Keynote Address:
Building Robust Biometric Systems: From Design to Deployment

Prof. Arun Ross, Professor, Michigan State University

Building Robust Biometric Systems: From Design to Deployment

Arun Ross

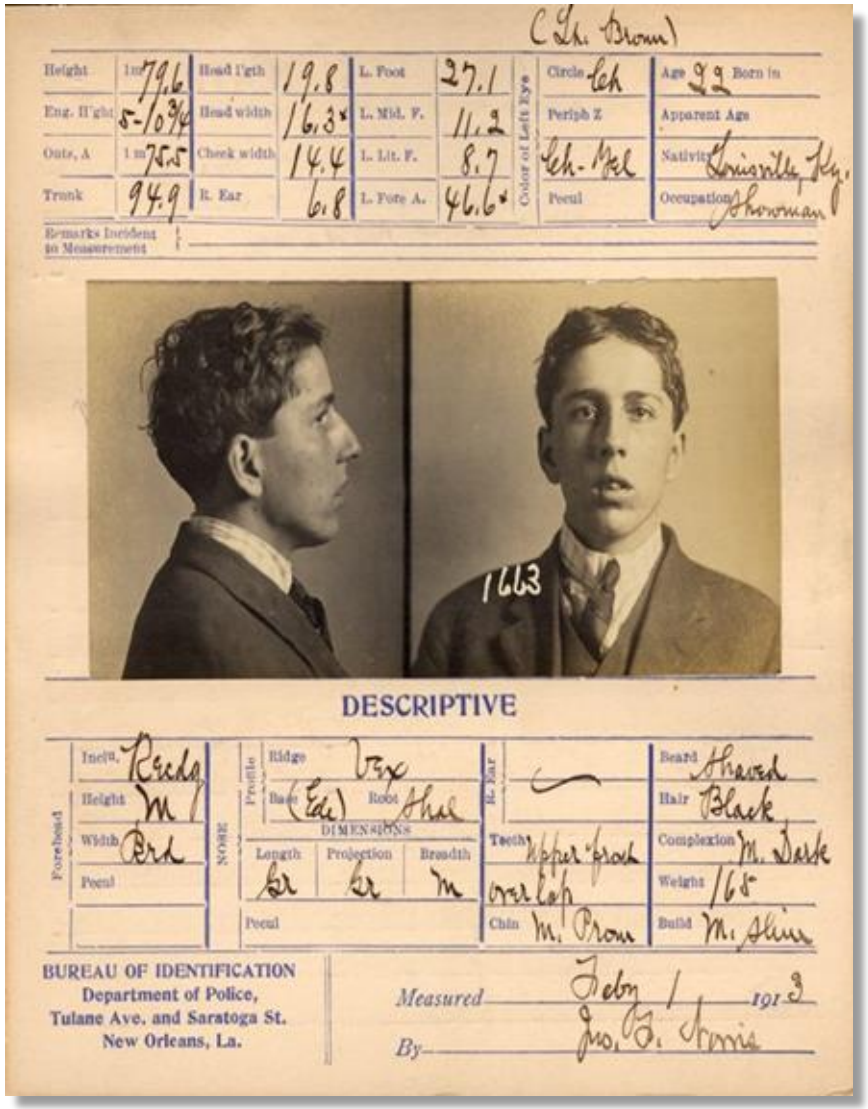
Professor | Michigan State University
Site Director | NSF Center for Identification Technology Research
President-Elect | IEEE Biometrics Council
Advisor | IAPR TC4 on Biometrics

rossarun@cse.msu.edu

What is Biometrics?

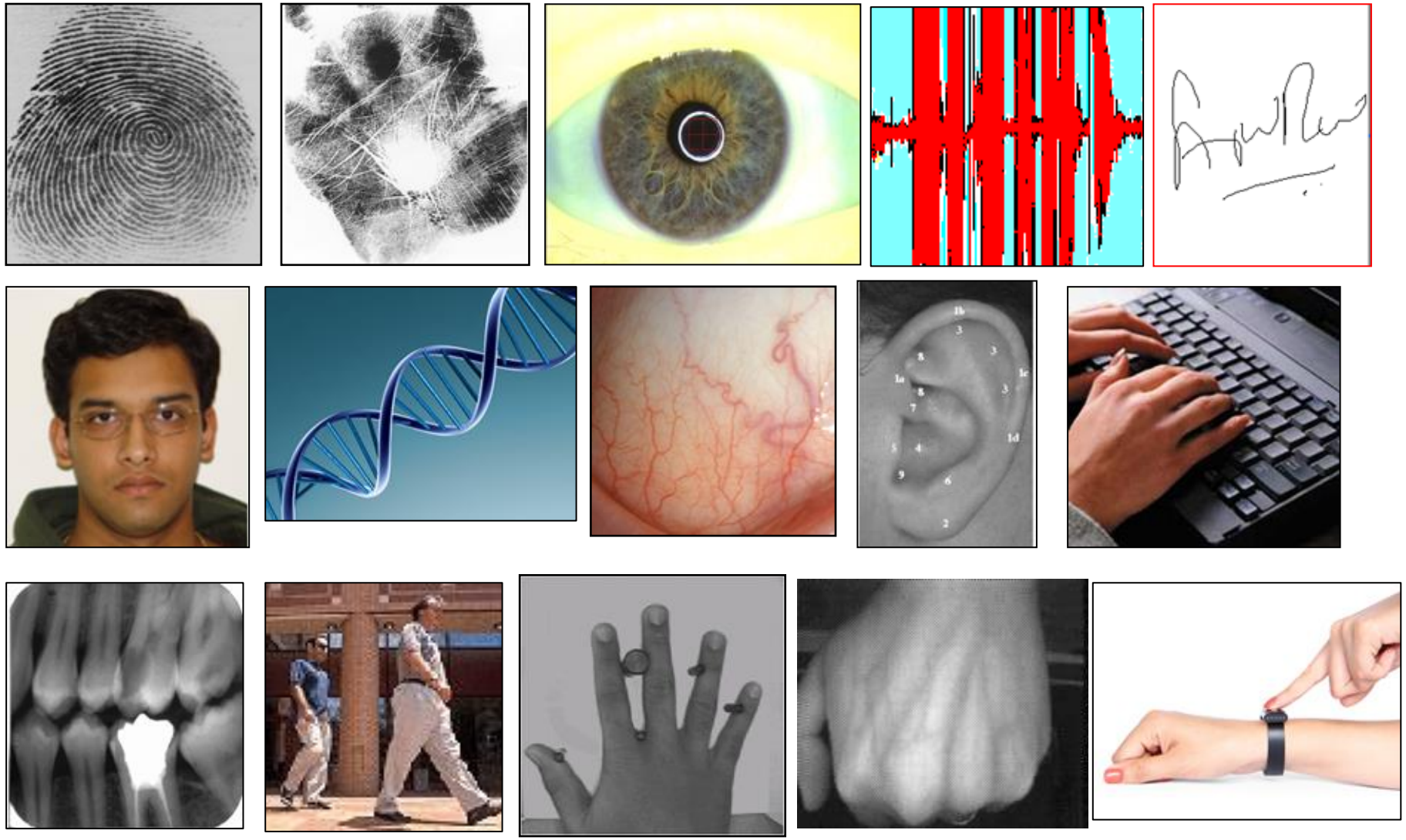
What is Biometrics?

