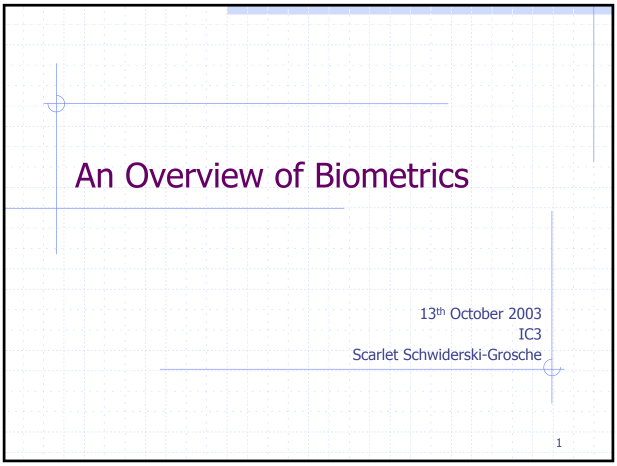
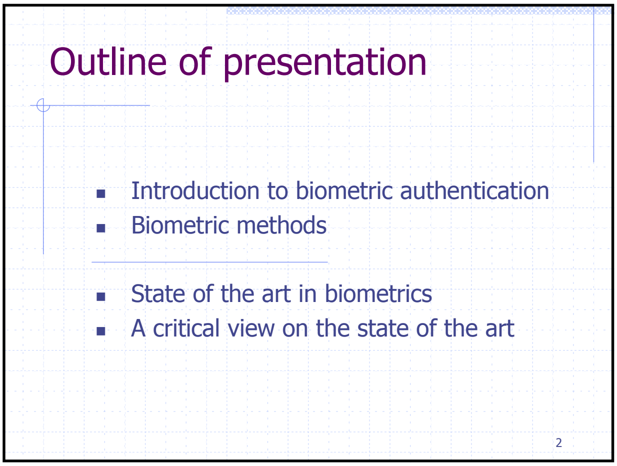


An Overview of Biometrics

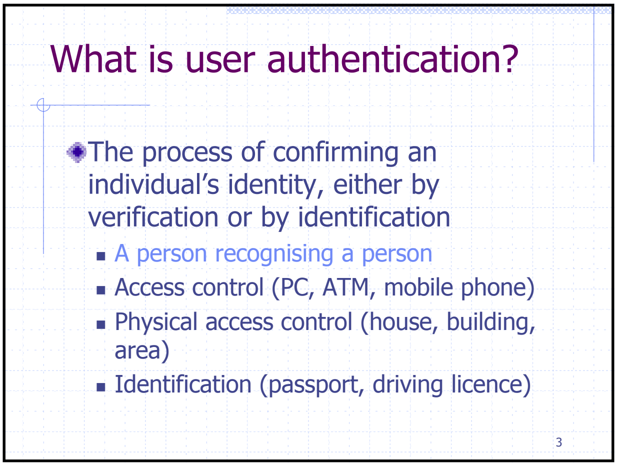
13th October 2003
IC3
Scarlet Schwiderski-Grosche



Outline of presentation

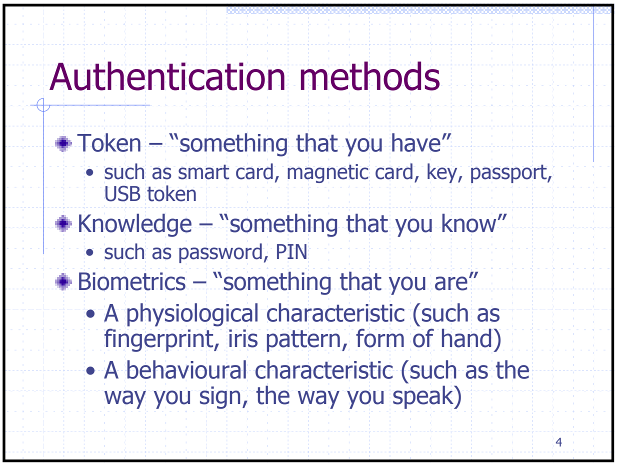
- Introduction to biometric authentication
- Biometric methods

