Privacy vs. Security: Aviation Biometric Systems

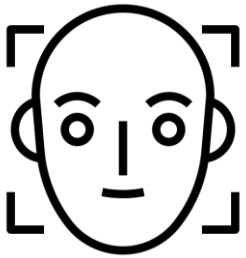
Anil K. Jain

Michigan State University

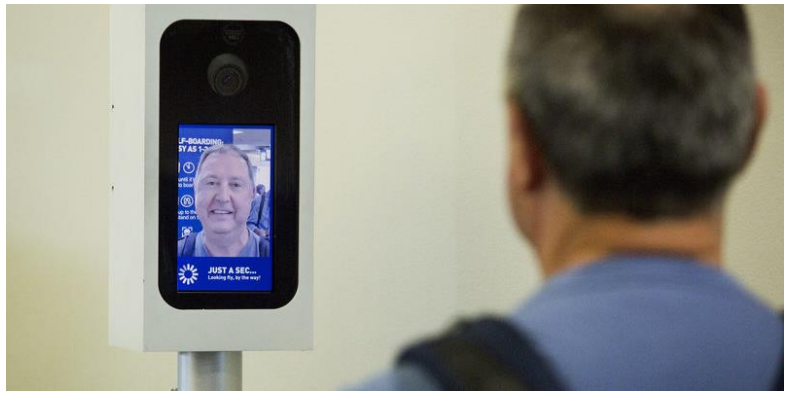
http://biometrics.cse.msu.edu/

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/
https://www.idemia.com/news/multi-biometrics-future-border-control-2016-04-21

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

Smoke pours from the twin towers of the World Trade Center after they were hit by two hijacked airliners