- Automated recognition of individuals based on their biological and behavioral traits
- Traits from which distinguishing, repeatable features can be extracted
- Examples include fingerprint, face, iris, voice, etc.



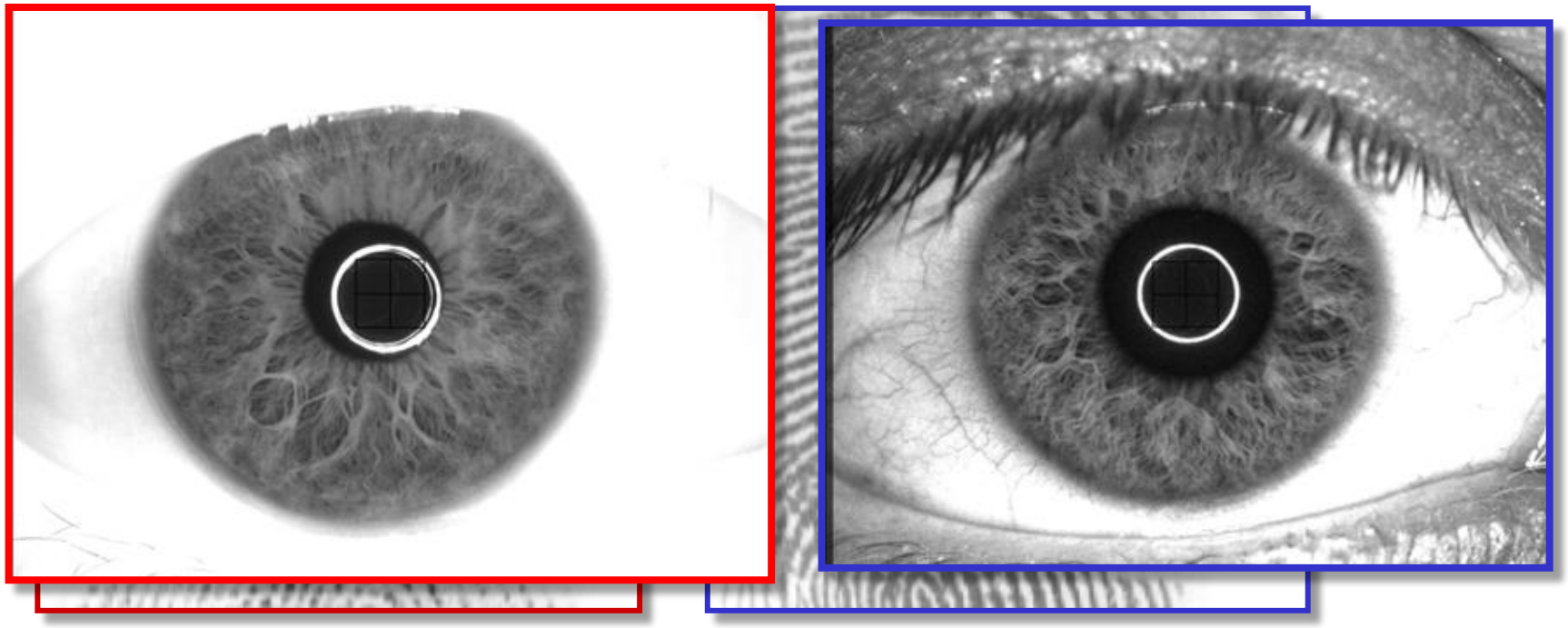
H.T. F. Rhodes, Alphonse Bertillon: Father of Scientific Detection, Harrap, 1956

