Anil K. Jain
Michigan State University
http://biometrics.cse.msu.edu
July 29, 2020

Biometrics: Vision 2020
Outline

• Background and milestones
• Applications
• State-of-the-art
• Where are we heading?
• Summary
Security Concerns

We now live in a society where individuals cannot be trusted based on their ID documents and PIN/passwords.

Interpol’s Stolen and Lost Travel Documents database contains ~84M records; It was searched nearly 3 billion times in 2018 by officials worldwide, resulting in more than 289,000 positive ‘hits’. 
Biometric Recognition

• **Bios: life** and **Metron: a measure** *(Morris, 1875)*

• **What makes each person unique?** *(Pollack, 1981)*

• “Automated recognition of individuals based on their behavioral and biological characteristics”

  ISO/IEC JTC1 2382-37:2012

Biometrics in Italy

Rome Fiumicino Airport pilots end-to-end biometric solution (Jan 2020)
https://www.futuretravelexperience.com/2020/01/rome-fiumicino-airport-pilots-end-to-end-biometric-solution/

FPC fingerprint sensor used in Italian biometric payment card trial for Intesa Sanpaolo banking group
Biometric Milestones

1858
- First use of fingerprints in British criminal case

1883
- Bertillonage invented

1889
- Galton / Henry fingerprint system adopted by Scotland Yard

1924
- Seventeen classes
  - Whorl (double loop), loop (left and right)
  - Arch cover 99% of fingerprints

1963
- Core Identimat: First commercial use of biometrics

1972
- FBI inaugurates full operation of "IAFIS"

2001
- FBI Next Generation Identification

2008
- Criminal booking

2013
- 9/11 terrorist attacks lead to govt. mandates to use biometrics in regulating intl. travel

2014
- Other operations

Timeline:

References:
- Y. Taigman, M. Yang, M. Ranzato, L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", CVPR 2014

Note: The image includes various biometric recognition technologies and their applications.
Biometric Traits
Most Popular Biometric Traits

Incheon, South Korea: Smart Entry
Australia: SmartGate
UAE: e-Border

Legacy databases, high accuracy and fast search

http://www.homestaykorea.com/?document_srl=73667&mid=bbs_koreainfo_news
https://tottnews.com/tag/smart-gates/
Biometrics Applications

Application requirements: throughput, usability, low cost, high accuracy, robust, secure
Biometrics Recognition System

• Learning: Representation (features) & similarity
• Operation mode: Authentication (1:1) vs. Search (1:N)
Face Authentication

Probe: claimed to be Kai

Gallery: Kai’s image

Similarity > T
Face Search

Probe

Gallery

Closed-set v. Open-set Search
Fingerprint Recognition

Query Print

Enrolled Fingerprint

Similarity = 0.9
Match!
Biometric Authentication Errors

Impostor Distribution

Genuine Distribution

Threshold

False Reject

False Accept

Match Score

P
Authentication: State of the Art

Fingerprint: TAR = 99.964% @ FAR = 0.01% (FVC-ongoing)
Iris: TAR = 99.82% @ FAR = 0.01% (NIST IREX II)
Face: TAR = 99.7% @ FAR = 0.1% (NIST FRVT 2019)
Evaluation Metrics for Face Identification

Identification Rate \((N, R, T)\) = \[
\frac{\text{# mate searches whose mate is in top } R \text{ rank and above threshold } T}{\text{# all mate searches } N}
\]

- Closed-set Retrieval Rate: \(R\) fixed, \(T = 0\) (no threshold requirement)
- Open-set Identification Rate: \(T\) fixed by FPIR, \(R=N\) (no rank requirement)
- FPIR (False Positive Identification Rate) is defined as:

\[
FPIR(T) = \frac{\text{# non-mate searches who return enrolled images with score above } T}{\text{# all non-mate searches}}
\]

Mugshot Images
## FRVT 2019 Face Identification Results

### Closed-set Retrieval Rate (%) @ Rank1

<table>
<thead>
<tr>
<th>Gallery Size</th>
<th>0.64M</th>
<th>1.6M</th>
<th>3M</th>
<th>6M</th>
<th>12M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>99.91</td>
<td>99.90</td>
<td>99.90</td>
<td>99.89</td>
<td>99.88</td>
</tr>
<tr>
<td>Vendor</td>
<td>NEC</td>
<td>SenseTime</td>
<td>SenseTime</td>
<td>SenseTime</td>
<td>SenseTime</td>
</tr>
</tbody>
</table>

### Open-set Identification Rate (%) @ FPIR=0.1%

<table>
<thead>
<tr>
<th>Gallery Size</th>
<th>0.64M</th>
<th>1.6M</th>
<th>3M</th>
<th>6M</th>
<th>12M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>99.84</td>
<td>99.82</td>
<td>99.79</td>
<td>99.46</td>
<td>95.49</td>
</tr>
<tr>
<td>Vendor</td>
<td>SenseTime</td>
<td>SenseTime</td>
<td>SenseTime</td>
<td>SenseTime</td>
<td>SenseTime</td>
</tr>
</tbody>
</table>

