Biometric Systems

Guide to AI and Data Courses · Part III: Signals, Images and Audio

Biometric traits | Verification, identification | Error rates | Spoofing | Privacy | Neighboring courses

Sercan KÜLCÜ · Giresun University · Computer Engineering

© Sercan Külcü. All rights reserved. · Interactive HTML version of these slides: https://sercankulcu.github.io/files/ai_courses/slides/Chapter_24_Biometric_Systems.html

INTRODUCTION

What Question Does It Ask?

> **How is a person recognized from their face, fingerprint or voice?**

Biometric systems recognize a person by **physical and behavioral traits** such as face, fingerprint, iris or voice. The course covers extracting a template from a sample, matching two templates and accepting or rejecting by a threshold; security and privacy are an inseparable part of that decision.

At a glance

APPROACH matching and verification	**INPUT** face, fingerprint, iris, voice	**OUTPUT** identity decision
SUCCESS MEASURE FAR, FRR, EER	**MATH LOAD** medium	**DATA NEEDS** few samples per person

A Short History

1892
Galton publishes "Finger Prints": fingerprints are shown to be unique and permanent.

1901
Scotland Yard starts using fingerprints with the Henry classification system.

1991
Turk and Pentland publish eigenfaces for face recognition.

1993
Daugman publishes his iris recognition method, the basis of today's iris systems.

2013
Fingerprint sensors (Touch ID) start to spread in smartphones.

2014
DeepFace and the deep networks after it approach human level in face verification.

THE COURSE

Core Concepts

Enrollment
Extracting a template from a person's sample and storing it.

Template
The feature vector stored instead of the raw image.

Verification (1:1)
"Is this person who they claim to be?"

Identification (1:N)
"Which enrolled person is this?"

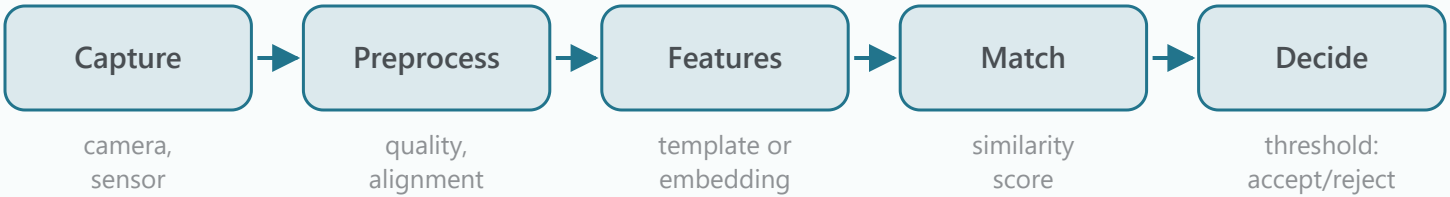
FAR and FRR
False accept and false reject rates; the threshold trades them off.

EER and DET curve
The point where both errors are equal; comparing systems.

Liveness detection
Catching attacks with photos, masks or fake fingers.

Multimodal biometrics
Combining face with voice, or fingerprint with iris.

A Typical Workflow



Example: A phone's face unlock captures the face with an infrared camera, detects and aligns it, extracts an embedding with a deep network, measures similarity to the enrolled template and unlocks if the score passes the threshold. A liveness check stops a photo from unlocking it.

THE COURSE

What Does the Course Cover?

1. Biometric systems: enrol, verify, identify
2. Measuring performance: FAR, FRR, ROC, DET, EER
3. Fingerprints: preprocessing, minutiae, matching
4. Face detection and alignment
5. Face recognition: eigenfaces, LBP, deep embeddings
6. Iris: segmentation, Daugman's code, Hamming distance
7. Speaker verification from voice
8. Behavioural biometrics: signature, gait, keystrokes
9. Multimodal biometrics and score fusion
10. Presentation attacks and liveness detection
11. Template protection and cancellable biometrics
12. Large-scale identification, indexing and standards

Skills you will gain

face processing with OpenCV and dlib

extracting face embeddings with InsightFace

plotting DET curves and computing EER

choosing a threshold by application risk

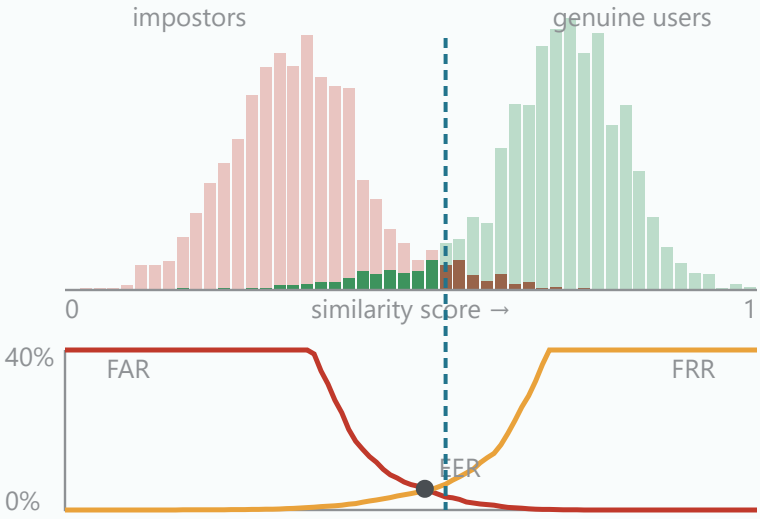
measuring performance per group

A typical semester; the order and coverage vary between universities.