Biometric Traits



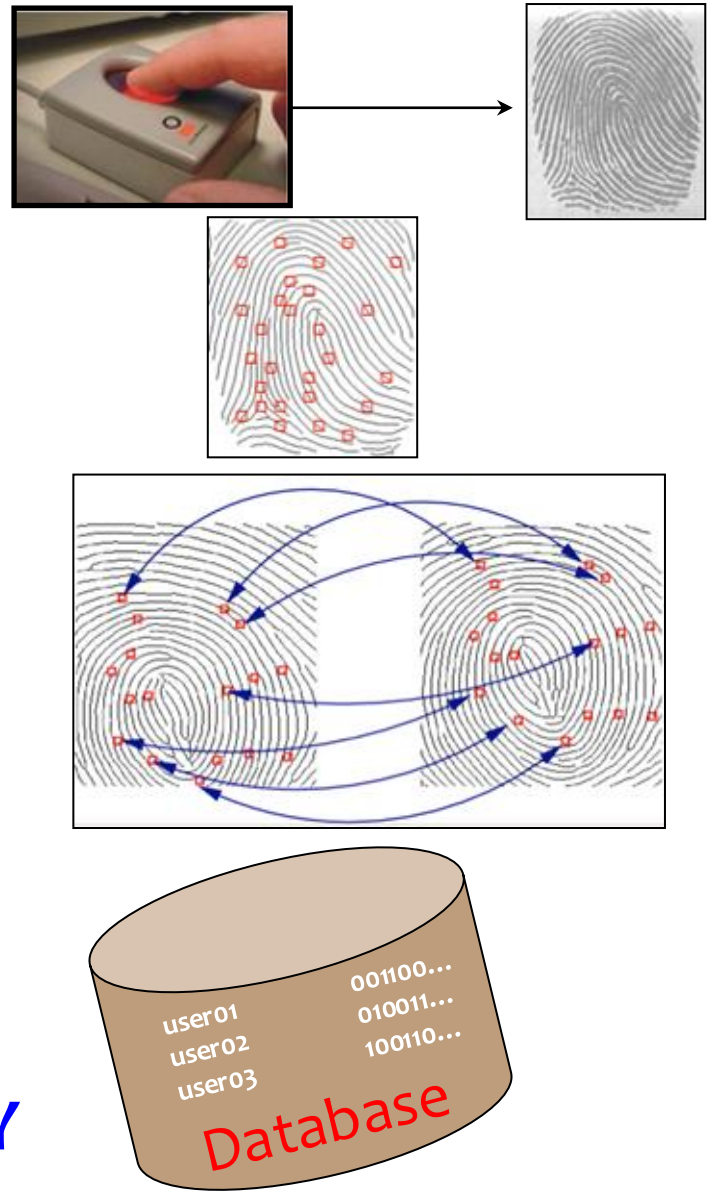
Biometric Matching or Comparison

- Given two biometric samples, compute a score that is a measure of the probability that two samples are from the same biometric source or from different biometric sources
- Two types of errors: False Match (False Positive) and False Non-Match (False Negative)



