Biometric User Authentication

Dr Rosanne English

Biometrics

- A sufficiently distinctive trait which can be measured, quantified and stored in such a way that it can be used in user access control
- Categories- Physical or behavioural

Stages

- Enrolment:Template extraction
- Modes of operation
  - verification
  - identification

Accuracy

True accept rate –proportion of genuine users who are appropriately authenticated

True reject rate- proportion of unauthorised users who are appropriately rejected

False accept rate – measure of the likelihood of false acceptance

False reject rate – measure of the likelihood of false rejection

Biometric Modes of Operation

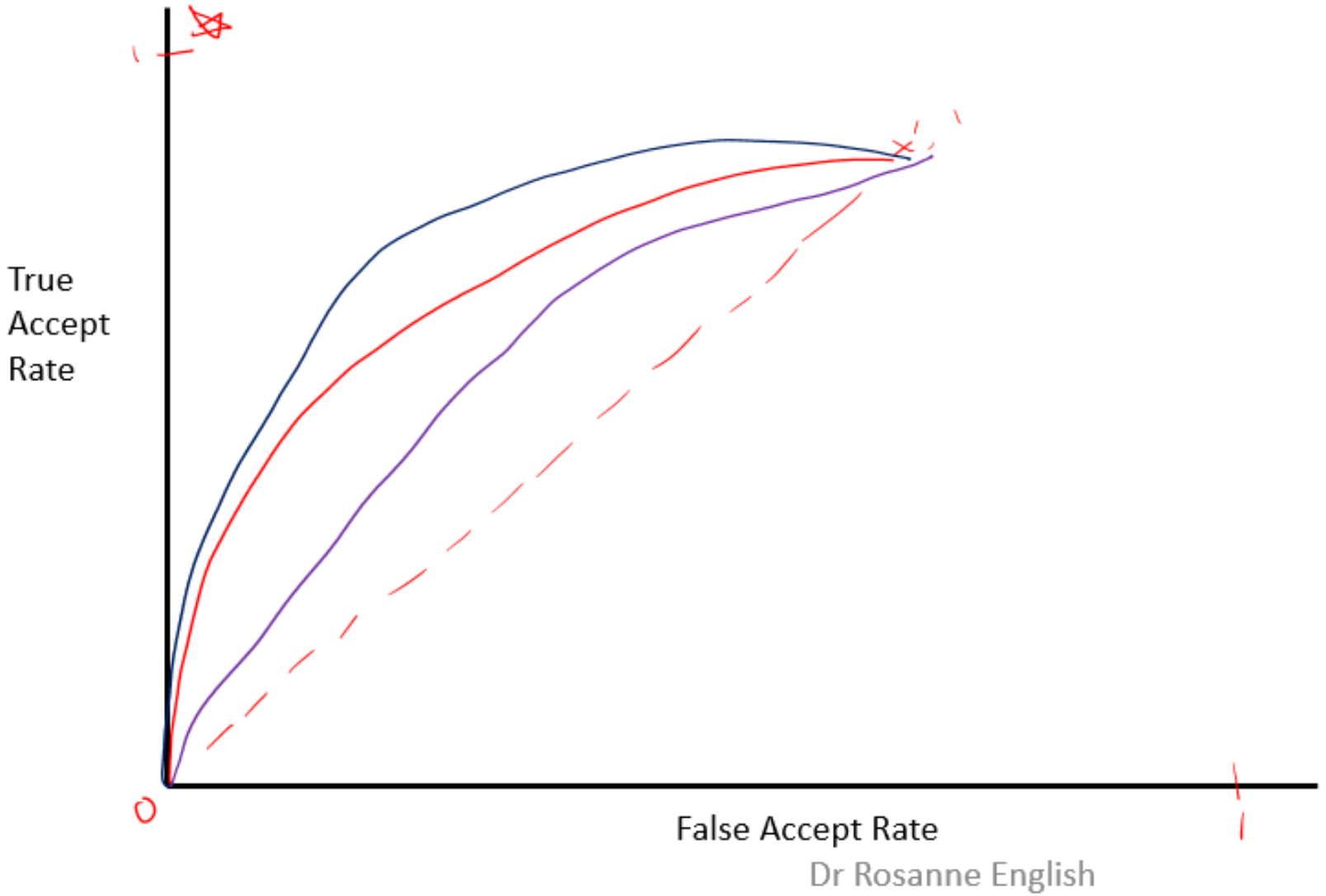
Identification mode

Using biometrics to find a user in a database (similar to an FBI watchlist where they don't know who they are looking for but have the biometric), the user doesn't claim an identity, you try to find their template in the database

Verification mode

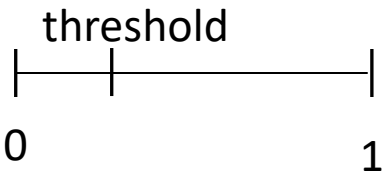
User claims the identity and the template is checked against the template stored for that user

Receiver Operating Characteristic (ROC) Curve

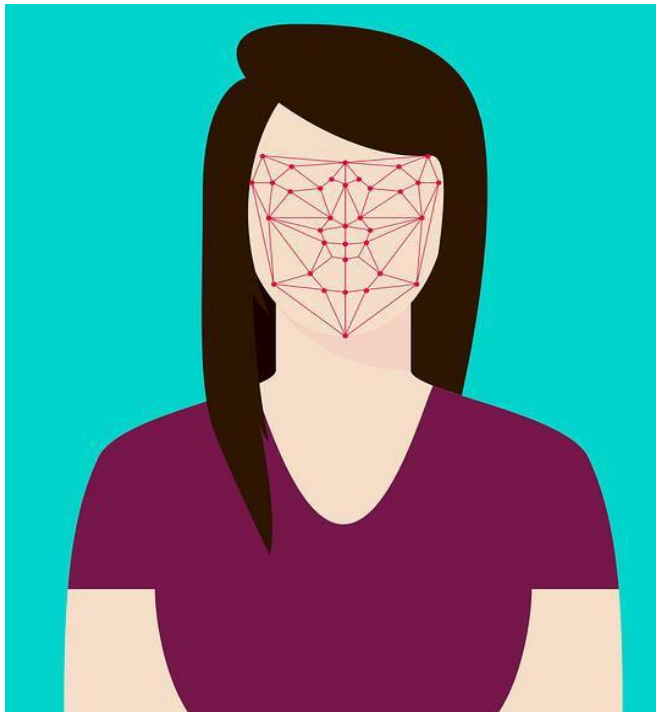


TAR = TP/(TP + FN)

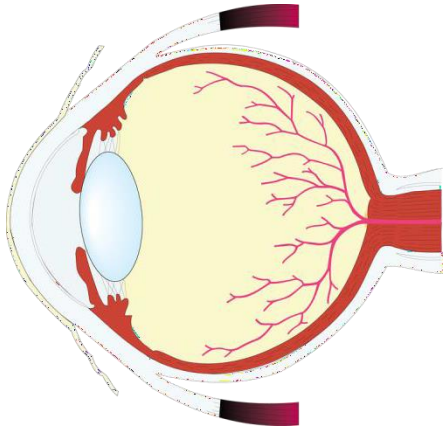
FAR = FP/(FP + TN)



