Privacy vs. Security: Aviation Biometric Systems

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

Privacy and Technology Colloquium, June 30, 2020
Three Most Popular Biometric Traits

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

Legacy databases, high accuracy for 1:N search, fast search

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

“We found collecting facial images is easy for both travelers and CBP Officers. The technology is intuitive and hassle-free, with traveler identity matches made quickly. The fact that mobile device users now have the option to use biometrics to unlock their phones also helped shape our decision.”

https://www.cbp.gov/travel/biometrics
Use of Biometrics at U.S. Airports


- Dec 2004: US-VISIT for ENTRY; two fingerprints of Visa holders used to (i) detect fraudulent/altered travel documents, (ii) prevent dangerous people from obtaining visas or entering U.S.

- Nov, 2007: DHS started 10-print collection at U.S. ports of entry to more accurately identify international travelers.
Face Recognition: Entry/Exit Program

- Executive Order 13780 March 6, 2017: complete biometric entry/exit system.
- Exit system will determine who has overstayed in the U.S. and who has not.
- International traveler’s entry/exit photo compared with DHS database (e.g., photos from U.S. passports and U.S. visas, flight manifest).

Privacy/Civil Liberties Concerns

Recognition rate, demographic bias, data security, retention policy, function creep
NIST FRVT Evaluation Datasets

Unconstrained Faces

Profile Faces

Mugshot Images

Webcam Images

Surveillance and Access Systems

Surveillance and Transactional Systems

Law Enforcement and Passport Type of Applications

Immigration and Transactional Systems
# 1:N Search Accuracy

## Error Rates on a 12M Face Image Search Database

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Error Rates $FNIR @ FPIR = 0.001$</th>
<th>Template Size $Bytes$</th>
<th>Memory Requirements $GB$</th>
<th>Search Speed* $milliseconds$</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEC</td>
<td>0.058</td>
<td>1712</td>
<td>20.5</td>
<td>697</td>
</tr>
<tr>
<td>Paravision</td>
<td>0.106</td>
<td>4096</td>
<td>49.2</td>
<td>1417</td>
</tr>
<tr>
<td>RankOne</td>
<td>0.116</td>
<td>165</td>
<td>2.0</td>
<td>393</td>
</tr>
<tr>
<td>Innovatrics</td>
<td>0.142</td>
<td>1076</td>
<td>12.9</td>
<td>414</td>
</tr>
<tr>
<td>Microsoft</td>
<td>0.154</td>
<td>1024</td>
<td>12.3</td>
<td>2312</td>
</tr>
<tr>
<td>Idemia</td>
<td>0.166</td>
<td>528</td>
<td>6.3</td>
<td>880</td>
</tr>
<tr>
<td>Cognitec</td>
<td>0.184</td>
<td>2052</td>
<td>24.6</td>
<td>2088</td>
</tr>
<tr>
<td>Neurotechnology</td>
<td>0.214</td>
<td>2048</td>
<td>24.6</td>
<td>1604</td>
</tr>
<tr>
<td>Toshiba</td>
<td>0.214</td>
<td>1548</td>
<td>18.6</td>
<td>7250</td>
</tr>
<tr>
<td>Cogent</td>
<td>0.224</td>
<td>1043</td>
<td>12.5</td>
<td>3131</td>
</tr>
<tr>
<td>Aware</td>
<td>0.264</td>
<td>3100</td>
<td>37.2</td>
<td>924</td>
</tr>
</tbody>
</table>

* Search time includes template generation and search speed
State-of-the-Art: Search

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

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 49 million mugshots & driver license photos.

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

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.
Fairness: Demographic Bias

At most 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, Nov. 11, 2019
A Novel Challenge for Face Recognition

Masks
Briefly remove your mask for identity verification
Template Protection: Match on Device

Serial Peripheral Interface (SPI)
Encrypt Raw Data

Processing is done in TEE (Trusted Execution Environment):
- Image pre-processing
- Feature extraction
- Alignment and recognition

GOODIX IN-DISPLAY FINGERPRINT SENSOR™
Matching in Encrypted Domain

Encrypted Templates have been enrolled into the database offline.

score = 0.96
Security vs. Privacy

ARE YOU WILLING TO TRADE CIVIL LIBERTIES FOR GREATER SECURITY?

THAT DEPENDS ON THE EXCHANGE RATE.
Airports of the Future

Summary

• Aviation biometrics is here to stay; more countries are adopting it

• Face, fingerprint and iris will continue to be popular; face has an edge because of its use in travel documents, non-contact and covert acquisition and high recognition accuracy in constrained acquisition

• NIST evaluations are only for “technology readiness”; how will we know the operational error?

• What recourse does a traveler have if he is wrongfully targeted

• Not sufficient attention to: evaluating low quality face searches and bias; likelihood of a match (convincing to a jury), data protection (govt. agencies maintain the biometric image databases),…