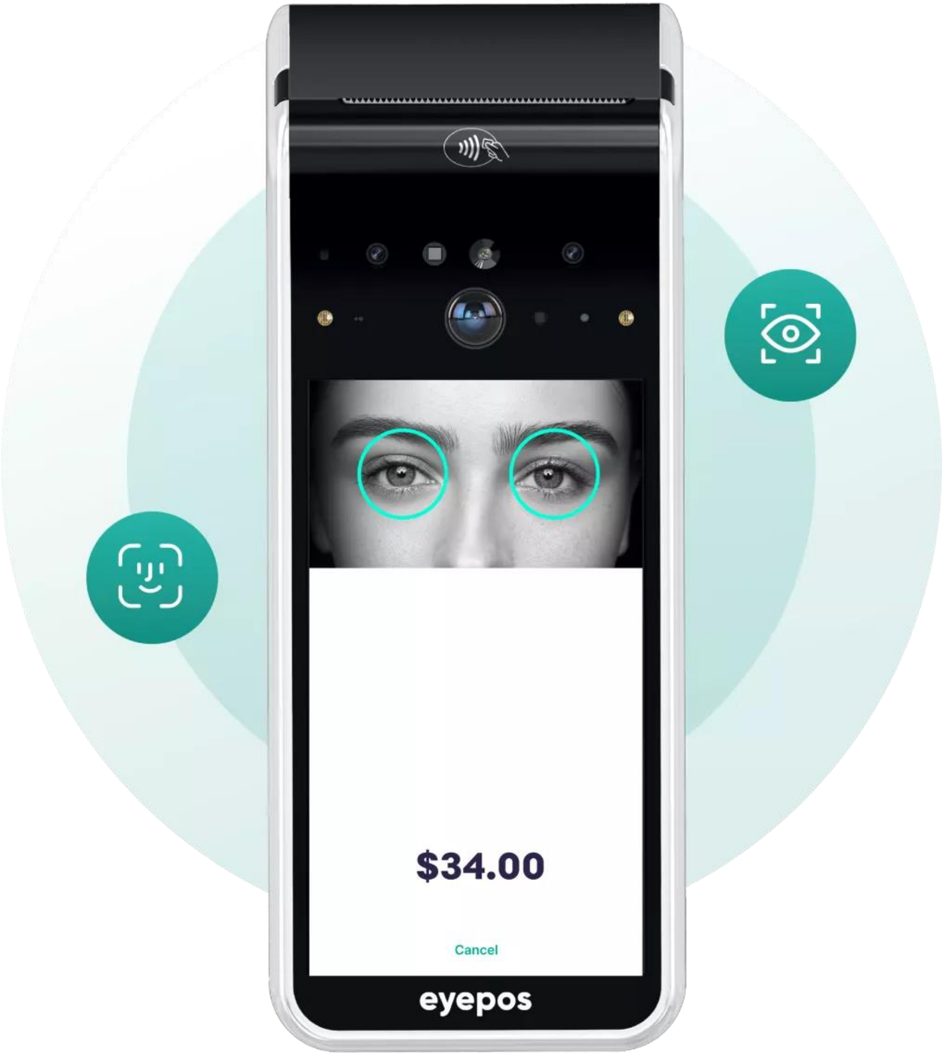
Face: FNIR = 0.03 (12M gallery)

[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/

Challenges, Concerns & Opportunities

- Laboratory collected biometric data vs. field collected data from operational biometric systems
- Recognition with noisy/distorted/occluded/partial images (contactless images, crime scene fingerprints, CCTV face video)
- Synthetic biometric image generation for data augmentation
- User consent and data privacy
- Presentation attack detection
- Sensor interoperability
- Privacy preserving matching

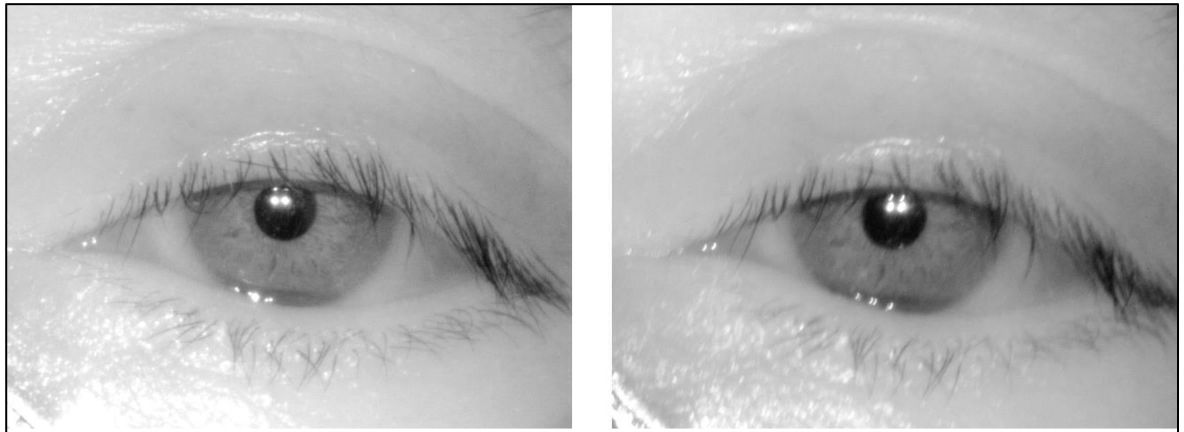
PayEye: Fusion of Iris and Face



Payment at Point of Sale

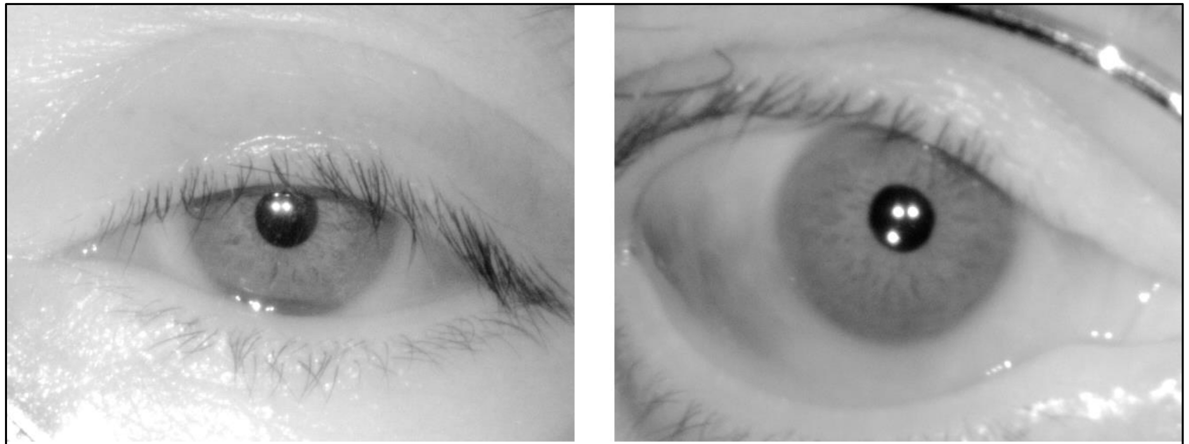
https://payeye.com/for-business-eye-payments/

Iris Images From Payeye



Dissimilarity score: 0.11

Matcher needs to work on images obtained in unconstrained environments, with characteristics different from images in public-domain iris databases



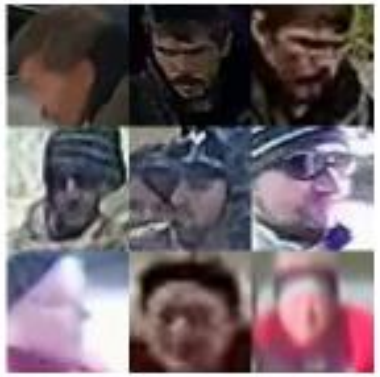
Dissimilarity score: 0.43

Face Image Quality vs. Recog. Performance

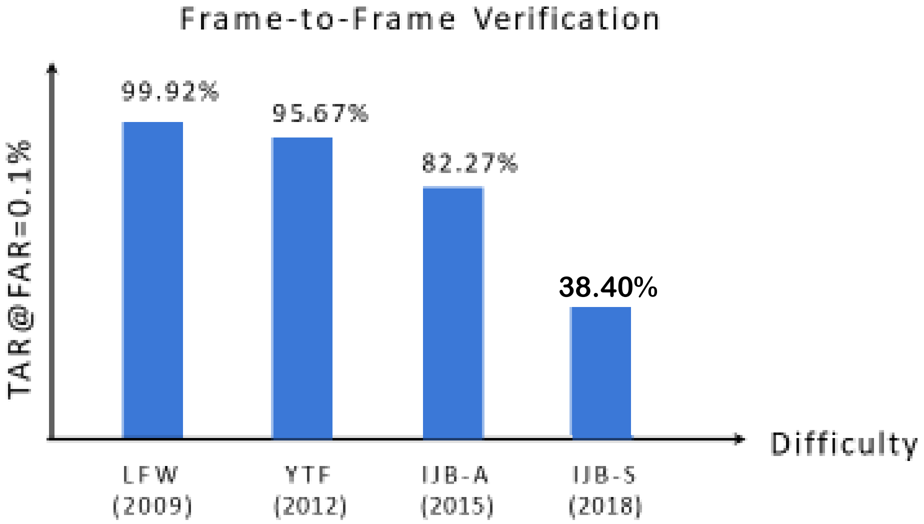
LFW (2009)

YTF (2012)

