ETHICAL CONSIDERATIONS

BIOMETRICS 28.11.2024

Emerging Applications

Amazon One (2020)

Personalization (2022)

Match on card (2022)

Consumer News

Amazon One Payment System Questioned By Senators Over Privacy Safety Of Users – Letter Sent To Amazon For Its Palm Biometric Payment System...

By Consider The Consumer on 08/25/2021

Senators Question Amazon One Collection of Biometric Data

On Friday, a trio of U.S. senators wrote to Amazon President and CEO Andy Jassy inquiring about his company's policy regarding the collection of biometric data from users as part of its new palm print payment system, Amazon One.

Amazon Rekognition

Deep learning-based image recognition service
Search, verify, and organize millions of images

Object and Scene Detection

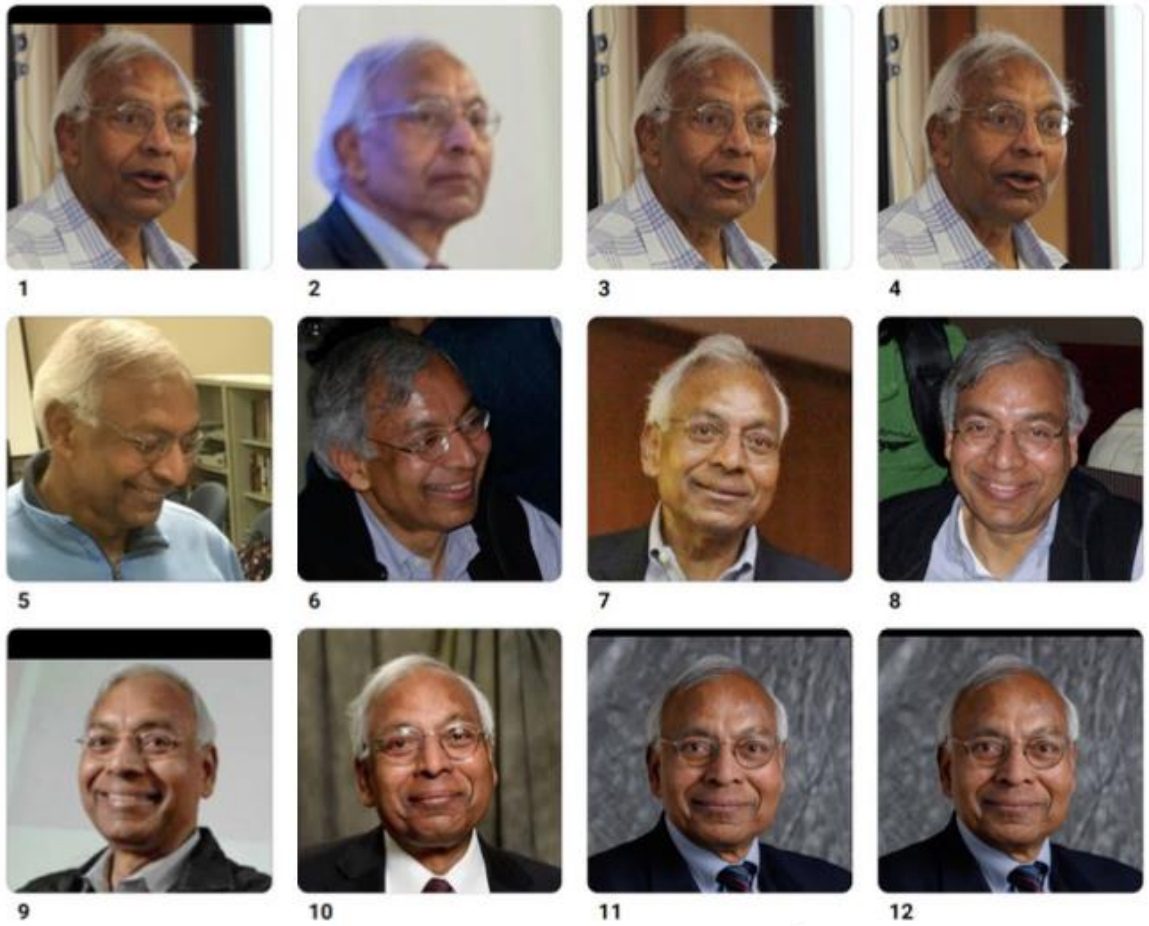
Facial Analysis

Face Comparison

Facial Recognition

Unconstrained Face Search

Query



Top 12 retrievals

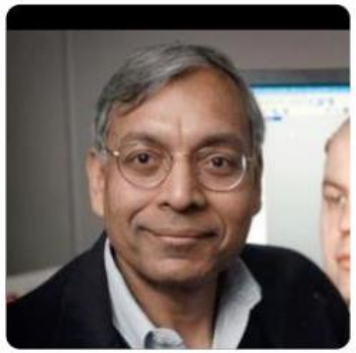
20 billion face image database (Clearview.AI)

Clearview.AI Retrievals: Large Time Gap

Original search image

Probe
(1970)

1



2

Image Index

1. Pioneering pattern recognition | College of Engineering. *https://www.egr.msu.edu/news/2018/12/04/pioneering-patter recognition* (MD5: b7cbc9670209d85fe488e155be883dc4)

2. Lynn F. Brumm Endowed Scholarship Honors Faculty Member | Giving to .... *https://givingto.msu.edu/stories/lynn-f-brumm-endowed-scholarship-honors-faculty-member* (MD5: f503dd0043d8bc2eac6ac9837214401e)