TRY IT

Who Should the Gate Let In?

A face recognition gate gives each person a similarity score between 0 and 1; if the score passes the threshold, the gate opens. Move the threshold or pick a scenario to see the trade-off between accepting impostors and rejecting genuine users.



Threshold = **0.55**

Airport | Phone unlock | EER point

FAR (impostor accepted) = **3.25%**
FRR (genuine rejected) = **6.45%**
In 10,000 attempts ≈ 325 impostors get in, 645 travelers are stopped.

EER ≈ 5.3% (threshold 0.52): the point where both errors are equal.

A biometric system never says “certain”: the two distributions overlap, and the threshold is set by which error costs more. The course teaches the feature extraction that produces these scores and evaluation with FAR/FRR.

CONTEXT

Prerequisites

Courses worth knowing before this one, and why they are needed.

Course	Why it is needed
Pattern Recognition	matching, verification and identification
Computer Vision	face recognition
Programming	reading images and working with vectors in Python
Data Structures	indexing to scan millions of templates quickly in 1:N search

CONTEXT

Are You Ready for This Course?

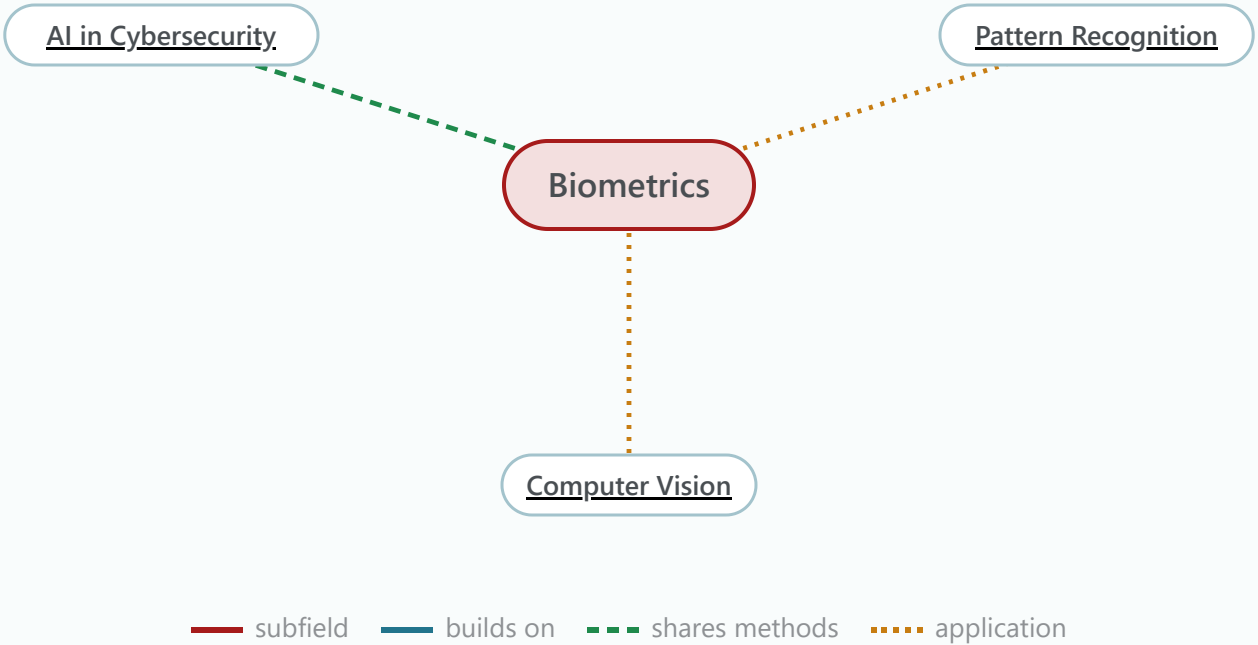
Ask yourself; for every "no", the right-hand column shows where to start.

Ask yourself	If not, start with
Can you load an image, crop it and convert it to greyscale?	Image Processing
Can you explain a classifier's ROC curve and false positive rate?	Pattern Recognition
Can you compute the cosine similarity between two vectors?	Linear Algebra
Can you process a folder of images with NumPy arrays in Python?	An intro programming course, then a short NumPy tutorial

If you can say "yes" to most of these, you are ready; one or two gaps can be closed during the semester.

