Introduction to Biometric Recognition

Anil K. Jain

Michigan State University

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

Shiv Nadar University, Chennai, January 31, 2024

Artificial Intelligence (AI)

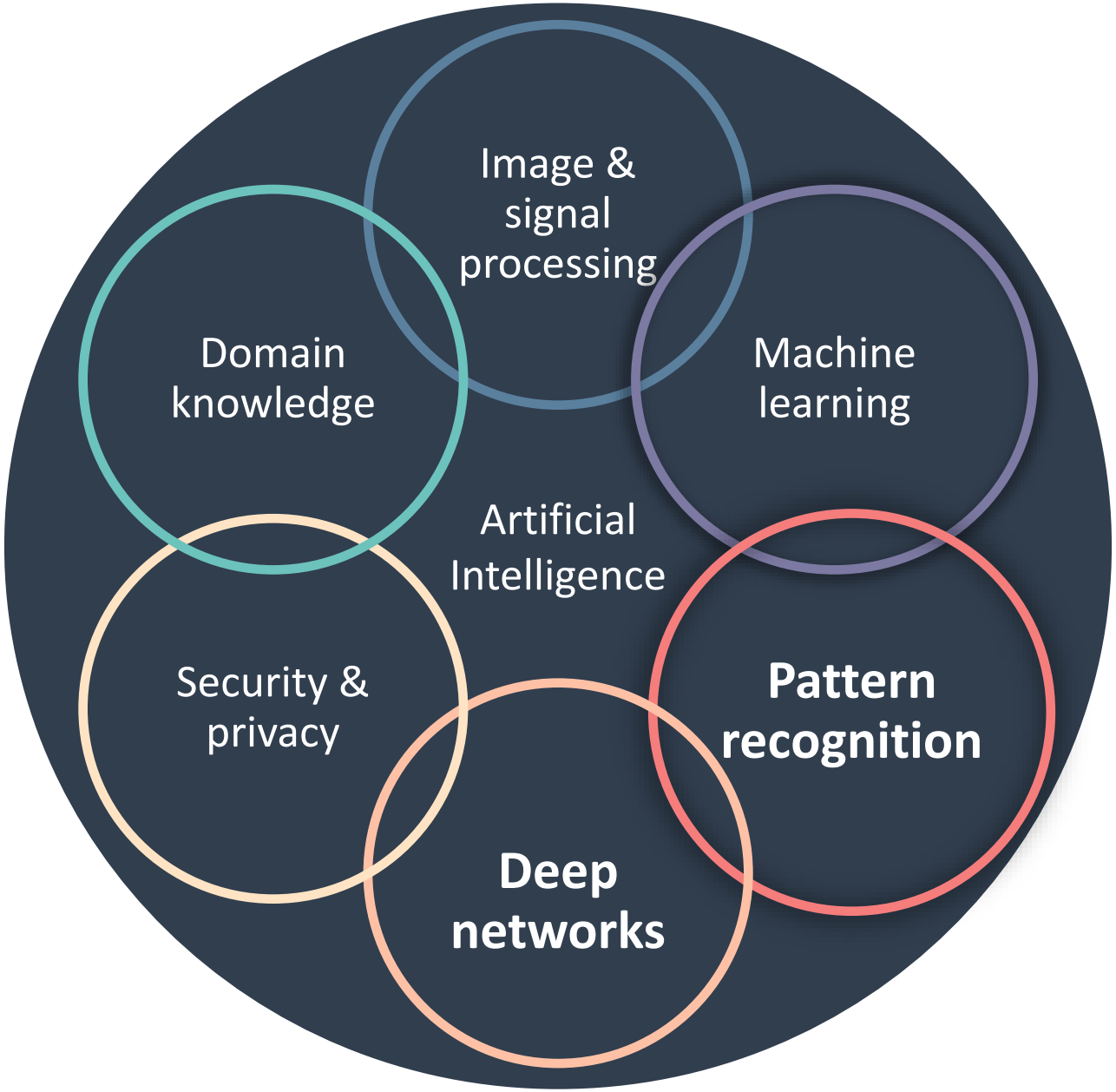
- …. making a machine behave in ways that would be called intelligent if a human were so behaving.

McCarthy, Minsky, Rochester & Shannon, 1956

- Turing test (1951) , “imitation game”, tests if a computer can successfully pretend to be a human in a dialogue via screen & keyboard. *Dictionary.com*

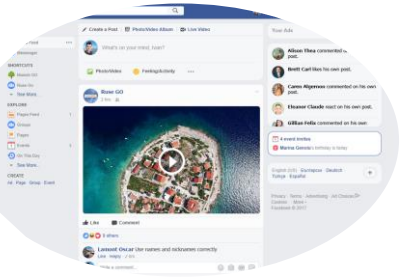
A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955, AI Magazine, Vol. 27(4), 2006

Artificial Intelligence: Many Facets



Most-Influential (AI) Technologies

Facebook's News Feed



2006

Netflix Streaming

2007

Facebook's Instagram

2010

Uber

2011

Tesla's Model S

2012

Apple iPad

2012

Ring's Doorbell

2013

Apple TouchID

2013

Amazon Alexa

2014

Apple Watch

2015

Apple FaceID

2017

https://www.washingtonpost.com/technology/2019/12/26/we-picked-most-influential-technologies-decade-it-isnt-all-bad/

AI Hype

"Adjusts settings, based on the load, to provide the most optimized washing cycle."

"We overestimated the arrival of autonomous vehicles." - Ford CEO Jim Hackett

Hype surrounding AI has peaked & troughed over the years as the abilities of the technology get overestimated and then re-evaluated.. *bbc.com/news/technology-51064369*

http://www.lgnewsroom.com/2019/09/lg-washing-machines-with-artificial-intelligence-and-direct-drive-motor-roll-out-region-wide/

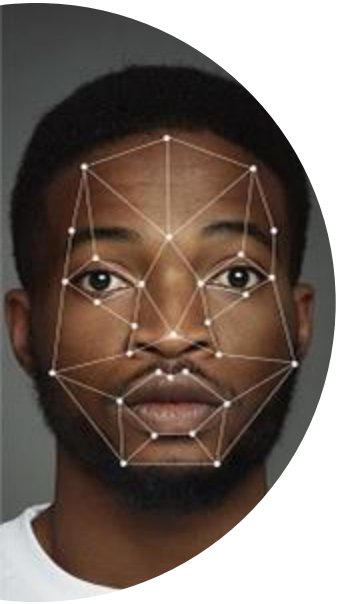
https://emerj.com/ai-adoption-timelines/self-driving-car-timeline-themselves-top-11-automakers/

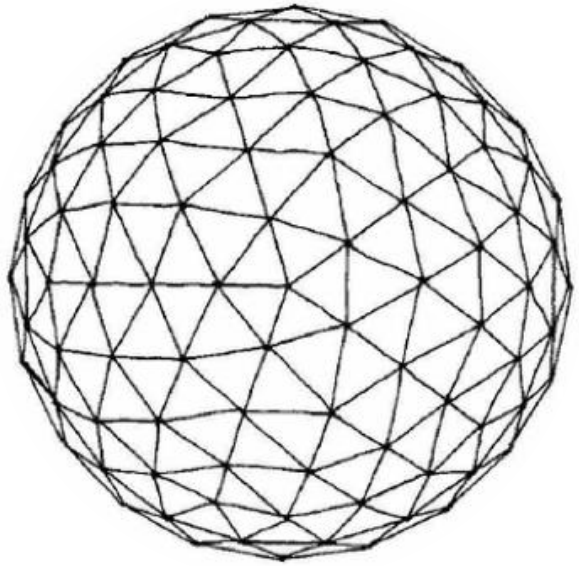
Pattern Recognition

By pattern recognition we mean the extraction of the significant features from a background of irrelevant detail. … it is the kind of thing that brains seem to do very well….that computing machines do not do very well yet. **O. G. Selfridge, 1955**

AI: General-purpose intelligence; P.R.: Domain-specific intelligence

Selfridge, “Pattern recognition and modern computers." In Proceedings of the Western Joint Computer Conf, pp. 91-93. March 1-3, 1955.

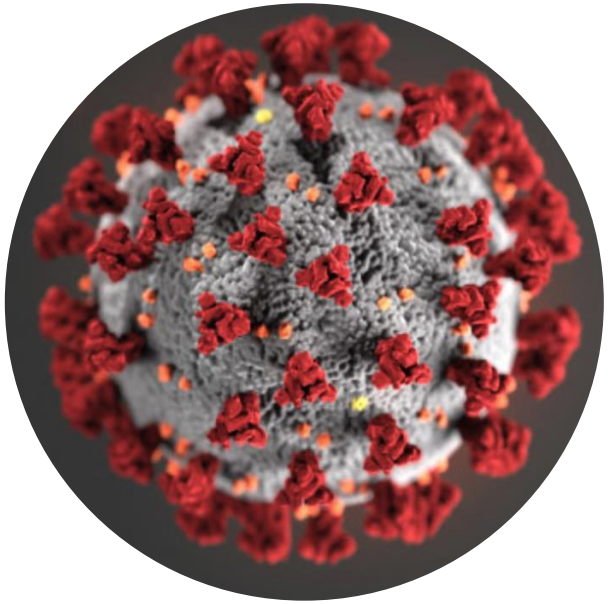




What is a Pattern?

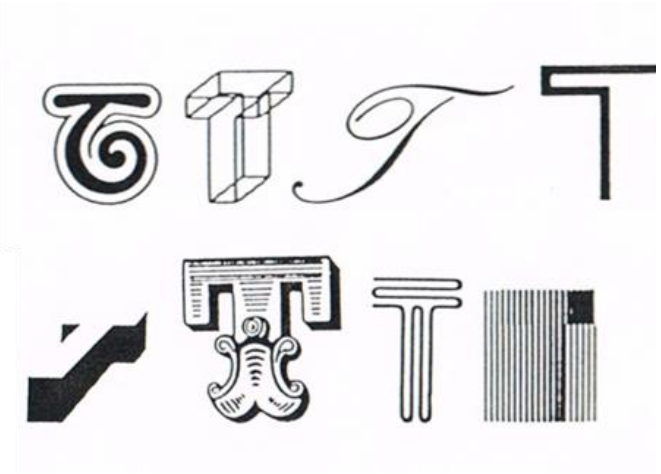
A pattern is the opposite of a chaos; it is an entity vaguely defined, that could be given a name.

S. Watanabe, 1985



Pattern Class

- Collection of similar, not necessarily identical, patterns
- Class is defined by a model or examples
- How to define similarity, fundamental to intelligent systems



American Elm

Ginkgo

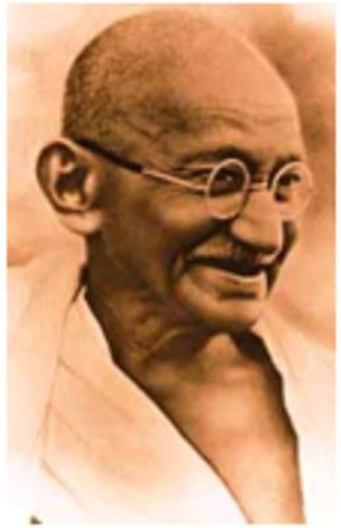
Wallow

Spruce

Larch

Birch

Palm








Intra-class Variability

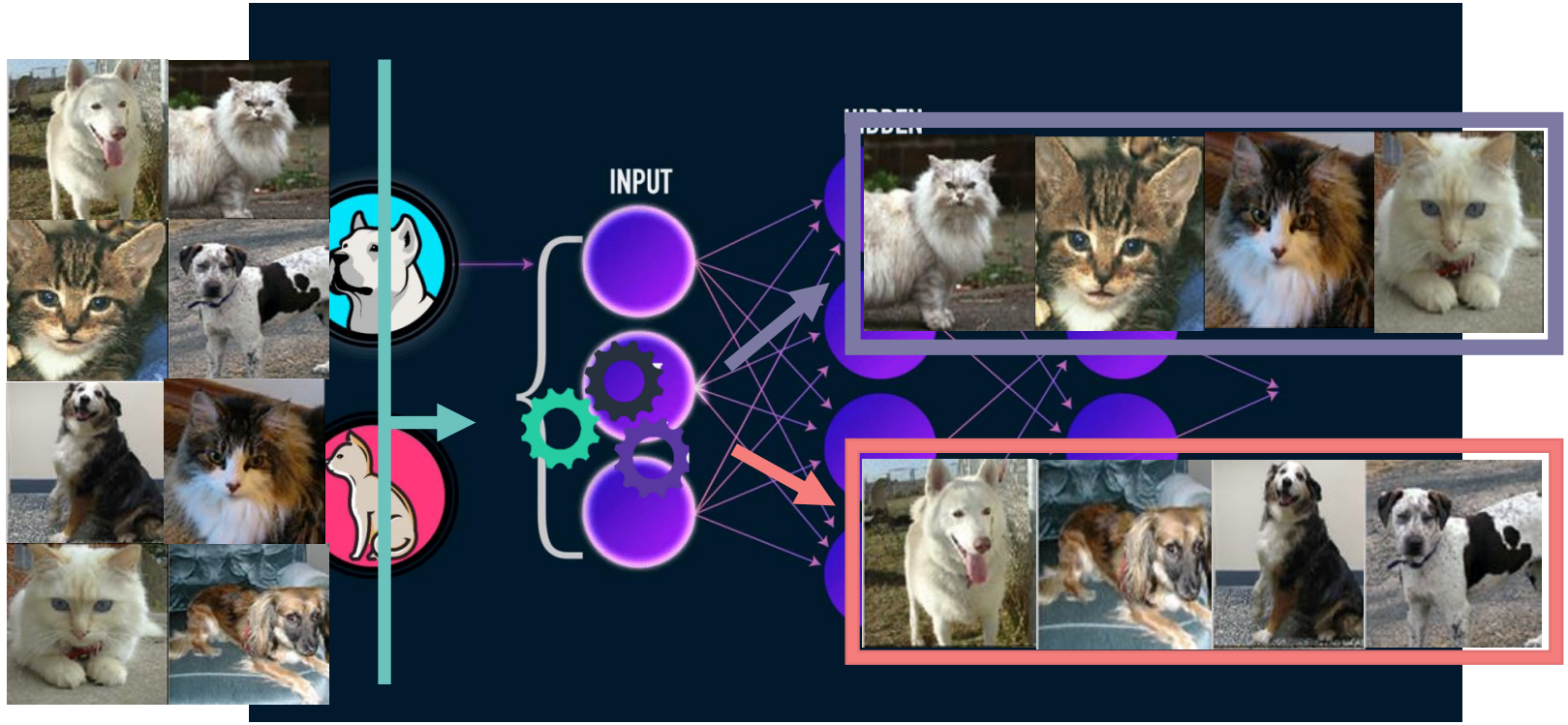
Inter-Class Similarity

Learn a compact & discriminative representation for pattern classes

www.cbsnews.com/8301-503543_162-57508537-503543/chinese-mom-shaves-numbers-on-quadruplets-heads

Recognition (Learning)

Assign patterns to known classes (classification) or group them to define classes (clustering)



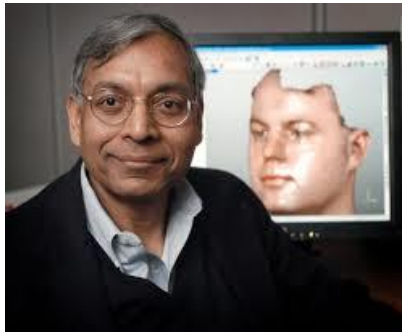
Clustering (Unsupervised learning)

Pairwise similarity

0.83

0.89

0.72



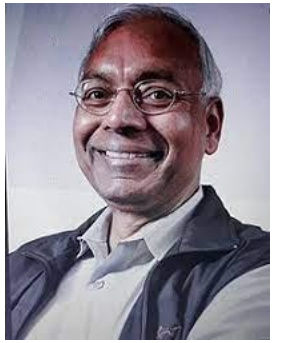
0.81

Probe

0.58

0.72

0.82



0.71

Threshold=0.54
@ FAR=1e-6

0.74

0.66

0.63

0.49

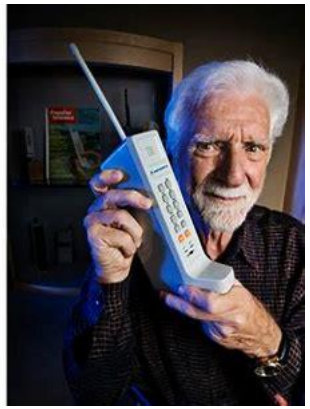
0.17

- **Representation**
- **Similarity measure**

https://roc.ai/

Gallery images

Biometric Recognition



The first mobile phone (1973)

Joseph Van Os / Getty Images

The Pantech GI100 (2004)

Touch ID, iPhone 5S (2013)

Apple Pay, iPhone 6 (2014)

Face ID, iPhone X (2017)

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
- **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 in 1991

Hand geometry recognition

Manual fingerprint comparison

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

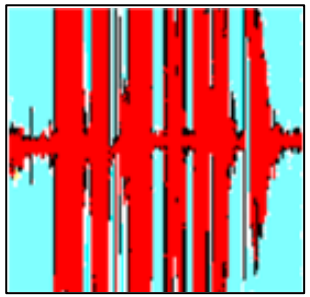
Biometric Recognition

- 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*

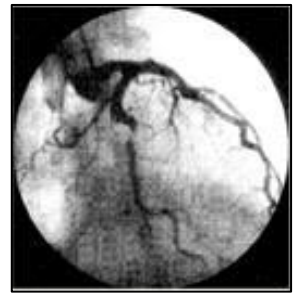
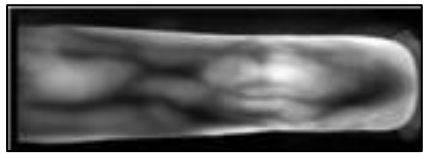
Stigler, “The Problematic Unity of Biometries”, BIOMETRIC5, S6 , Sept. 2000; Pollack, “Technology: Recognizing the Real You”, NYT, Sep. 24, 1981

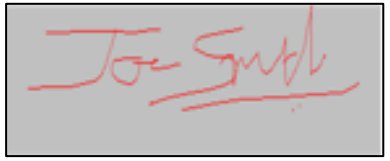
Biometric Traits

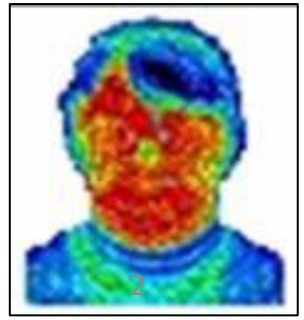




Multi-factor (Face +PIN) and Multi-modal (palmprint + palm vein) identification

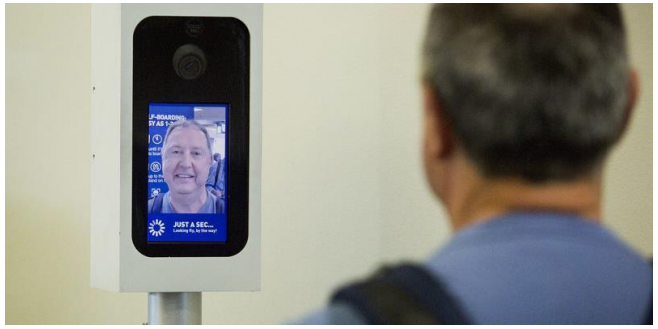
Which Biometric Trait?

