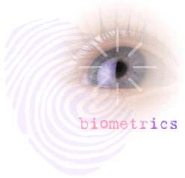
Biometric Systems



Igor Böhm

igor.boehm@fabalabs.org

Florian Testor

florian.testor@students.jku.at

Roadmap

- Introduction
- Biometric System Examples
- Live demonstration of **Face Detection**
- Problems with biometrics and possible solutions through information fusion → *Multi biometrics*
- Selected application scenarios

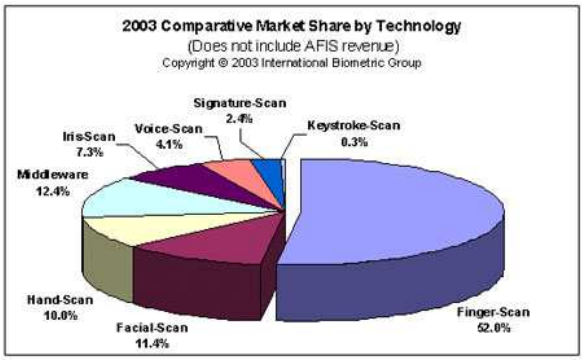
Introduction

Definition and usage of the term **"Biometrics":**

- **Early 20th century** - *the term "Biometrics" described the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences.*
- **Recent usage** - *is referring to the emerging field of technology devoted to identification of individuals on the basis of their biological traits.* $\rightarrow$ **Biometric authentication** *based on "who you are" rather than by "what you posses" or "what you remember".*

Biometric Examples

- **with physical characteristics:** face, fingerprint, palm and hand geometry, iris, retina, voice.
- **with behavioural characteristics:** signature, key stroke patterns, gait, voice.



Fingerprint

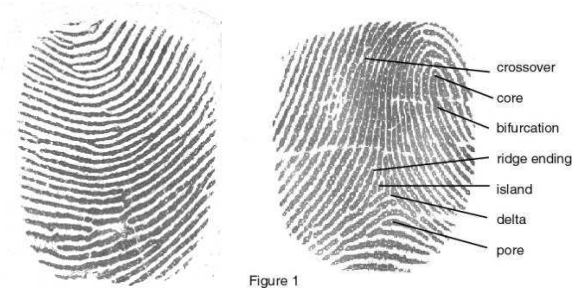
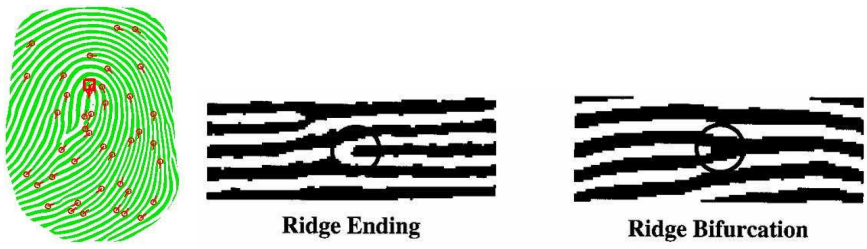


Figure 1

- The most research has been conducted on fingerprints.
- Oldest and best known biometric trait.
- The identification is based on two premises:
  - Persistence
  - Individuality

- different methods of pattern matching.
- matching minutiae points (endings of ridges or a ridge bifurcation)



- problem with fingerprints is the high False Reject Rate (FRR), often caused by low quality fingerprints.

Handscan

- Early scanners: ≥ 20 years ago.
- Measuring and analysing the shape of the hand.
- **Characteristics:** *thickness, width and length of fingers, finger curves, width and height of the back of the hand, distances between joints and the overall bone structure*

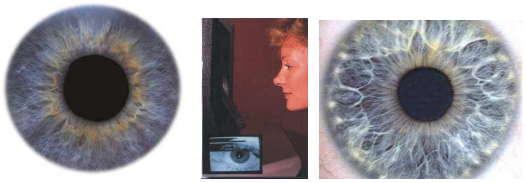
- Two binary photos, one from above and one from beside the hand.
- Over 90 measurements.
- Verification requires to enter user ID.

Signature

- The static image of one's signature *(consistent)*
- **Behavioural parts:** *speed, stroke, pen pressure and timing (vary with each signing)*
- Problems:
  - signature is never entirely the same every time
- Allowing these variations $\Leftrightarrow$ results in better protection.

Iris

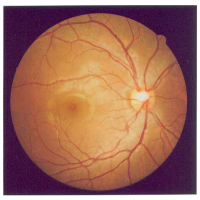
- Coloured ring surrounding pupil.
- **Characteristics:** *rings, freckles and furrows*
- Stays unchanged throughout lifetime.