CONTEXT

Neighbouring Courses



OVERLAP

Overlapping Courses

Relation	Course	Shared ground
application	This course applies the methods of Pattern Recognition	matching, verification and identification
application	This course applies the methods of Computer Vision	face recognition
shares methods	Shares methods with AI in Cybersecurity	authentication, spoof detection

DIFFERENCES

Where It Differs (1/2)

Criterion	Biometrics	Pattern Recognition	Computer Vision
Core question	How is a person recognized from their face, fingerprint or voice?	How do we decide from measurements which class an object belongs to?	How does a computer understand what is in an image or a video?
Approach	matching and verification	statistical decision theory	extracting meaning from images
Input	face, fingerprint, iris, voice	measurement or feature vector	image or video
Output	identity decision	class label	label, box, depth, 3D structure
Success measure	FAR, FRR, EER	classification error	accuracy, mAP, IoU
Math load	medium	medium-high: probability, linear algebra	high: geometry, linear algebra
Data needs	few samples per person	labeled examples	many labeled images

- **Pattern Recognition:** Pattern recognition assigns a sample to classes; biometrics recognizes people, with as many classes as people, always growing.
- **Computer Vision:** Computer vision tries to understand everything in an image; biometrics is a narrow, security-focused task that asks only identity.

DIFFERENCES

Where It Differs (2/2)

Criterion	Biometrics	AI in Cybersecurity	Speech and Audio
Core question	How is a person recognized from their face, fingerprint or voice?	How does AI catch attacks, and how is it attacked itself?	How are words, speakers and events extracted from a sound wave?
Approach	matching and verification	security knowledge plus ML	acoustic signal and language model
Input	face, fingerprint, iris, voice	network traffic, logs, files	audio waveform
Output	identity decision	alert, class, risk score	text, speaker, sound event
Success measure	FAR, FRR, EER	detection rate, false alarm rate	word error rate (WER)
Math load	medium	medium	medium-high
Data needs	few samples per person	imbalanced and constantly changing	many hours of recordings

- **AI in Cybersecurity:** AI in cybersecurity catches attacks; biometrics is authentication itself and must resist spoofing attacks.
- **Speech and Audio:** Speech recognition finds what was said; speaker recognition, a biometric, finds who said it.

PRACTICE

Applications

Phone unlock
Unlocking devices by face and fingerprint.

Border control
Automated gates using e-passport photos.

Forensics
Searching crime-scene prints in databases.

Banking
Remote customer verification, payment approval.

Access control
Building entry and staff time records.

Civil registration
Preventing duplicates in national ID systems.

PRACTICE

Risks and Ethics

Mass surveillance

Real-time face recognition in public spaces makes it possible to track everyone without asking; many countries restrict it by law.

Arrests from false matches

In the US there are documented cases of innocent people being detained on the strength of a false face recognition match.

Function creep

Face or fingerprint data collected for door access can be reused for other purposes; GDPR and similar laws treat it as special data.

Central template stores

Holding millions of templates in one place exposes everyone at once; the 2015 US OPM breach leaked 5.6 million fingerprints.

In depth: Explainable AI and AI Ethics.

PRACTICE

Tools and Datasets

Tools and libraries

OpenCV · dlib · InsightFace · NIST NBIS · SpeechBrain

Well-known datasets

LFW (Labeled Faces in the Wild) · VGGFace2 · FVC2004 (fingerprint) · CASIA-Iris · VoxCeleb (speaker)

Biometric data is **personal data**: it falls under KVKK and GDPR; some face datasets were withdrawn for this reason.

PRACTICE

Common Misconceptions

Common belief	In fact
Biometric systems make no mistakes.	Every system makes false accepts and false rejects; the threshold chooses between them.
Biometric data can be changed like a password.	A face or fingerprint cannot be changed; a leaked template is a permanent risk, so templates need protection.
Accuracy is the same for everyone.	Performance can vary with age, skin tone and sensor; evaluation is done per group.
A match means the person is there.	Presentation attacks use photos, masks or recorded voice; liveness detection is needed.

NEXT STEPS

After This Course

Courses that build on or extend this one

This course is mostly an end point: it builds on the others.

Related careers

Biometrics engineer

Computer vision engineer

Identity and access management specialist

Digital forensics specialist

Biometrics is where pattern recognition and vision meet security. From here you can move to deep face recognition and speaker recognition, to cybersecurity through spoof detection, or to explainable AI and ethics through questions of fairness and privacy.

NEXT STEPS

Further Reading

- Jain, Ross and Nandakumar, *Introduction to Biometrics*, Springer, 2011.
- Li and Jain (eds.), *Handbook of Face Recognition*, 2nd ed., Springer, 2011.
- Maltoni, Maio, Jain and Feng, *Handbook of Fingerprint Recognition*, 3rd ed., Springer, 2022.
- Daugman, "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology* 14(1), 2004.

The End

Chapter 24: Biometric Systems

← Previous chapter · Map of the field · Next chapter →