- 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



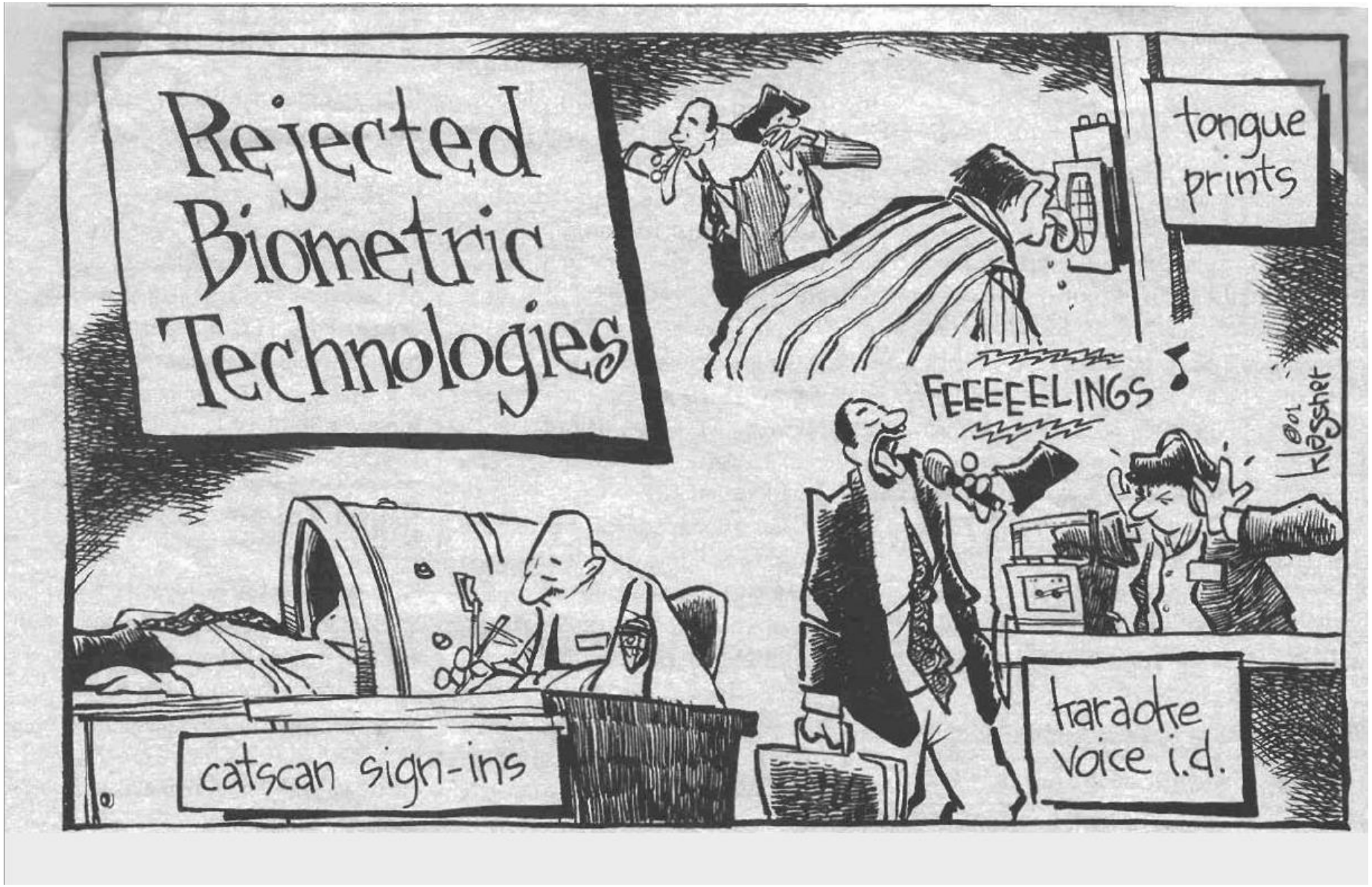
Australia: SmartGate

Amsterdam: Privium border passage

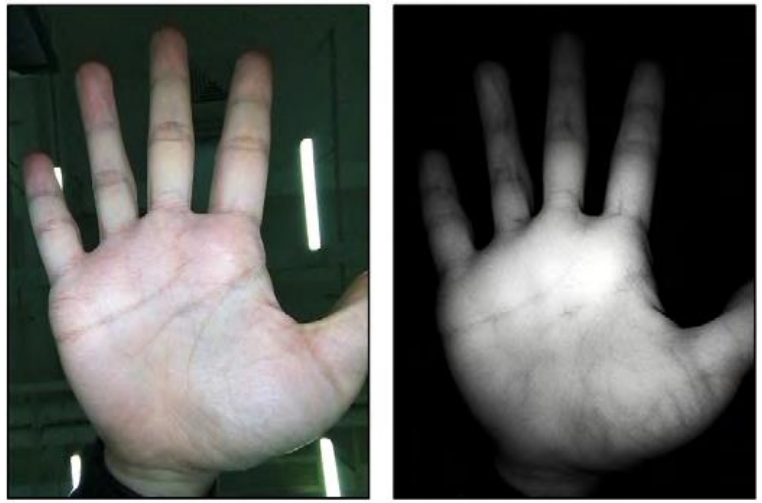
1. *Satisfy individuality and permanence properties*
2. Demostrate high accuracy in NIST evaluations
3. Fast search (1:N comparison) of large legacy databases (in millions)

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



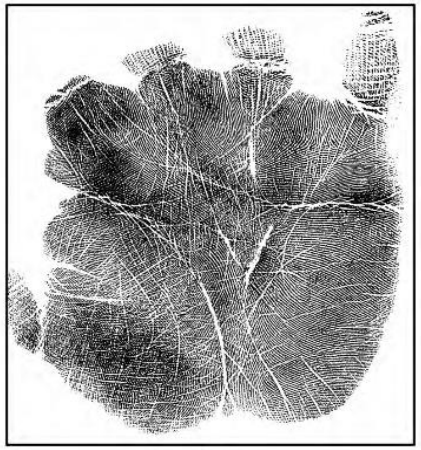
Growing Interest in Palm Biometric



(a) (b)

(a) Palmprint, (b) Palmvein

(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?

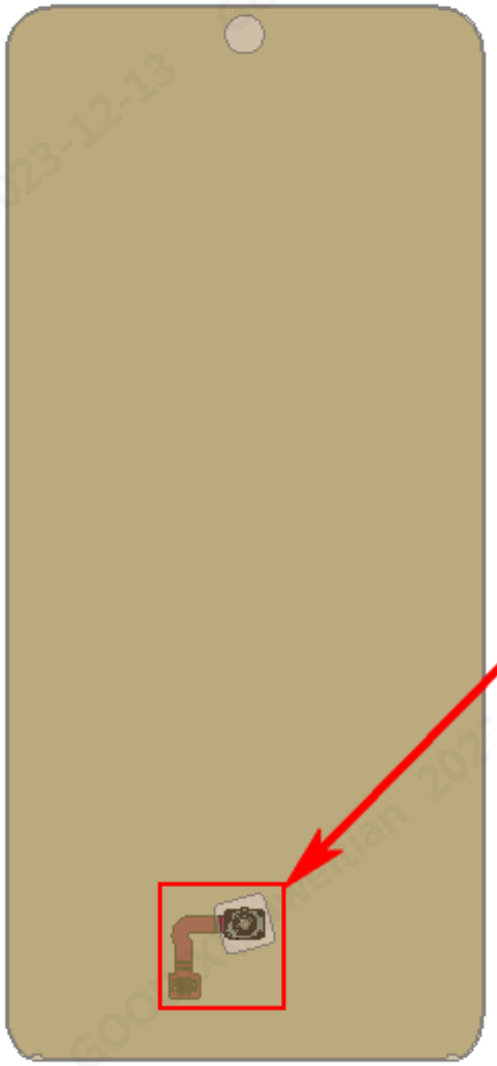
Fingerprint enabled ATM

Drivers of Biometric Recognition

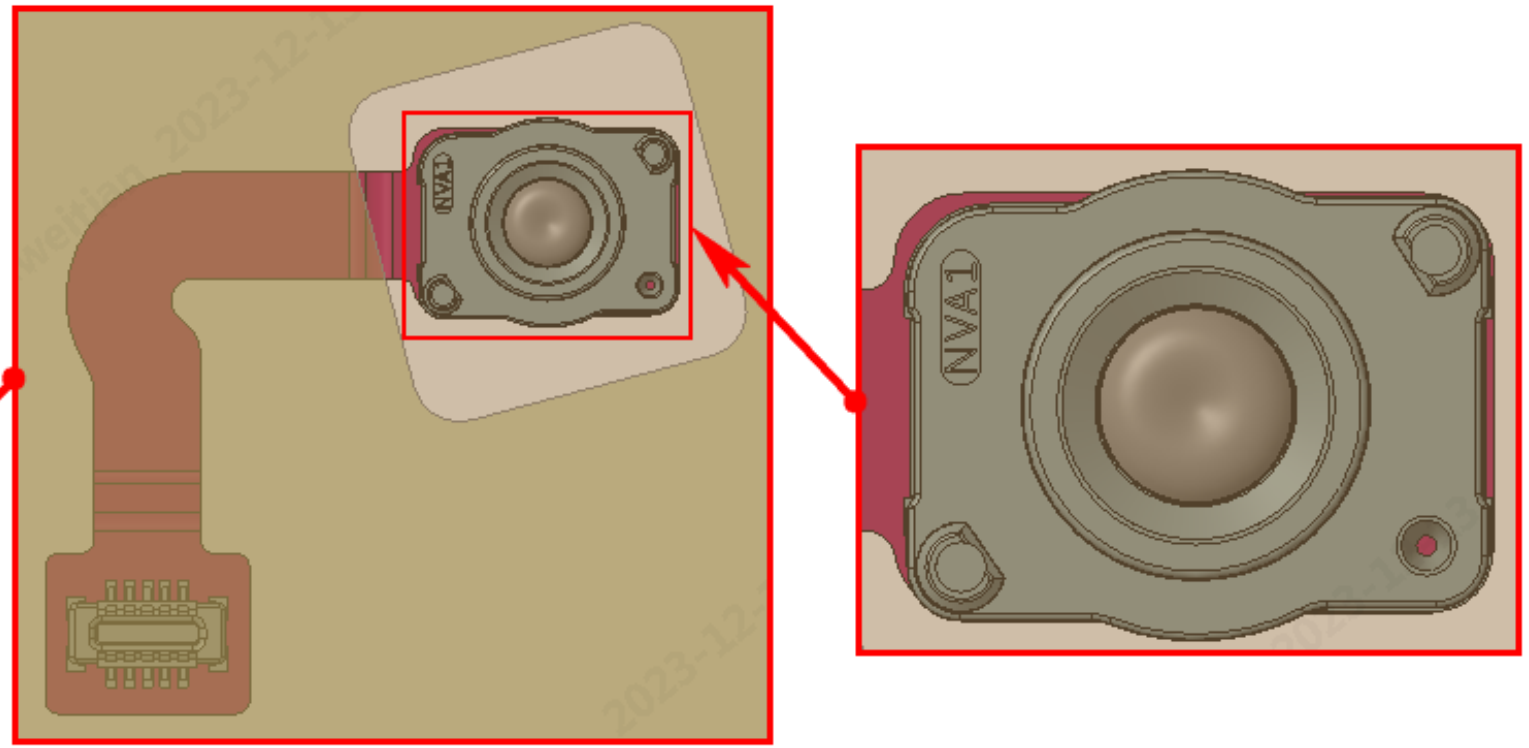
Requirements: Accuracy, throughput, cost, integration, usability, security, privacy

Enablers of Biometric Recognition

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



FP module pasted on screen frame



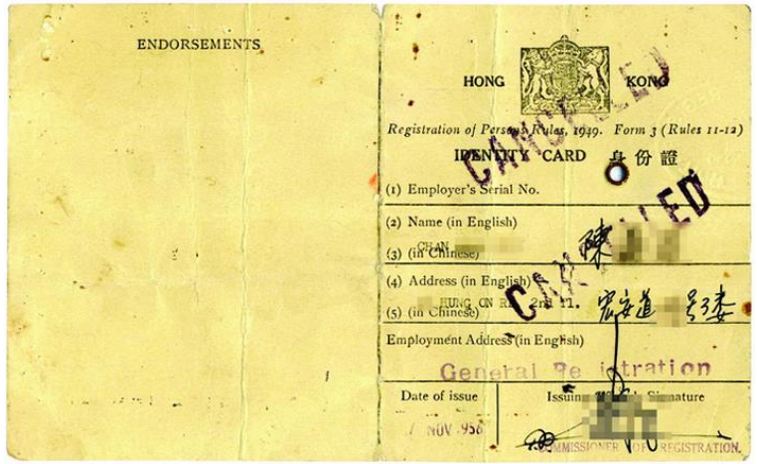
Length: 5.8 mm
Width: 4.3 mm
Depth: 4.2 mm

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

Enablers of Biometric Recognition

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

HK ID Cards: Paper to Smart Card



Paper Identity Card (1949)

Laminated Identity Card (1960)

Smart Identity Card (2003)

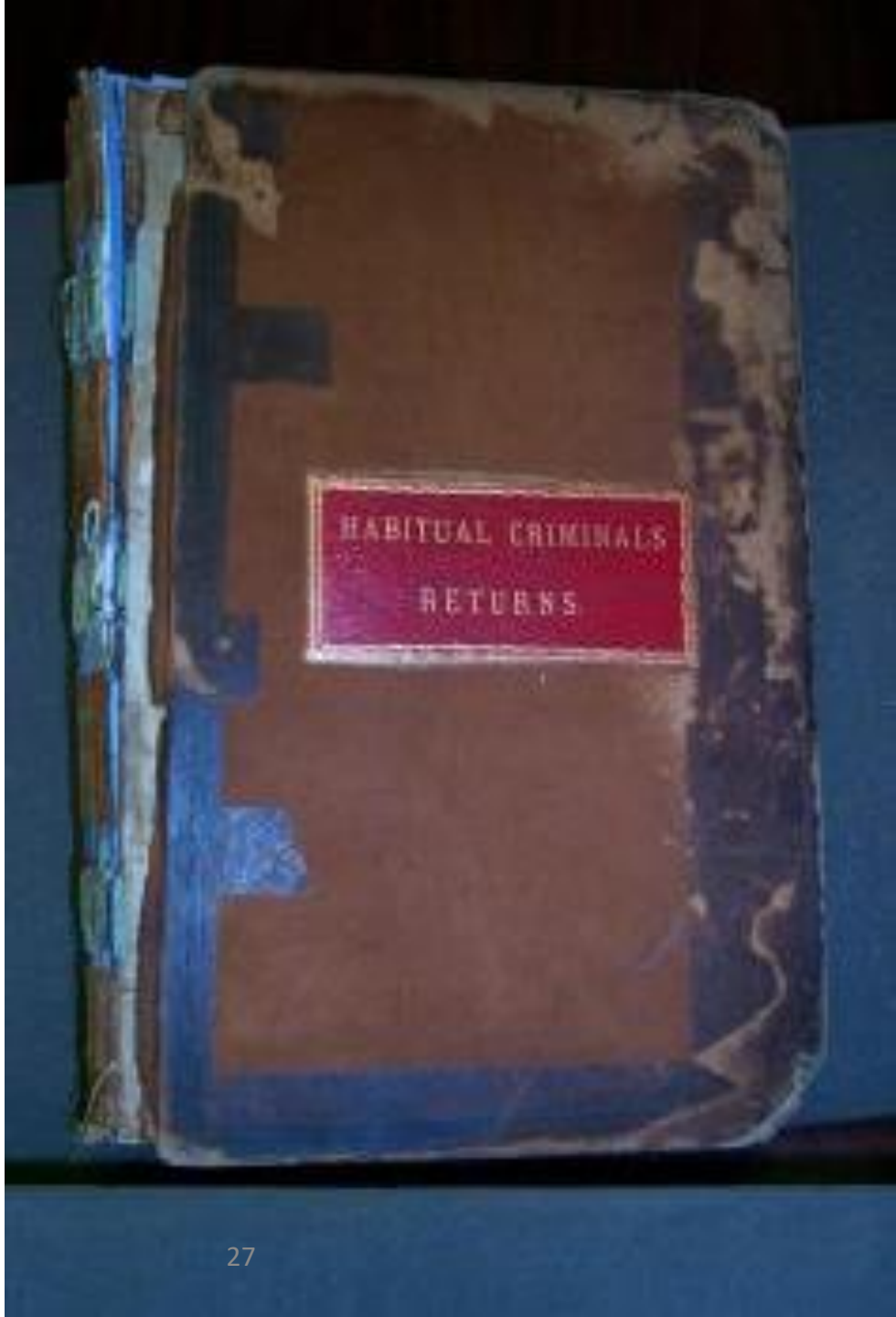
New Smart Identity Card (2018)

Better durability, security features for protection of personal data.

