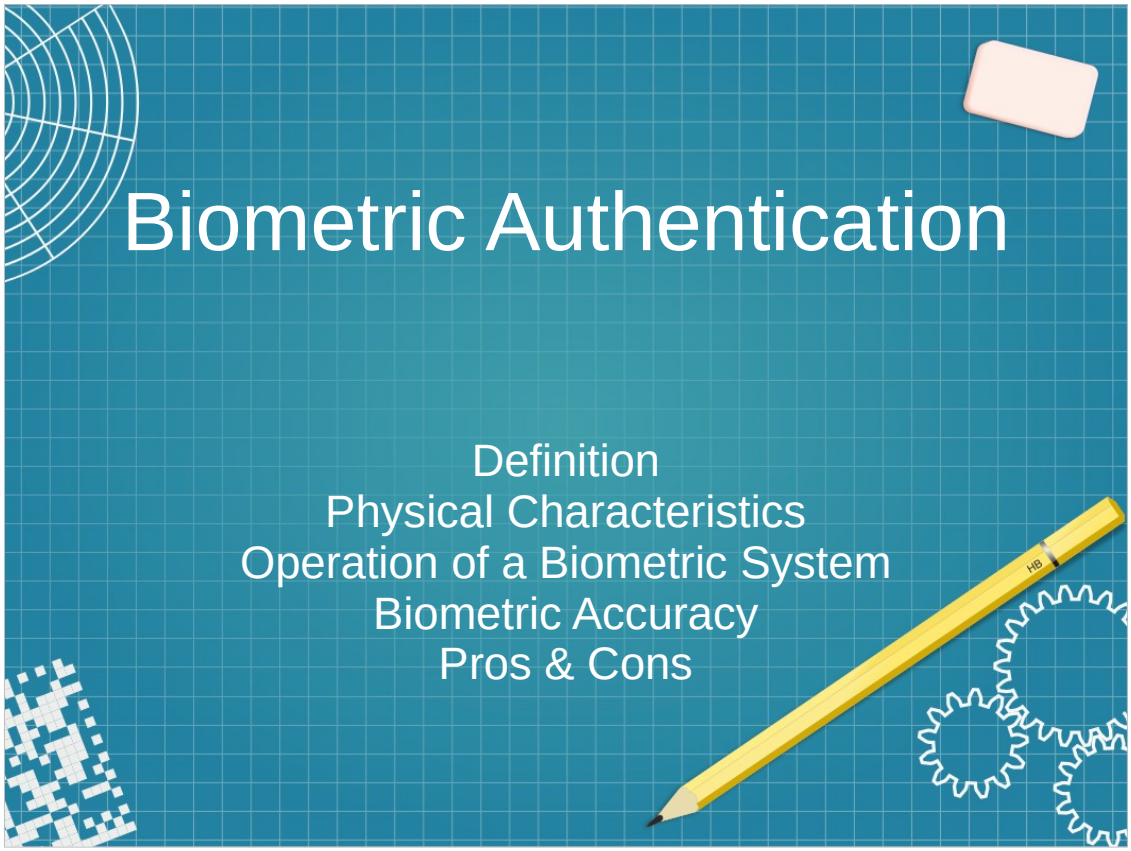
Biometric Authentication

Definition
Physical Characteristics
Operation of a Biometric System
Biometric Accuracy
Pros & Cons



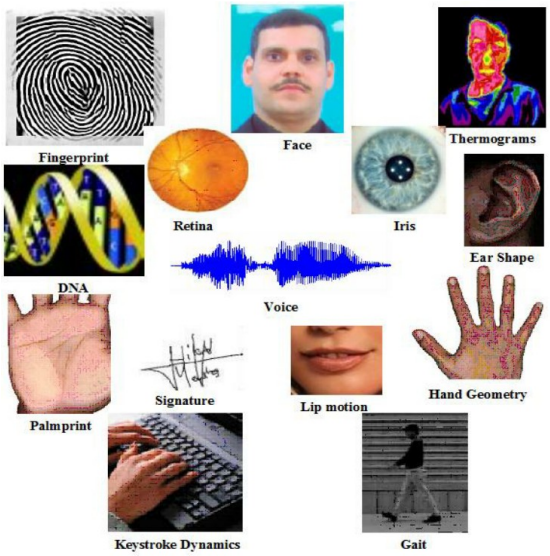
Definition

- Biometric Authentication = process of authenticating a user to a system based on one or more of their unique physical characteristics