in a terrorist attack September 11, 2001 in New York City. Getty Images/Robert Giroux

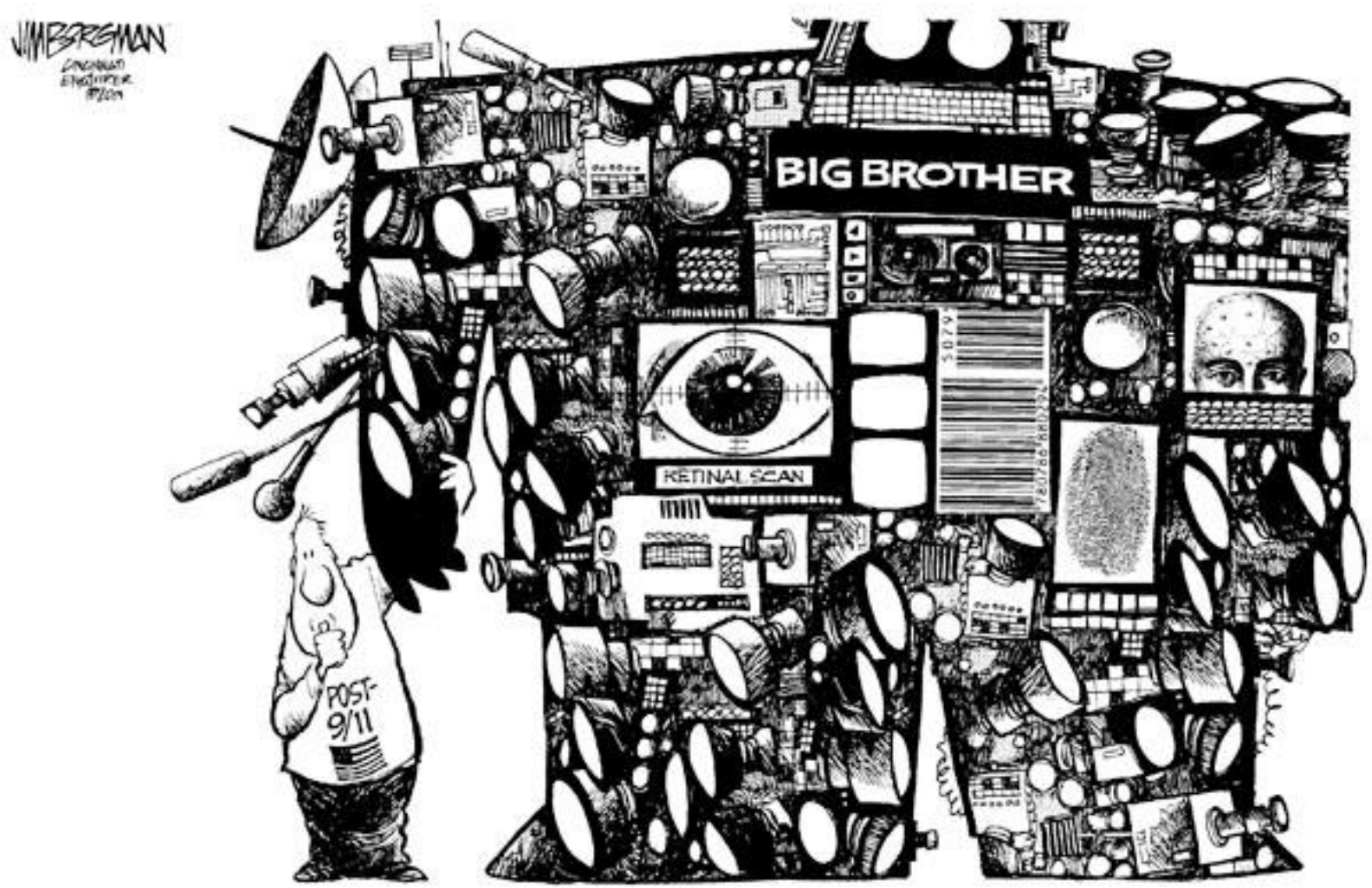
- USA PATRIOT Act (2001); Enhanced Border Security and Visa Entry Reform Act (2001).
- Dec 2004: US-VISIT for **ENTRY; two** fingerprints of Visa holders used to (i) detect fraudulent/altered travel documents, (ii) prevent dangerous people from obtaining visas or entering U.S.
- Nov, 2007: DHS started **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).