Physiological Biometrics



Face Recognition

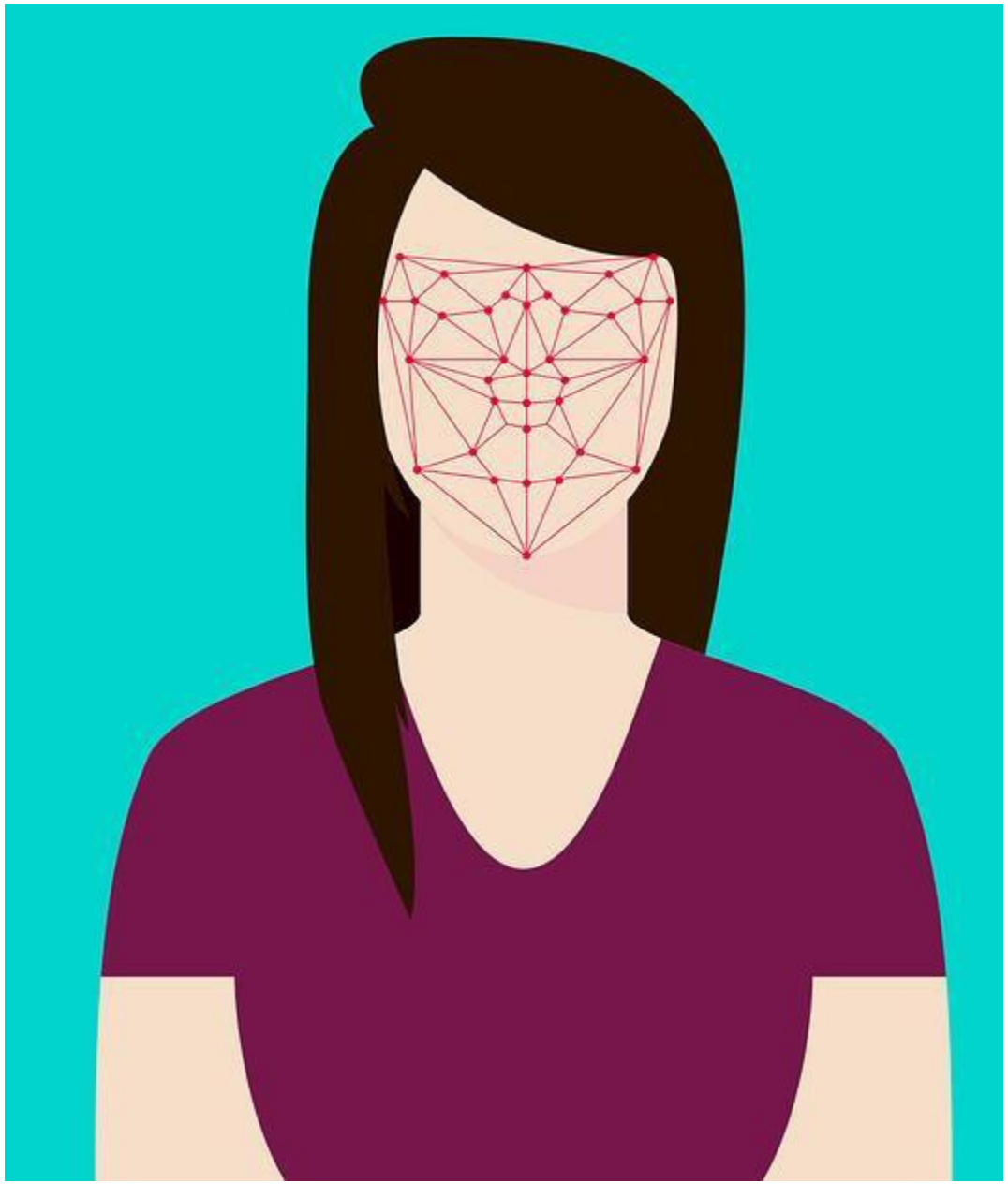


Retina and Iris Recognition

Fingerprint Recognition

Facial Recognition

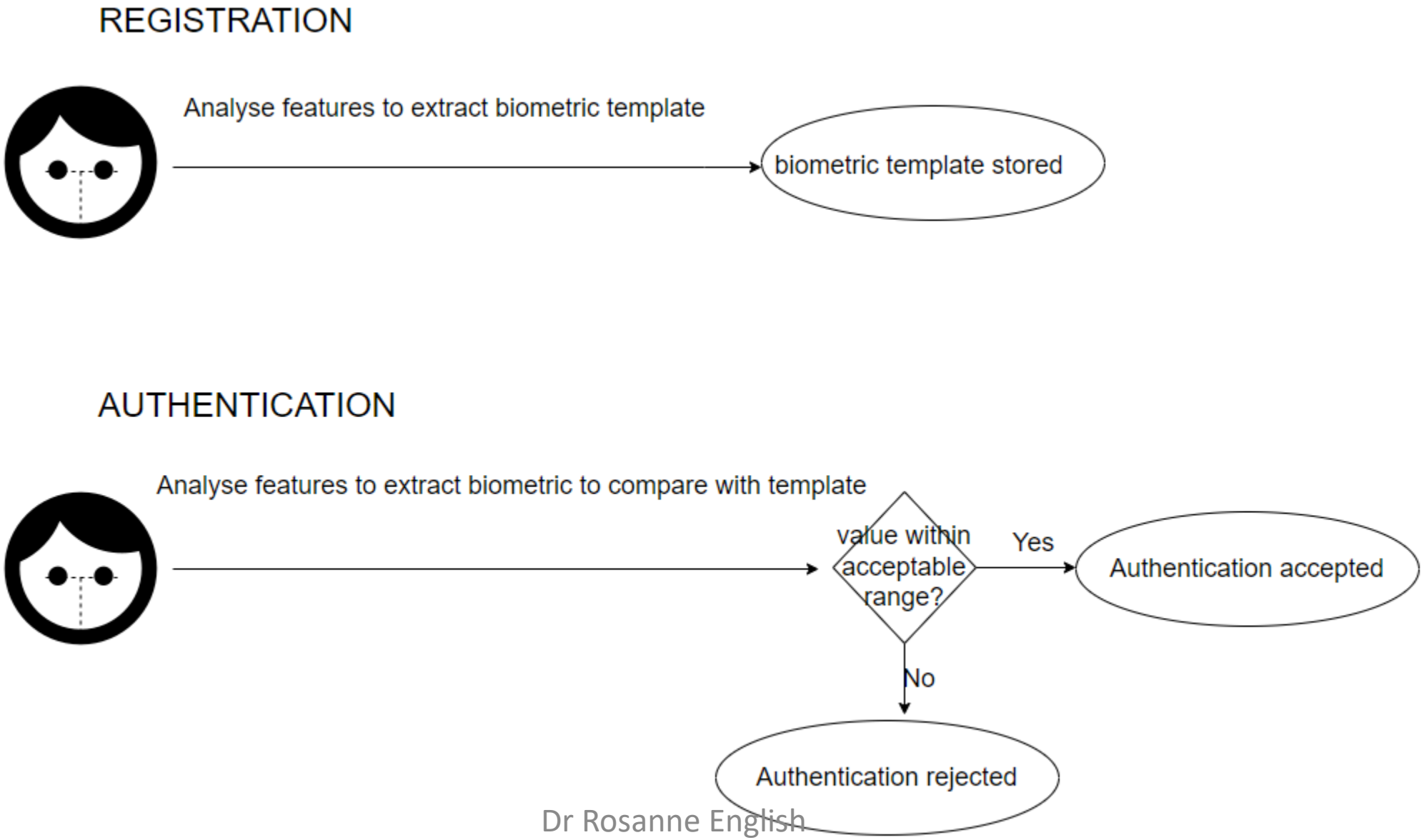
- Maps facial geometry to extract features
- One algorithm is “eigenfaces”, Turk and Pentland (1991)
- Lots more exist
- NIST run regular testing on variety of vendor facial recognition, see an example report



Facial Recognition – The Reality

- Real world use can be patchy
- unreliable, use in law enforcement particularly worrying
- number of news incidents, try to find some!
- 2021 example of facial recognition failure