- State of the art in biometrics
- A critical view on the state of the art



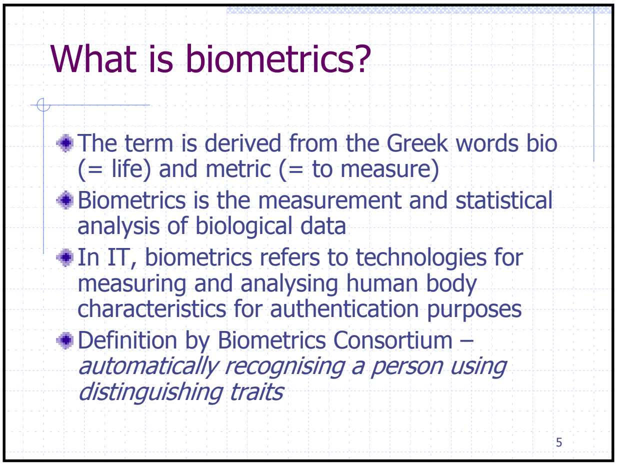
What is user authentication?

- The process of confirming an individual's identity, either by verification or by identification
  - A person recognising a person
  - Access control (PC, ATM, mobile phone)
  - Physical access control (house, building, area)
  - Identification (passport, driving licence)



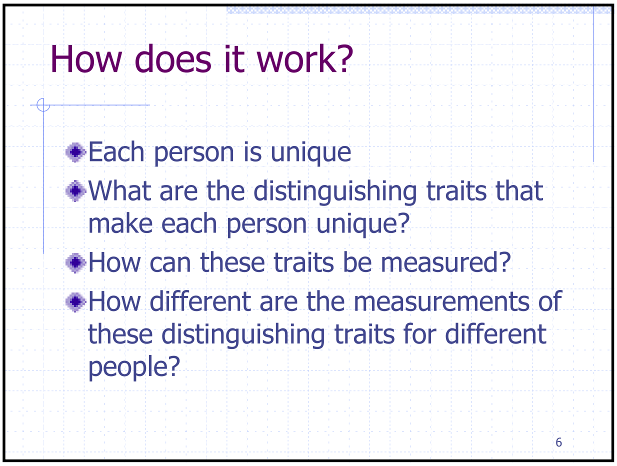
Authentication methods

- Token – "something that you have"
  - such as smart card, magnetic card, key, passport, USB token
- Knowledge – "something that you know"
  - such as password, PIN
- Biometrics – "something that you are"
  - A physiological characteristic (such as fingerprint, iris pattern, form of hand)
  - A behavioural characteristic (such as the way you sign, the way you speak)



What is biometrics?

- The term is derived from the Greek words bio (= life) and metric (= to measure)
- Biometrics is the measurement and statistical analysis of biological data
- In IT, biometrics refers to technologies for measuring and analysing human body characteristics for authentication purposes
- Definition by Biometrics Consortium – *automatically recognising a person using distinguishing traits*



How does it work?

- Each person is unique
- What are the distinguishing traits that make each person unique?
- How can these traits be measured?
- How different are the measurements of these distinguishing traits for different people?

Verification vs. identification

- Verification (one-to-one comparison) – confirms a claimed identity
  - Claim identity using name, user id, …
- Identification (one-to-many comparison) – establishes the identity of a subject from a set of enrolled persons
  - Employee of a company?
  - Member of a club?
  - Criminal in forensics database?