Biometric Recognition is Not New

Habitual Criminal Act (1869)

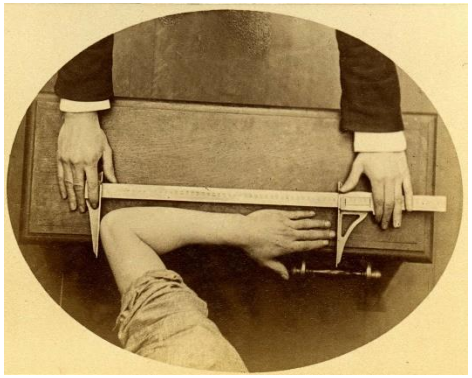
"What is wanted is a means of classifying the records of habitual criminals, such that as soon as the particulars of the personality of any prisoner (whether description, measurements, marks, or photographs) are received, it may be possible to ascertain readily, and with certainty, whether his case is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

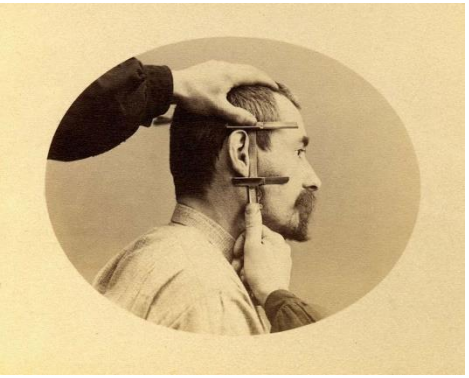


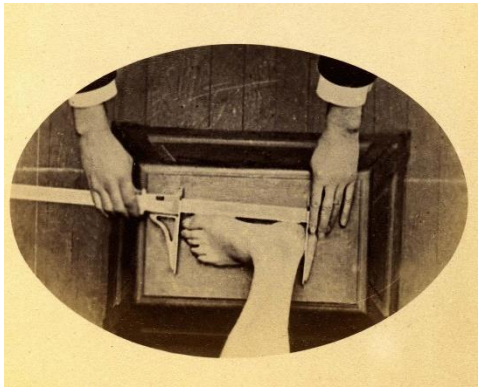
https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1968&context=ohlj

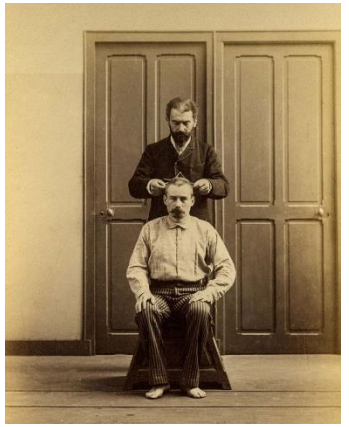
The Bertillon System that Cataloged Criminals by their Physical Measurements (1879)

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/

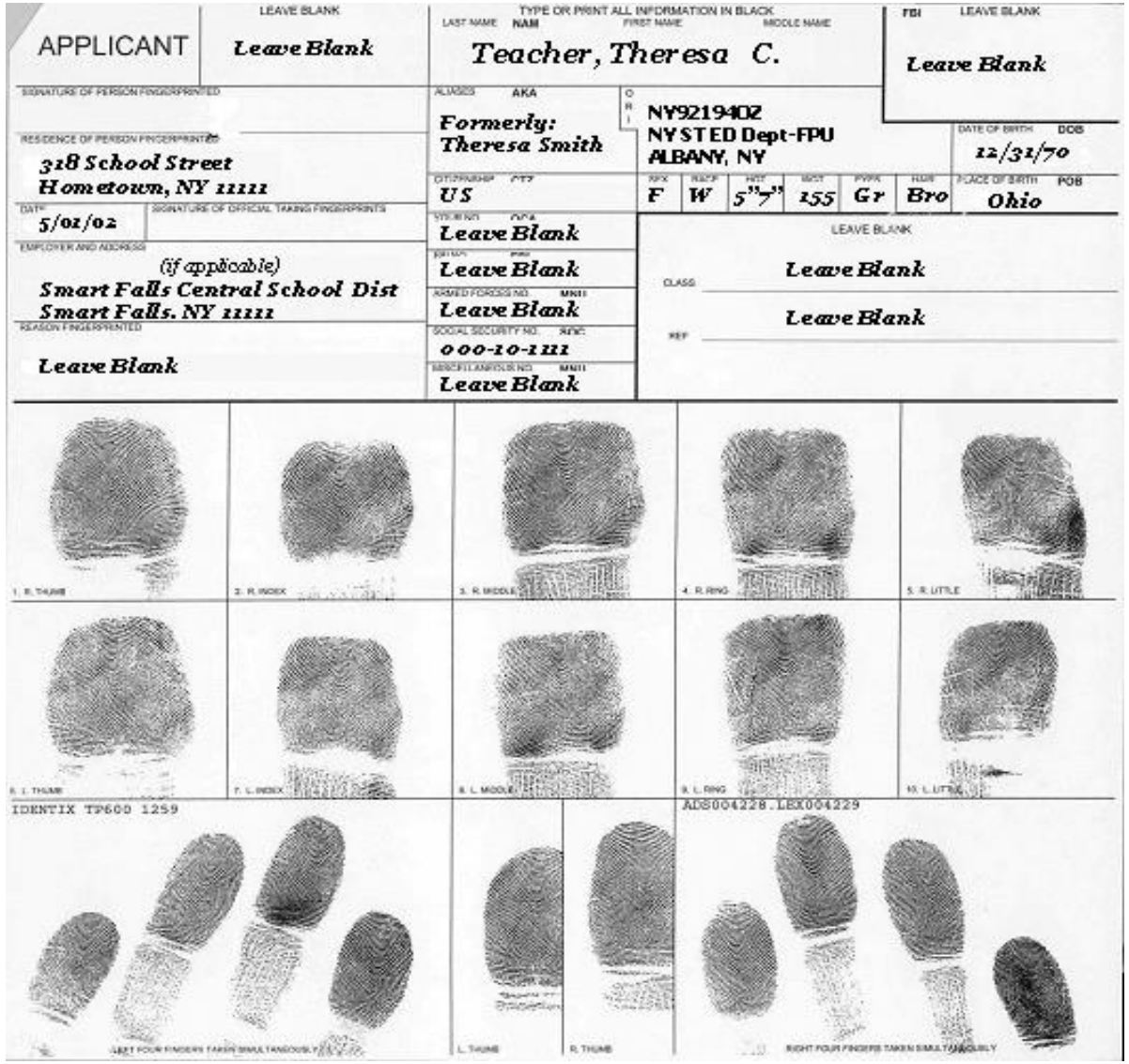
Fingerprints (1880)

"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

Teacher, Theresa C.

Leave Blank

Formerly: Theresa Smith

NY9219402
NYSTED Dept-FPU
ALBANY, NY

318 School Street
Hometown, NY 11111

5/01/02

12/31/70

F W 5'7" 155 Gr Bro

Ohio

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

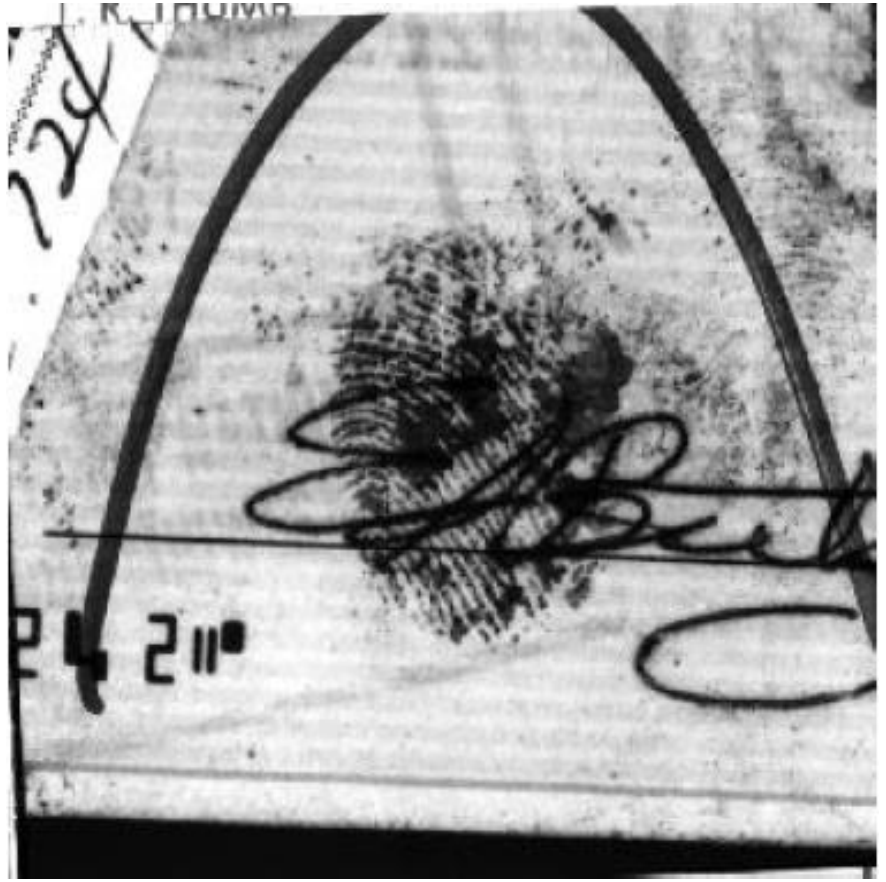
000-10-1111

Leave Blank

IDENTIX TP600 1259

ADS004228.LEX004229

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."*

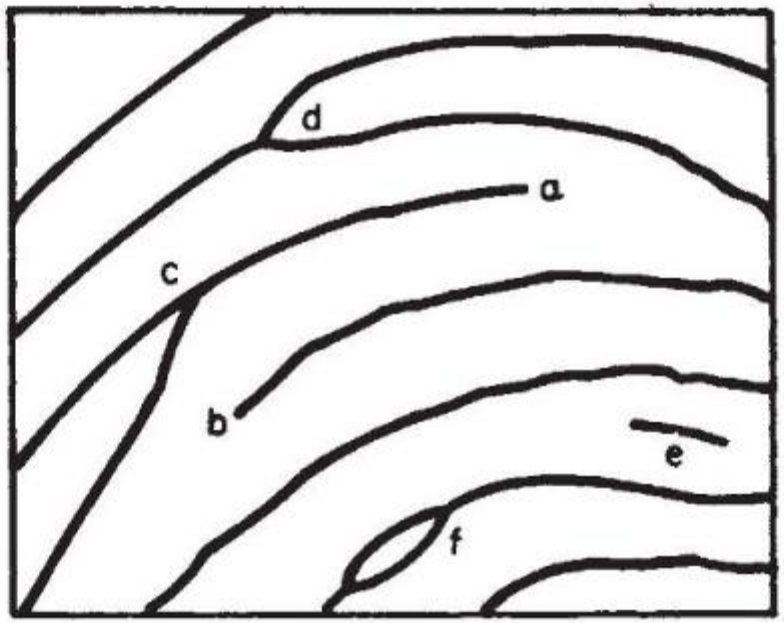
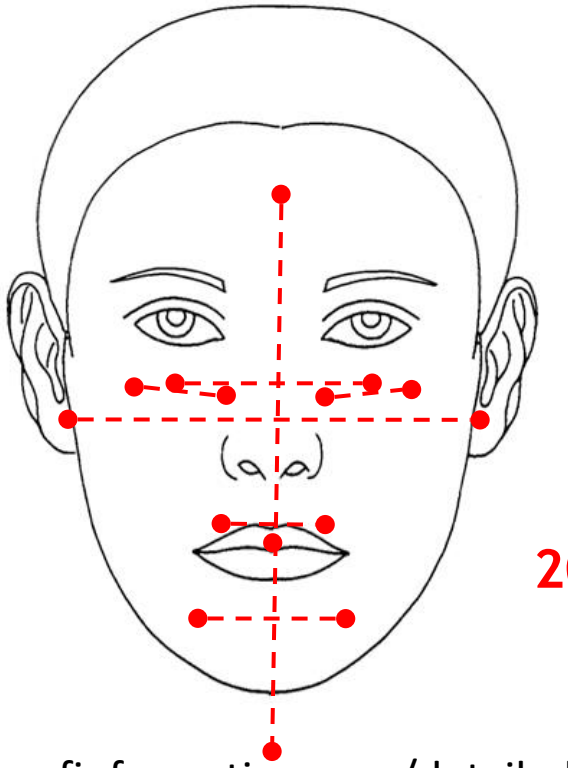


Fig. 1. Portion of fingerprint pattern (diagrammatic, enlarged) after Galton, showing minutiæ. *a* and *b* are ridge ends, *c* and *d* are ridge branchings or valley ends, *e* is an island, and *f* is an enclosure. The ridge end and valley end are the principal minutia types, accounting for almost all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



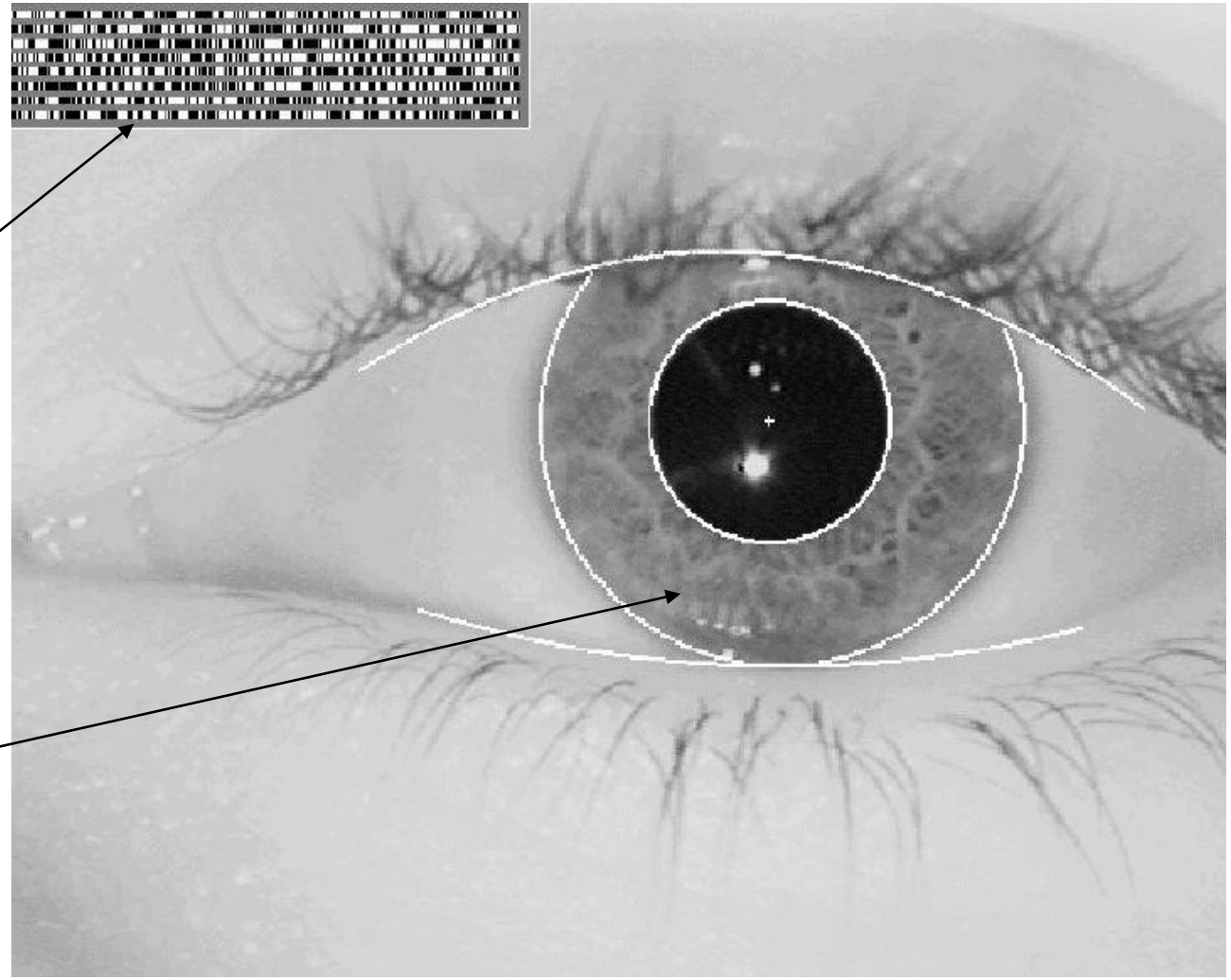
20 inter-point distances for matching

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

Identimate (1972)

First commercial use of biometrics

Iris Recognition (Daugman,1993)