https://www.cnn.com/travel/article/airports-facial-recognition/index.html (8th October 2019)

Privacy/Civil Liberties Concerns



Recognition rate, demographic bias, data security, retention policy, function creep

NIST FRVT Evaluation Datasets

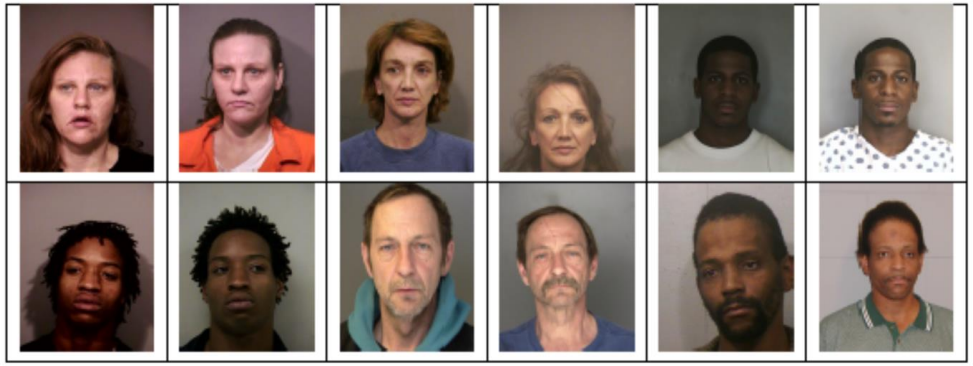
Unconstrained Faces

Surveillance and Access Systems

Profile Faces

Surveillance and Transactional Systems

Mugshot Images



Law Enforcement and Passport Type of Applications

Webcam Images

Immigration and Transactional Systems

1:N Search Accuracy

Error Rates on a 12M Face Image Search Database

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

* Search time includes template generation and search speed

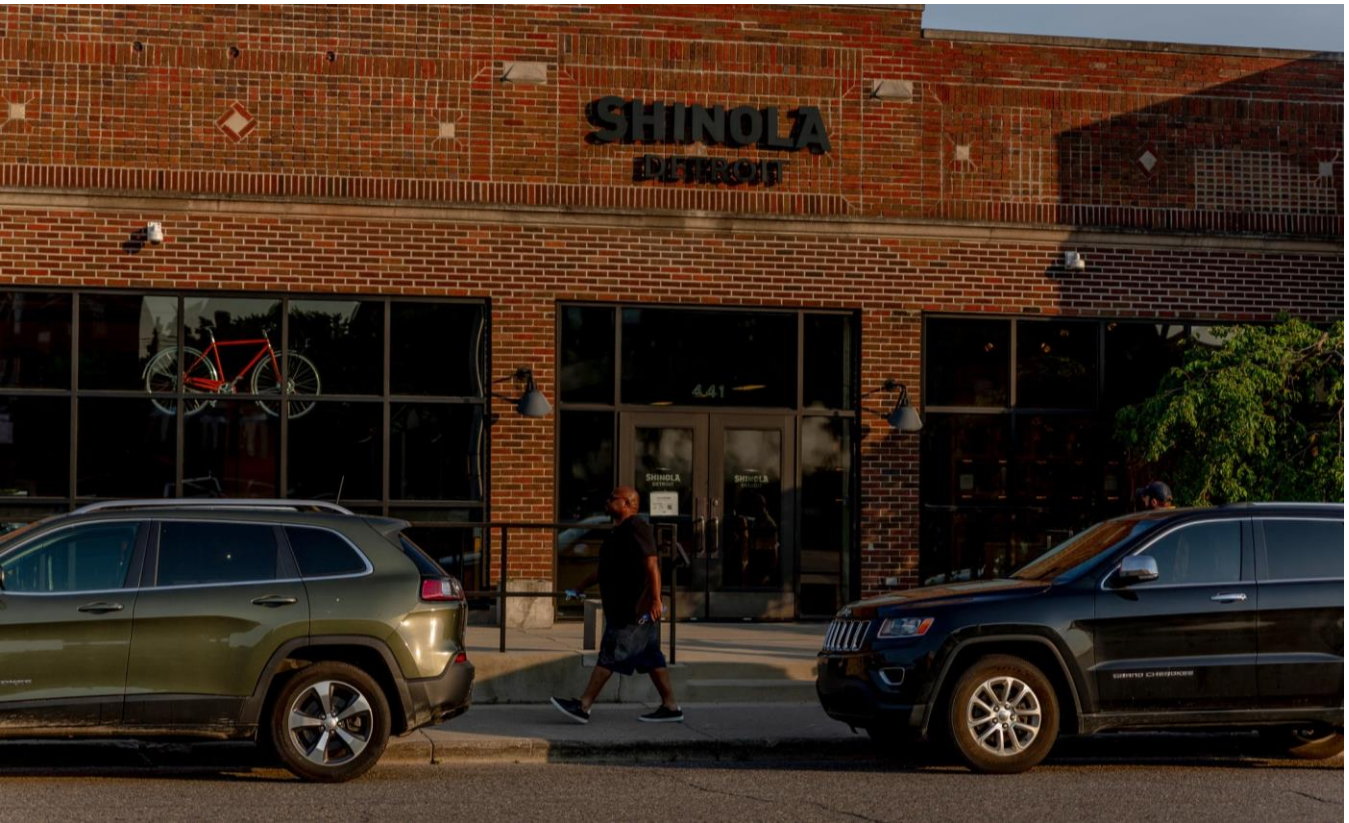
State-of–the-Art: Search

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

J. Deng, J. Guo, N. Xue, & S. Zafeiriou. “Arcface: Additive angular margin loss for deep face recognition.” In CVPR 2019.