Biometric identifiers

- Universality
- Uniqueness
- Stability
- Collectability
- Performance
- Acceptability
- Forge resistance

Biometric technologies

- Covered in ANSI X9.84-2003:
  - Fingerprint biometrics – fingerprint recognition
  - Eye biometrics – iris and retinal scanning
  - Face biometrics – face recognition using visible or infrared light (called facial thermography)
  - Hand geometry biometrics – also finger geometry
  - Signature biometrics – signature recognition
  - Voice biometrics – speaker recognition

Other biometric methods

- Found in the literature:
  - Vein recognition (hand)
  - Palmprint
  - Gait recognition
  - Body odour measurements
  - Ear shape
  - DNA
  - Keystroke dynamics

Static vs. dynamic biometric methods

- Static (also called physiological) biometric methods – authentication based on a feature that is always present
- Dynamic (also called behavioural) biometric methods – authentication based on a certain behaviour pattern

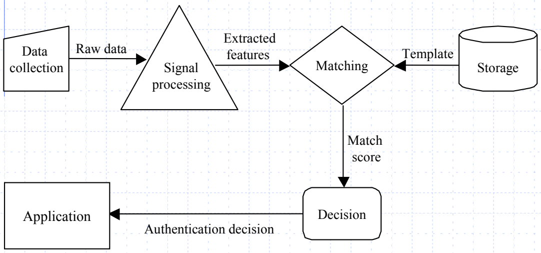
Classification of biometric methods

- Static
  - Fingerprint r.
  - Retinal scan
  - Iris scan
  - Hand geometry
- Dynamic
  - Signature r.
  - Speaker r.
  - Keystroke dynamics

Biometric system architecture

- Major components of a biometric system:
  - Data collection
  - Signal processing
  - Matching
  - Decision
  - Storage
  - Transmission

Biometric system model



Data collection

Raw data

Signal processing

Extracted features

Matching

Template

Storage

Match score

Decision

Authentication decision

Application

Data collection subsystem

- Also called data acquisition
- Comprises input device or sensor that reads the biometric information from the user
- Converts biometric information into a suitable form for processing by the remainder of the biometric system
- Examples: video camera, fingerprint scanner, digital tablet, microphone, etc.

Requirements for data collection

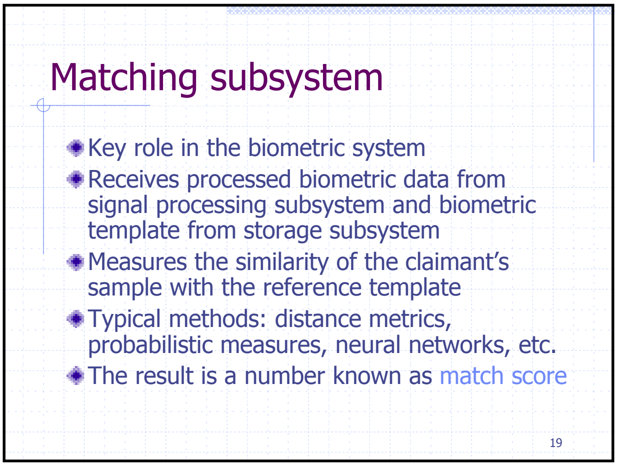
- Sampled biometric characteristic must be similar to the user’s enrolled template
- The users may require training
- Adaptation of the user’s template or re-enrolment may be necessary to accommodate changes in physiological characteristics
- Sensors must be similar, so that biometric features are measured consistently at other sensors

Changes in data collection

- The biometric feature may change
- The presentation of the biometric feature at the sensor may change
- The performance of the sensor itself may change
- The surrounding environmental conditions may change

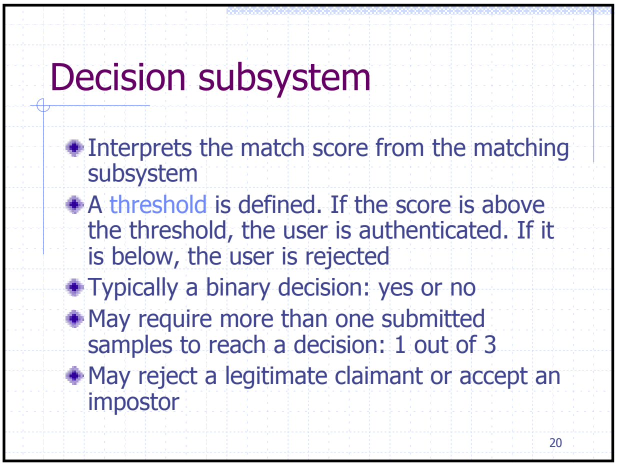
Signal processing subsystem

- For feature extraction
- Receives raw biometric data from the data collection subsystem
- Transforms the data into the form required by matching subsystem
- Discriminating features extracted from the raw biometric data
- Filtering may be applied to remove noise