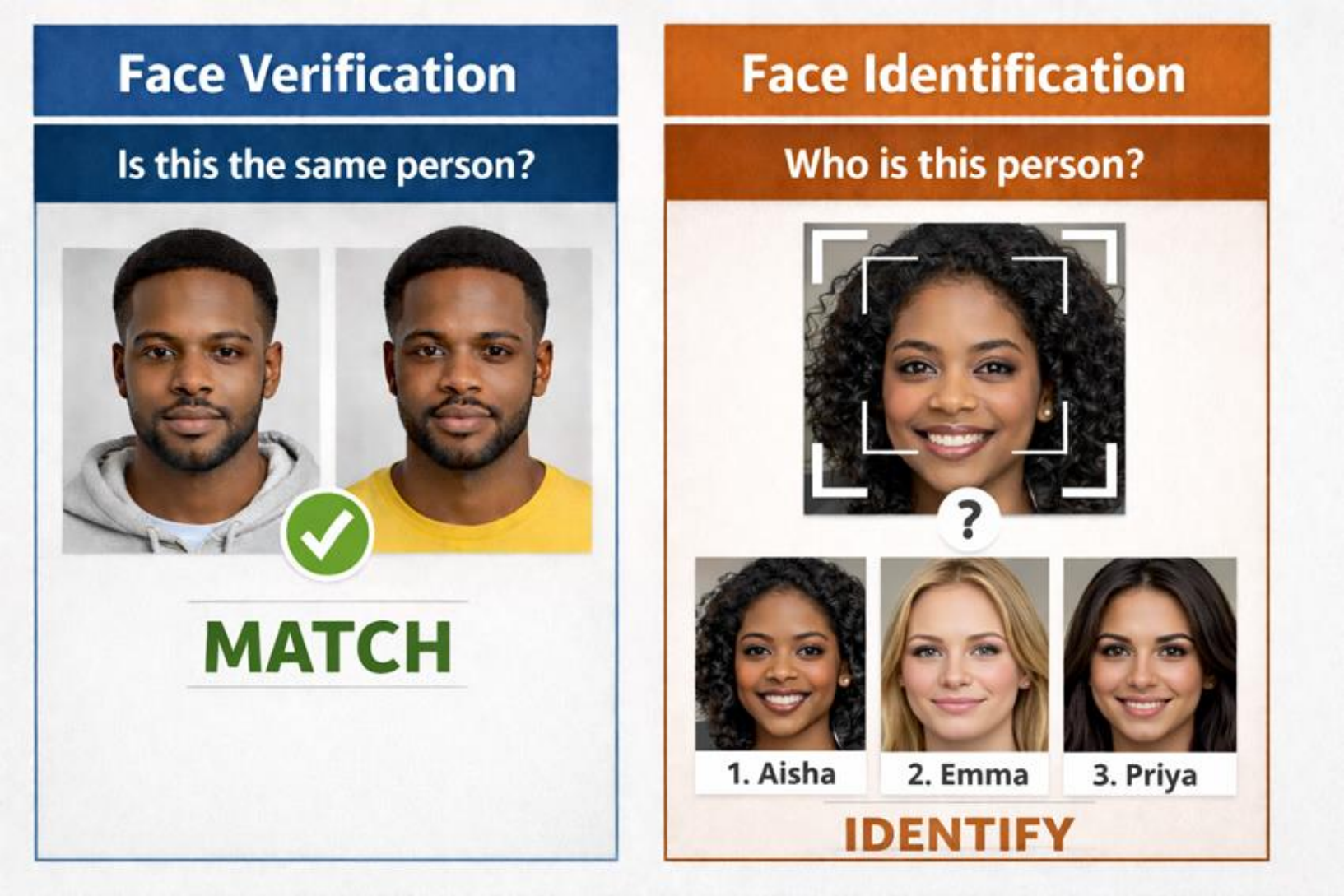
Components of a Biometric System

- **Sensor**: To acquire biometric data
- **Feature extractor**: To extract a discriminative set of features from the data
- **Comparator**: To compare two extracted feature sets and produce **a score**
- **Database (Gallery)**: To store biometric templates or reference data of individuals



PROBE and GALLERY

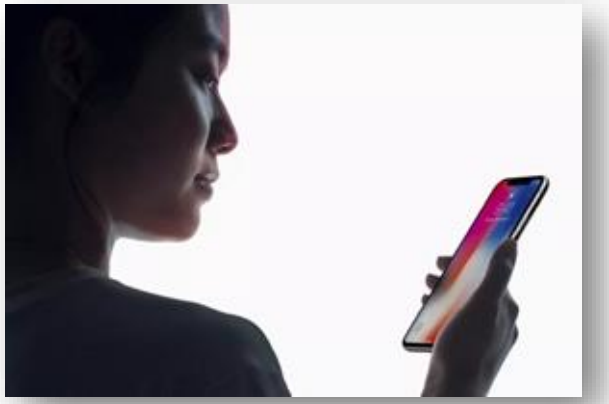
Verification vs Identification



Biometric Applications

Iris: Health Care

Fingerprint: US OBIM



Face: Apple FaceID

Fingerprint: Refugee Services

Finger Vein: ATMs

DeepFace: CNN for Face Recognition

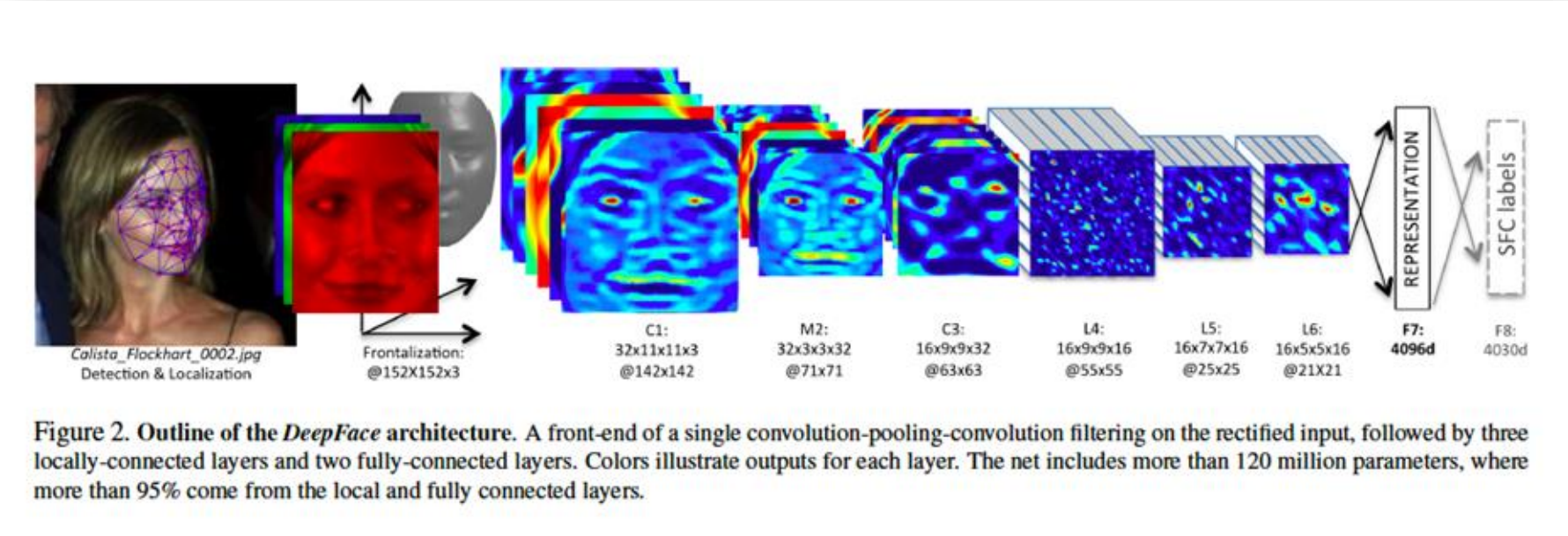


Figure 2. **Outline of the *DeepFace* architecture**. A front-end of a single convolution-pooling-convolution filtering on the rectified input, followed by three locally-connected layers and two fully-connected layers. Colors illustrate outputs for each layer. The net includes more than 120 million parameters, where more than 95% come from the local and fully connected layers.