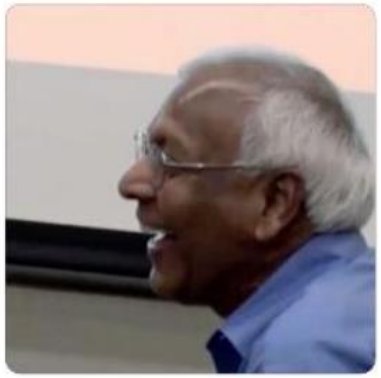
Top 2 retrievals

Gallery: 20 billion face images

Clearview.AI Retrievals: Occlusion

Original search image

5



7

11

12

Retrieved images

NTIA Initiative

- Major self-regulatory initiative intended to address privacy concerns associated with facial recognition technology.
  - Advocates and industry groups were attempting to develop a voluntary, enforceable code of conduct for the use of facial recognition technology and generally define the contours of transparency and informed consent.
- Stumbling block: nine consumer advocacy groups withdrew due to a lack of consensus on a minimum standard of consent re: commercial use of facial recognition technology.
- Self-regulatory guidelines were issued, but without any significant privacy requirements.

future tense ASU | NEW AMERICA | SLATE

future tense THE CITIZEN'S GUIDE TO THE FUTURE | JUNE 16 2015 7:04 PM

Frustrated Privacy Advocates Say Industry Has No Interest in Facial Recognition Safeguards

By Lily Hay Newman

14

Shoppers look for Black Friday deals at Somerset Collection mall on Nov. 29, 2013, in Troy, Michigan. Soon, you might not be just another face in the crowd when you go shopping.

Photo by Joshua Lott/Getty Images

The FBI has been developing a powerful and **extensive facial recognition database** for years now. **Facebook has one, too.** (For tagging! Right? Guys?) But if the technology seems a little creepy to you, you're not alone. Google even **banned facial recognition apps** on Glass in 2013. Now a Department of Commerce working group meant to reconcile these issues is struggling after all nine privacy advocates on the committee quit.

#ORDERTOCOMPLY

Facial recognition

The CNIL issues order to CLEARVIEW AI

THE SYSTEM

Clearview AI collects photographs and videos freely available on the Internet, including social media. Thanks to this collection, **the company markets access to its search engine** in which a person can be searched using a photograph. To do so, it establishes a **"biometric template"** without the consent of the persons concerned.

THE INVESTIGATIONS

Several complaints were sent to the CNIL, which was also warned by **Privacy International**.
These complaints revealed the difficulties encountered by the complainants in exercising their rights with Clearview AI.

THE BREACHES

1. **Unlawful processing of personal data because the collection of the photographs and the use of biometric data are done without a legal basis.**

2. **Lack of satisfactory and effective consideration of the rights of individuals**, particularly of requests for access to their data.

THE DECISION

The Chair of the CNIL has decided to order CLEARVIEW AI to cease this illegal processing and to delete the data within two months.

CNIL.

Wrongfully Accused by an Algorithm

(a)