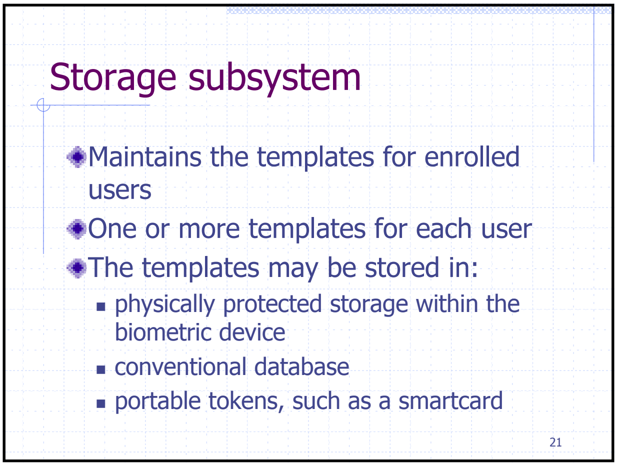
Matching subsystem

- Key role in the biometric system
- Receives processed biometric data from signal processing subsystem and biometric template from storage subsystem
- Measures the similarity of the claimant's sample with the reference template
- Typical methods: distance metrics, probabilistic measures, neural networks, etc.
- The result is a number known as match score



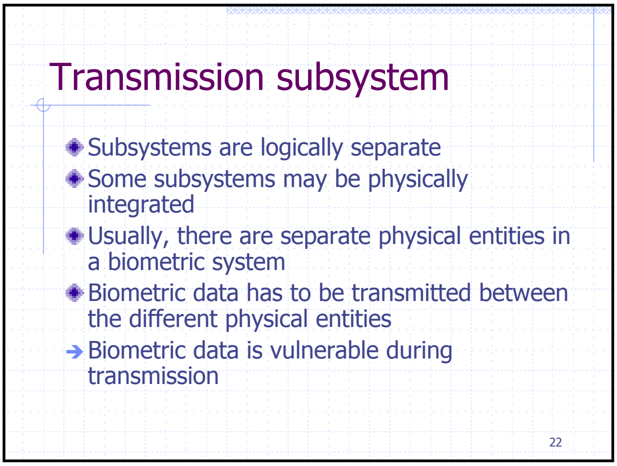
Decision subsystem

- Interprets the match score from the matching subsystem
- A threshold is defined. If the score is above the threshold, the user is authenticated. If it is below, the user is rejected
- Typically a binary decision: yes or no
- May require more than one submitted samples to reach a decision: 1 out of 3
- May reject a legitimate claimant or accept an impostor



Storage subsystem

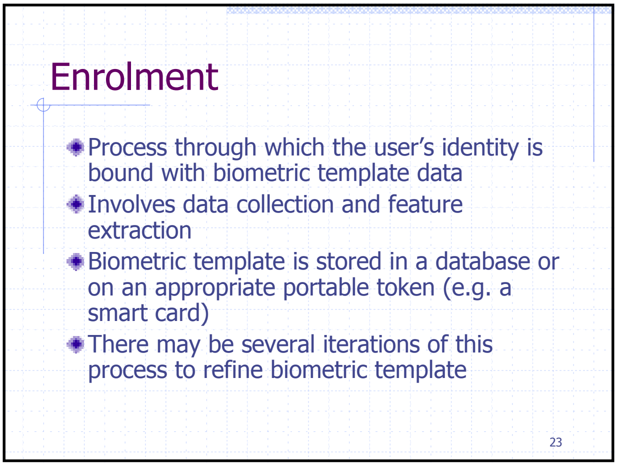
- Maintains the templates for enrolled users
- One or more templates for each user
- The templates may be stored in:
  - physically protected storage within the biometric device
  - conventional database
  - portable tokens, such as a smartcard