Taigman et al., DeepFace: Closing the Gap to Human-Level Performance in Face Verification", CVPR 2014

- The neural network learns a function to map the input pixels to an output class
- In the process, the network learns filters that can be used to extract features from the input image

Massive Improvement in Face Recognition Accuracy

- Gallery size = 1.6M identities
- "The most accurate algorithm in 2018, microsoft-4, gives FNIR = 0.002 vs. the 2014 result for NEC of FNIR = 0.041" (Miss rate Rank = 1)
- "This constitutes almost a twenty-fold reduction in false negatives"
- "The massive accuracy gains are consistent with an industrial revolution associated with the incorporation of convolutional neural network-based techniques into the prototypes"

Patrick Grother, Mei Ngan, and Kayee Hanaoka. Ongoing face recognition vendor test (FRVT) part 2: Identification, NISTIR 8238, 2018.

Deep Neural Networks (DNNs)

- DNNs can automatically learn what type of features to extract from the input image
- Heavily data-driven approach
  - Requires copious amounts of training data
- Training is computationally expensive
  - Requires Graphics Processing Units (GPUs)
- But the actual **decision** is rendered quickly

Factors to Consider
For Building Robust Biometric Systems

Intra-user Variations

© Nostra

FNMR: False Non-Match Rate (False Negative)

Inter-user Similarities

TWIN BROTHERS
© Martin Schoeller

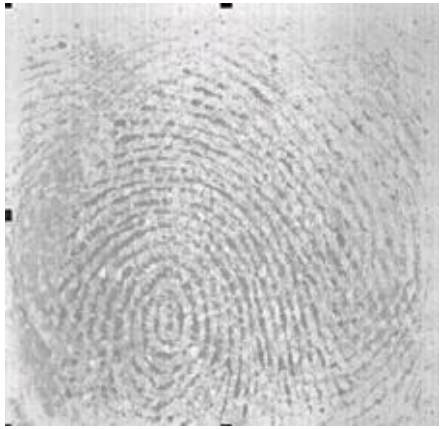
MOTHER DAUGHTER
© PleasantonWeekly.Com

FMR: False Match Rate (False Positive)

Noisy Data

During enrolment

During verification



Noise due to smearing, residual deposits, cuts and folds, etc.

Can impact both FMR and FNMR

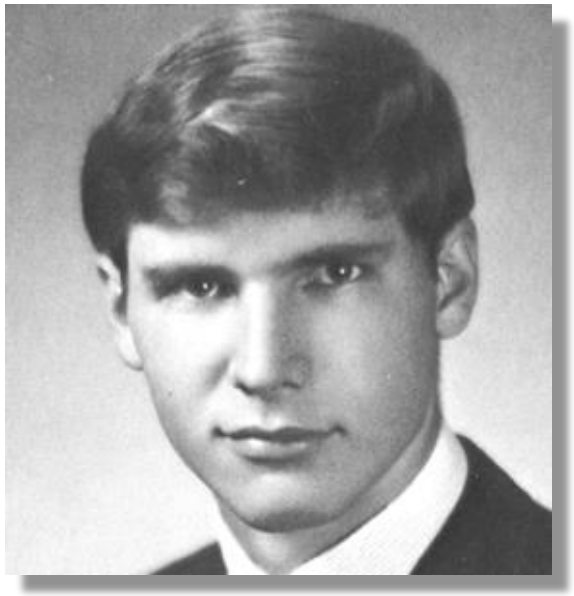
Non-universality

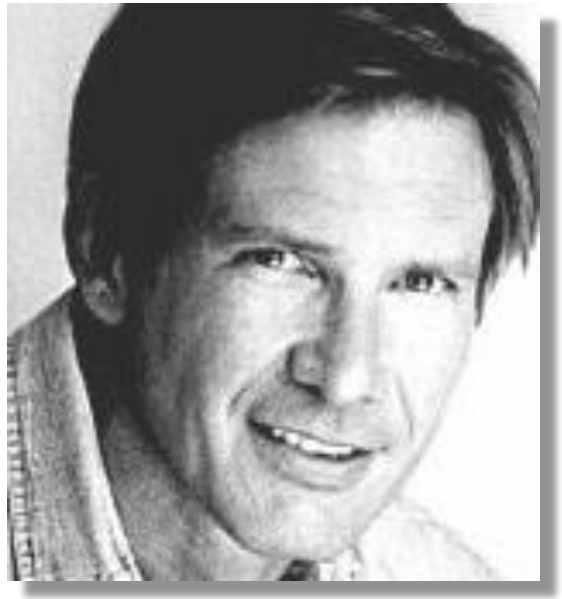
- Some people may consistently offer poor quality fingerprint images which means they have to be identified by some other means

Four impressions of a user's print exhibiting incomplete ridge information

FTE: Failure-to-Enroll Problem

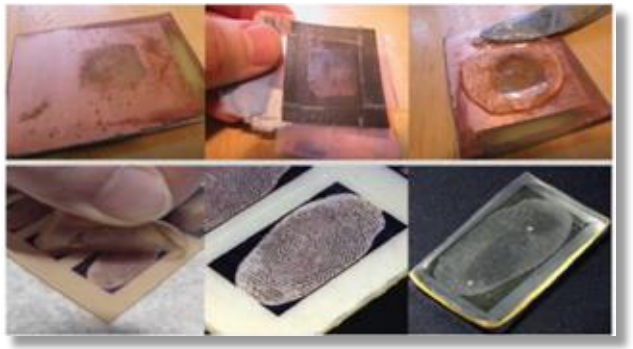
Biometric Ageing

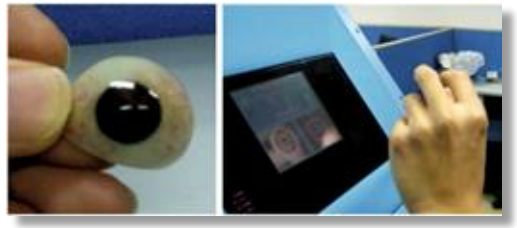




Presentation Attacks

- Spoofing: Altering one's trait or creating a physical artifact in order to "spoof" another person's trait