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

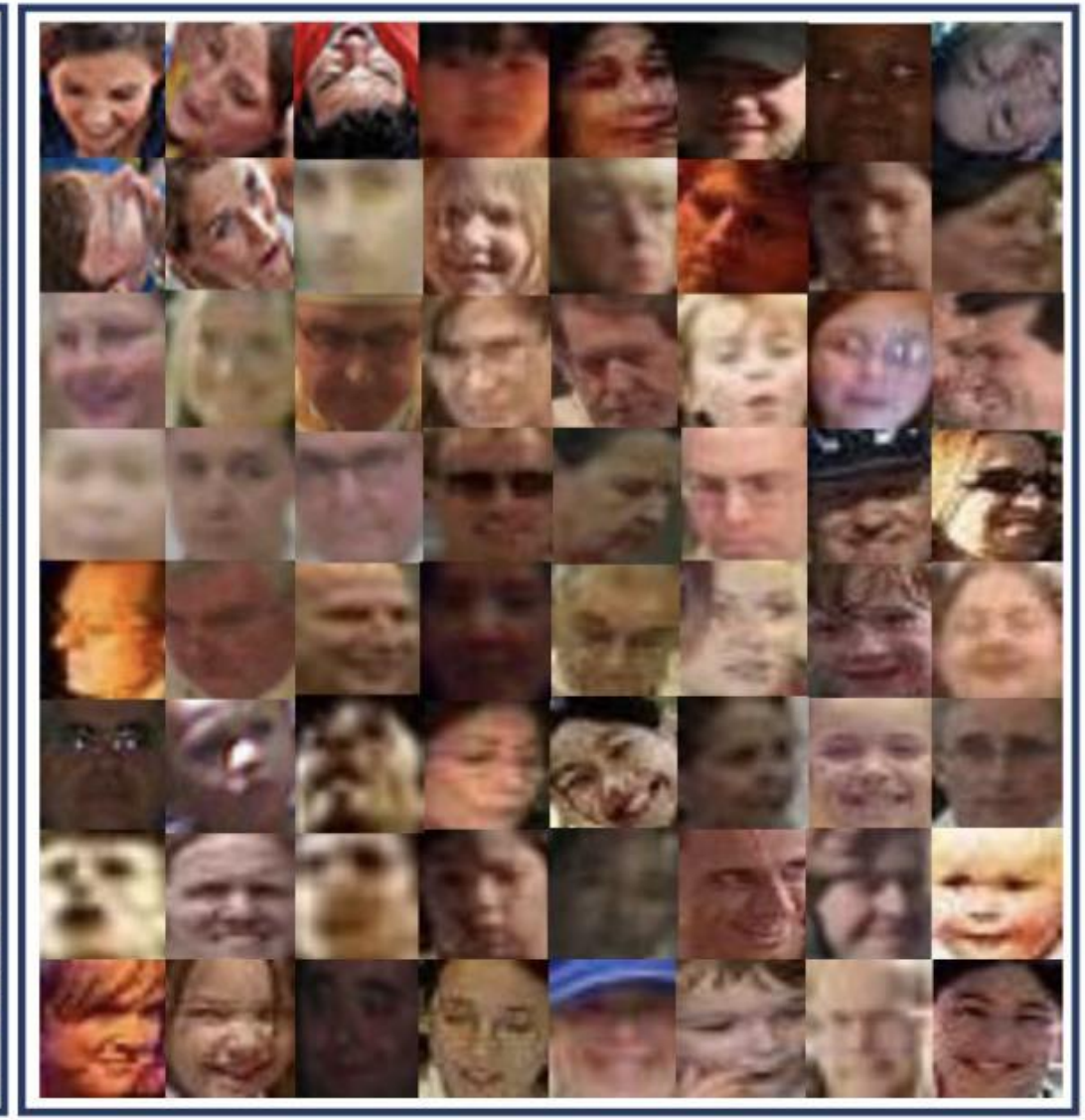
Probe Image	Investigative Lead
	

(b) Investigative Lead Report

FR system wrongfully identified (a) Robert William when the CCTV frame in (b) was searched against a 49M gallery; forensic experts did not conduct a manual examination of the candidate list

New York Times, "Wrongfully Accused by an Algorithm," https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, 2020.

TinyFace Dataset



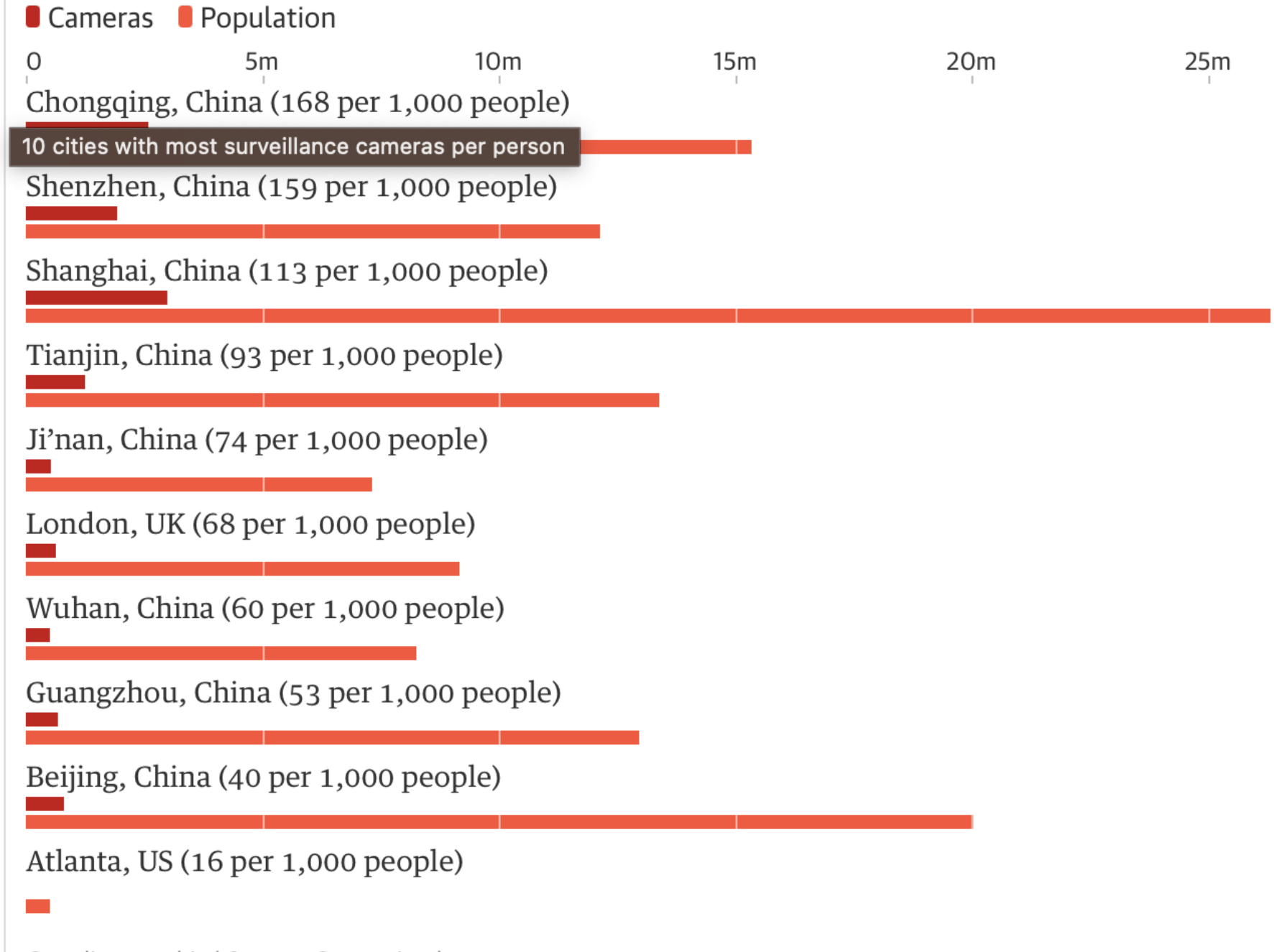
- **Low resolution face images (average 20×16 pixels) of ~5K identities.** (https://qmul-tinyface.github.io/)
- Rank-1 accuracy + **75.80%**

Chongqing:
World's Most Heavily Surveilled City

2.58 m cameras for 15 m people (one camera/six residents); 1 billion worldwide by 2021

https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

10 cities with most surveillance cameras per person



MBZUAI

Face Spoofs

Live

TAR @ 2.0% FAR:

Paper Mask

100%

Half Mask

96%

Mannequin

95%

Paper Cut

95%

Impersonation

90%

Replay

72%

Silicone Mask

56%

Print

51%

Cosmetic

44%

Paper Glasses

43%

Transparent

39%

FunnyEye

33%

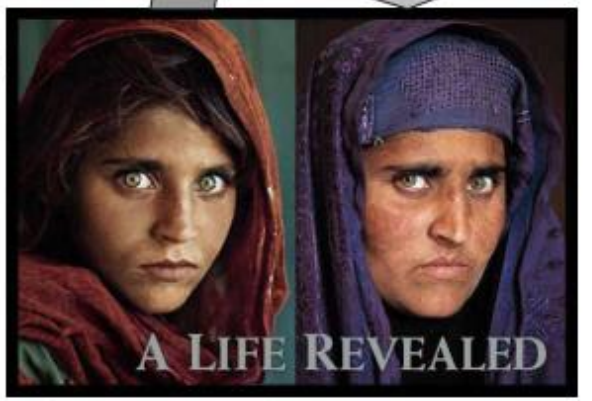
Obfuscation

31%

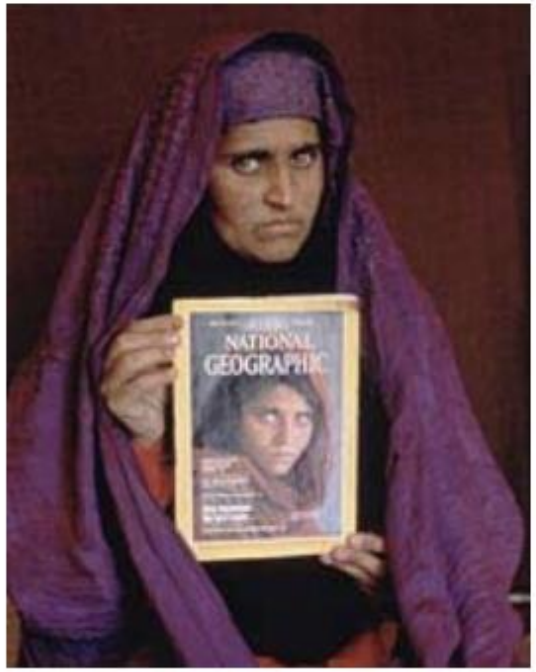
All spoofs except Mannequin, Impersonation, Transparent, and Obfuscation belong to the same person in Live

D. Deb and A. K. Jain, "Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach", arXiv:2006.02834, 2020.

Iris Biometric got really famous in the lost Afghan girl story..



Source: National Geographic Magazine



- In 1994 National Geographic photographer Steve McCurry took a picture of a little Afghan girl called Sharbat Gula in refugee camp in Pakistan.
- Her photo (she had amazing green eyes) made it to National Geographic 100 best Pictures!
- McCurry later tried to trace and find the girl, until finally 17 years later he located a girl with those same haunting green eyes.

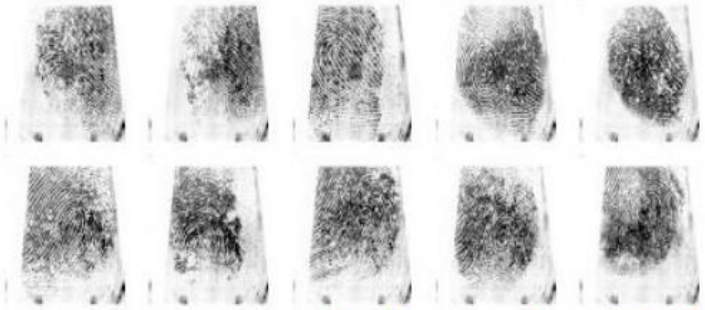
http://news.nationalgeographic.com/news/2002/03/0311_020312_sharbat.html

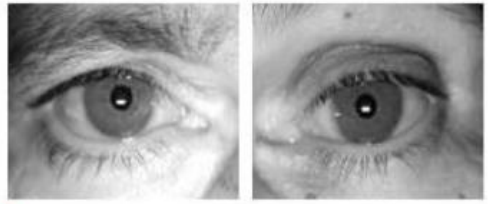
17 years passed…how to verify if this was the same girl?

- Hard-ship changed the girl's appearance. But she had those same haunting green eyes…
- The Explorer team got verification using U.S. FBI iris scanning technology. They used iris image from old taken photograph and compared to the new one.
- Iris code declared a 'match'!
- This was indeed the same girl! Iris biometric made it possible to verify this.

Aadhaar: World's Largest Biometric System

Fusion of 10 fingers, face & two irides for de-duplication





Gallery size: ~1.4 billion

~50 million authentications/day

https://uidai.gov.in/

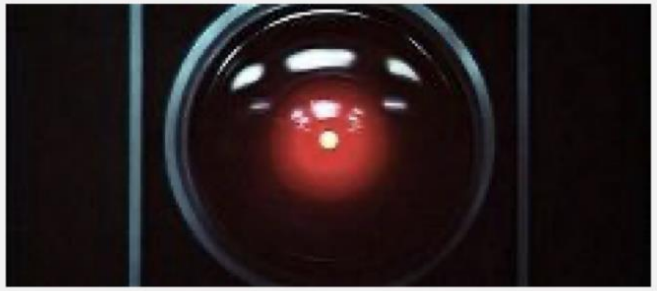
MBZUAI

Scalability

- **World population (2020) = 7.8 billion; #births/year = 130 million; projected to increase to 9.8 billion in 2050**
- **The United Nations Sustainable Development Goal (SDG) Target 16.9: "to provide legal identity for all, including birth registration" by 2030**