Facial Biometric Process



Iris Recognition

- Iris patterns between people are very different
- Highly accurate, claimed to produce 1 in 1-2 million false positives

Iris Recognition

- Enrolment
  - Infrared camera takes pictures
  - Pattern of the iris is extracted and analysed resulting in co-ordinates
  - These are used to make comparisons upon verification
- Verification
  - Image taken, features extracted and compared

Iris Biometric Process

REGISTRATION

Infrared camera captures iris, image analysed for iris patterns to extract biometric template → biometric template stored

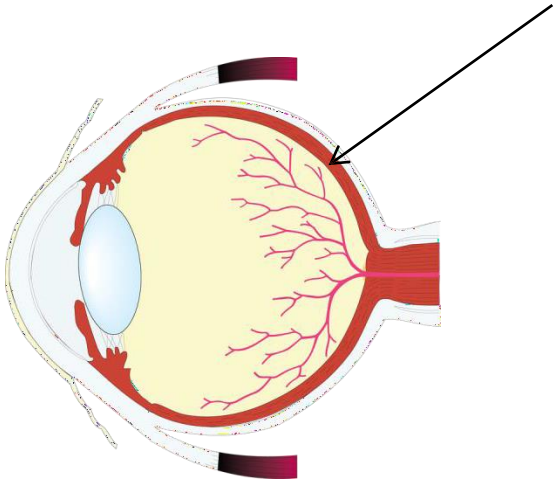
VERIFICATION

Infrared camera captures iris, image analysed to extract biometric to compare with template → value within acceptable range?

- Yes → Authentication accepted
- No → Authentication rejected

Retinal Scan

- More invasive than iris scanning
- Can change over time with disease
- High accuracy



Retinal Scan

- More invasive than iris scanning
- Requires specialist equipment (low light camera)
- Can change over time with disease
- Network of blood vessels provide basis of the template
- High accuracy

Retina Scan Biometric Process

REGISTRATION

lowlight camera (specialist equipment) captures image of retina, image analysed for blood vessel patterns to extract biometric template

→ biometric template stored

VERIFICATION

lowlight camera captures image of retina, image analysed for blood vessel patterns to extract biometric template

→ value within acceptable range?

- Yes → Authentication accepted
- No → Authentication rejected

Retinal Scan

- Enrollment
  - Scan is completed in low light
  - Requires special equipment
  - Features of the network of blood vessels formed into template
- Verification
  - Scan is executed
  - Features extracted, compared with stored template

Fingerprint Recognition

- Consist of ridges(lines) and valleys (white space between ridges)
- These form arches, loops and whorls
- Impacted by e.g. wet fingers, age and can be fooled

Fingerprint Patterns

Basic Patterns:

ARCHES

LOOPS

WHORLS

Minutiae Patterns:

RIDGE ENDINGS

ARCHES

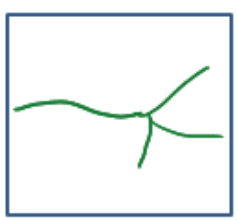
DOT

BIFURCATION

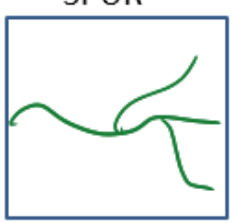
BRIDGE

SPUR

EYE



TRIFURCATION



DOUBLE BIFURCATION

Fingerprint Recognition

- Enrollment
  - Fingerprint is scanned, with many rotations and images taken
  - Unique features (e.g. where a ridge splits in two) are extracted and stored in a template
- Verification
  - Fingerprint is scanned
  - Features extracted, and compared with template

Behavioural Biometrics

Gait Analysis

Keystroke dynamics:
Dwell time
Flight time

Acceptability and other concerns

- Privacy concerns
- Failure to capture (issue in enrolment or in authentication)
- False accept and false reject should be low, but can be difficult to balance with cost and other factors
- Use of AI can incorporate bias
- Spoofing