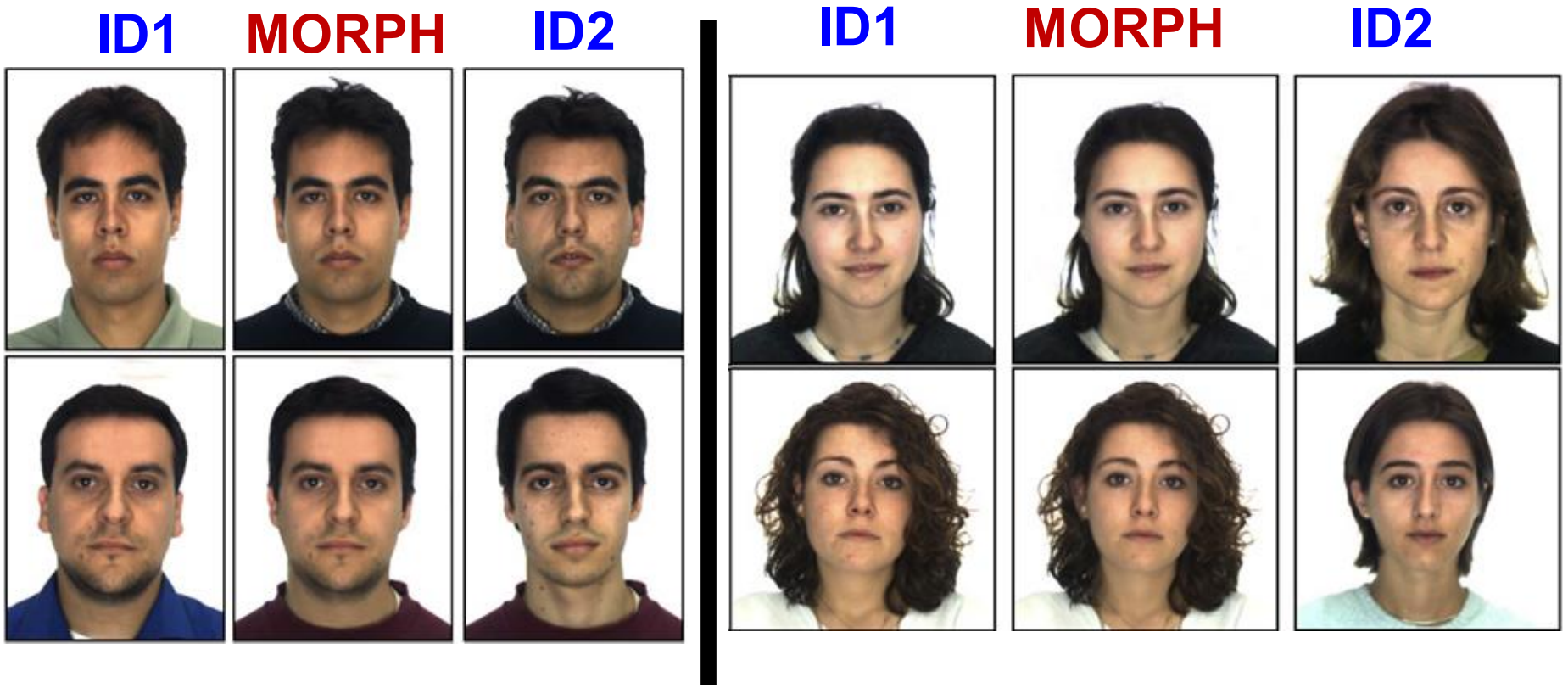
Deepfakes



https://thispersondoesnotexist.com/

Morph Attacks

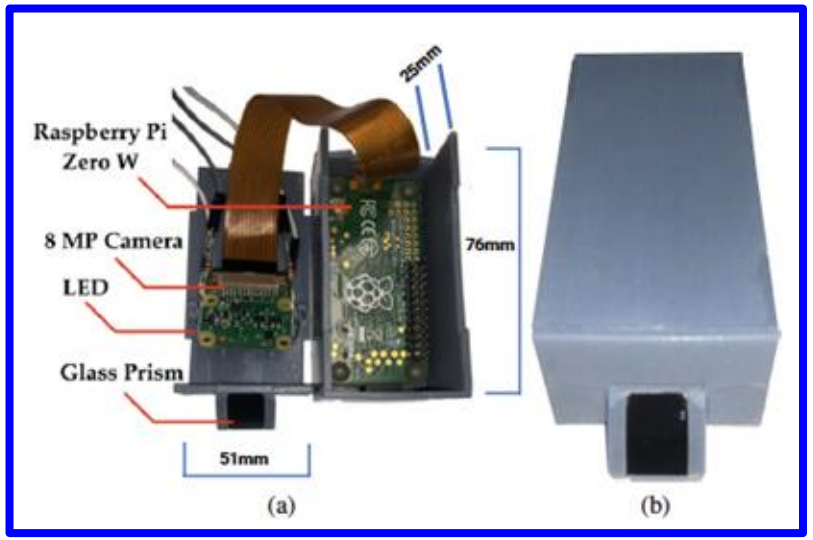
- Morphed Faces: Combining two face images
- Morph image matches against two identities!