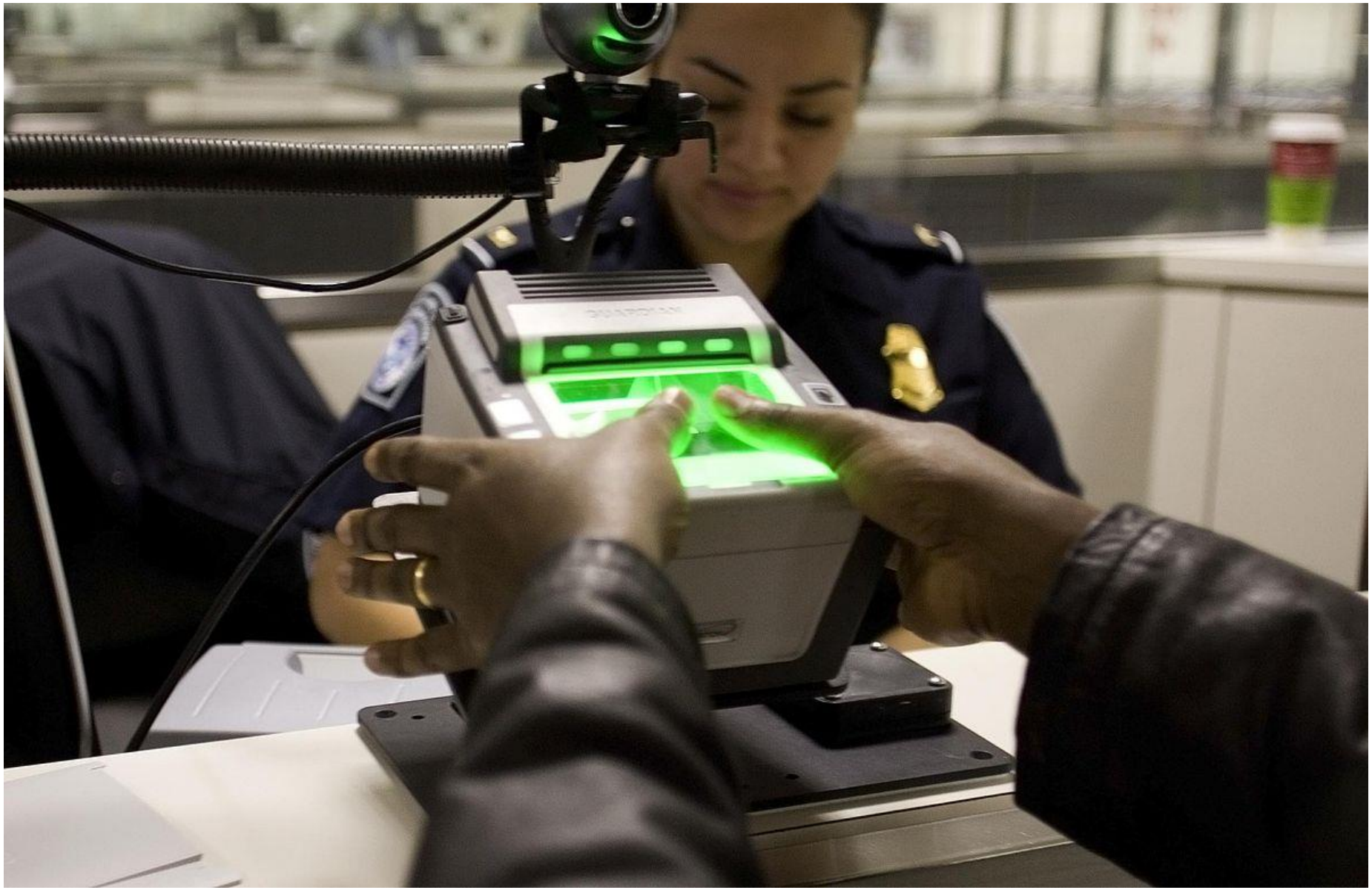
2048-bit representation of iris texture

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.

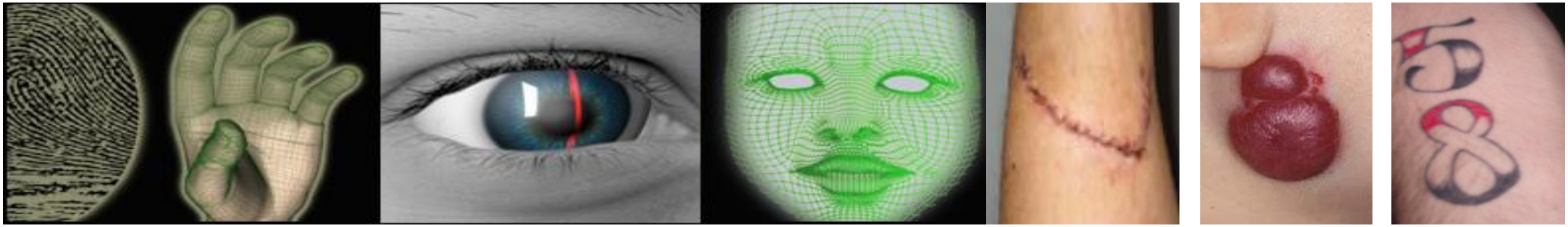
9/11 Terrorist Attacks (2001)

US-VISIT (2003)



Walt Disney Theme Park (2005)

FBI Next Generation Identification (2008)

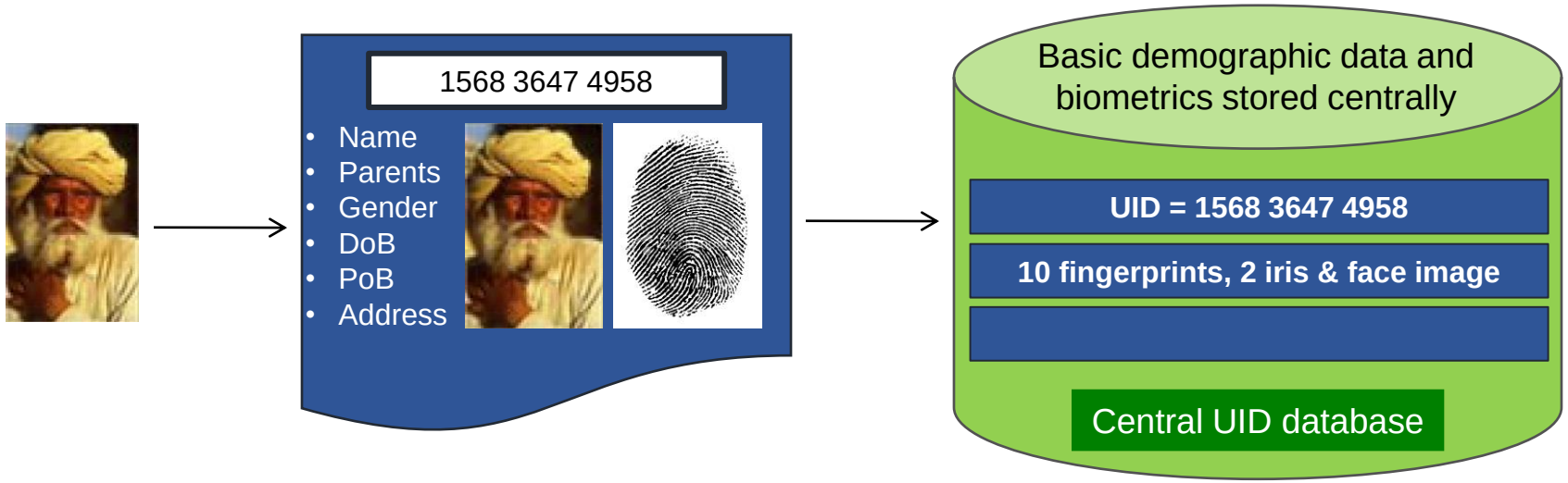


First AFIS in1980s; IAFIS launched in 1999; use of **soft biometrics** (SMT)

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."



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

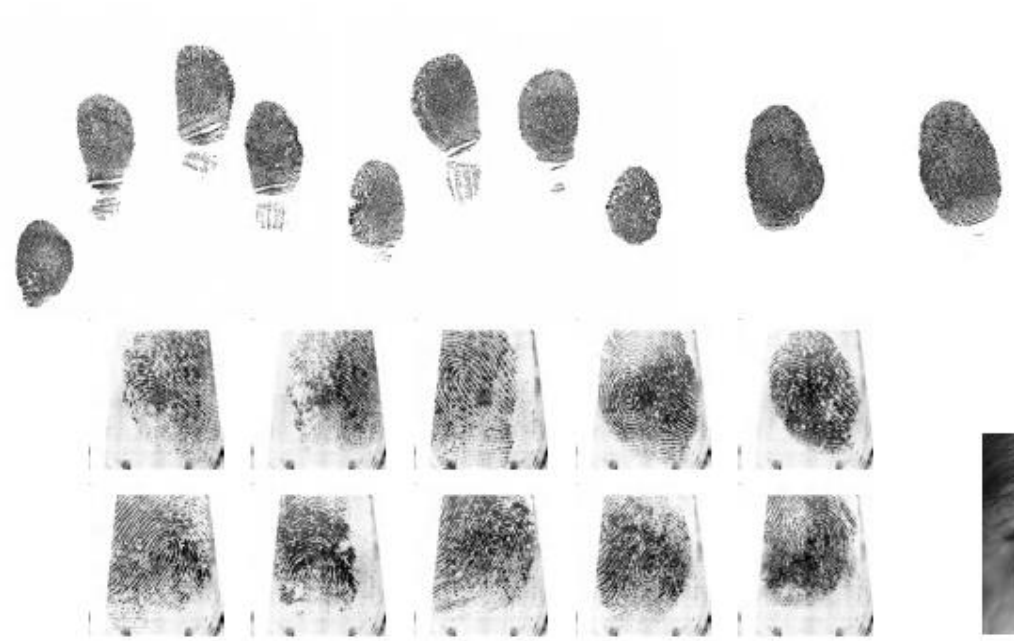
https://uidai.gov.in/

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

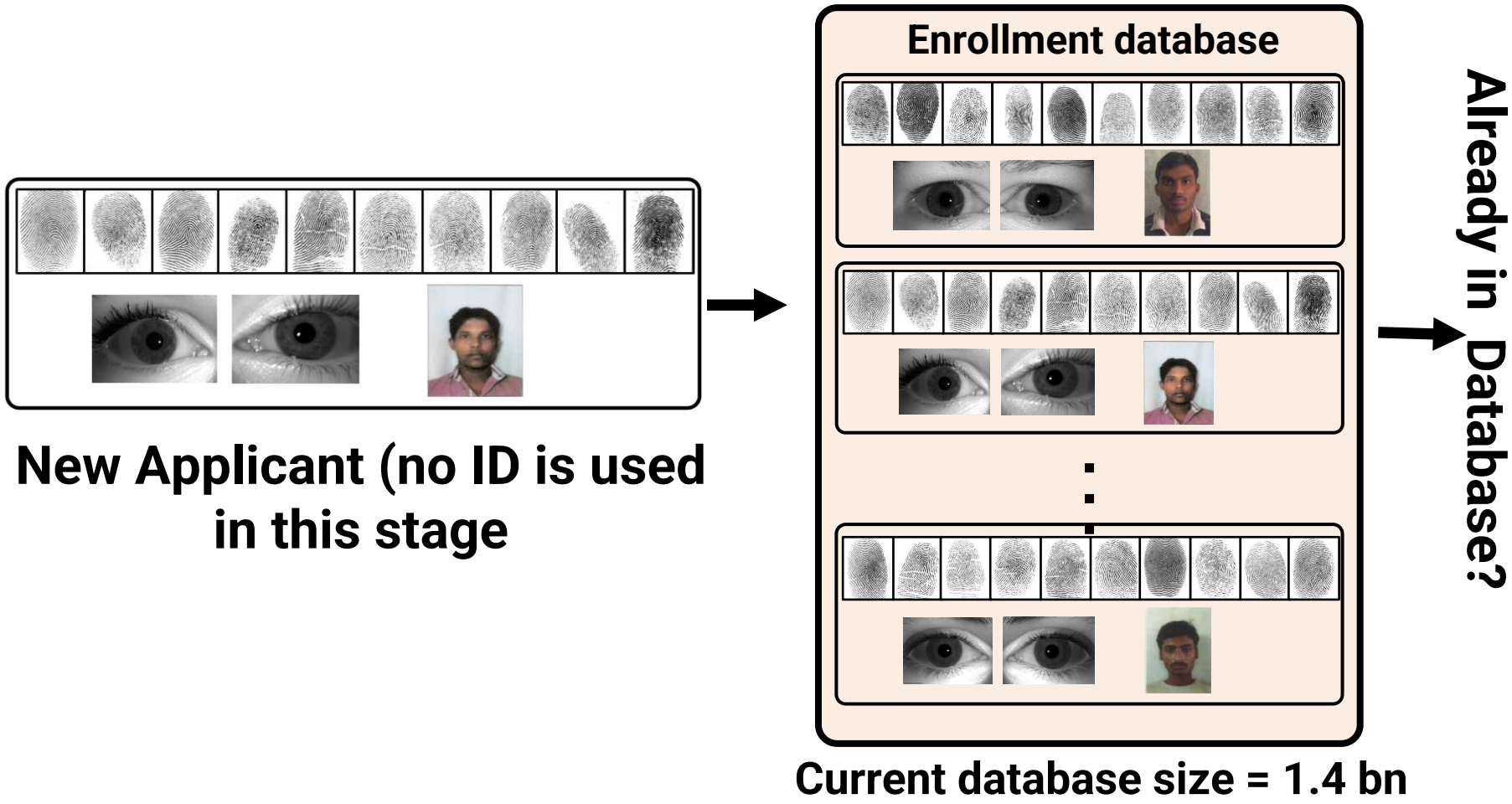
How Does Aadhaar Work?

Enrollment



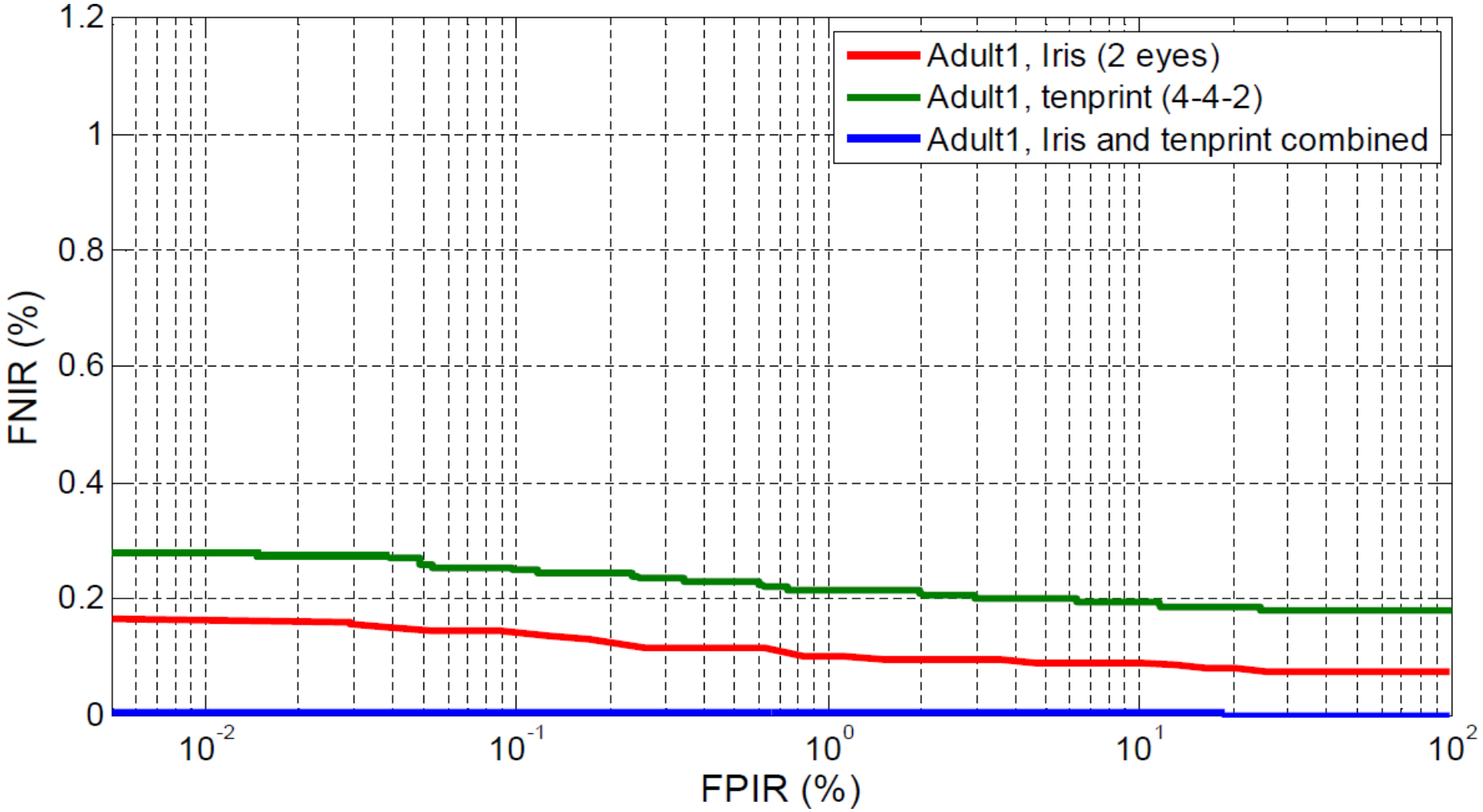
- 10 slap (4-4-2) fingerprints, 2 irises & face image are captured along with minimal demographic information
- Minimum age of enrollment is 5 years; re-enrollment at age 15;

De-duplication (1:N Comparison)