- Digital photograph *(high resolution, iris radius 90-150 pixel, user-camera-distance not more than 1 meter)*
- **Algorithm:** *find iris, map the distinct patterns and characteristics.*

Retina

- The layer of blood vessels situated at the back of the eye.



- **Devices:** difficult to use *(⇒ high FRR)*, user close to devices but not in direct contact.
- Infrared light source, vascular patterns are reflected.
- Precise and invulnerable biometric trait.

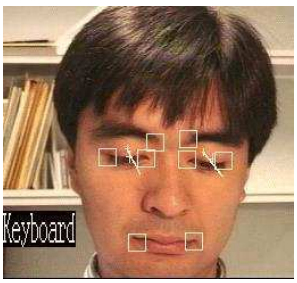
Voice

- **Voice** recognition is not **speech** recognition!
- Distinctive aspects of voice to identify or verify individuals.

- Pass phrase *(*$1 - 1.5$ *seconds)* or sequence of numbers.
- Long enrolment process *(repeating phrase or numbers several times)*.
- **Problems:** voice changes *(having a cold)*

Face

- Analysing facial characteristics such as distance between the eyes, the length of the nose, and the angle of the jaw.
- Create a unique template.



- **Problems:** *finding face (lighting and colouring, different cameras and varying angle of the camera).*
- Casinos, San Francisco International Airport, AI(Artifical Intelligence)

Problems

Reasons for problems:

- biometric traits tend to **vary** with time
- **variation** itself is *very* variable from one person to another
- constantly changing surroundings

Classifying problem categories:

- Noise:
  - cut on ones finger (fingerprint)
  - varying lighting conditions (face detection)
  - person having a cold (voice detection)

- Distinctiveness:
  - even if the biometric trait used is unique, there may be large similarities in the feature sets used to represent these traits
- Non-universality:
  - arises when it is not possible to extract certain biometric traits from all users

Multi biometric Systems

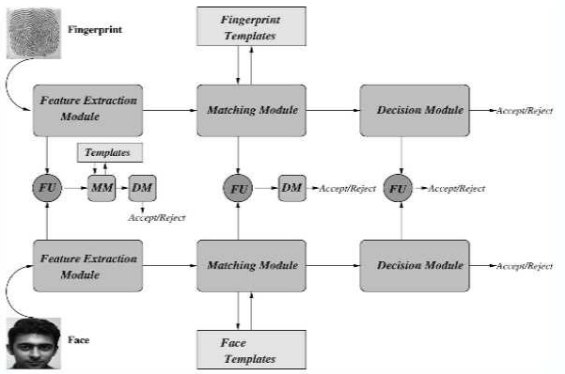
- identification based on **unimodal** biometric systems is problematic and unreliable
- combining multiple biometric traits with an efficient **fusion** scheme overcomes most of the problems and results in an increase of efficiency and reliability
- **spoofing** of biometric data becomes harder because of necessity to spoof several traits simultaneously

Possible levels for fusion

- fusion at **feature extraction level**
- fusion at **matching score level**
- fusion at **decision level**

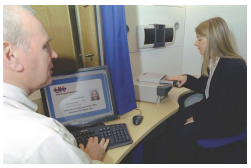
Types of fusions

- single-biom. mult. **representation**
- single-biom. mult. **matchers**
- multiple-biom. **fusion**



UK biometric passport trial

- 6 months trial, 10000 participants.
- Facial recognition, iris and fingerprint biometrics


- Results from the trial will help inform the UK Government's plans to introduce biometrics to support improved identity authentication and help prevent identity

Homeland Security

U.S V.I.S.I.T

"US-VISIT is part of a continuum of security measures that begins overseas, when a person applies for a visa to travel to the United States, and continues on through entry and exit at U.S. air and seaports and, eventually, at land border crossings. The US-VISIT program enhances the security of U.S. citizens and visitors by verifying the identity of visitors with visas"

Super Bowl in Tampa Florida (2001)

- First extensive usage of a face detection system with 20 cameras. Faces of all visitors have been compared with faces of know criminals and terrorists.
- 19 hits but **NO** arrests!
- Conclusions: high FAR, FRR unknown.

Virginia Beach (2002)

- 3 million visitors per year, approx. 20 persons get picked up per year.
- Face database contains picture of known criminals, missing persons, endangered persons (alzheimer etc.),...
- Success of the system less known but examples from the UK show that just the pure presence of the cameras decreases crime rate by $\frac{1}{3}$.

Social Services and Biometrics

- **Goal:** prevent multiple registrations of a single person for social benefit claims.
- Checking for each user if he or she is not already registered (negative identification).
- So even if a person tries to register a second time using a different name, social benefits will only be received **once**.
- Since it is harder to spoof biometric data than documents this method works much better against fraud.

List of Slides