Transmission subsystem

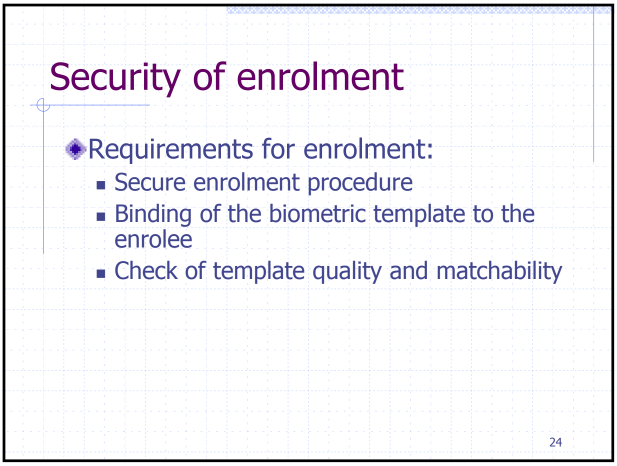
- Subsystems are logically separate
- Some subsystems may be physically integrated
- Usually, there are separate physical entities in a biometric system
- Biometric data has to be transmitted between the different physical entities

→ Biometric data is vulnerable during transmission



Enrolment

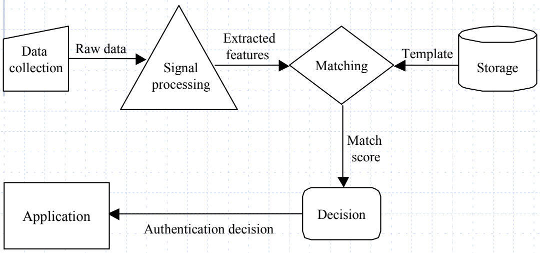
- Process through which the user's identity is bound with biometric template data
- Involves data collection and feature extraction
- Biometric template is stored in a database or on an appropriate portable token (e.g. a smart card)
- There may be several iterations of this process to refine biometric template



Security of enrolment

- Requirements for enrolment:
  - Secure enrolment procedure
  - Binding of the biometric template to the enrolee
  - Check of template quality and matchability

Biometric system model



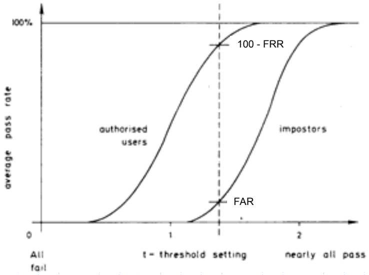
Possible decision outcomes

- A genuine individual is accepted
- A genuine individual is rejected (error)
- An impostor is rejected
- An impostor is accepted (error)

Errors

- Balance needed between 2 types of error:
  - *Type I:* system fails to recognise valid user ('false non-match' or 'false rejection')
  - *Type II:* system accepts impostor ('false match' or 'false acceptance')
- Application dependent trade-off between two error types

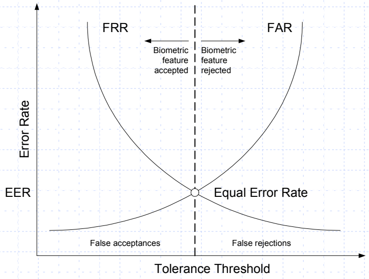
Pass rates



Tolerance threshold

- Error tolerance threshold is crucial and application dependent
- Tolerance too large causes Type II errors (impostors admitted)
- Tolerance too small causes Type I errors (legitimate users rejected)
- Equal error rate (EER): false non-match (FRR) = false match (FAR)

Error curves of biometric authentication methods



Biometric technologies

- Fingerprint recognition
- Hand geometry reading
- Retinal scan
- Iris scan
- Face recognition
- Signature recognition
- Speaker verification