NIST IJB-A (2015)



NIST IJB-S (2018)



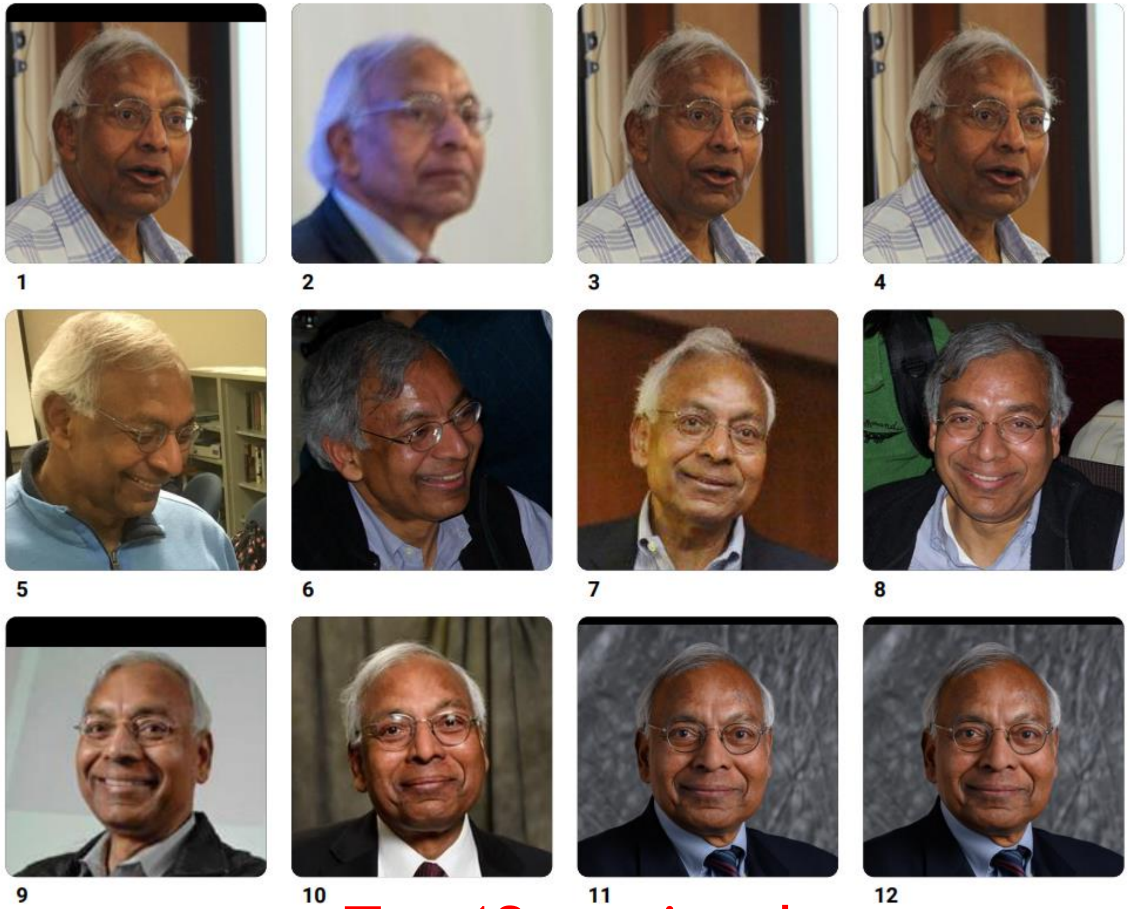
	Gallery Size	Rank1	Rank5
IJB-A	112	97.5	98.4
IJB-S (S2B)	202	60.5	66.0
IJB-S (S2B) With DA	**202**	**64.5**	**71.1**

DA: Data augmentation with synthetic data

Liu, Kim, Jain, Liu, "Controllable and Guided Face Synthesis for Unconstrained Face Recognition", ECCV, 2022

Progress in Unconstrained Face Search

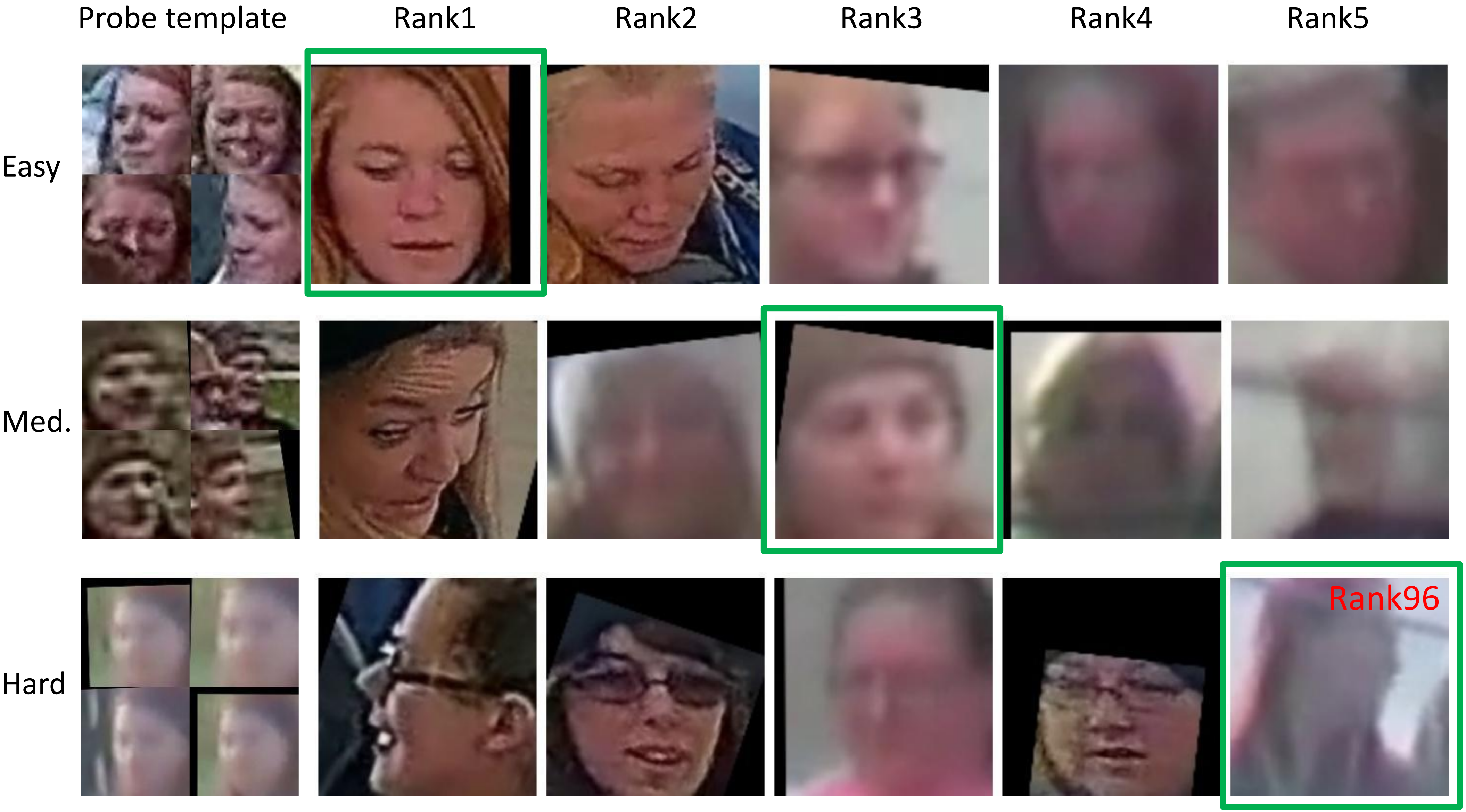
Probe



Top 12 retrievals

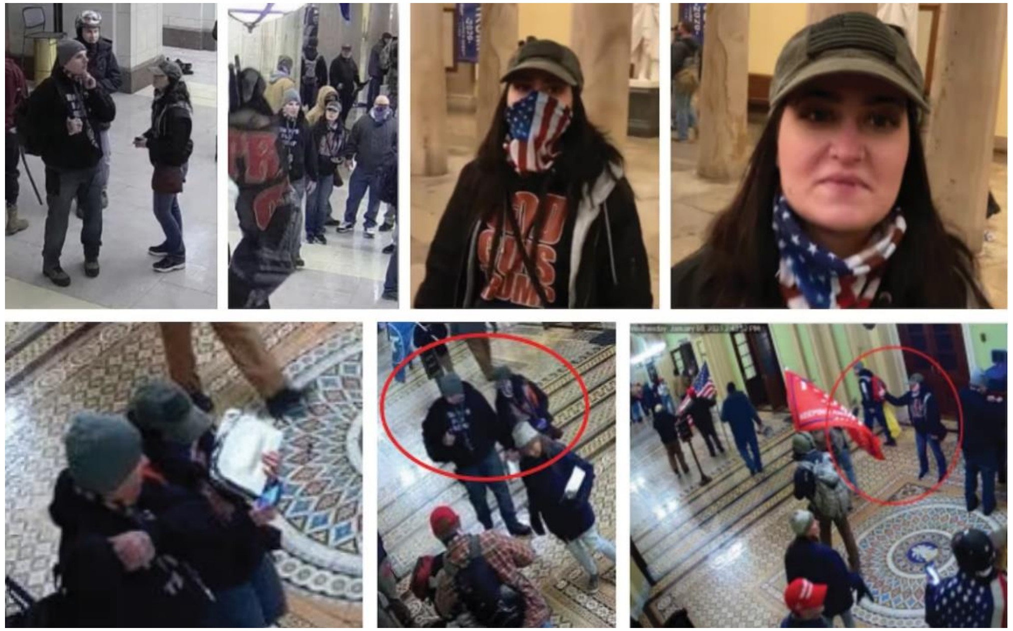
Gallery: 20 billion face images (courtesy Clearview.Ai)

Face Recognition in Video is Difficult



Liu, Kim, Jain, and Liu, "Controllable and Guided Face Synthesis for Unconstrained Face Recognition", ECCV, 2022.