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 M mugshots & driver license photos
- **“This is not me,”** Robert Julian-Borchak Williams told investigators. **“You think all Black men look alike?”**



https://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

Fairness: Demographic Bias

At most 1% difference in accuracies between race and gender classes

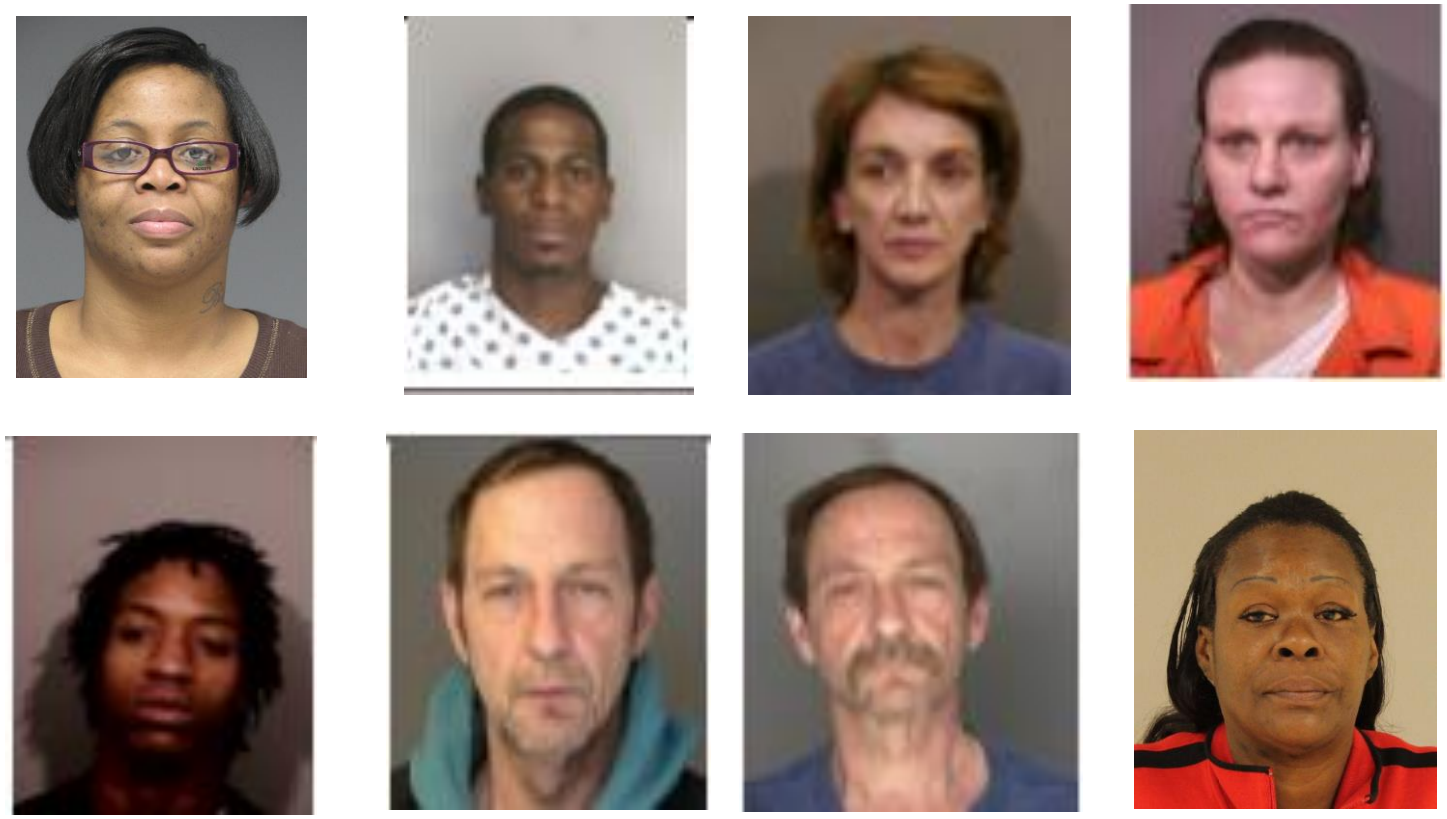


Figure 64: "For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males.", NIST.gov Face Recognition Vendor Test (FRVT) 1:1 Ongoing, Nov. 11, 2019

A Novel Challenge for Face Recognition

Template Protection: Match on Device

Serial Peripheral Interface (SPI)