https://www.worldometers.info/world-population/

Biometrics in the Movies



2001: A Space Odyssey (1968)
Voice recognition

Blade Runner (1982)
Biometric scan for empathy

Star Trek II: The Wrath of Khan (1982)
Iris recognition

Judge Dredd (1995)
Biometric-authenticated weapon

Gattaca (1997)
DNA typing

Enemy of the State (1998)
Facial recognition; mass surveillance

Bourne Identity (2002)
Palm reader

Minority Report (2002)
Eye replacement for iris recognition

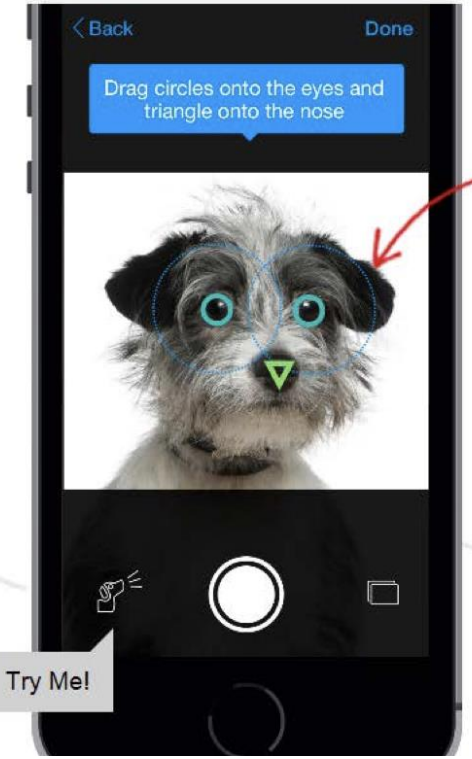
X-Men: Days of Future Past (2014)
Fingerprint scan spoofed

Facial Recognition for Pets Could Help Cities Save Furry Lives

Facial recognition is an emerging technology typically fraught with controversy, but most seem to agree that for animals, there's nothing but potential.

Finding Rover

Home Blog Spots Partners Login Regist



1 Take a front-facing photo

A good picture is easy to take with our bark button.

2 Mark the e and nose

Simply drag onto the pho

3 We verify t

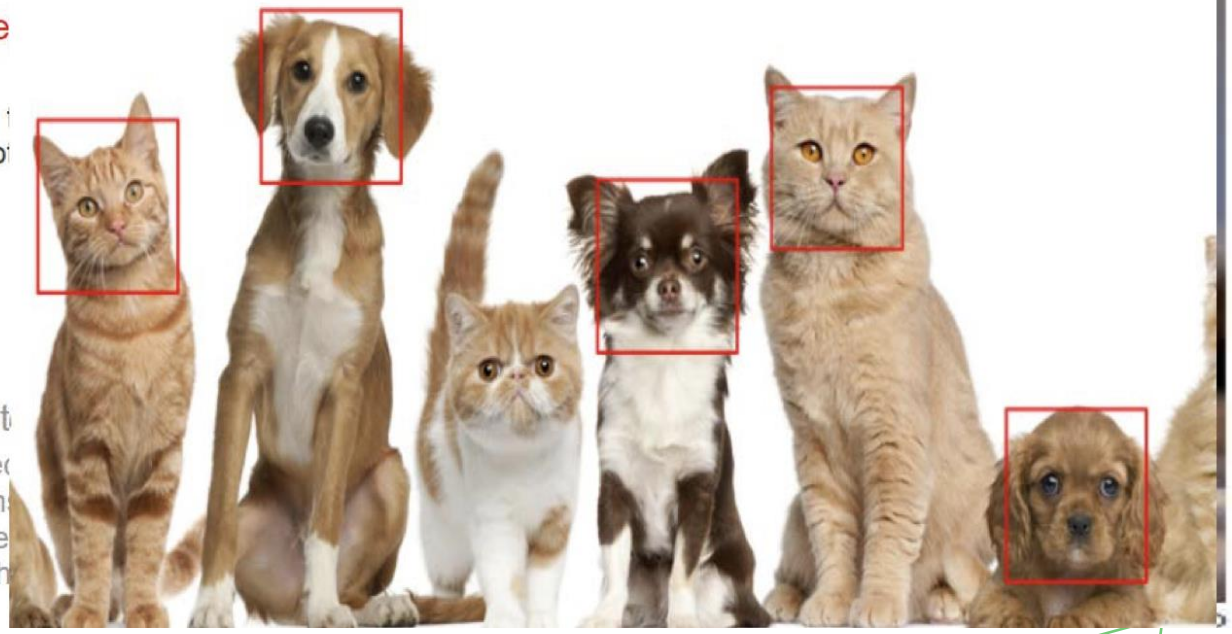
Our facial rec system scan dog's unique and keeps th just in case.