America's Surveillance Networks Helped the FBI Catch the Capitol Mob



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.)

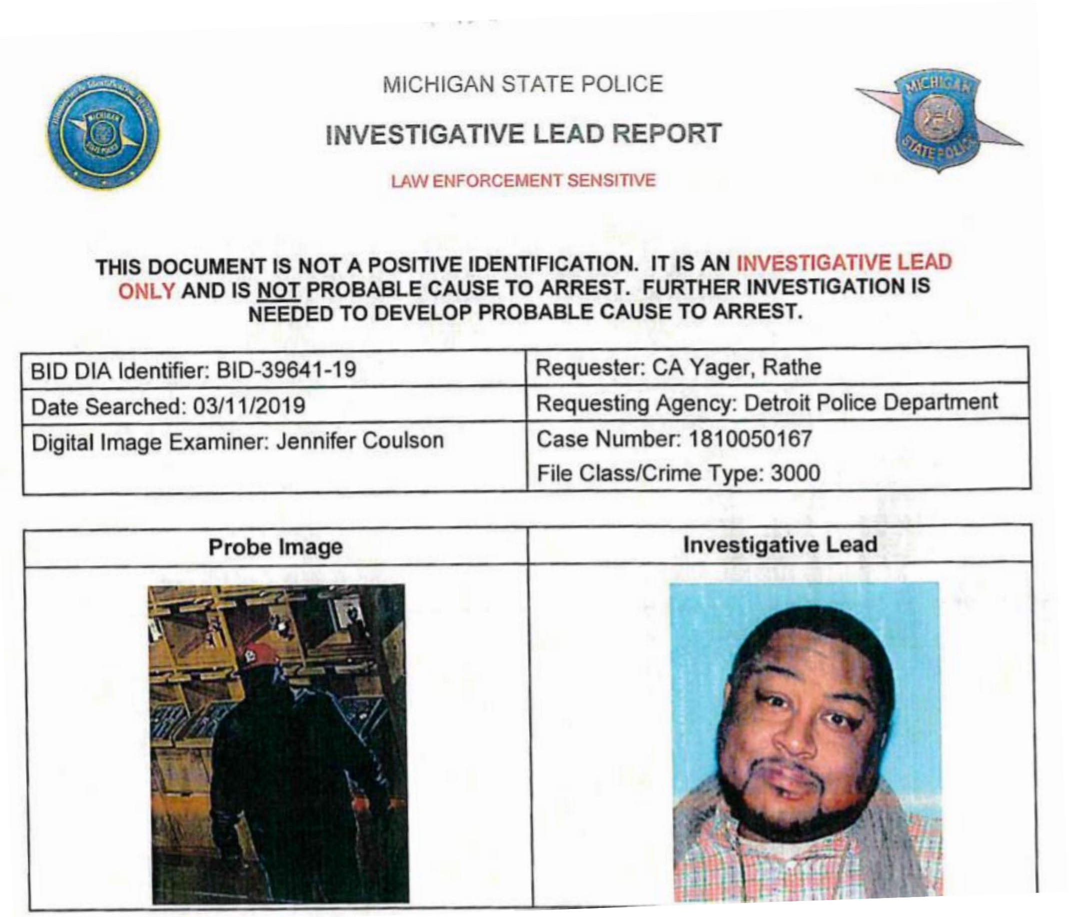
FBI used a mix of techniques, from license plate readers to facial recognition to identify rioters

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 me,” Robert Julian-Borchak Williams told investigators after he was arrested*
- *“You think all Black men look alike?”*

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



MICHIGAN STATE POLICE

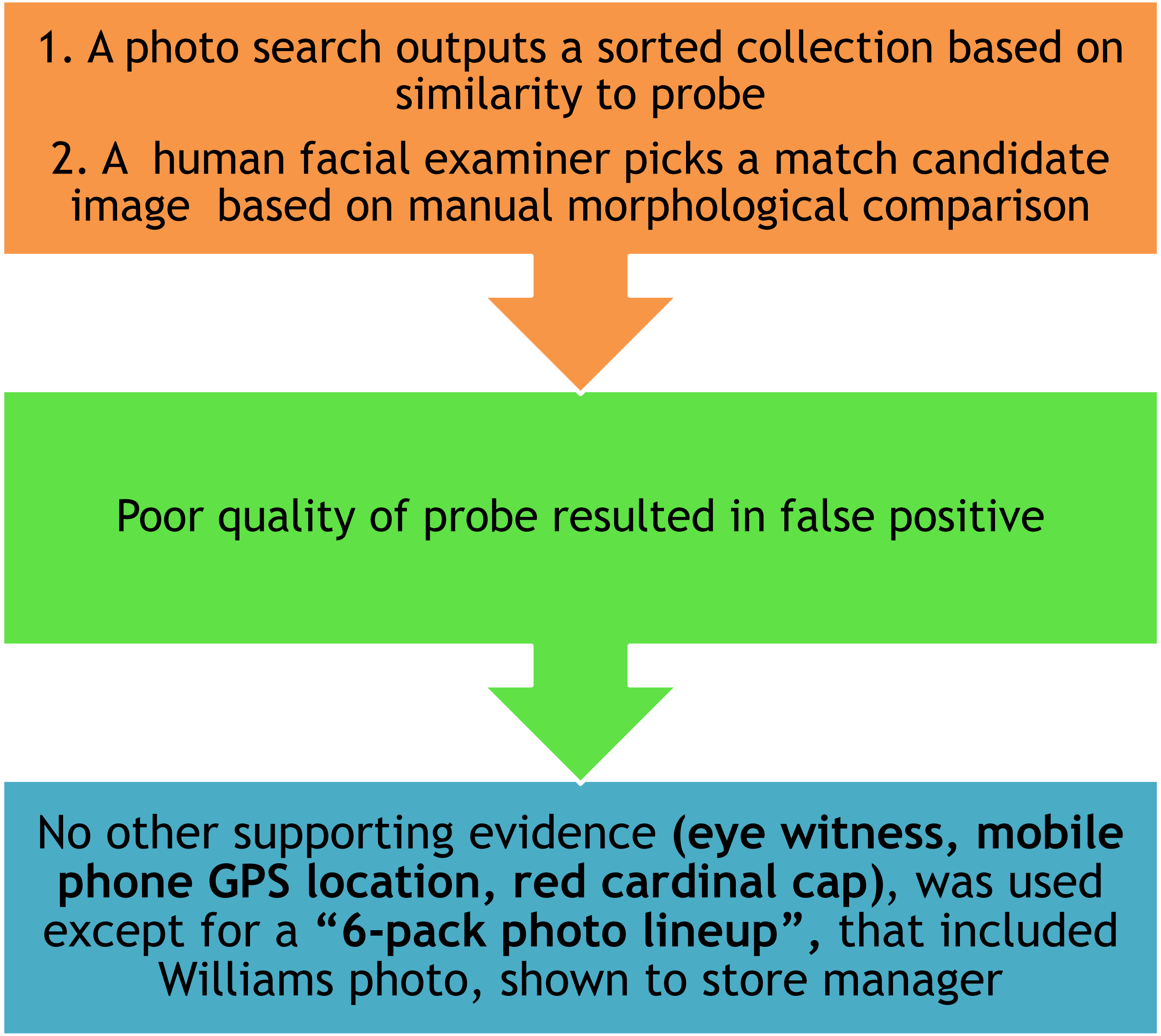
INVESTIGATIVE LEAD REPORT

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



1. A photo search outputs a sorted collection based on similarity to probe

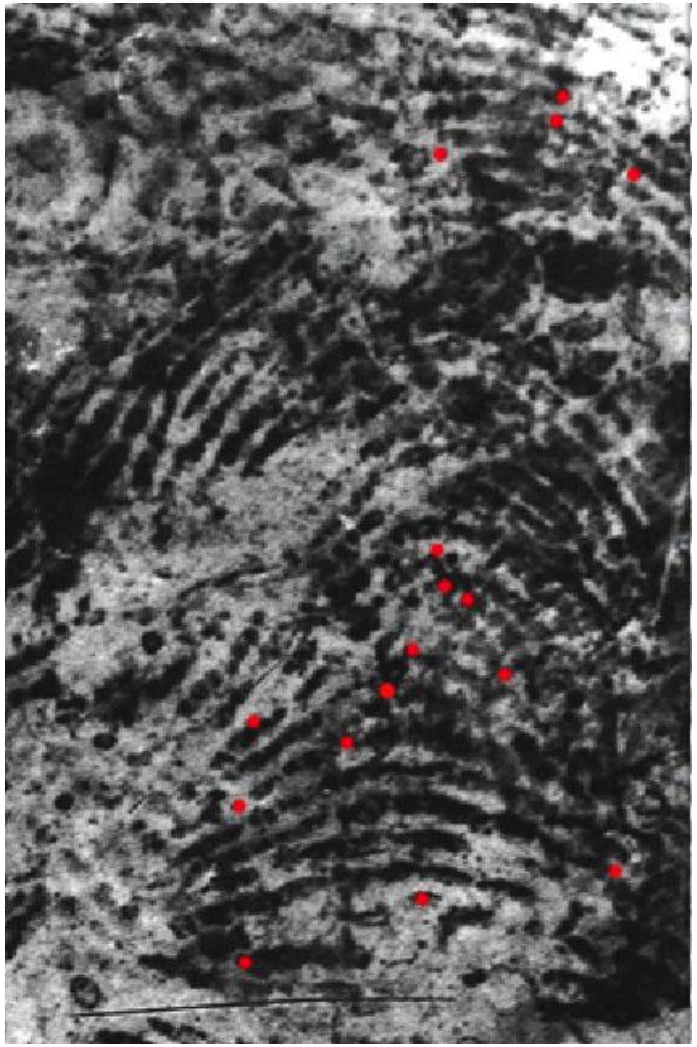
2. A human facial examiner picks a match candidate image based on manual morphological comparison