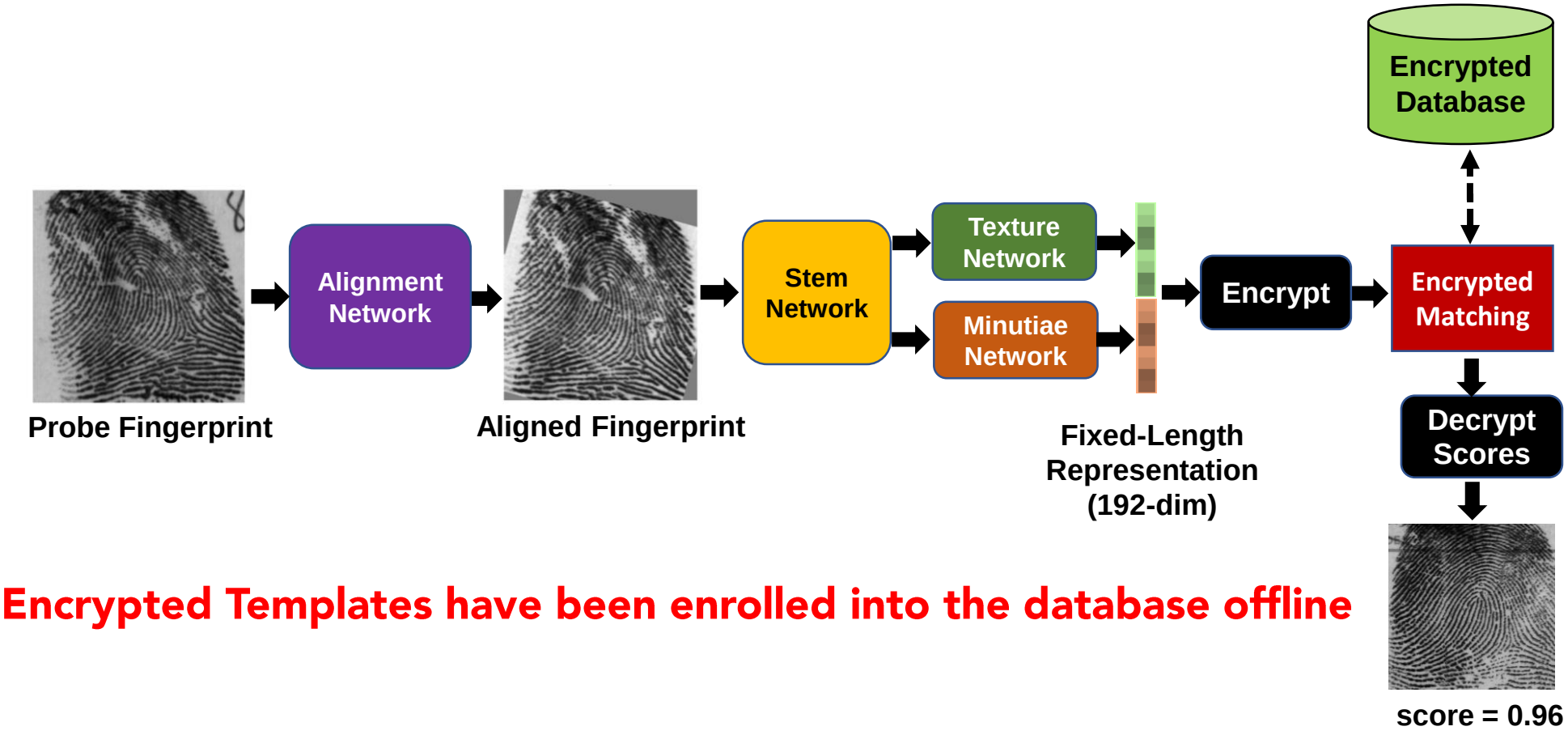
Encrypt Raw Data

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

Security vs. Privacy

Airports of the Future

https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/facial-recognition-to-be-deployed-at-top-20-us-airports-should-you-be-concerned

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),…