ArcSoft

Technology
our core

Product
software & apps

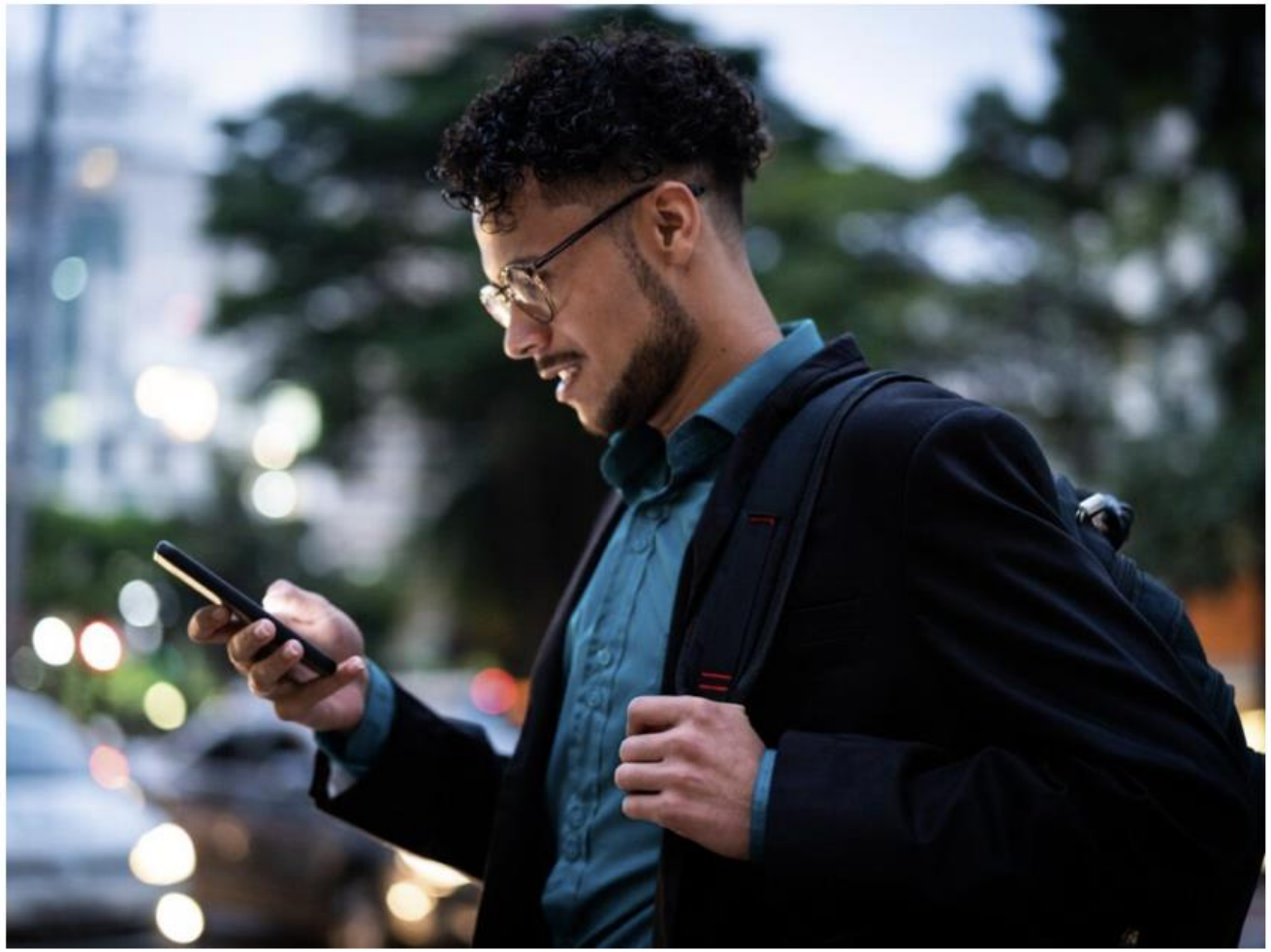
Corporate
who we are



NIST plans new biometrics test for presentation attack detection systems

Apr 5, 2022, 5:08 pm EDT | Chris Burt

CATEGORIES Biometric R&D | Biometrics News | Liveness Detection



The National Institute of Standards and Technology, the U.S. Commerce Department's body for setting the bar in biometrics and other advanced technologies, is launching a new version of its Face Recognition Vendor Test for technology to fight biometric spoof attacks.

MOST READ THIS WEEK

Ethiopia moves closer to ePassports and digital ID with Toppan agreement

Worldcoin soon back to business in Kenya as co-founder eyes next growth phase

EU's biometric Entry/Exit System may have a launch date

Australia to rebrand myGovID following audit recommendation

Tag certified for biometric Mastercards, Zwipe and HID introduce recycled PVC cards