Poor quality of probe resulted in false positive

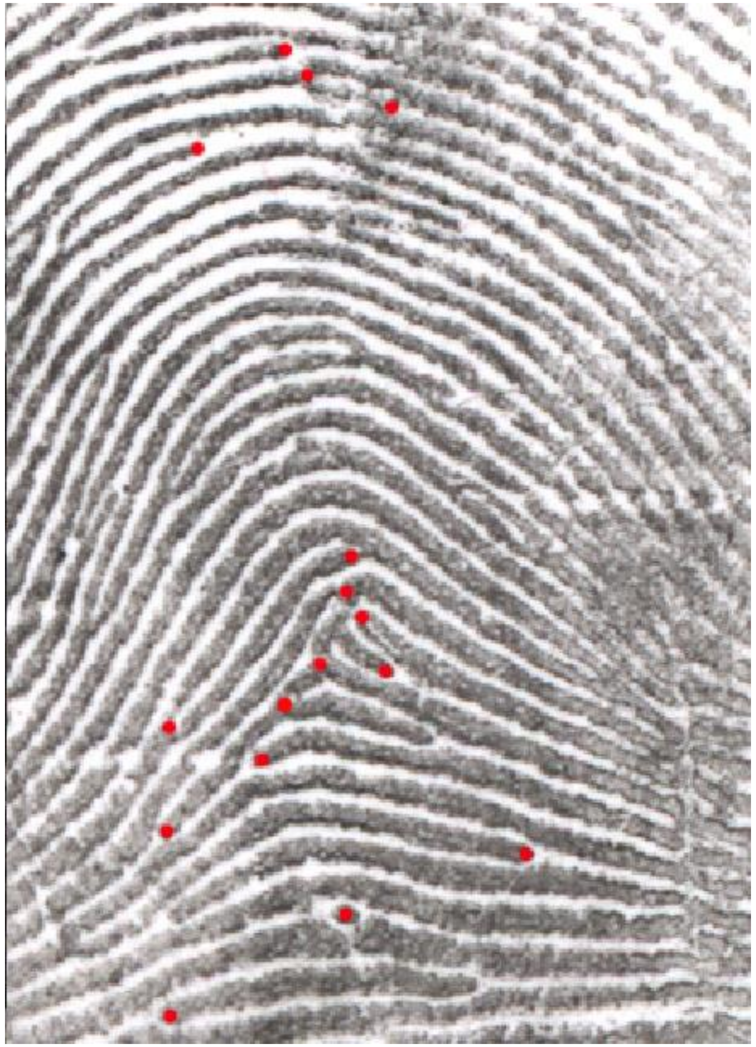
No other supporting evidence **(eye witness, mobile phone GPS location, red cardinal cap)**, was used except for a **“6-pack photo lineup”**, that included Williams photo, shown to store manager

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

Wrongful Apprehension of Brandon Mayfield



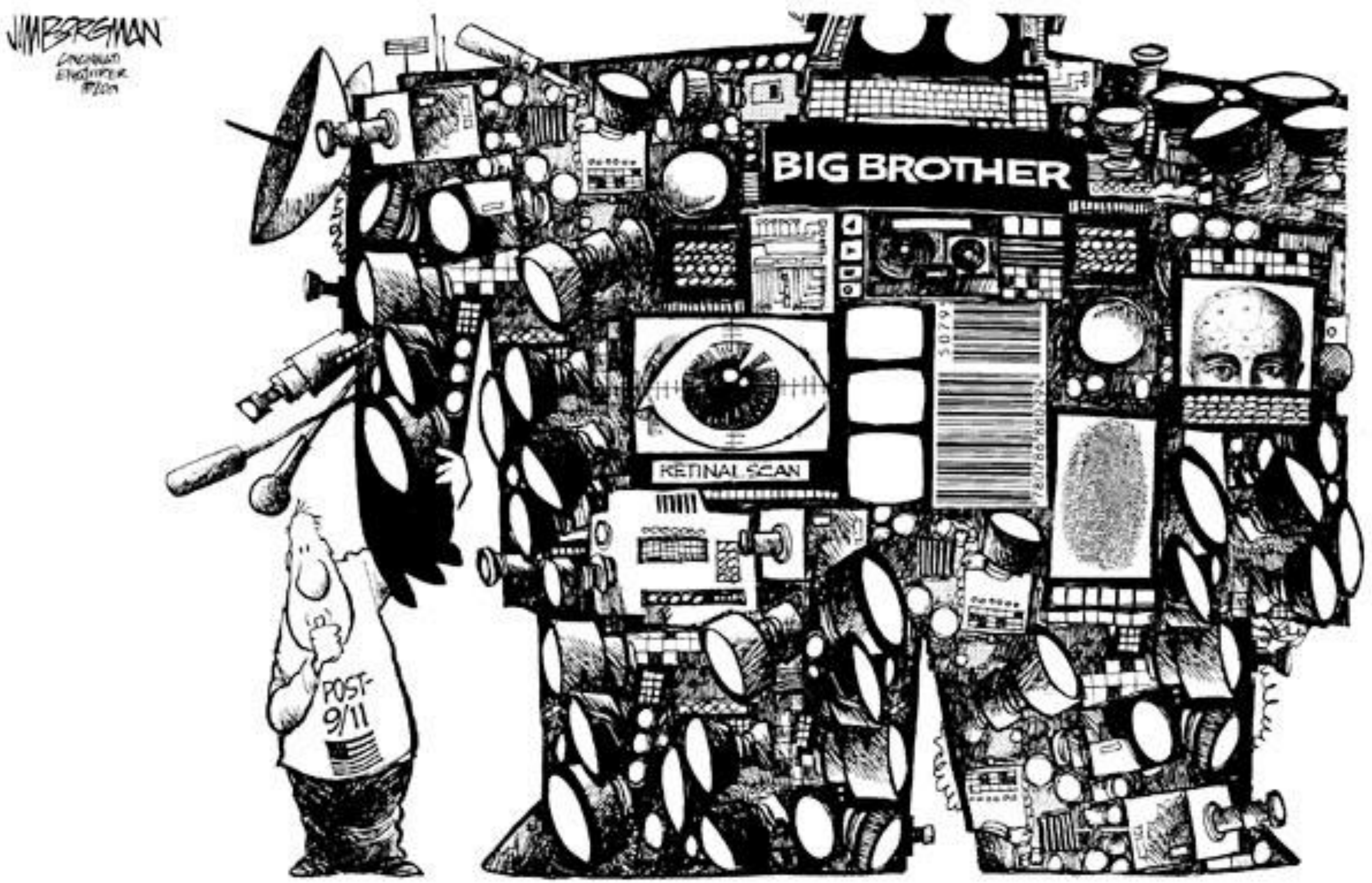
Partial print at site of Madrid train bombing (2004)