Key points:
- pattern recognition
- more complex (than passwords & tokens)
- more expensive (than passwords & tokens)
- not yet standard tool of authentication on computer systems

Physical Characteristics

- Facial
- Fingerprints
- Hand geometry
- Retina
- Iris
- Signature
- Voice



Facial characteristics:
- location & shape of eyes, eyebrows, nose, lips
- shape of chin
- infrared camera: thermogram – vascular system

Fingerprints:
- patterns of ridges and furrows

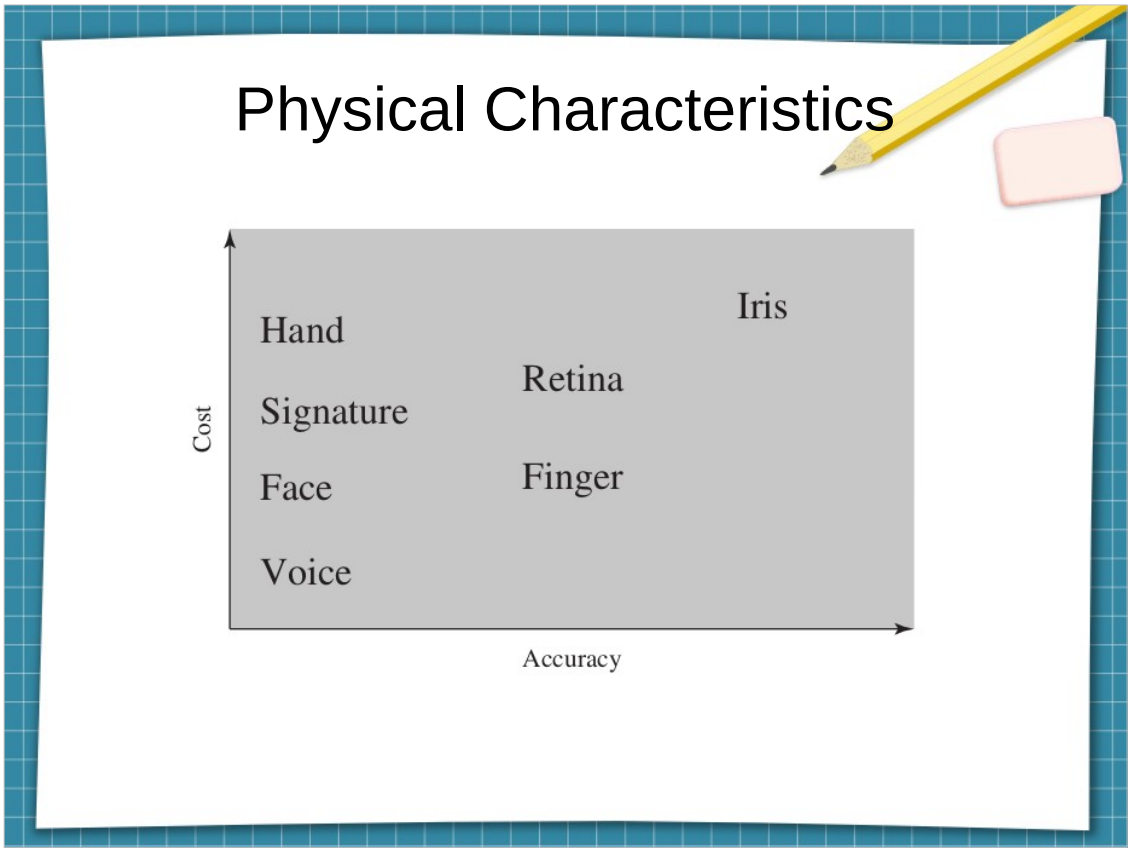
Hand geometry:
- shape, lengths & widths of fingers

Retinal pattern:
- pattern of veins beneath retinal surface
- recognized by projecting low-intensity visual/infrared light into the eye

