Introduction to Biometric Recognition

Anil K. Jain
Michigan State University
http://biometrics.cse.msu.edu/

Shiv Nadar University, Chennai, January 31, 2024
•.... 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
Artificial Intelligence: Many Facets

- Image & signal processing
- Machine learning
- Pattern recognition
- Deep networks
- Security & privacy
- Domain knowledge
Most-Influential (AI) Technologies

- Facebook's News Feed: 2007
- Netflix Streaming: 2006
- Facebook's Instagram: 2010
- Tesla's Model S: 2011
- Uber: 2010
- Ring's Doorbell: 2012
- Apple iPad: 2012
- Amazon Alexa: 2013
- Apple TouchID: 2013
- Apple Watch: 2015
- Apple FaceID: 2017

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


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

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
Intra-class Variability
Inter-Class Similarity

Learn a compact & discriminative representation for pattern classes

Recognition (Learning)

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

Clustering (Unsupervised learning)
Pairwise similarity

Threshold=0.54
@ FAR=1e-6

- Representation
- Similarity measure

See https://roc.ai/
Biometric Recognition

- The first mobile phone (1973)
- Touch ID, iPhone 5S (2013)
- Apple Pay, iPhone 6 (2014)
- Face ID, iPhone X (2017)
- Vivo In-Display Scanner (2018)

We check our phones, on average, 58 times each day; Touch ID offered convenience & security

Requirements: high accuracy, low cost, low latency, high usability, hackproof

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*

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

1. Satisfy *individuality* and *permanence* properties
2. Demonstrate 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/
Rejected Traits

Rejected Biometric Technologies

tongue prints

FEELINGS

catscan sign-ins

harothe voice i.d.
Growing Interest in Palm Biometric

(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
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 US$1)...
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)

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

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

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)

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)

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

9/11 Terrorist Attacks (2001)
Walt Disney Theme Park (2005)
First AFIS in 1980s; IAFIS launched in 1999; use of soft biometrics (SMT)

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

“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)

New Applicant (no ID is used in this stage)

Enrollment database

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

Who Does this fingerprint belong to?

Query may or may not be present in the database (gallery)

No claim of identity made
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..

Representation

Data → Hand-crafted Features → Learning Algorithm → Prediction

Domain knowledge

Data → Representation Learning → 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

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

Fusion of Multiscale Features

Two-Stage Matching

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
• 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)

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/
Matcher needs to work on images obtained in unconstrained environments, with characteristics different from images in public-domain iris databases.
### Face Image Quality vs. Recog. Performance

<table>
<thead>
<tr>
<th></th>
<th>Gallery Size</th>
<th>Rank1</th>
<th>Rank5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IJB-A</td>
<td>112</td>
<td>97.5</td>
<td>98.4</td>
</tr>
<tr>
<td>IJB-S (S2B)</td>
<td>202</td>
<td>60.5</td>
<td>66.0</td>
</tr>
<tr>
<td>IJB-S (S2B) With DA</td>
<td>202</td>
<td>64.5</td>
<td>71.1</td>
</tr>
</tbody>
</table>

**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

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

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?”

Poor quality of probe resulted in false positive

- 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

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

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)

Fingerprint Alteration

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

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

Real or Synthetic Fingerprint Images

Real or Synthetic Fingerprint Images
Data Augmentation: Accuracy improvement

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

Evaluated on NIST SD27 (1:N experiment)

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 may or may not be present (enrolled) in the gallery
First Visit to China (1984)