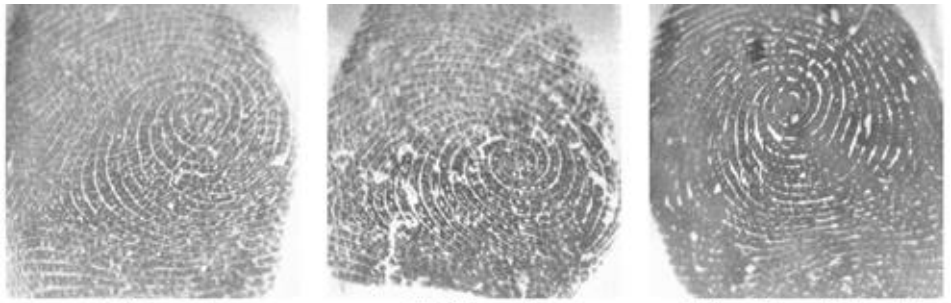


New Developments

Infant Fingerprints: Vaccination Tracking

1900 PPI fingerprint reader for infants





(a) 13 days old (b) 15 days old (c) 3 months and 5 days old

J. J. Engelsma, et al., "Infant-Prints: Fingerprints for Reducing Infant Mortality", in CVPR Workshop on *CV4GC*, 2019

Large Language Models: Explainable Biometric Recognition

Match Verdict: Match

Similarity Attributes:

Facial Structure has a broad, rounded shape with similar jaw and cheekbone width. Similar eye size, shape, and spacing. Comparable width and nasal tip. Same lip thickness and mouth shape. Dark, thick, and similarly arched eyebrows. Similar Proportions appear well-aligned. Consistent light skin tone and texture. Eye region contours and spacing are alike. Ears are not clearly visible. Similar forehead height and straight hairline.

Distinctive Differences:

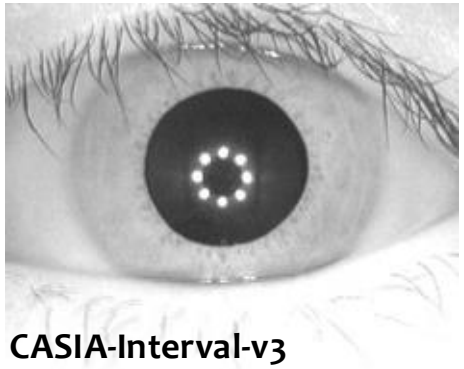
Pose variation: left image has a strong upward tilt. Lighting differs slightly. Subtle change in expression.

Overall Reasoning:

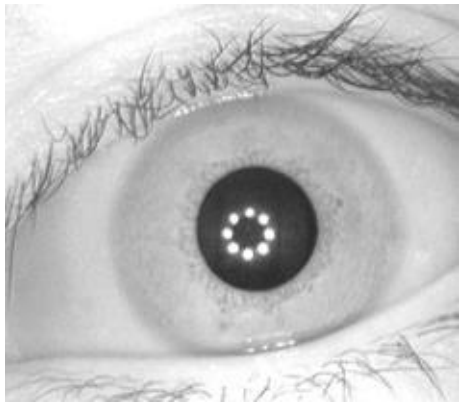
Despite differences in angle and lighting, identity-relevant features strongly align, supporting the likelihood that both images are of the same person.

One-to-One Verification

CASIA-Interval-v3



CASIA-Interval-v3



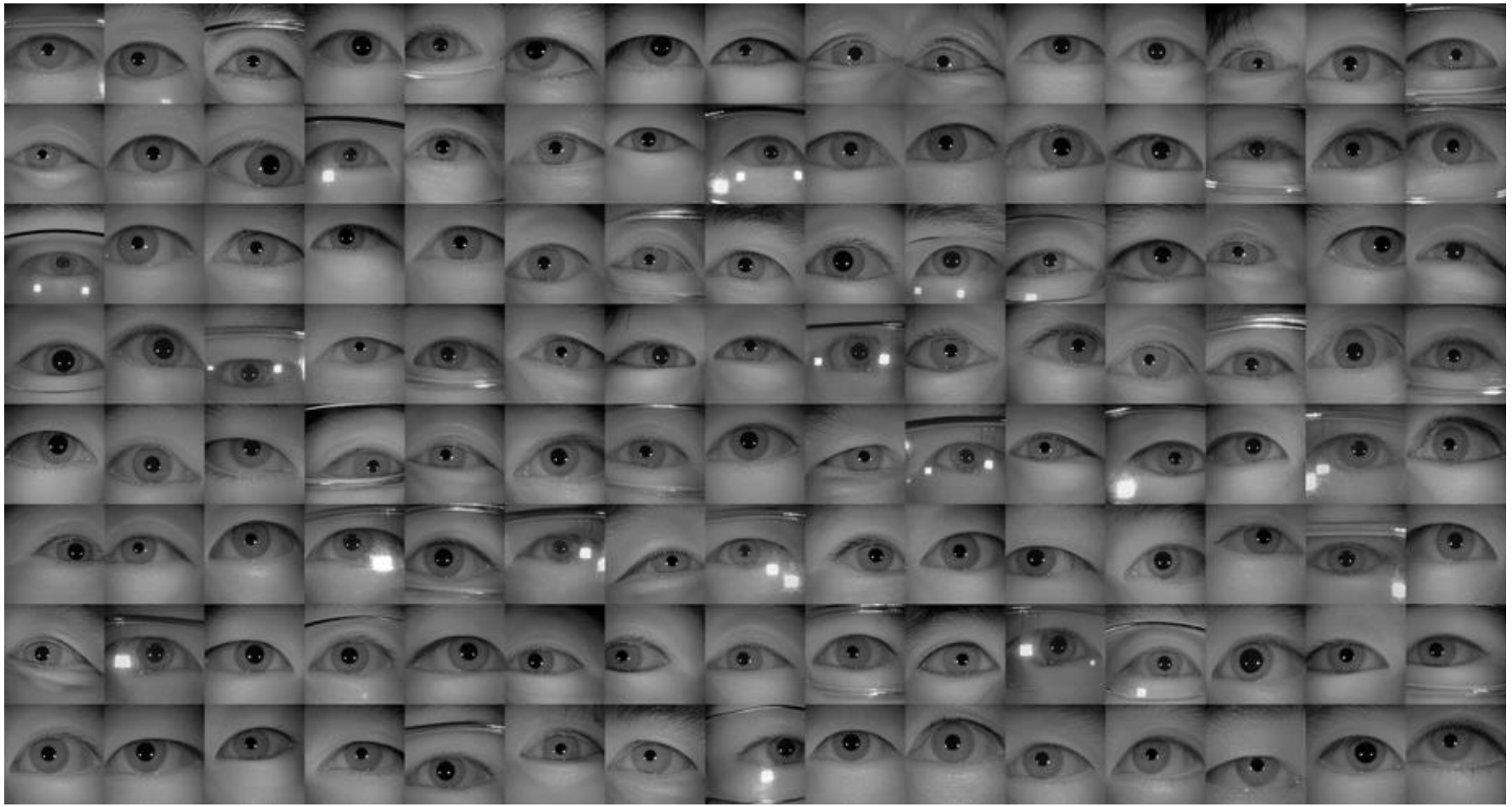
Prompt: "Great! Could you perform a similar analysis on the new attached images?"