Canada makes another move towards age verification for porn sites

Biometrics launch for gumshoes and robot restaurants

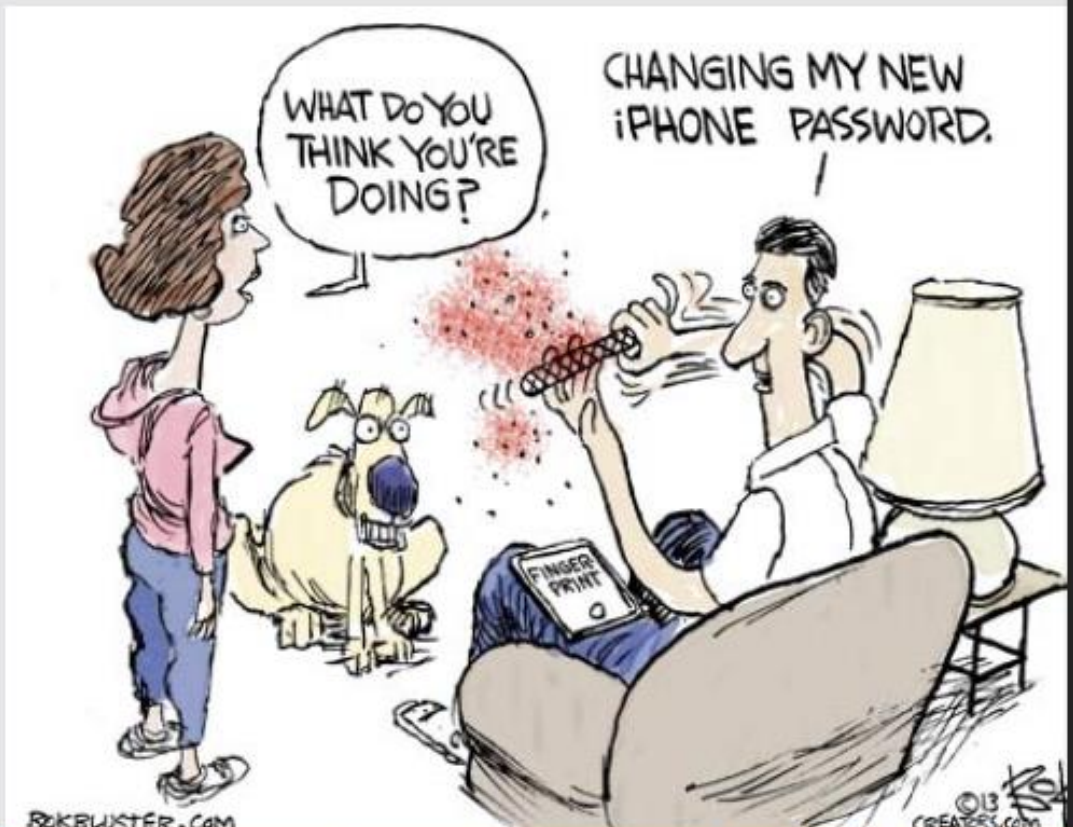
Presentation Attacks

- Spoofing is common term used most in past decade.
- ISO Standards underway:
  - **Presentation Attack** Definition: Presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system*

- Why?

  Posing as another individual
  - Positive ID applications

  Hiding your identity
  - Negative ID applications
  - May form 'new' identity for positive ID



Fingerprint Presentation Attacks

- **Cooperative**

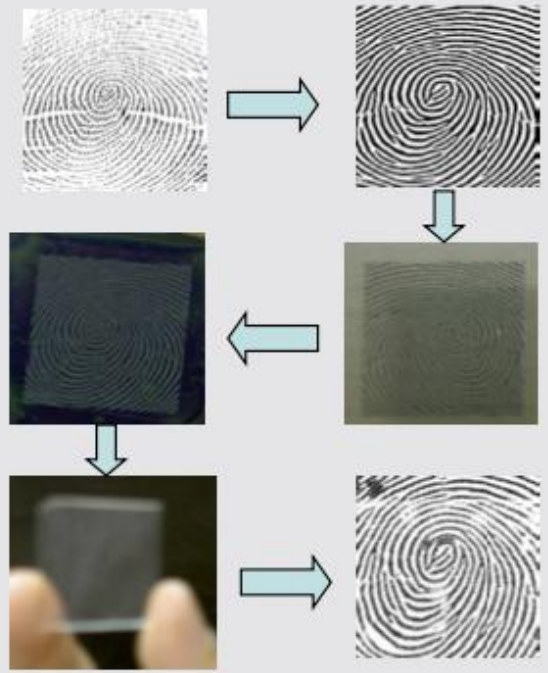
  Characteristic captured directly from individual with assistance (e.g. finger mold)

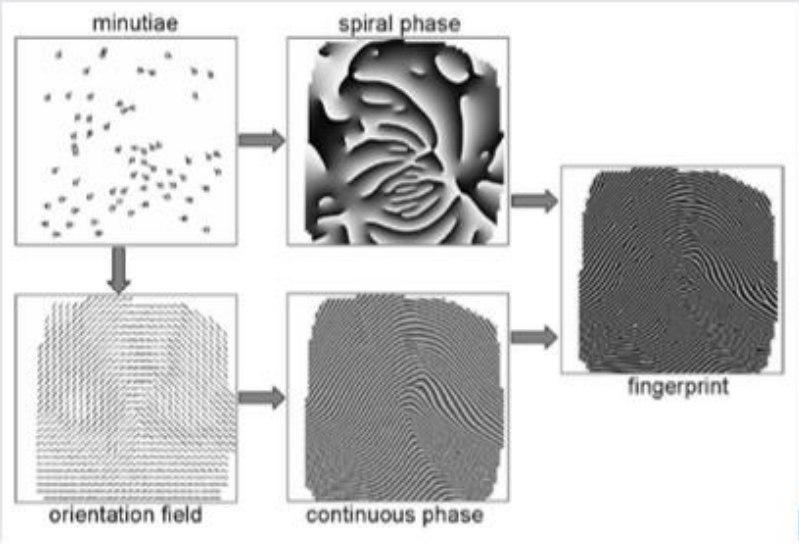
- **Latent**

  Characteristic captured indirectly through lifting a latent sample

- **Synthetic**

  Synthetic characteristic, not mapped to real person (e.g. synthetic fingerprint)





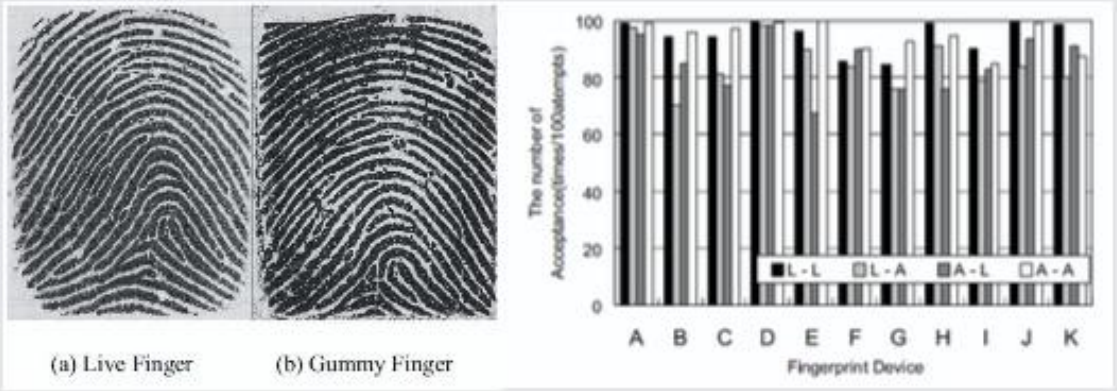
Feng and Jain, Advances in Biometrics article, 2011 [1].