AFIS incorrectly returned Brandon Mayfield's prints

https://oig.justice.gov/sites/default/files/archive/special/s0601/final.pdf

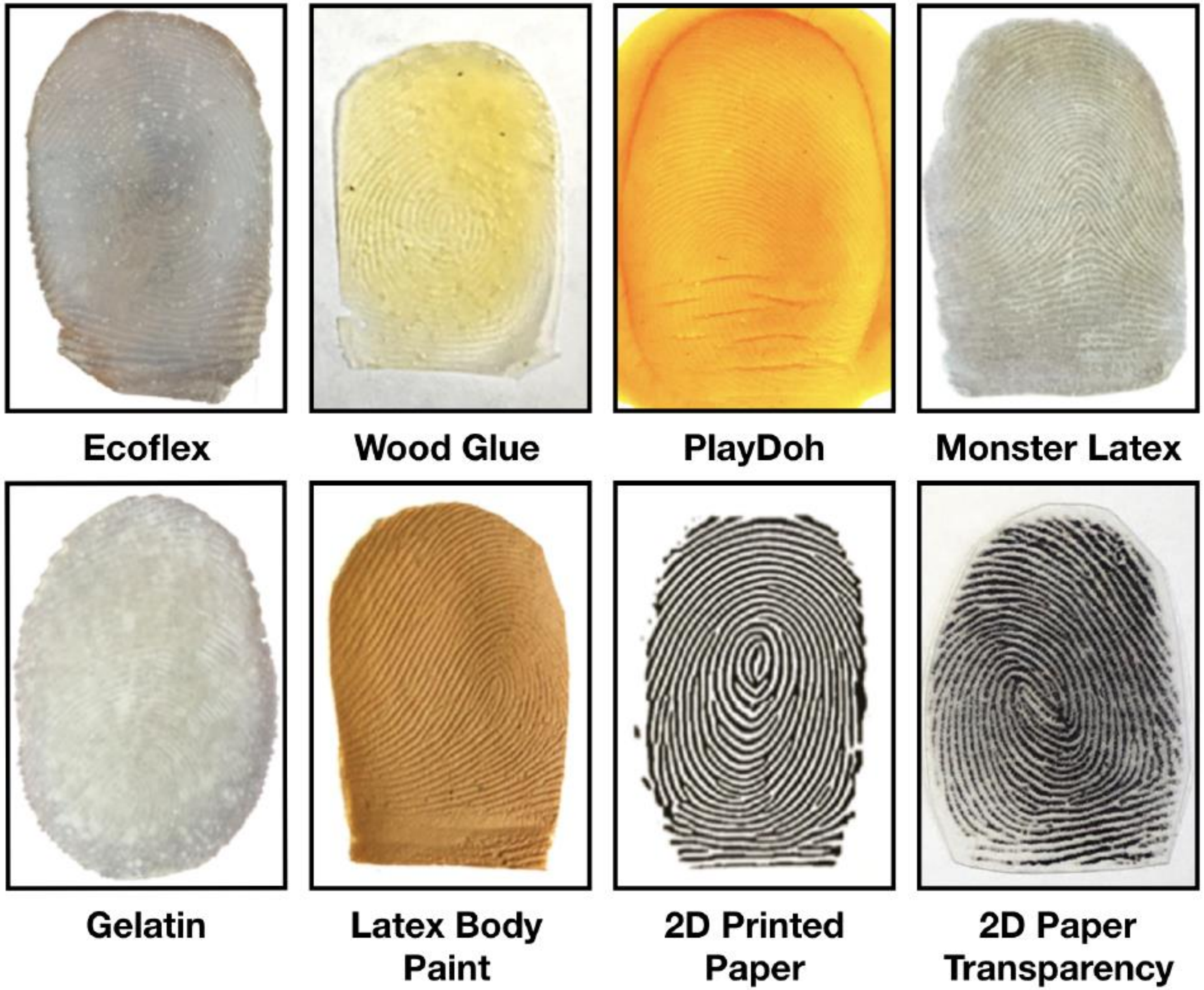
Privacy and Civil Liberty Concerns



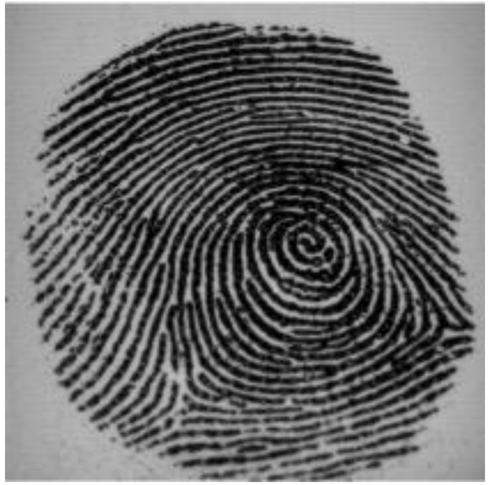
Wrongful conviction, demographic bias, template security, retention policy, function creep

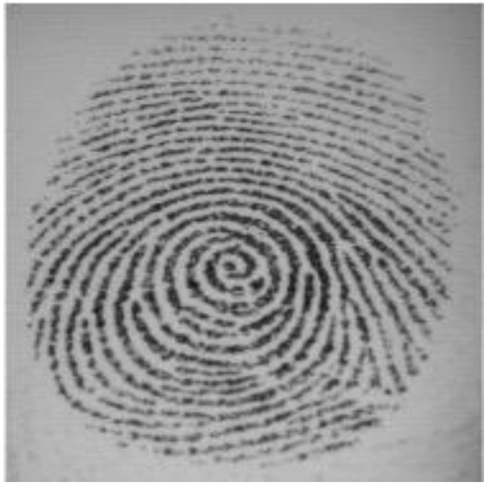
Presentation Attacks

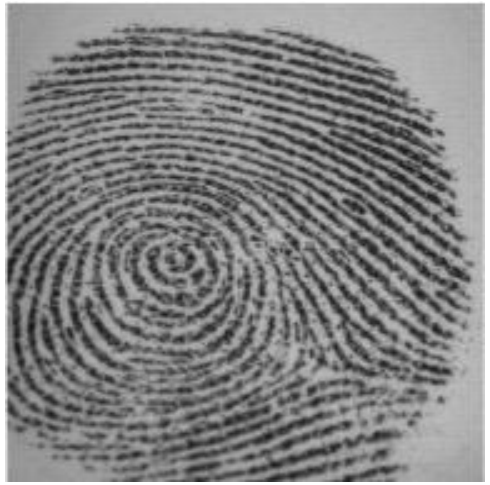
A bad actor uses someone else's biometric data, commonly known as “spoofs,” to impersonate someone else

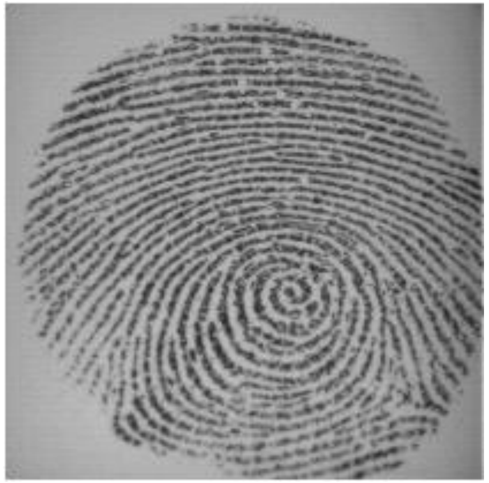


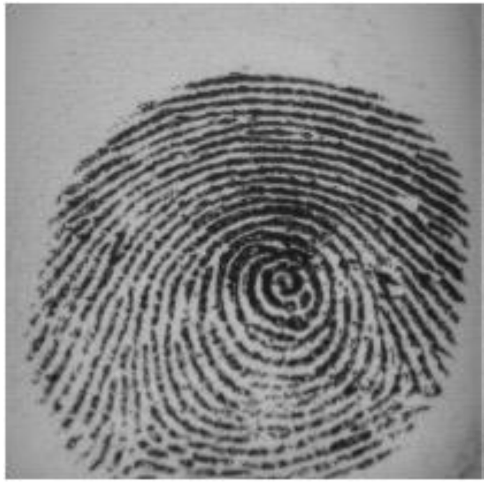
Which Images Are Spoof?



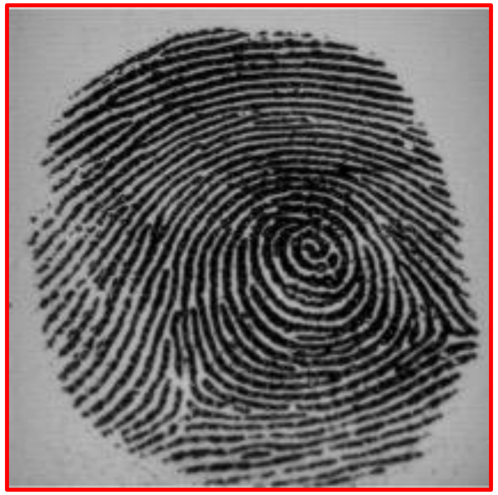


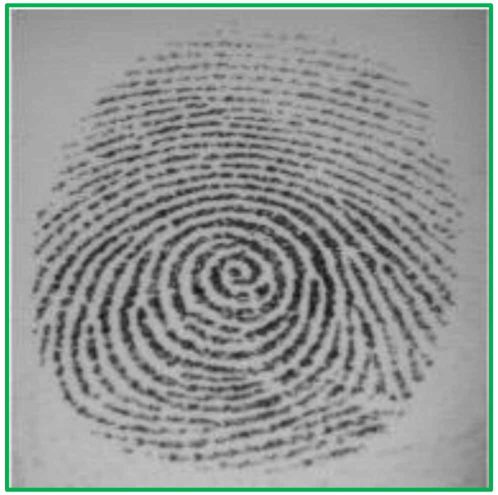


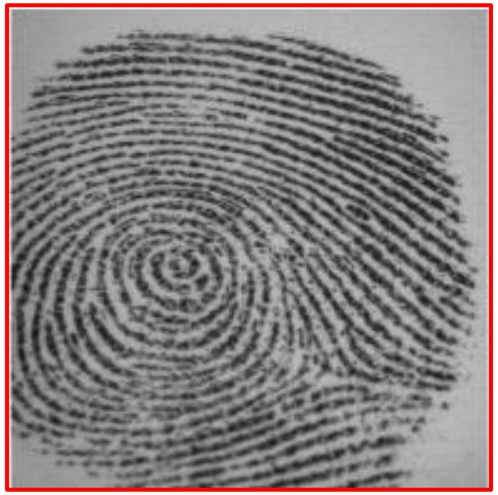


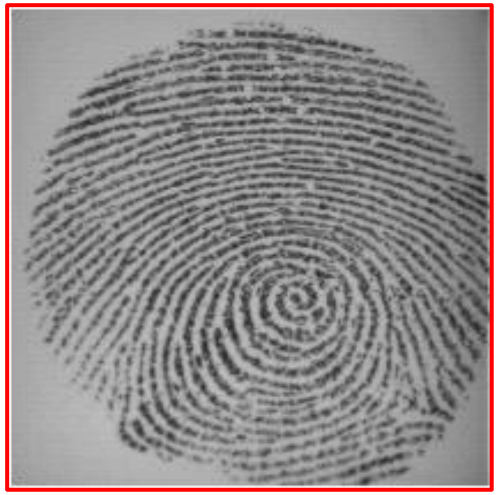


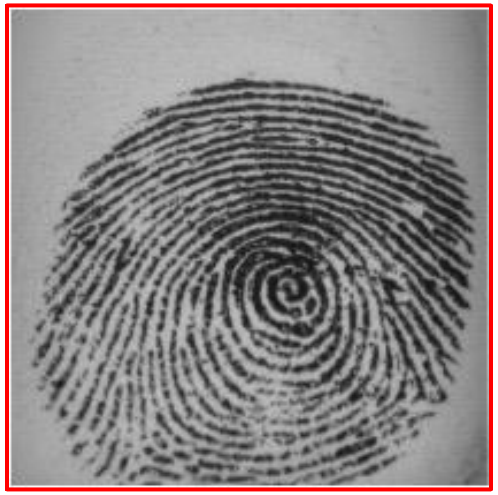
Which Images Are Spoof?