- 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

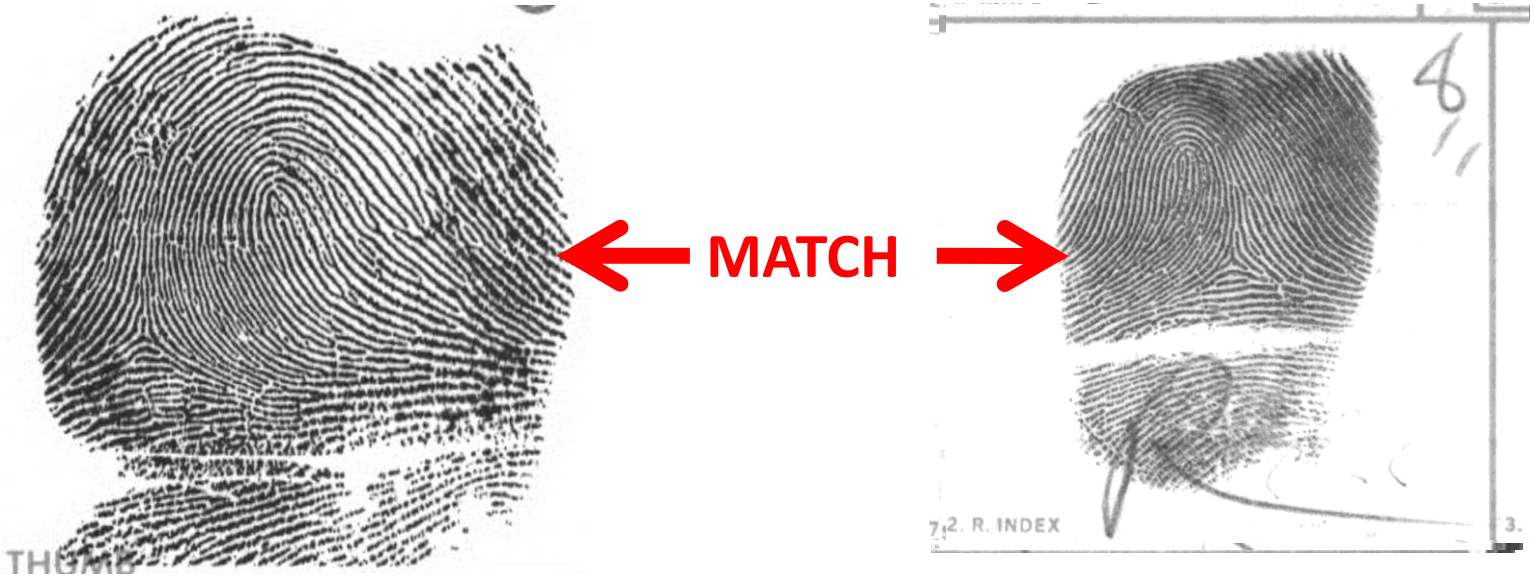
Person claims he is John

John’s enrolled fingerprint

Representation (set of features) and similarity measure

Fingerprint Identification

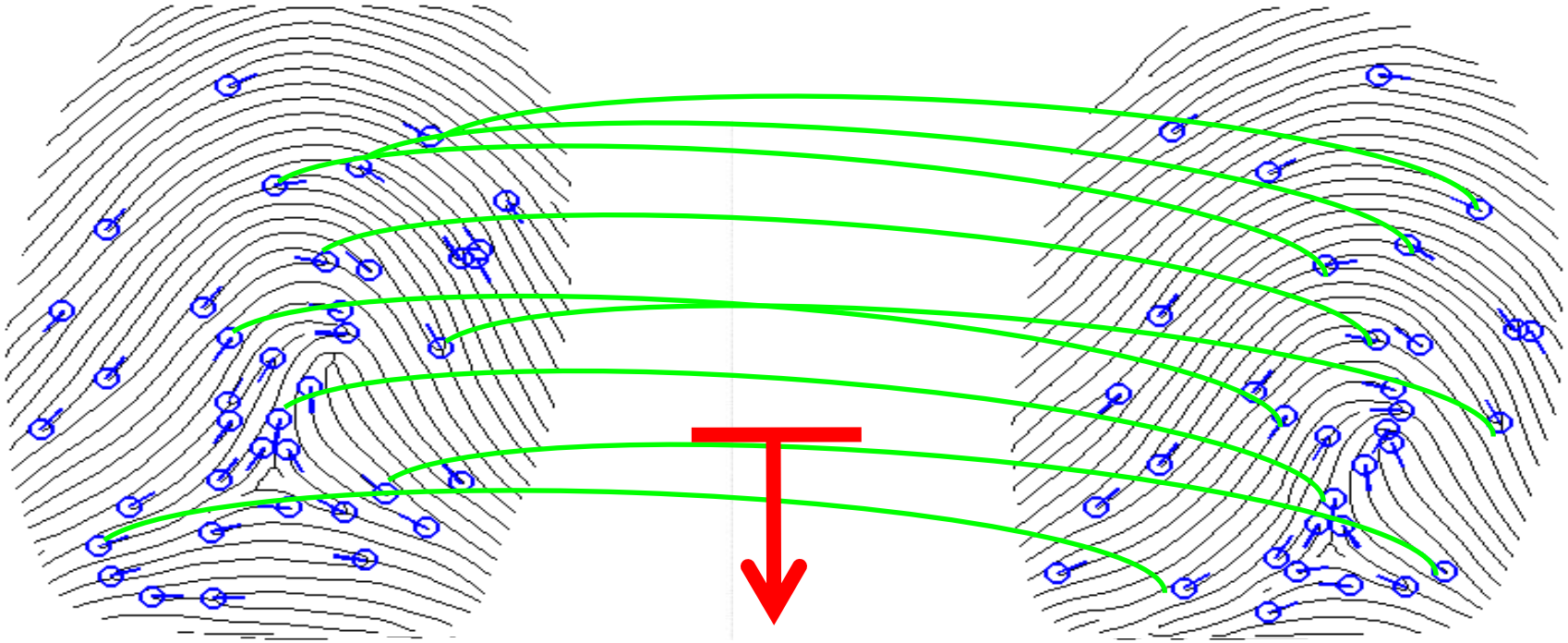
Query *Database*



No claim of identity made

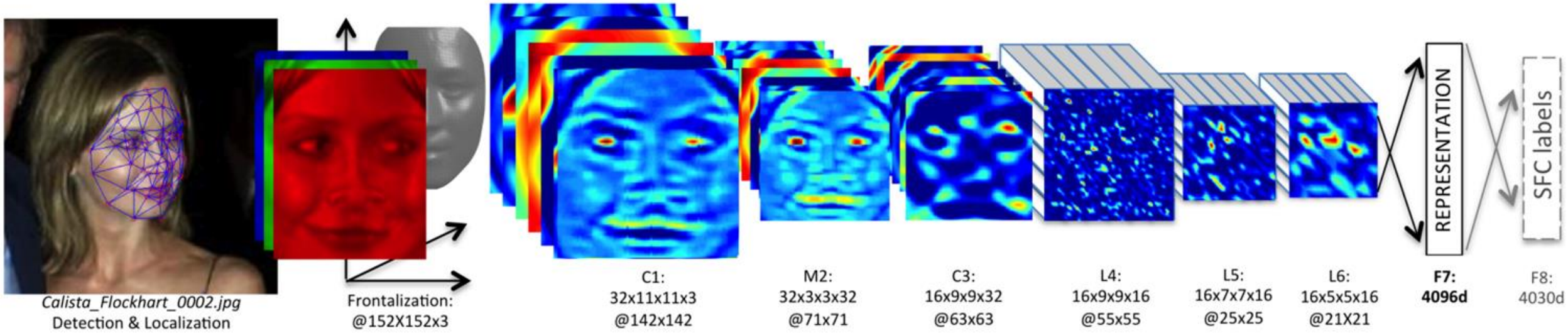
- Who Does this fingerprint belong to?
- Query may or may not be present in the database (gallery)

Fingerprint Authentication (1:1 comparison)



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

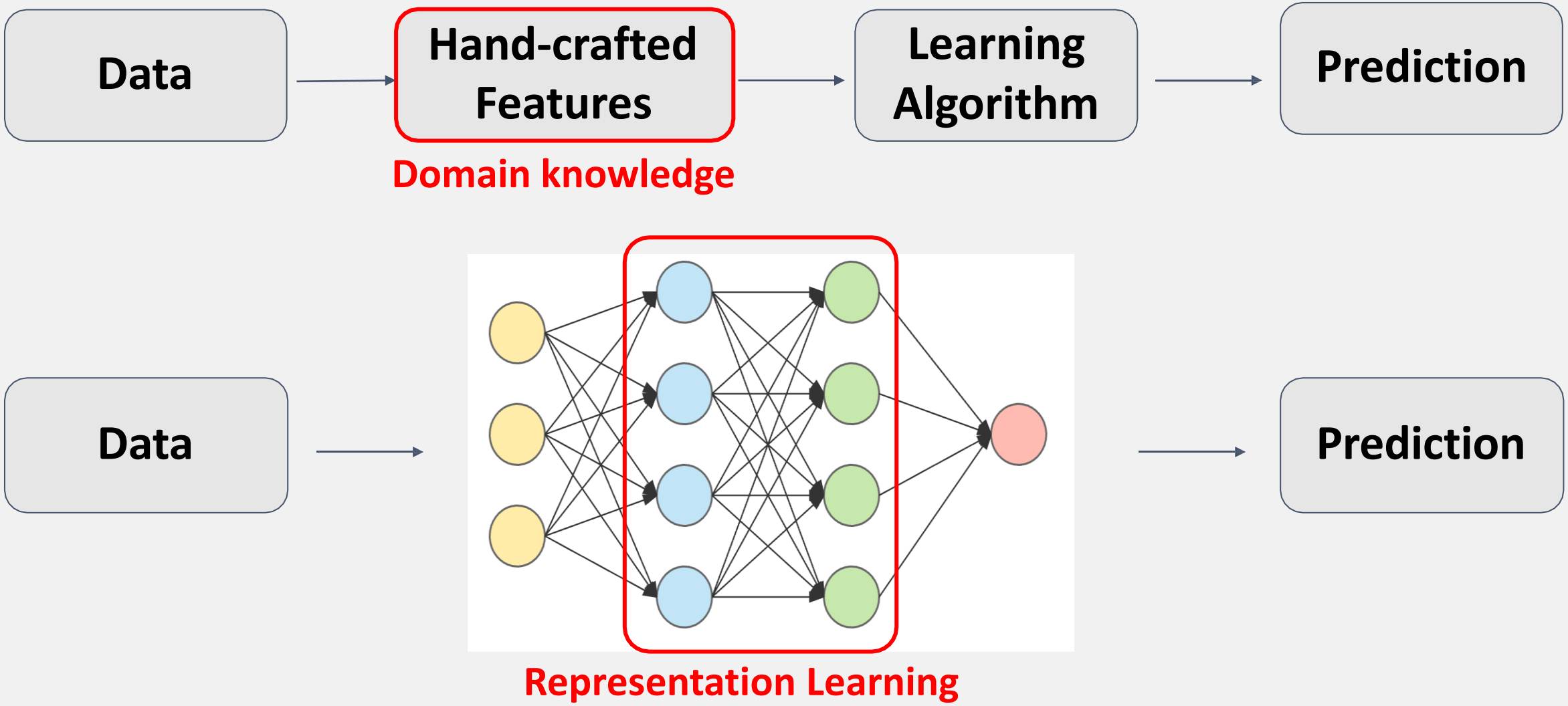
Deep Networks in Biometrics
Deepface (2014)



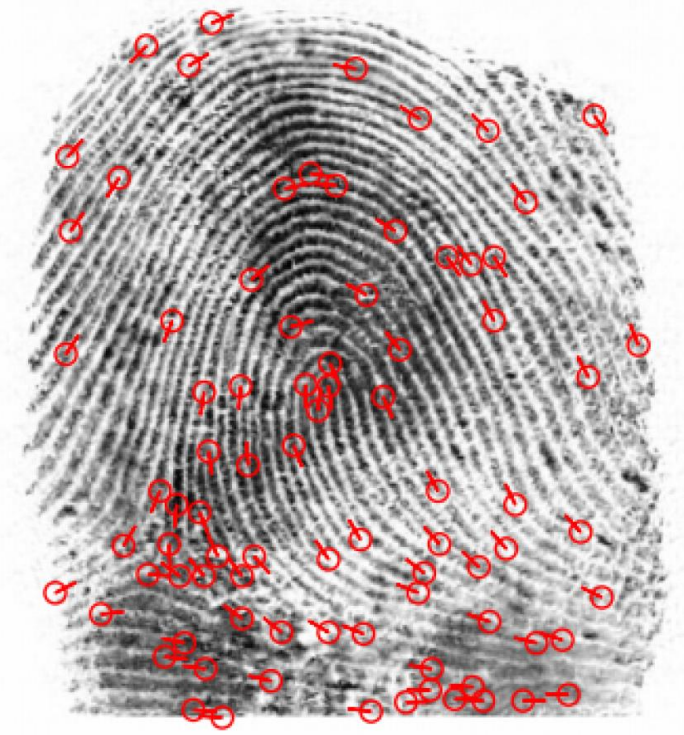
- Multiple layers of neurons stacked together and connected to a small area in previous layer (120M parameters)
- Progress in face recognition: deep features, web crawled data, processing power
- **What about network design, loss function, embedding domain knowledge..**

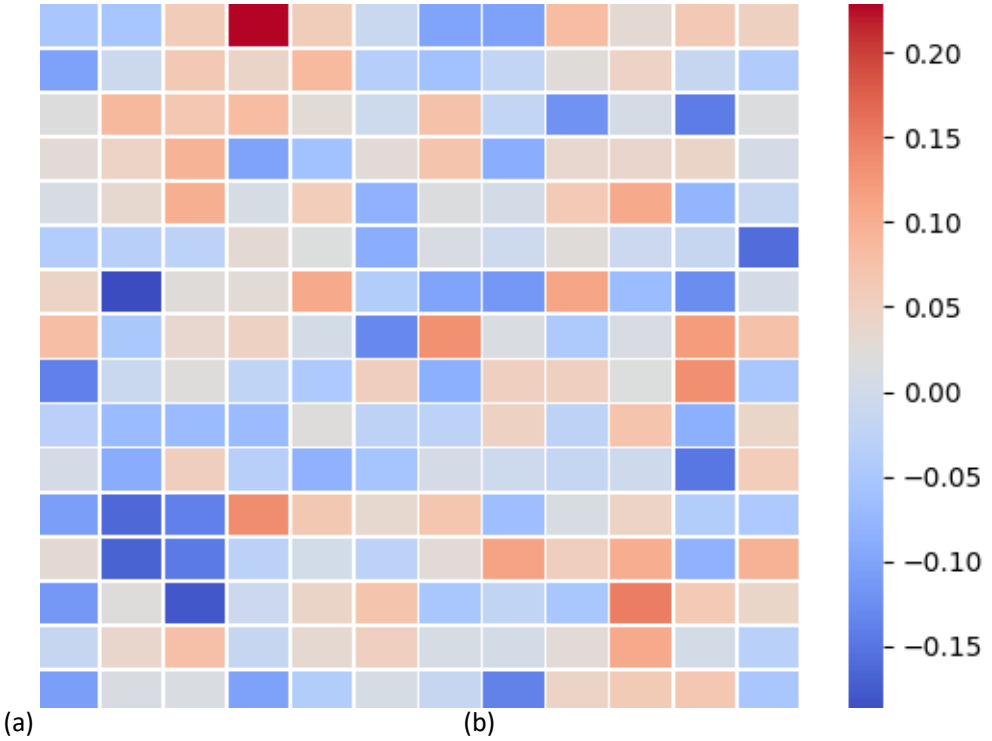
Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. "Deepface: Closing the gap to human-level performance in face verification." CVPR, 2014

Representation



Two Representations for Fingerprints

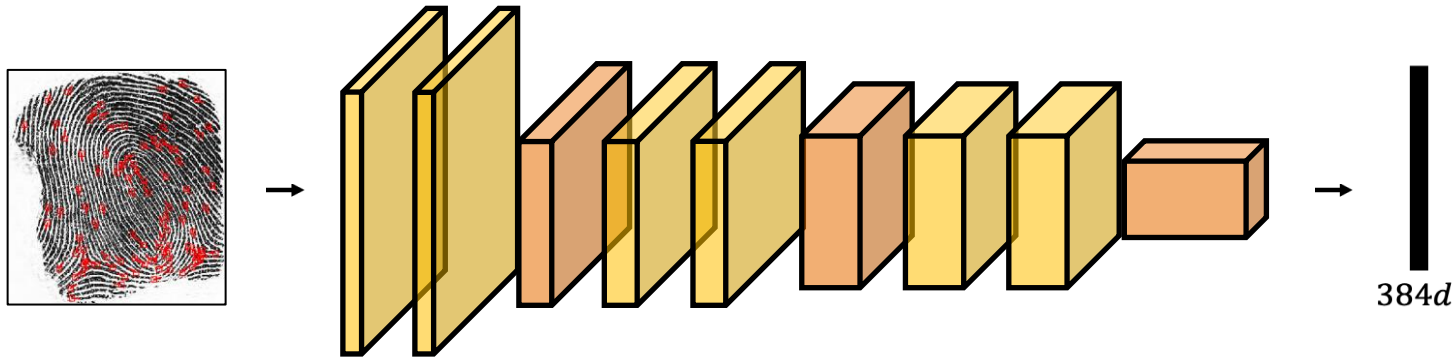




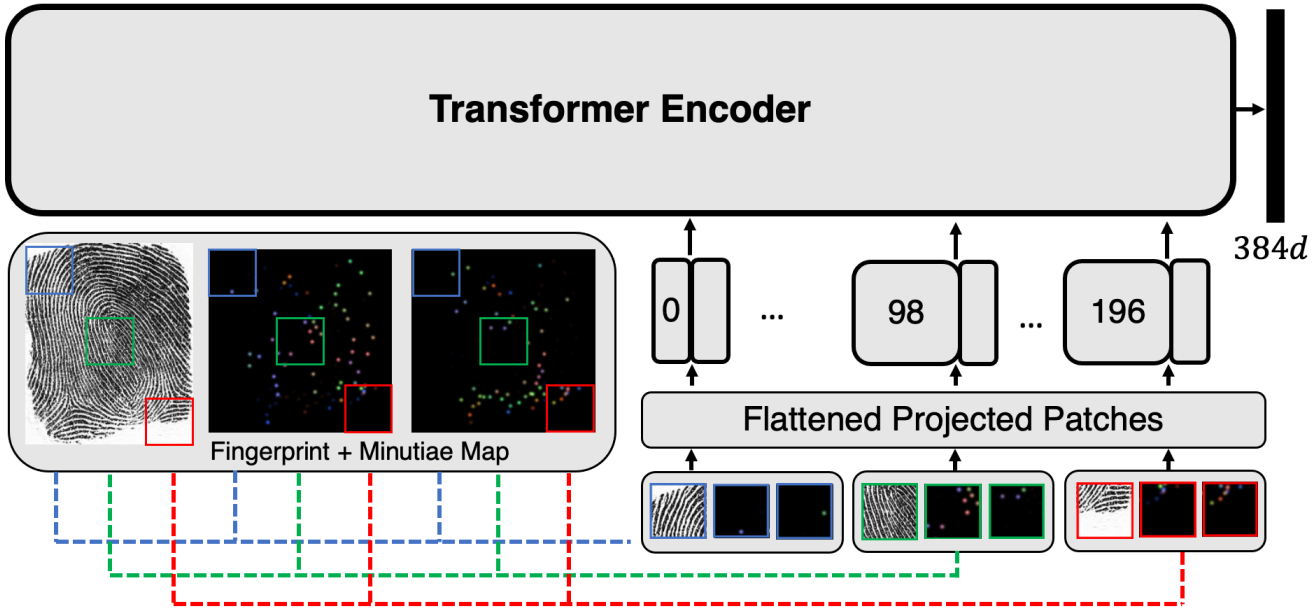
- Minutiae representation vs. 192-dim (192 bytes) embeddings
- Comparing embeddings is 3-times faster than minutiae comparison