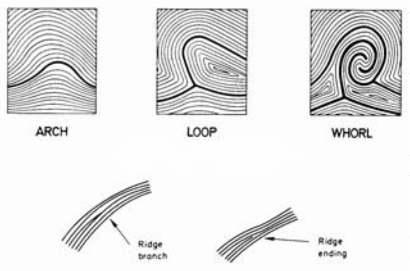
Life detection

- Make sure that input at biometric sensor originates with life user

Fingerprint recognition

- Ridge patterns on fingers uniquely identify people
- Classification scheme devised in 1890s
- Major features: arch, loop, whorl
- Each fingerprint has at least one of the major features and many "small features" (so-called minutiae)

Features of fingerprints

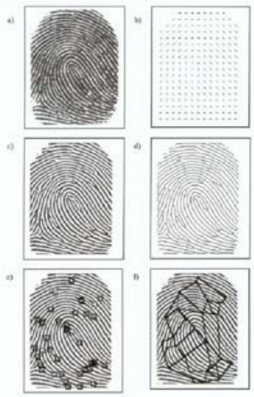


Fingerprint recognition (cont.)

- In an automated system, the sensor must minimise the image rotation
- Locate minutiae and compare with reference template
- Minor injuries are a problem
- Life detection is important (detached real fingers, gummy fingers, latent fingerprints)

Fingerprint authentication

- Basic steps for fingerprint authentication:
  - Image acquisition
  - Noise reduction
  - Image enhancement
  - Feature extraction
  - Matching



Fingerprint processing

a) Original

b) Orientation

c) Binarised

d) Thinned

e) Minutiae

f) Minutiae graph

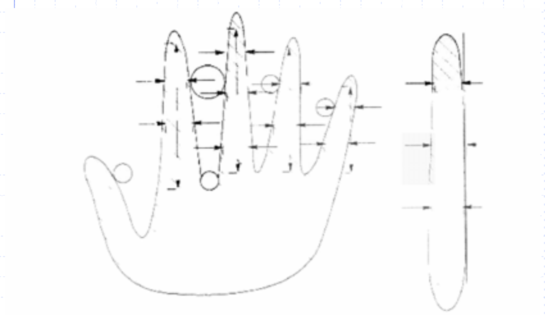
Assessment – fingerprint recognition

- Advantages
  - Mature technology
  - Easy to use/non-intrusive
  - High accuracy (comparable to PIN authentication)
  - Long-term stability
  - Ability to enrol multiple fingers
  - Comparatively low cost
- Disadvantages
  - Inability to enrol some users
  - Affected by skin condition
  - Sensor may get dirty
  - Association with forensic applications

Hand geometry

- Features: dimensions and shape of the hand, fingers, and knuckles as well as their relative locations
- Two images taken, one from the top and one from the side

Hand geometry measurements



Assessment – hand geometry

- Advantages
  - Mature technology
  - Non-intrusive
  - High user acceptance
  - No negative associations
- Disadvantages
  - Low accuracy
  - High cost
  - Relatively large readers
  - Difficult to use for some users (children, arthritis, missing fingers or large hands)

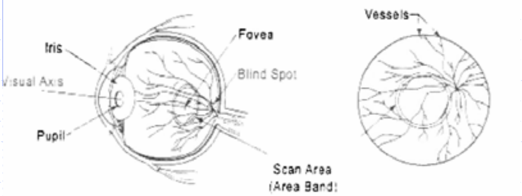
Eye biometrics

- Iris scanning
  - Coloured portion of the eye surrounding the pupil – trabecular meshwork
  - Complex iris pattern is used for authentication
- Retinal scanning
  - Retinal vascular pattern on the back inside the eyeball
  - Pattern of blood vessels used for authentication

Retinal scanning

- Accurate biometric measure
- Genetic independence: identical twins have different retinal pattern
- Highly protected, internal organ of the eye

Retina: eye and scan circle



Assessment – retinal scanning

- Advantages
  - Potential for high accuracy
  - Long-term stability
  - Feature is protected from variations (regarding external environment)
  - Genetic independence
- Disadvantages
  - Difficult to use
  - Intrusive
  - Perceived health threat
  - High sensor cost