Coli, et al, 2006 [2].

CITeR

Presentation Attack Testing on Conventional Systems

- Matsumoto et al., 2002 [3]
  - Testing acceptance rate of gelatin and silicone fingers (in terms of matching)
- Thalheim et al., 2002 [4]
  - Tested various techniques for spoofing biometric systems
  - Reactivating latent print and fingerprint on adhesive film
- Galbally et al., 2010 [5]
  - Optical and thermal sweeping sensors shown to be vulnerable to direct (presentation) attacks
- LivDet competitions 2009-13 [6]



Presentation Attack Detection (PAD)

- Presentation Attack Detection (PAD) *

  Automated determination of a presentation attack

- Examples of PAD

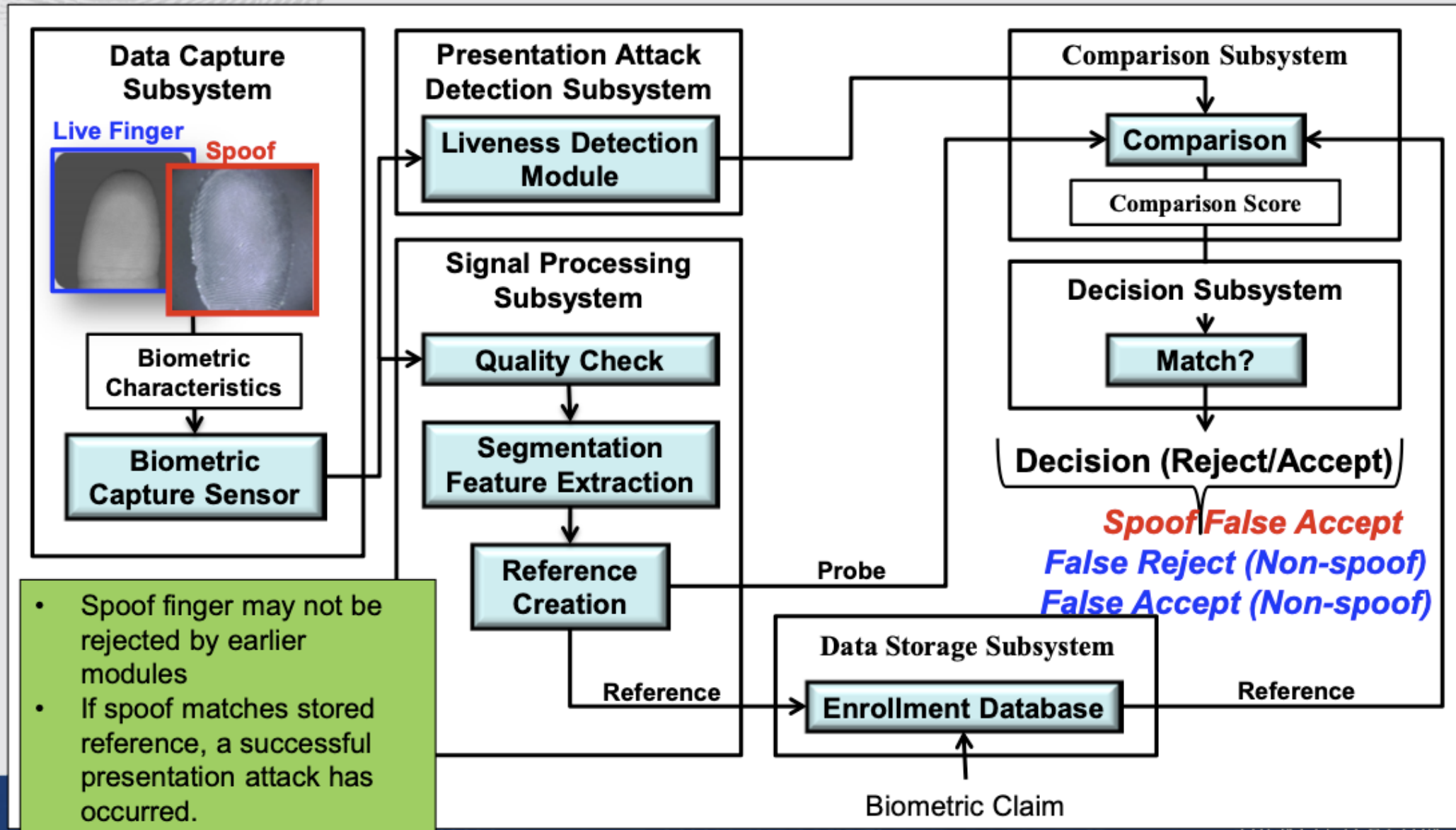
  Liveness detection (failure)

  Artefact detection

  Altered biometric detection

  Others terms that have been used: anti-spoofing, biometric fraud, spoof detection, authenticity detection, etc.

What about matching? (Spoof Input)



- Spoof finger may not be rejected by earlier modules
- If spoof matches stored reference, a successful presentation attack has occurred.

Summary

- Performance metrics for PAD system

  Normal Presentation Classification Rate (NPCR): percentage normal presentations that are accepted as normal presentations

  Attack Presentation Classification Rate (APCR): percentage of attack presentations correctly classified as attack presentations

- Performance metrics for combination of PAD subsystem and Comparison subsystem

  False accept rate (FAR): Percentage of imposters accepted by the syster

  False reject rate (FRR): Percentage of genuine users rejected by the syst

  Spoof False Accept Rate (SFAR)--Percentage of spoof samples that are accepted by the system (i.e. by matching and PAD)