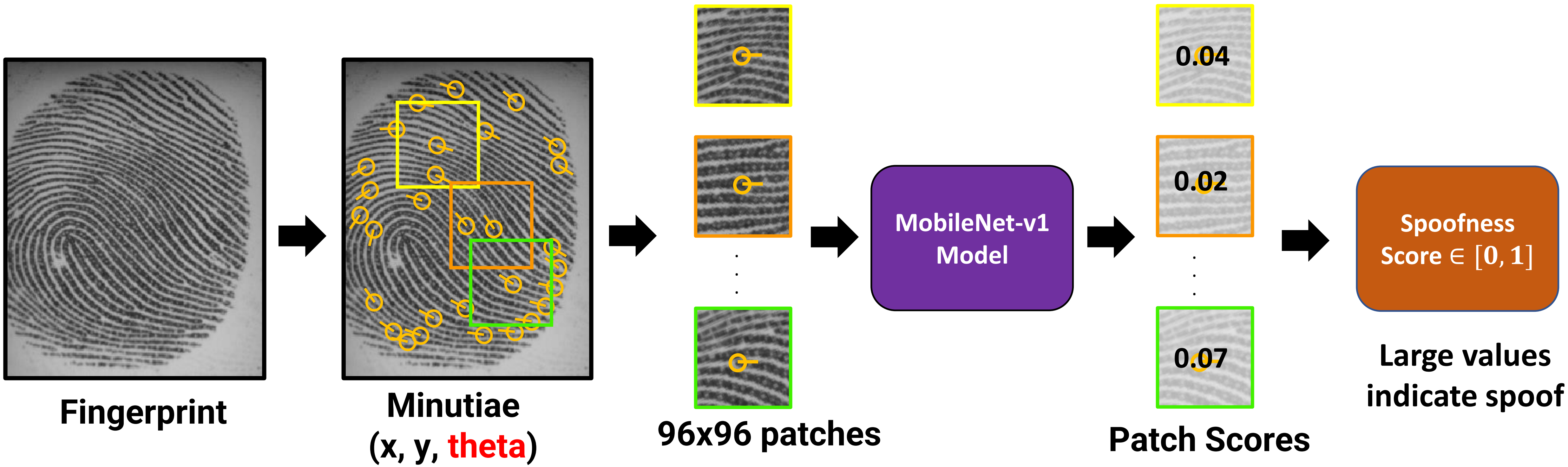








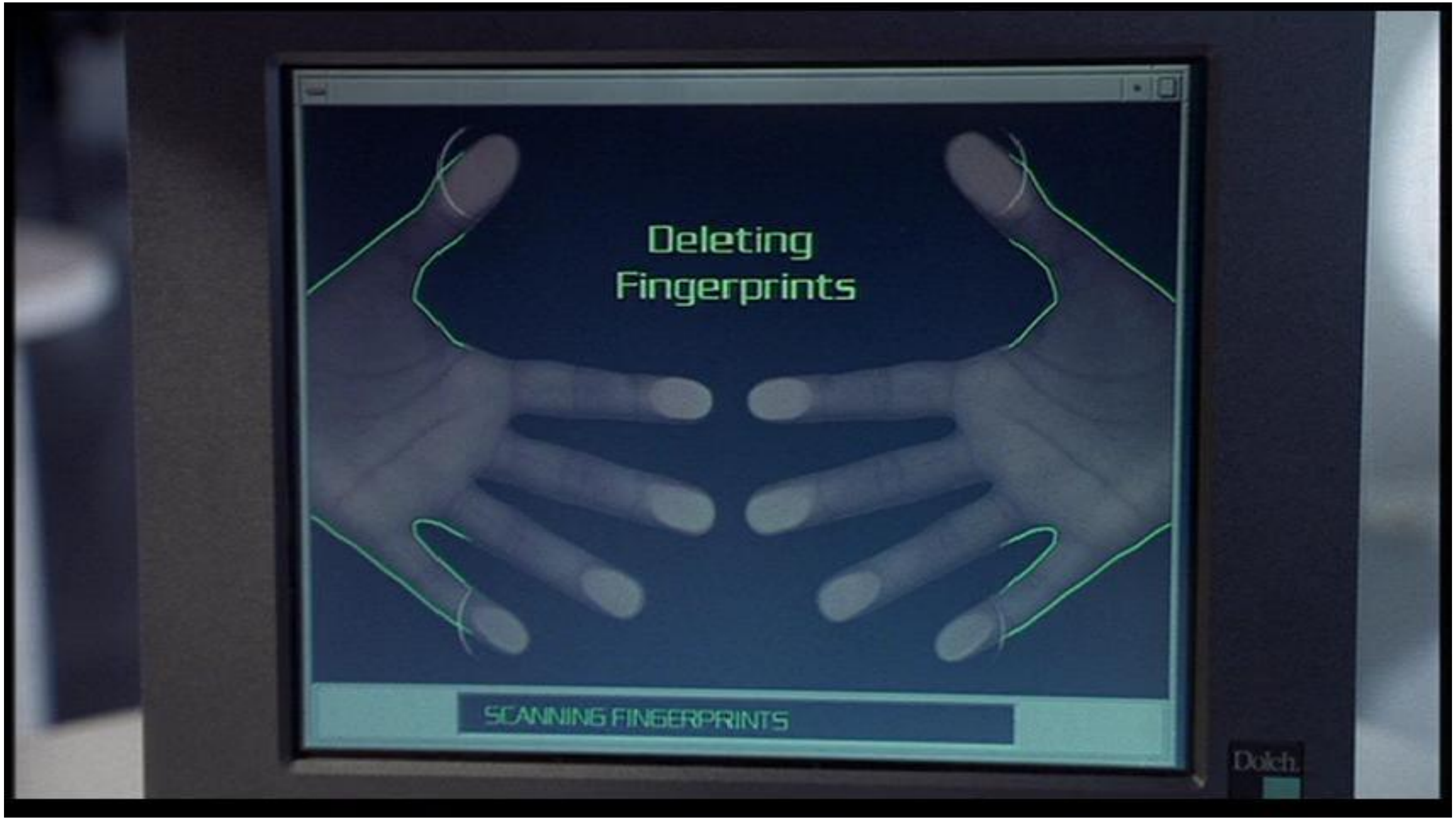
Fingerprint Spoof Buster



- Advantages of minutiae centered & aligned patches: robust to image size; large no. of patches for training; localization of partial spoof area

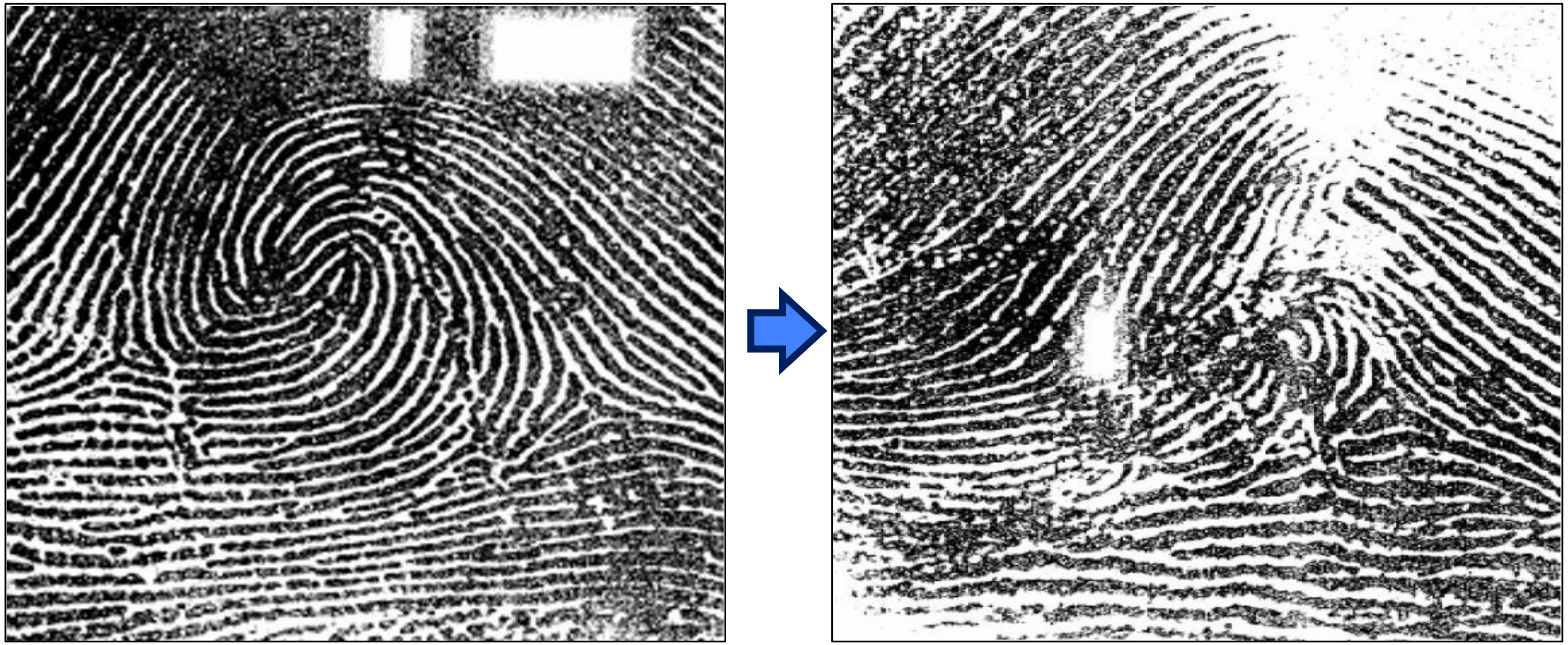
Chugh, Cao, and Jain, "Fingerprint Spoof Buster: Use of Minutiae-centered Patches", IEEE TIFS, 2018