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

Networks for Learned Fingerprint Features

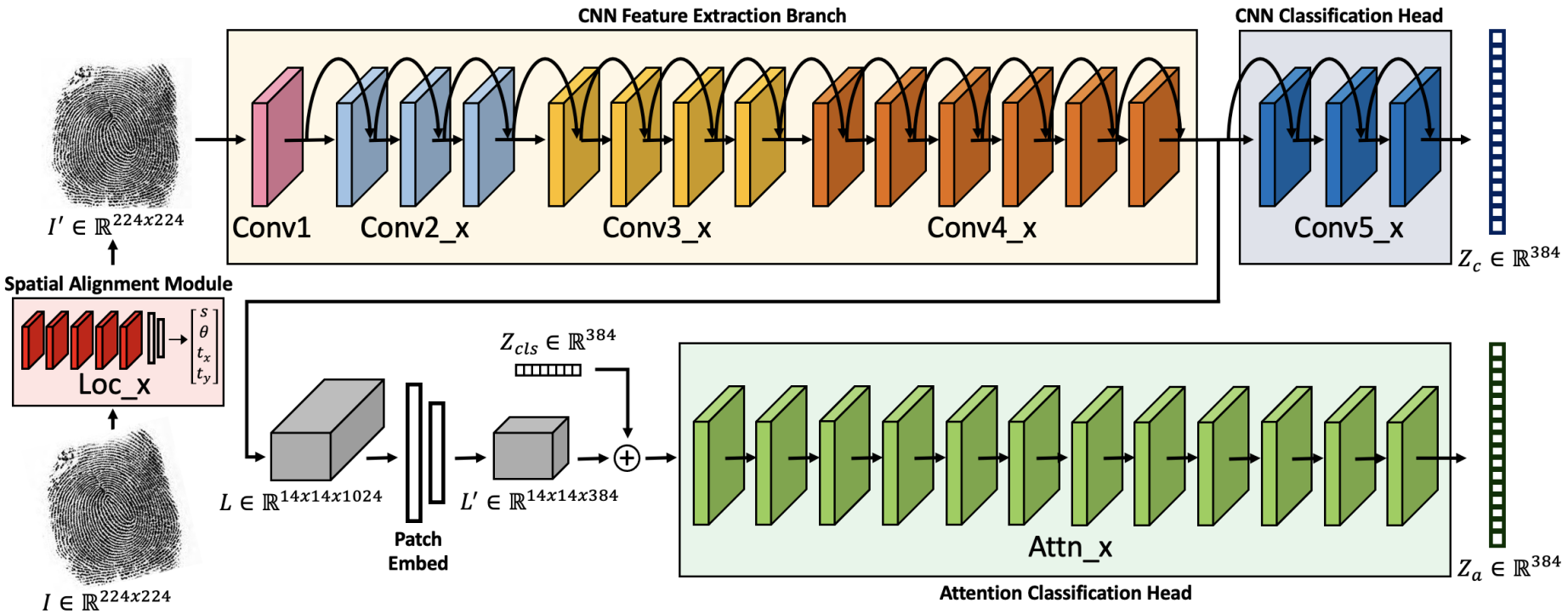


(a) CNN (ResNet-v50, Inception-V4, DeepPrint, etc.)



(b) Vision Transformer (ViT)

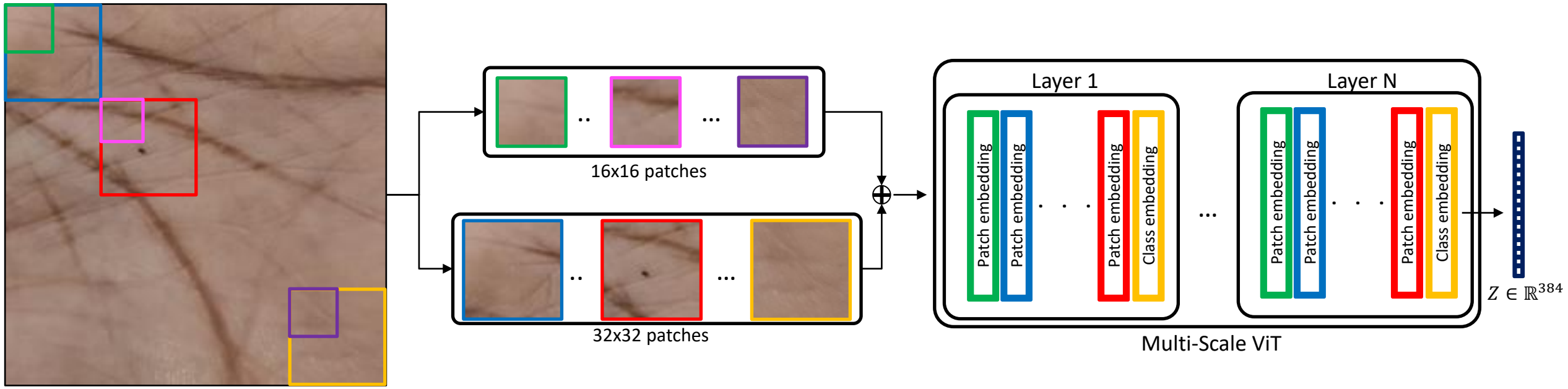
Fusion of Different Learned Features



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

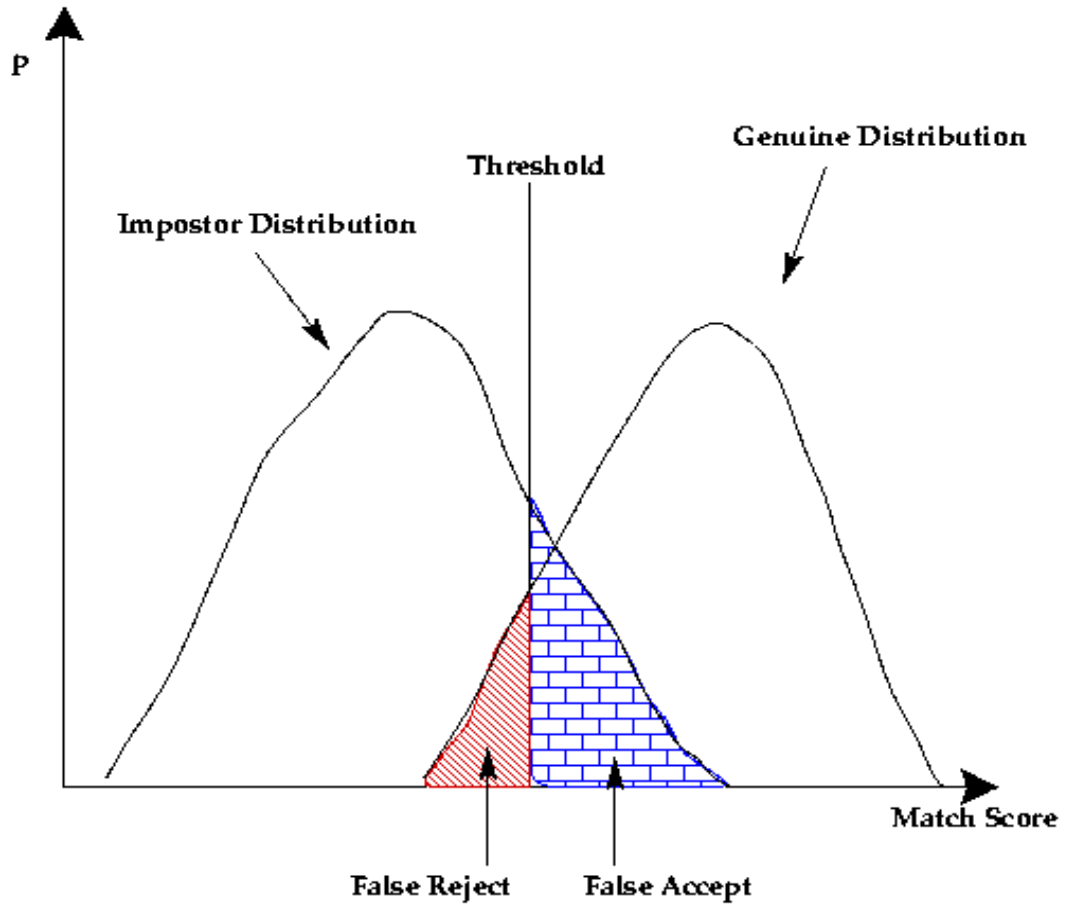
COTS
(updates rankings)

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)

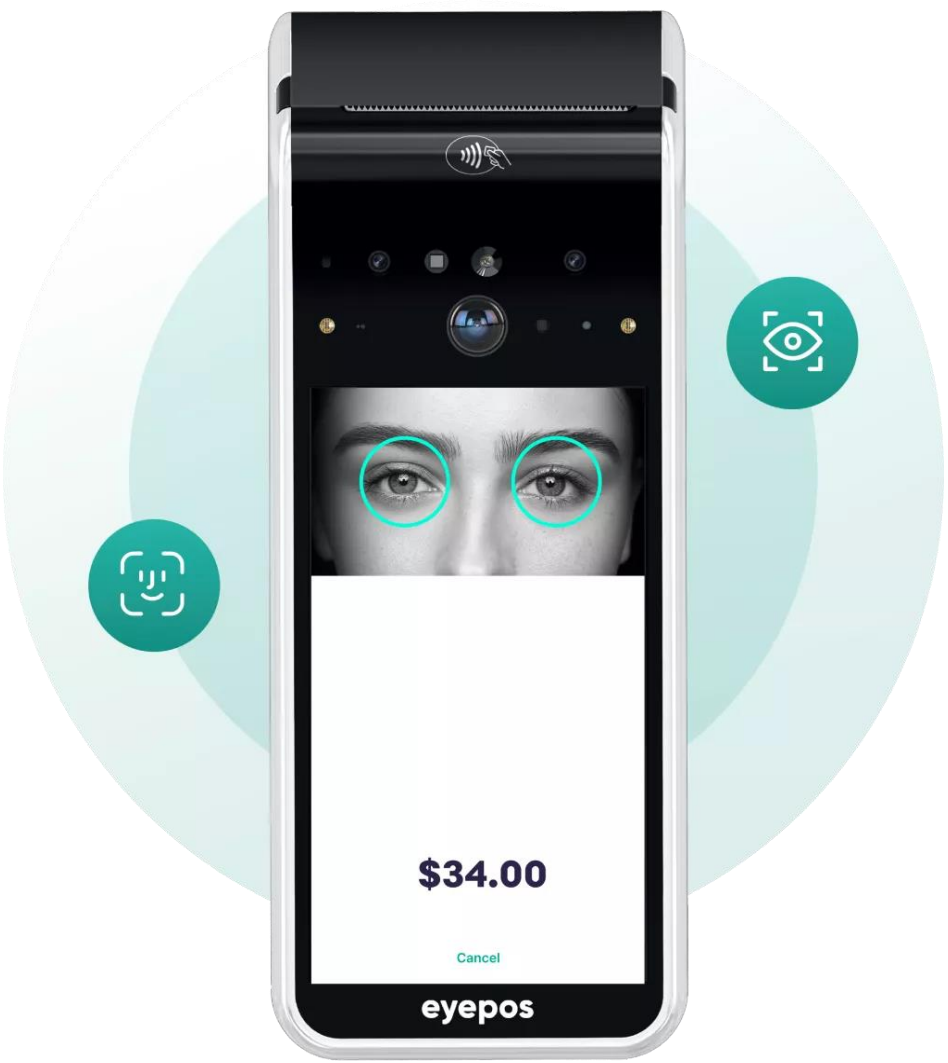
Face: FNIR = 0.03 (12M gallery)

[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

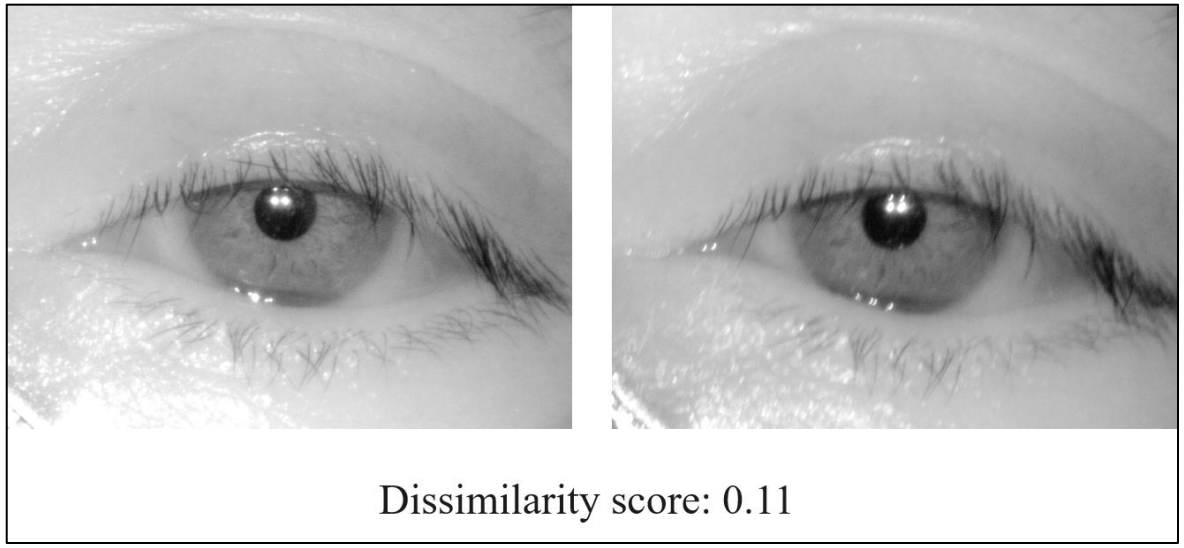
PayEye: Fusion of Iris and Face



Payment at Point of Sale

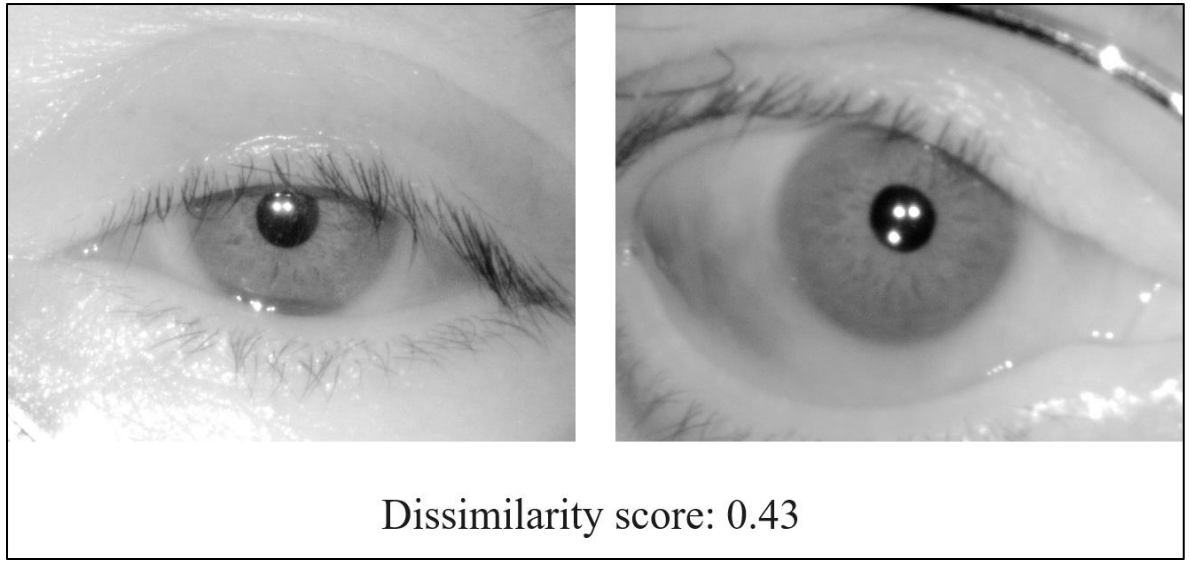
https://payeye.com/for-business-eye-payments/