[https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf](https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf)
State-of-the-Art: Search

Results on IJB-C using ArcFace* (Rank-1 retrieval = 94%)

Aadhaar: World’s Largest Biometric System

12-digit unique ID based on biometrics

“To empower residents of India with a unique identity and a digital platform to authenticate anytime, anywhere.”
Enrollment

Minimal documentation for enrollment
De-duplication

Fusion of face, fingerprint and iris to detect duplicates

Enrollment database

Already Exists in the Database?
Authentication
Fingerprint Quality Challenges in Aadhaar

No. of false minutiae = 0
No. of false minutiae = 7
No. of false minutiae = 27
2020 Vision

Scalability

Accuracy

No Noise
Low
Medium
High
Noise

No Noise
90%
99%
99.99%
99.999%

90%
99%
99.99%
10
1
3
5
7
10
Legal Identity for All

- The United Nations (UN) Sustainable Development Goal (SDG) Target 16.9: “to provide legal identity for all, including birth registration” by 2030
- A verifiable & trusted ID for All would be an order of magnitude larger than Aadhaar (#births/day = 360K; per year = 130M)
Need for Labeled Data

• Large-scale annotated biometric data for learning and evaluation

• Privacy laws (e.g. GDPR) make it difficult to collect and share data

• **Data rich & data deprived groups**

• Lawsuit filed against startup, Clearview AI; it has scraped 3 bn face images from Facebook, YouTube, and other sites), *NYT Feb 6, 2020*

ImageNet: 14M images from 22K classes collected from the web [http://www.image-net.org](http://www.image-net.org)
Fundamental Premise of Biometrics

• **Individuality:** How many distinct identities can be resolved using biometrics?

• **Persistence:** How does recognition accuracy change with increasing time gap between enrolled and query biometric?
Capacity of Face Recognition

- #Identities resolved at a specified FAR and feature space (FAR of 0.01% and SphereFace model)

IJB-A, capacity = 1.1 x 10^4

IJB-C, capacity = 2.0 x 10^2

Gong, Boddeti, Jain, "On the Intrinsic Dimensionality of Face Representation", arXiv:1803.09672, 2018
Persistence of Face

• Longitudinal face data of 20K subjects
• Findings: 99% of the subjects could be recognized @ 0.01% FAR up to 6 years irrespective of age, gender & race

Best-Rowden and Jain, "Longitudinal Study of Automatic Face Recognition", PAMI, 2017
Fairness: Demographic Bias

About 1% difference in accuracies between race and gender classes

Figure 64: “For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males.”, NIST.gov Face Recognition Vendor Test (FRVT) 1:1 Ongoing, 2019
Image Quality vs. Performance

- LFW (2009) - 99.92%
- YTF (2012) - 95.67%
- NIST IJB-A (2015) - 82.27%
- NIST IJB-S (2018) - 4.86%
Detroit police linked armed robberies at an ATM after matching a tipster’s description of the suspect’s distinctive tattoos.
Latent Fingerprint Recognition

Latents (first column) from NIST SD27 which could not be matched with their mates (second column) at rank-1 by COTS latent AFIS (Rank-1 accuracy = 67%)
Brendan Mayfield was wrongly accused of the Madrid train bombing (2004) after his partial fingerprints matched those found at the bombing site.
A Novel Challenge for Face Recognition

Masks
Briefly remove your mask for identity verification
Identical Twins

Simple attacks: (b) printed photograph, (c) replay attacks (video). Advanced attacks: (d-h) 3D masks, (i-k) make-up attacks, or (l-n) partial attacks [1]. A live face is shown in (a) for comparison. Here, the spoofs in (b-c, k-n) belong to the same person in (a).

Performance under known v. unknown attacks (generalization)

Digital Image Manipulation

Match on Device

Serial Peripheral Interface (SPI)

Encrypt Raw Data

To secure fingerprint, processing is done in TEE (Trusted Execution Environment):

- Image pre-processing
- Feature extraction
- Alignment and recognition

GOODIX IN-DISPLAY FINGERPRINT SENSOR™
Biometrics: Privacy Concerns

One billion surveillance cameras will be watching around the world in 2021—and more than half of those cameras will be in China

Security vs. Privacy

Are you willing to trade civil liberties for greater security?

That depends on the exchange rate.
Wrongfully Accused by an Algorithm

• In October 2018, someone shoplifted five watches, worth $3,800, from a Shinola store in Detroit

• A frame from low-quality CCTV footage was used to search against 49M mugshots & driver license photos

• “This is not me,” Robert Julian-Borchak Williams told investigators. “You think all Black men look alike?”

Airports of the Future

Summary

• Automated person recognition is becoming a necessity; No substitute to biometrics for effective person recognition.

• Biometrics enhances security, eliminates fraud, offers user convenience and eliminates some level of subjectivity.

• Biometric readers are relatively cheap -- fingerprint, face and voice sensors are embedded in mobiles; match on device.

• Recognition accuracy is limited in unconstrained acquisitions and uncooperative subjects.

• Deployed systems should (i) protect template, (ii) resistant to spoof attacks, (iii) not infringe on civil liberties, …….