Will Smith in “Men in Black” (1997)



https://en.wikipedia.org/wiki/Men_in_Black_(1997_film)

Fingerprint Alteration



Winkler (1933) changed double-loop fingerprint to left loop to evade identification

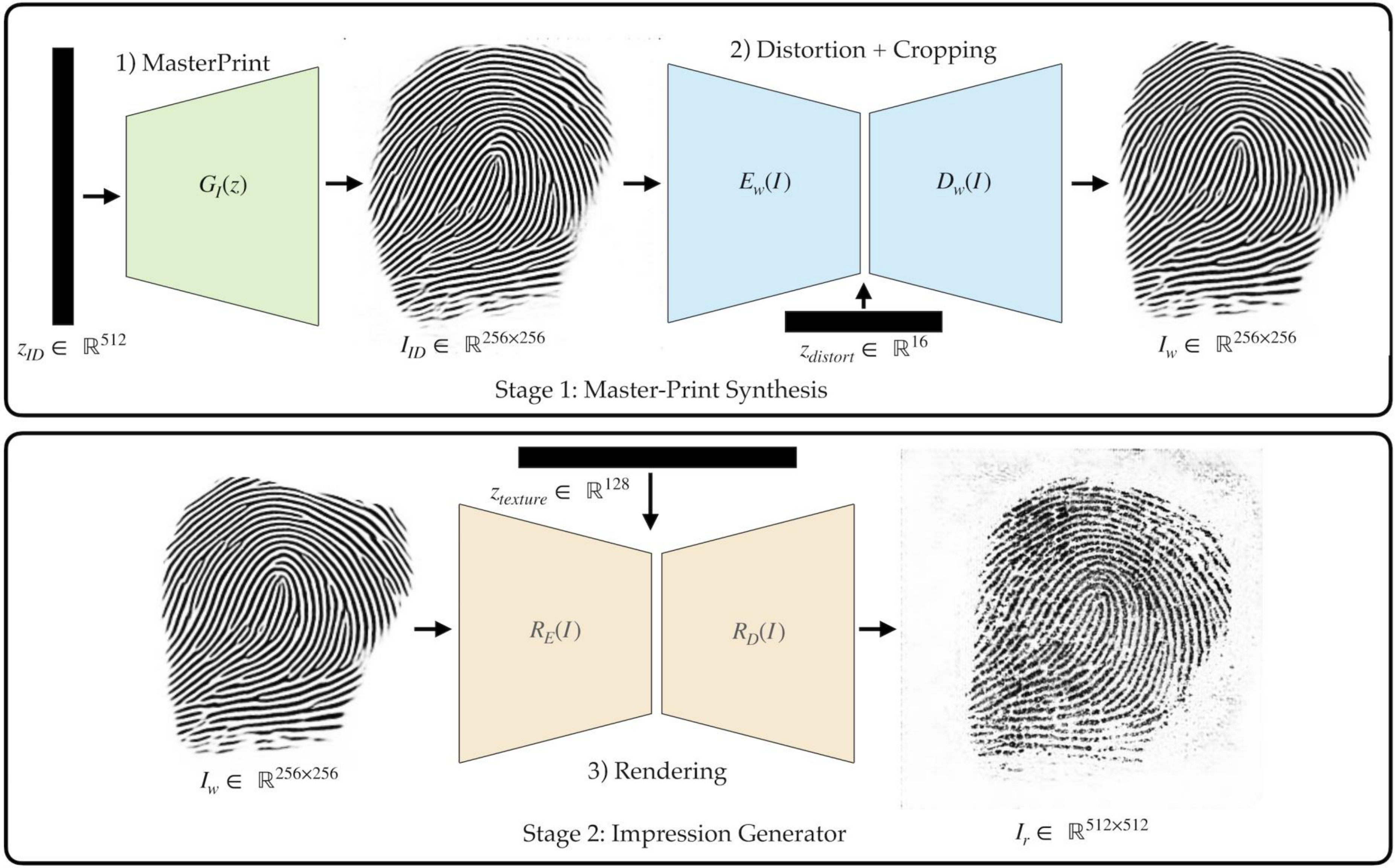
S. Yoon, J. Feng and A. K. Jain, "Altered Fingerprints: Analysis and Detection", IEEE T-PAMI, 2012

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?**

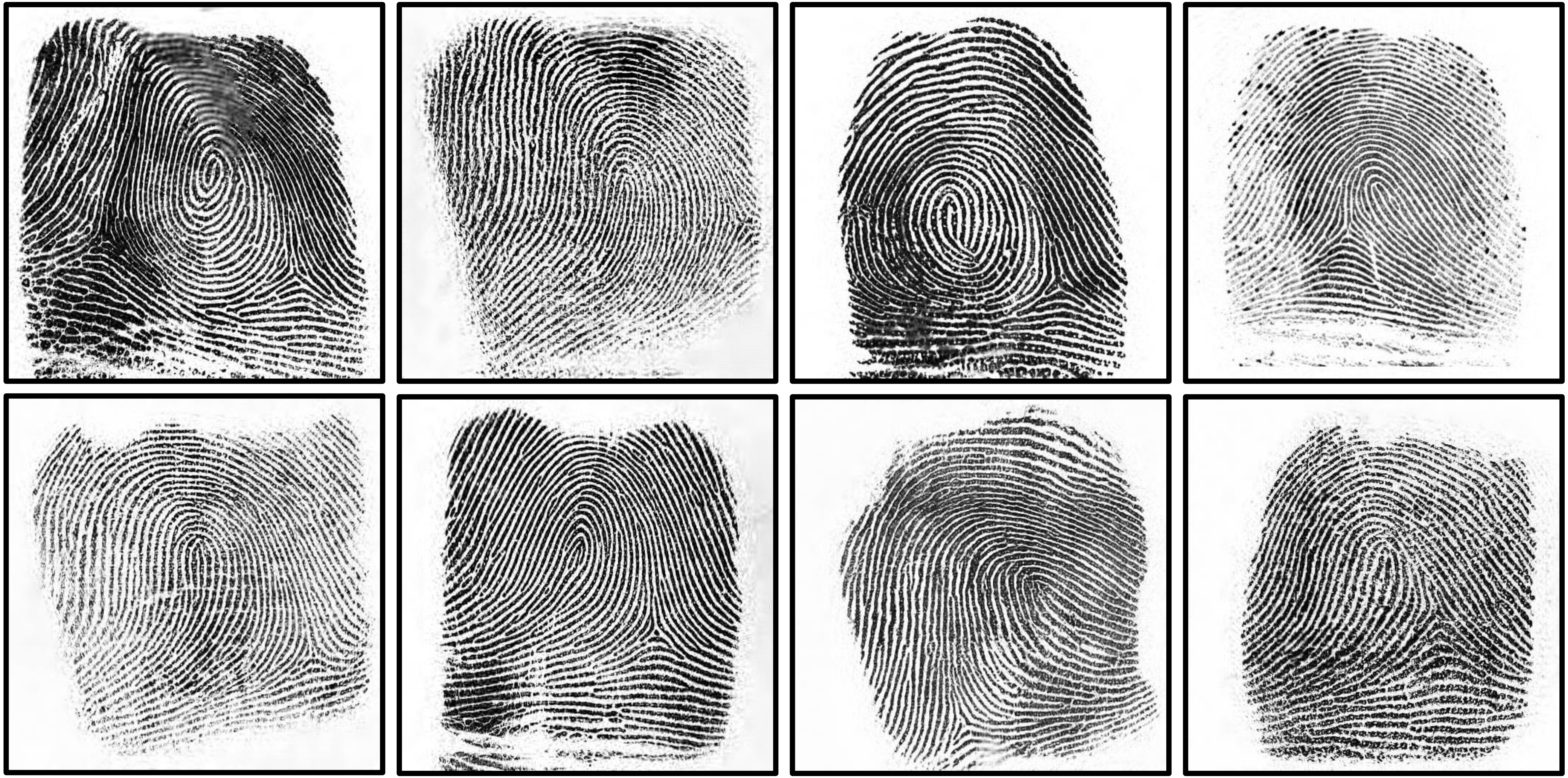
https://gdpr.eu/

Synthetic Fingerprint Generation


1) MasterPrint
$G_I(z)$
$z_{ID} \in \mathbb{R}^{512}$
$I_{ID} \in \mathbb{R}^{256\times256}$
2) Distortion + Cropping
$E_w(I)$
$D_w(I)$
$z_{distort} \in \mathbb{R}^{16}$
$I_w \in \mathbb{R}^{256\times256}$
Stage 1: Master-Print Synthesis
$z_{texture} \in \mathbb{R}^{128}$
$R_E(I)$
$R_D(I)$
$I_w \in \mathbb{R}^{256\times256}$
3) Rendering
Stage 2: Impression Generator
$I_r \in \mathbb{R}^{512\times512}$