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

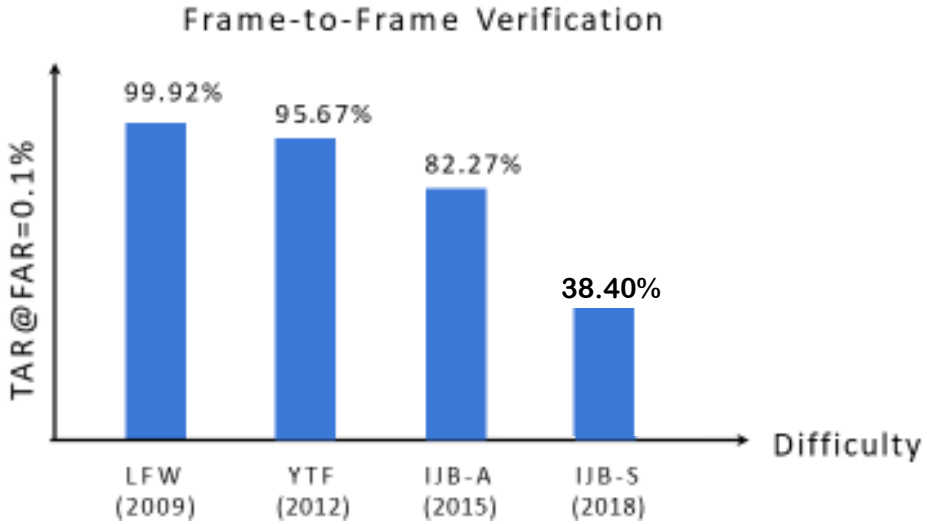
Face Image Quality vs. Recog. Performance

LFW (2009)

YTF (2012)

NIST IJB-A (2015)

NIST IJB-S (2018)



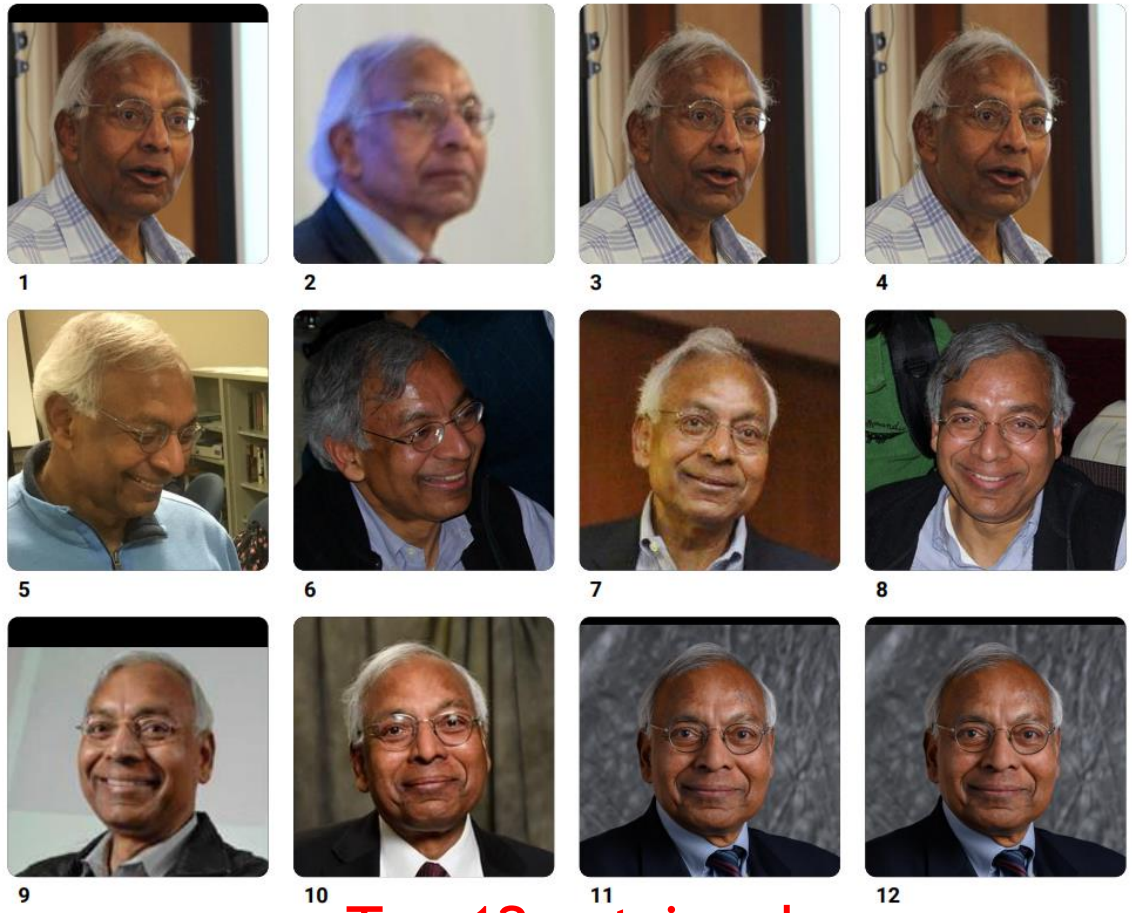
	Gallery Size	Rank1	Rank5
IJB-A	112	97.5	98.4
IJB-S (S2B)	202	60.5	66.0
IJB-S (S2B) With DA	**202**	**64.5**	**71.1**

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

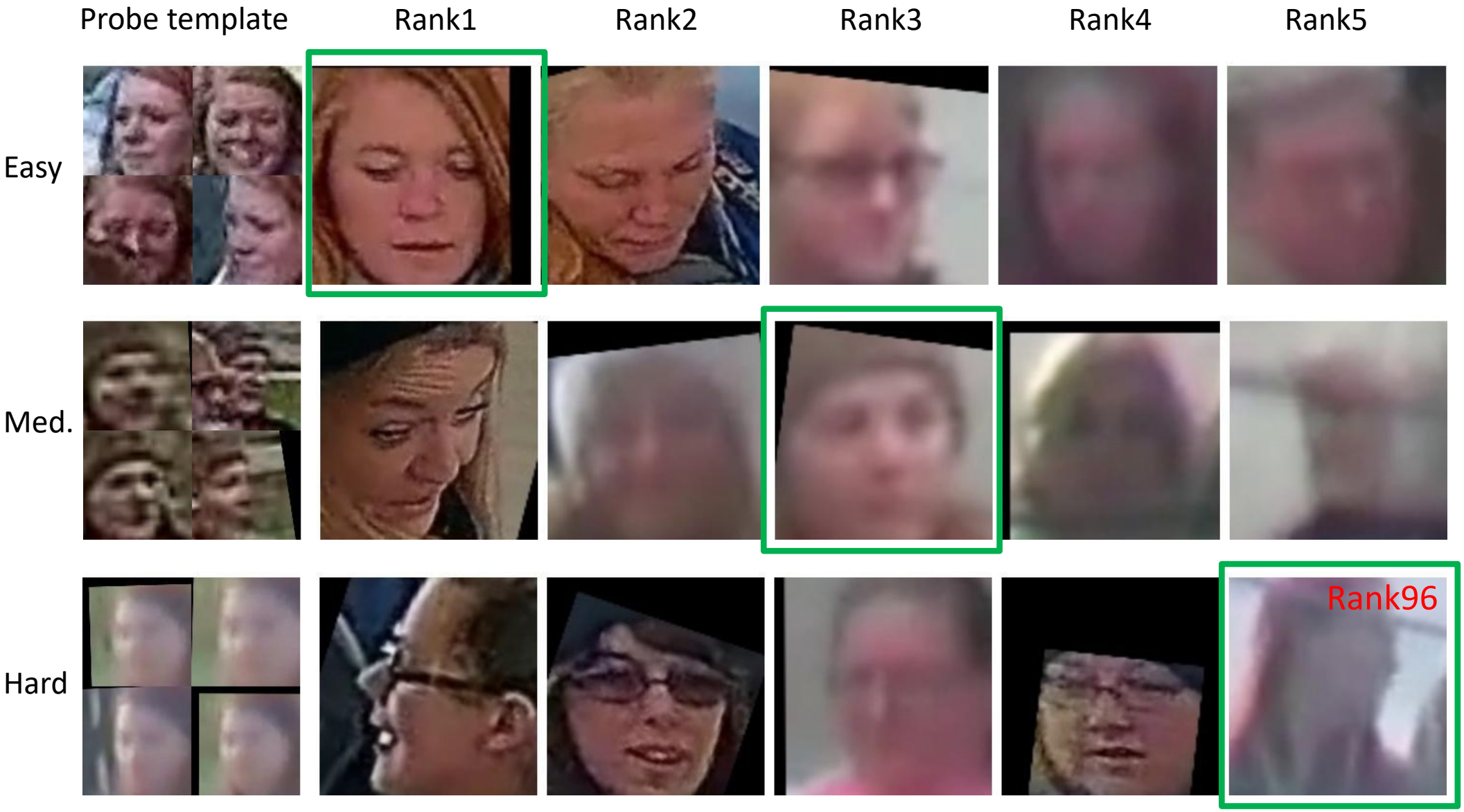
Probe



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
	

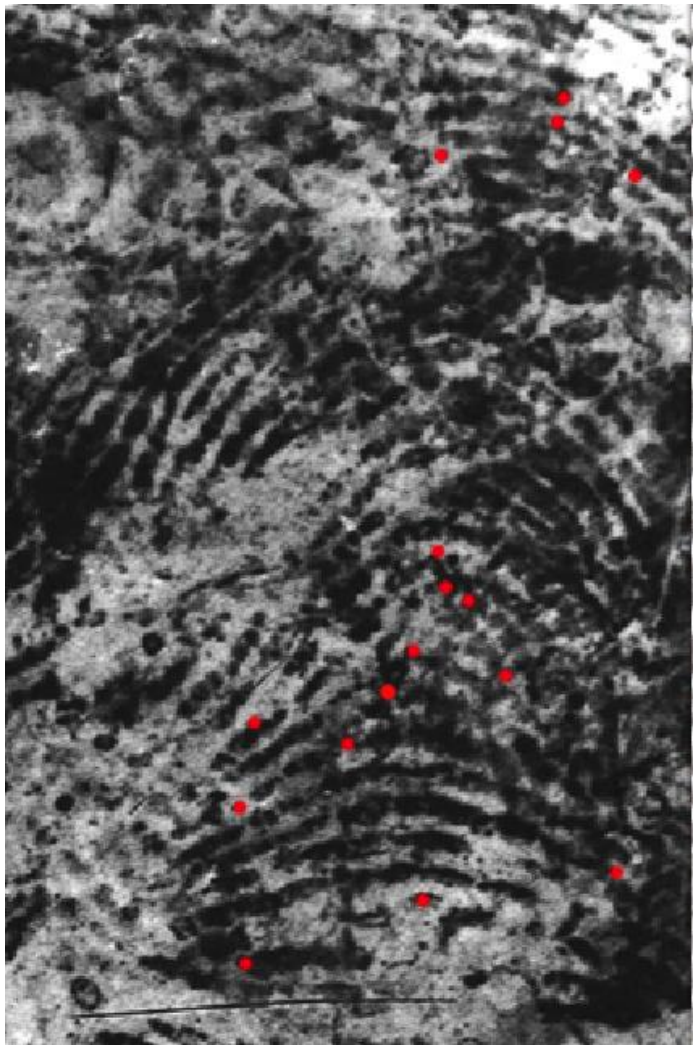
- **A biometric matcher, as designed, returns a similarity between two images**
- **How to prevent different identities from having "high" similarity"?**

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

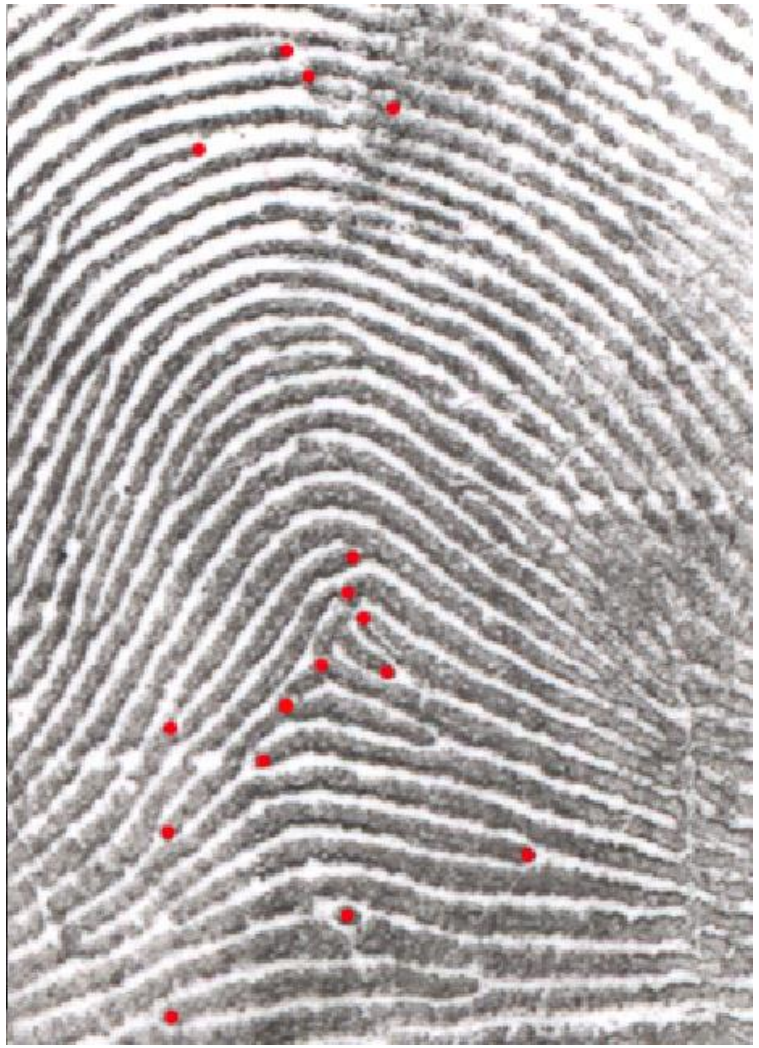
Poor quality of probe resulted in false positive

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



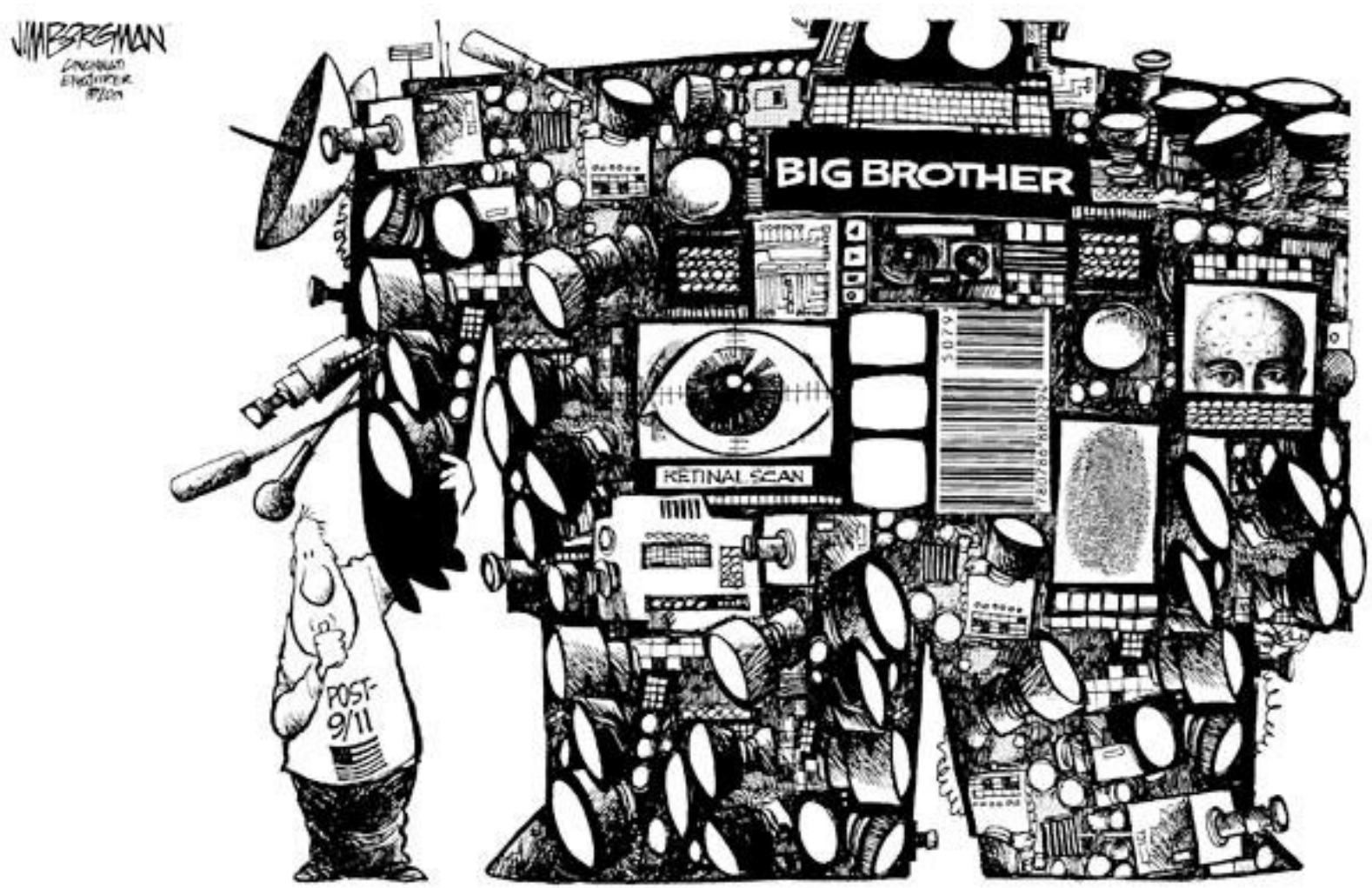
Partial print at site of Madrid train bombing (2004)