Iris:
- structure of the iris

Signature:
- handwriting analysis

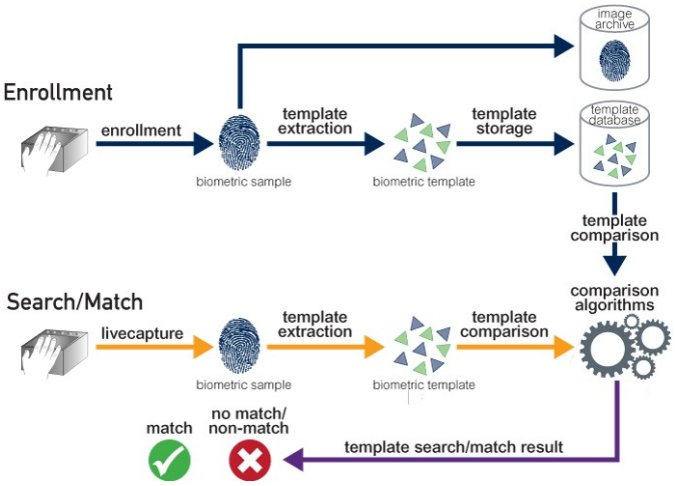
Voice:
- voice signature



Cost vs Accuracy:
- Explain diagram

Operation

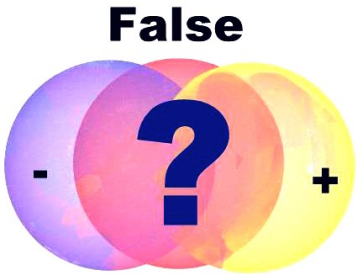
- Enrollment of the user
- Verification
- Identification



Steps:
1. user is enrolled into the system
* registration of name + PIN + biometric characteristic
* system stores biometric digitally
* password is optional
2. Depending on application
- verification: user login
- identification: user recognition

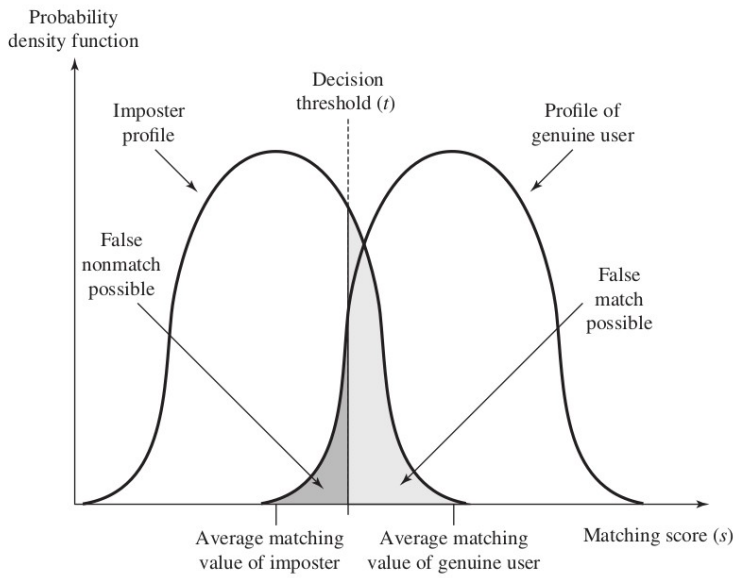
Accuracy

- Template comparison vs Template exact match
- False match rate vs False non-match rate



Accuracy: Check for simmilarity
False match rate: different person's biometrics match errorneously
False non-match rate: same person's biometrics errorneously do not match

Accuracy



Example:

Fingerprints – results vary based on the sensor noise, sweat, swells or other finger temporary malformations… and so on

High security vs low security – what to do when at intersection of the curves.

Iris scanning – no false matching in over 2 million cross-comparisons

Pros & Cons

- Cheap
- Adoption on it’s way
- High Accuracy

- Expensive
- Not widely adopted
- Low Accuracy

Pros & Cons

- Hard to fake
- Increase in convenience
- Strong authentication & accountability
- Safety

- Privacy concerns
- Integration difficulty
- User acceptance

Presentation text: Daniel Șerbănescu
Created on: 24-02-2019