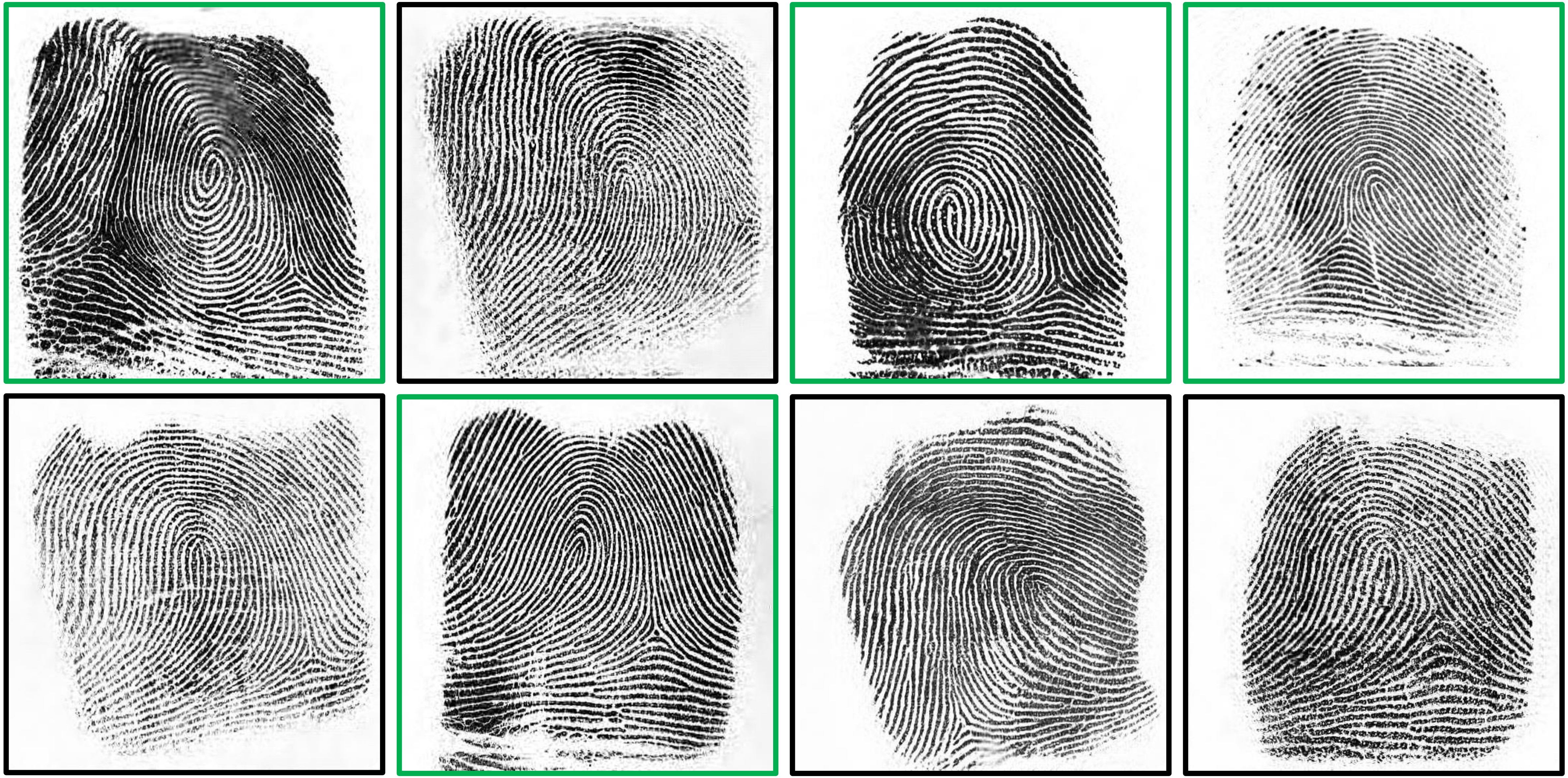
Engelsma, Grosz and Jain, ”PrintsGAN: Synthetic Fingerprint Generator", IEEE TPAMI, 2023.

Real or Synthetic Fingerprint Images



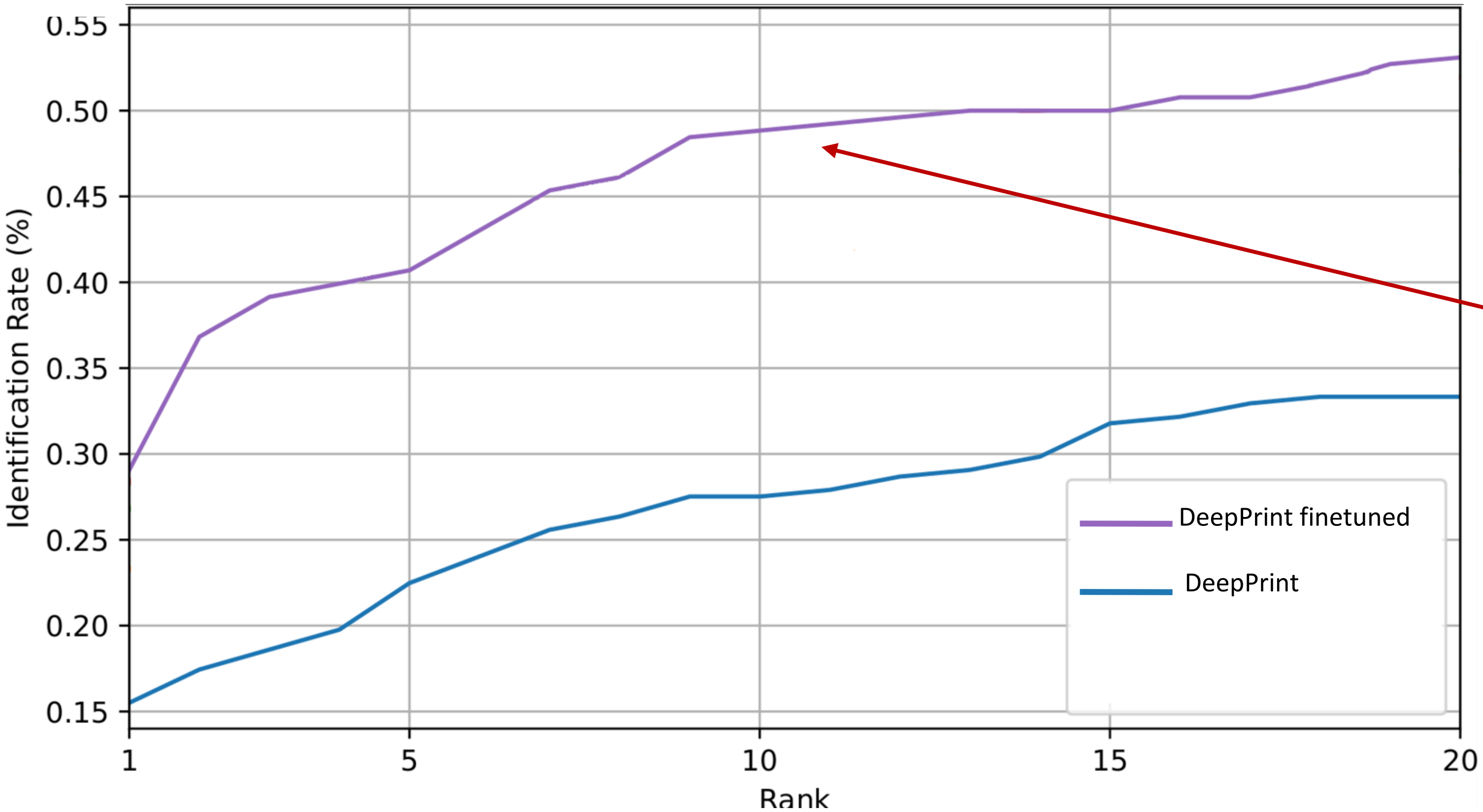
J. J. Engelsma, S. A. Grosz and A. K. Jain, "PrintsGAN: Synthetic Fingerprint Generator", IEEE TPAMI, 2022

Real or Synthetic Fingerprint Images



Data Augmentaion: Accuracy improvement

CMC curves for DeepPrint and DeepPrint finetuned with **synthetic latent fingerprints**



Accuracy improvement

Evaluated on NIST SD27 (1:N experiment)
DeepPrint: https://arxiv.org/abs/1909.09901

Take Home Message

- Biometrics is intertwined with applications
- Research must consider application requirements (accuracy, template size, latency, user behavior, presentation attack,..
- Face, fingerprint and iris will continue to dominate, but room for other modalities for specific commercial use cases
- Need to continually improve accuracy, especially for unconstrained scenarios and large scale search
- Accuracy on lab collected datasets is not representative of performance on deployed systems due to unexpected user behavior
- Deep network is not a panacea; embedding domain knowledge is important
- Building an app to demo your research is extremely useful