AFIS incorrectly returned Brandon Mayfield's prints

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

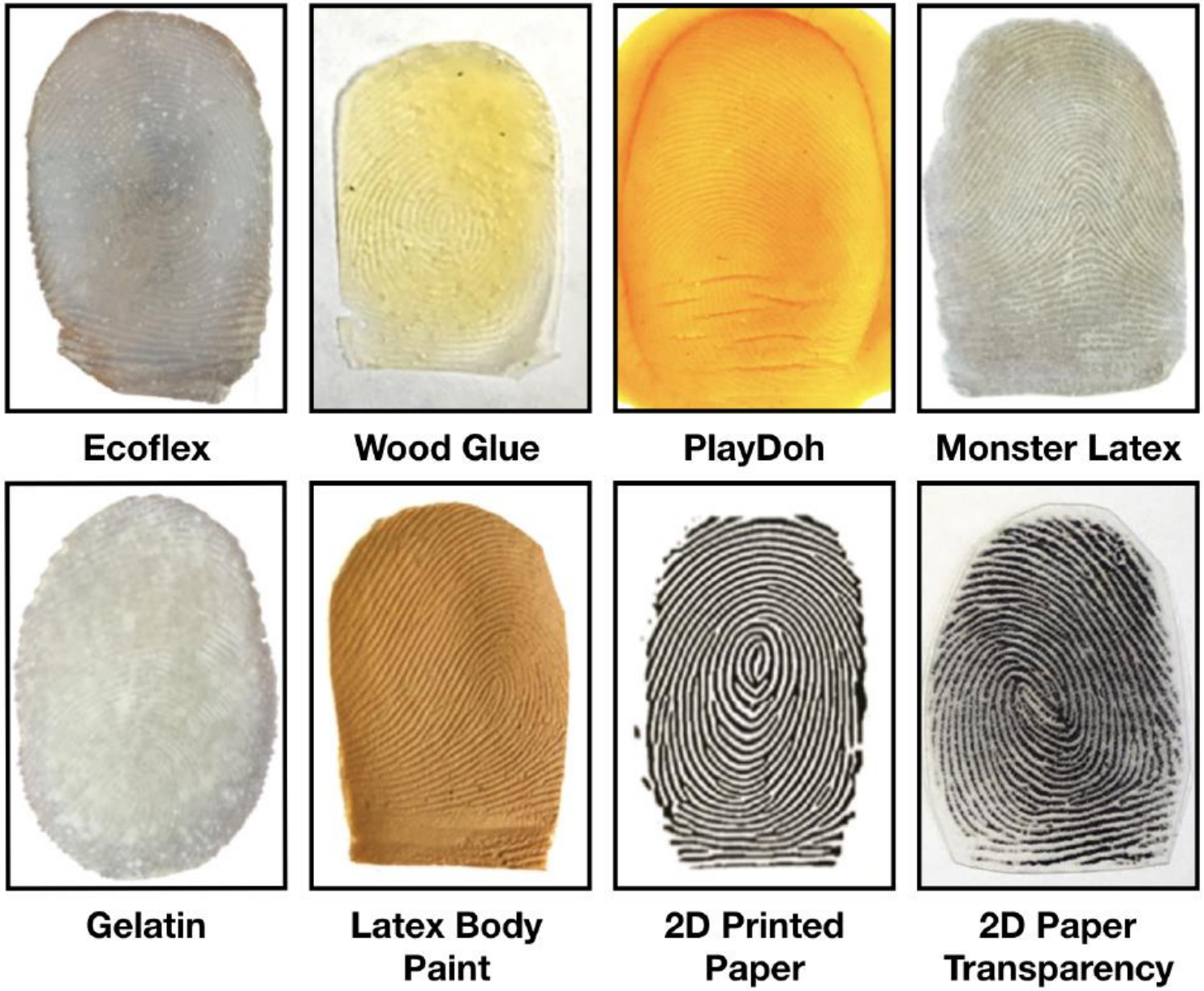
Privacy and Civil Liberty Concerns



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?



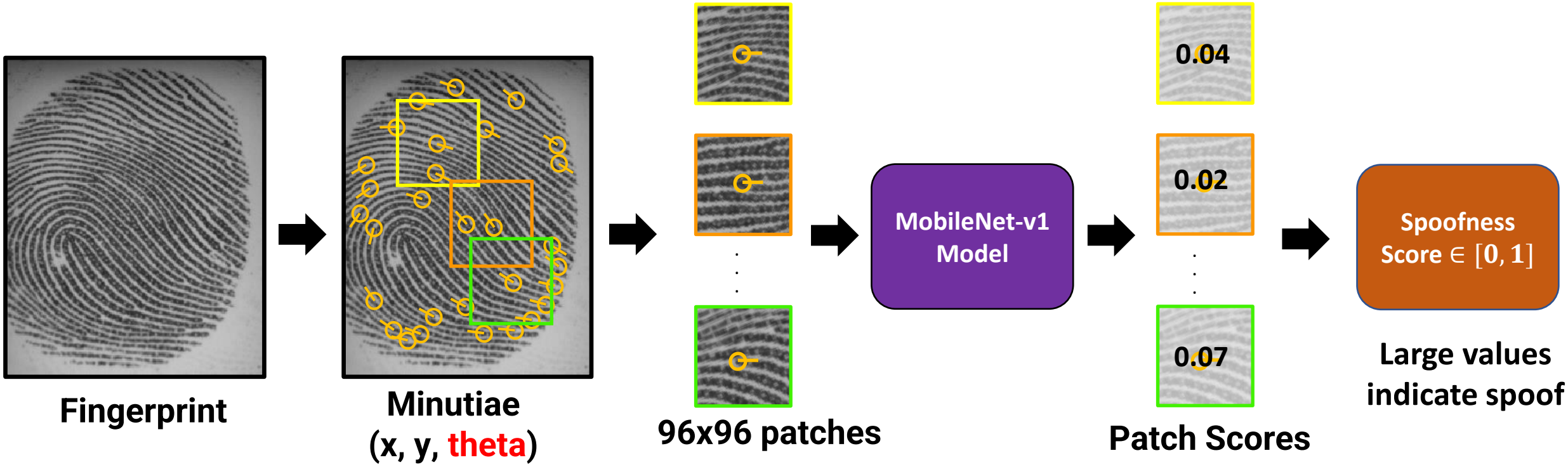


Which Images Are Spoof?





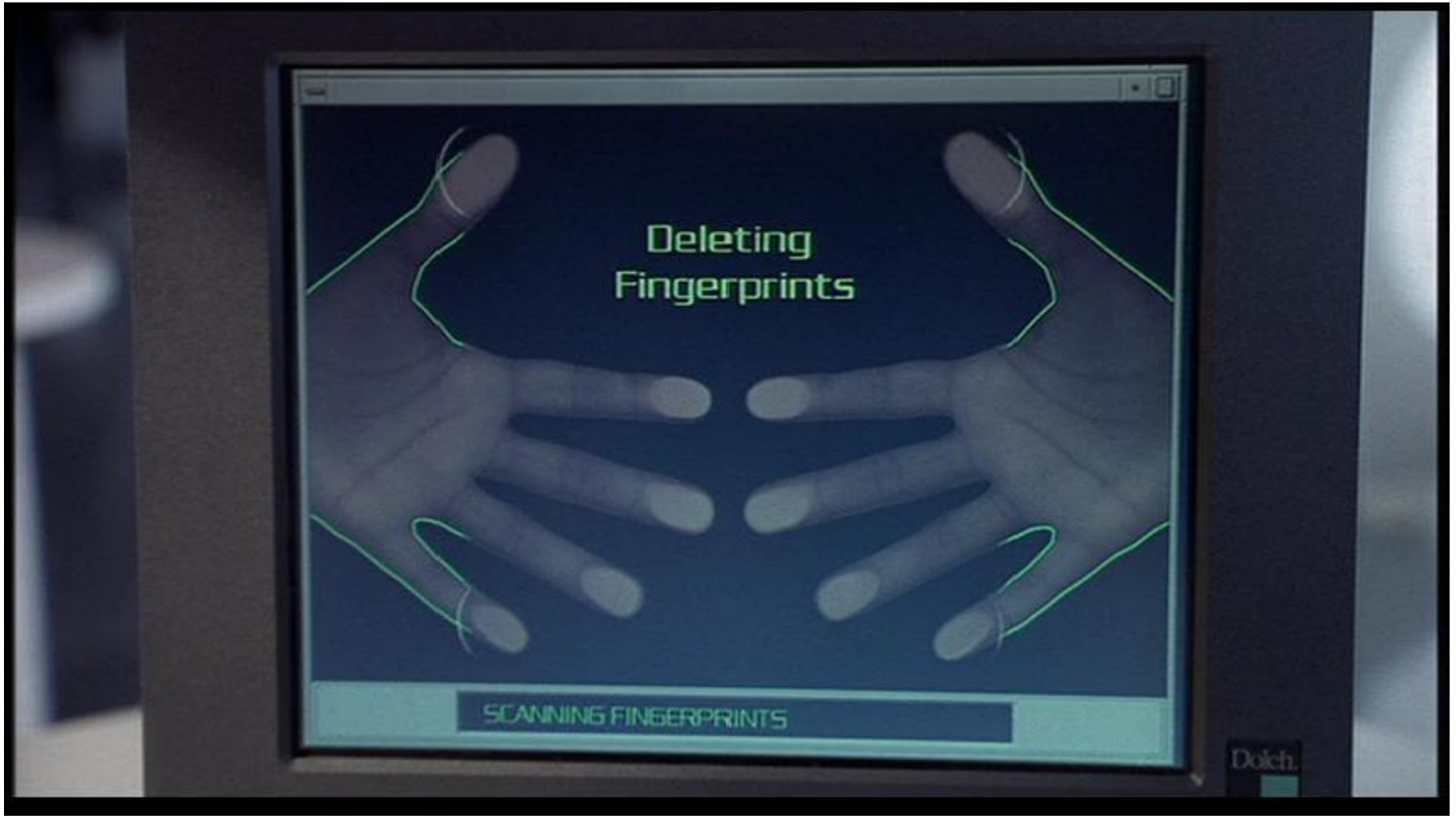
Fingerprint Spoof Buster



- 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

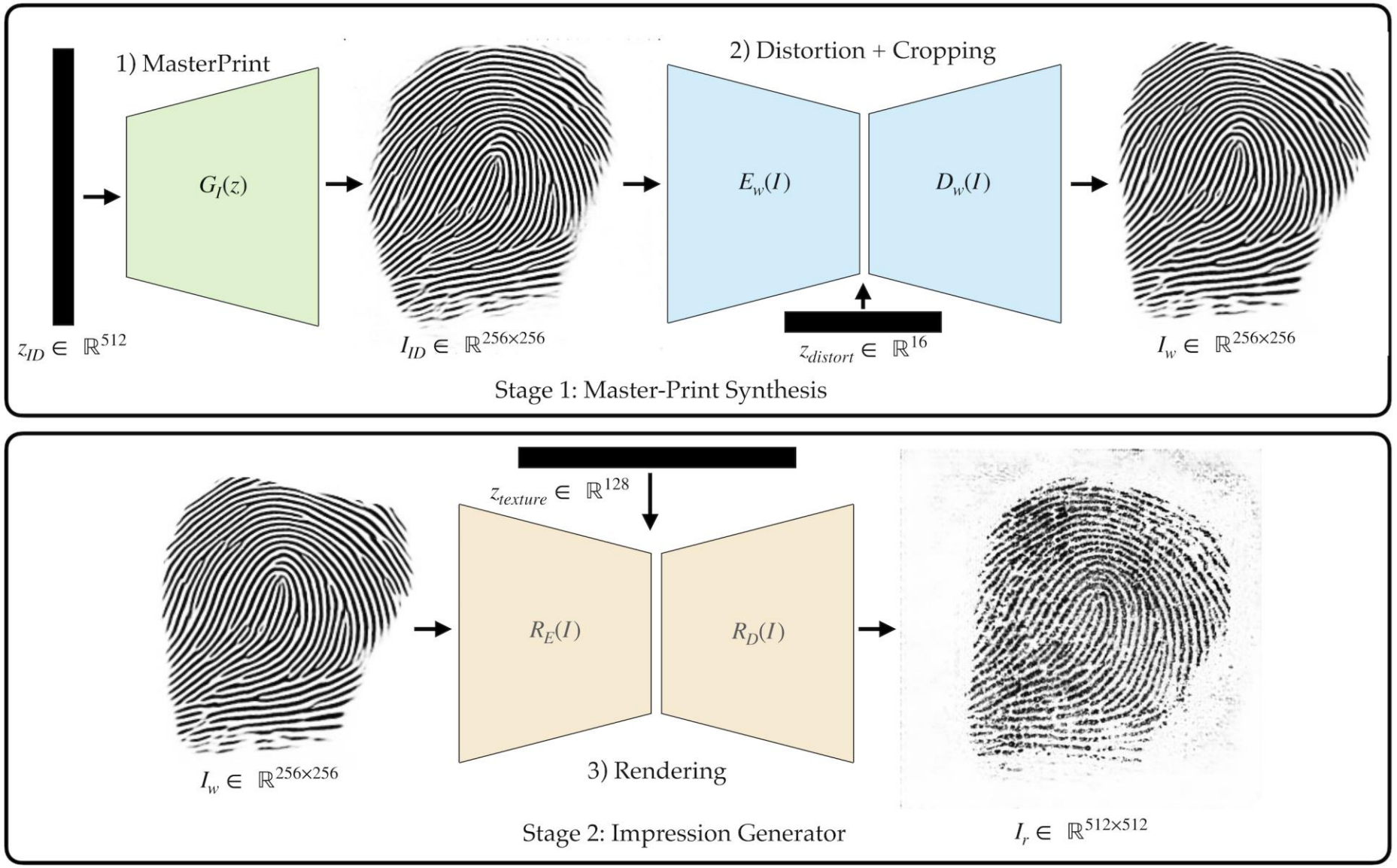
S. Yoon, J. Feng and A. K. Jain, "Altered Fingerprints: Analysis and Detection", IEEE T-PAMI, 2012

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



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

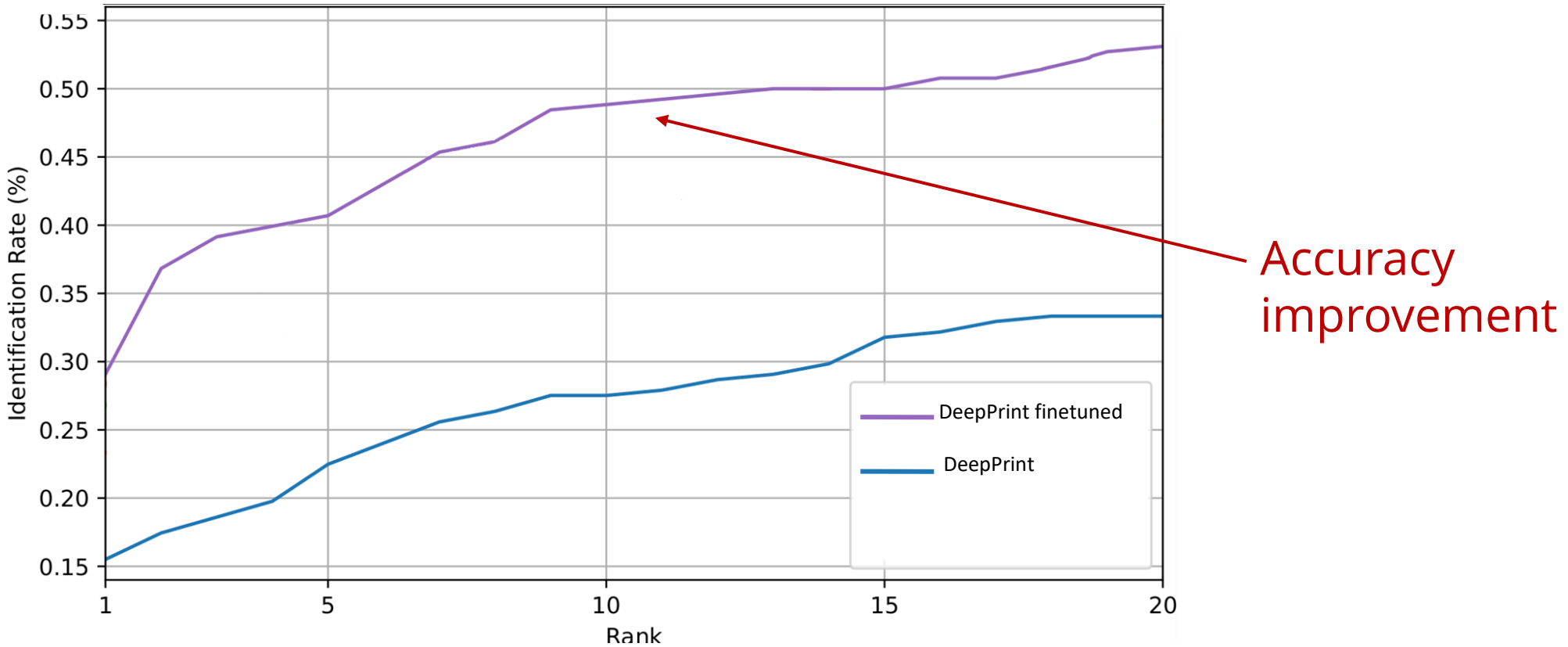
Real or Synthetic Fingerprint Images

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**



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

Face Identification (1:N Comparison)

Probe

Gallery

Probe may or may not be present (enrolled) in the gallery

First Visit to China (1984)