GPT-4 Answer: "Based on visual information and the uniqueness of iris patterns as an identifier, there appear to be enough differences. Therefore, they could be from different individuals. "

Correct Answer: "Different individuals"

Farmanifard and Ross, ChatGPT meets Iris Biometrics, IJCB 2024

Generating Synthetic Biometric Data

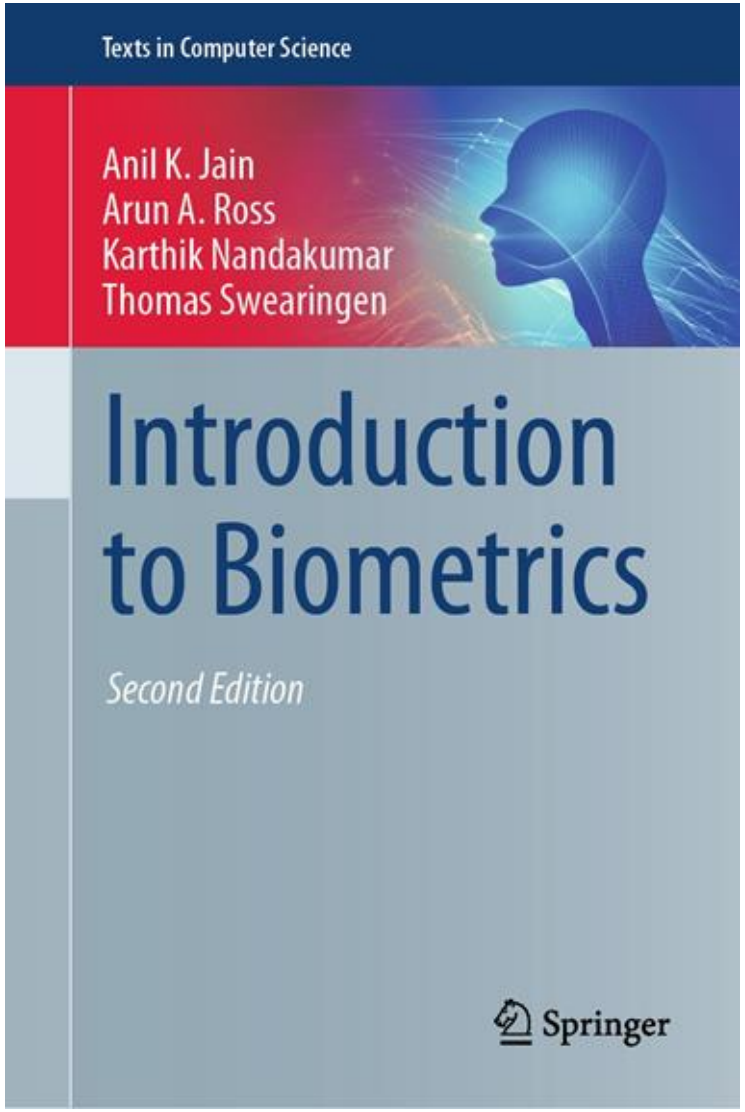


- For training neural networks
- For rare-scenario testing
- For enhancing privacy

Summary

- Biometrics is a fascinating pattern recognition problem with several societal benefits
- Advancements in other domains including AI have opened new opportunities for biometrics
- GenAI has led to the generation of synthetic data
- Methods to detect presentation attacks, morph attacks and DeepFakes are being developed
- Concerns about privacy and ethics are being addressed

Introduction to Biometrics: A Textbook



1. Introduction
2. Deep Learning Primer
3. Fingerprint Recognition
4. Face Recognition
5. Iris Recognition
6. Speaker Recognition
7. Additional Biometric Traits
8. Multibiometrics
9. Security of Biometric Systems

Building Robust Biometric Systems: From Design to Deployment

Arun Ross

Professor | Michigan State University
Site Director | NSF Center for Identification Technology Research
President-Elect | IEEE Biometrics Council
Advisor | IAPR TC4 on Biometrics
rossarun@cse.msu.edu