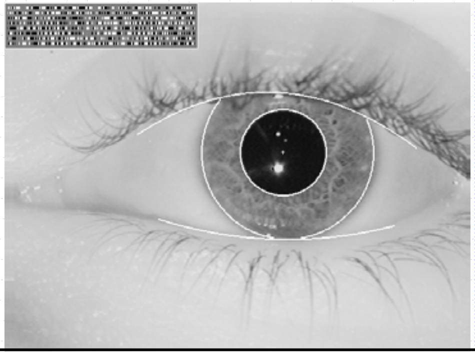
Iris scanning

- Iris pattern possesses a high degree of randomness: extremely accurate biometric
- Genetic independence: identical twins have different iris patterns
- Stable throughout life
- Highly protected, internal organ of the eye
- Patterns can be acquired from a distance (1m)
- Not affected by contact lenses or glasses

Iris scanning

- Iris code developed by John Daugman at Cambridge University
- Extremely low error rates
- Fast processing
- Monitoring of pupil's oscillation to prevent fraud
- Monitoring of reflections from the moist cornea of the living eye

The iris code



Assessment – iris recognition

- Advantages
  - Potential for high accuracy
  - Resistance to impostors
  - Long term stability
  - Fast processing
- Disadvantages
  - Intrusive
  - Some people think the state of health can be detected
  - High cost

Face biometrics

- Static controlled or dynamic uncontrolled shots
- Visible spectrum or infrared (thermograms)
- Non-invasive, hands-free, and widely accepted
- Questionable discriminatory capability

Face recognition

- Visible spectrum: inexpensive
- Most popular approaches:
  - Eigenfaces,
  - Local feature analysis.
- Affected by pose, expression, hairstyle, make-up, lighting, glasses
- Not a reliable biometric measure

Assessment – face recognition

- Advantages
  - Non-intrusive
  - Low cost
  - Ability to operate covertly
- Disadvantages
  - Affected by appearance and environment
  - Low accuracy
  - Identical twins attack
  - Potential for privacy abuse

Facial thermogram

- Captures the heat emission patterns derived from the blood vessels under the skin
- Infrared camera: unaffected by external changes (even plastic surgery!) or lighting
- Unique but accuracy questionable
- Affected by emotional and health state

Assessment of facial thermogram

- Advantages
  - Non-intrusive
  - Stable
  - Not affected by external changes
  - Identical twins resistant
  - Ability to operate covertly
- Disadvantages
  - High cost (infrared camera)
  - New technology
  - Potential for privacy abuse

Signature recognition

- Handwritten signatures are an accepted way to authenticate a person
- Signature generating process is a trained reflex - imitation difficult especially ‘in real time’
- Automatic signature recognition measures the dynamics of the signing process

Dynamic signature recognition

- Variety of characteristics can be used:
  - angle of the pen,
  - pressure of the pen,
  - total signing time,
  - velocity and acceleration,
  - geometry.

Assessment of signature recognition

- Advantages
  - Resistance to forgery
  - Widely accepted
  - Non-intrusive
  - No record of the signature
- Disadvantages
  - Signature inconsistencies
  - Difficult to use
  - Large templates (1K to 3K)
  - Problem with trivial signatures

Speaker verification

- Linguistic and speaker dependent acoustic patterns
- Speaker’s patterns reflect:
  - anatomy (size and shape of mouth and throat),
  - behavioural (voice pitch, speaking style)
- Heavy signal processing involved (spectral analysis, periodicity, etc.)

Speaker recognition systems

- Text-dependent: predetermined set of phrases for enrolment and identification
- Text-prompted: fixed set of words, but user prompted to avoid recorded attacks
- Text-independent: free speech, more difficult to accomplish

Assessment – speaker recognition

- Advantages
  - Use of existing telephony infrastructure or simple microphones
  - Easy to use/non-intrusive/hands free
  - No negative association
- Disadvantages
  - – Pre-recorded attack
  - – Variability of the voice (ill or drunk)
  - – Affected by background noise
  - – Large template (5K to 10K)
  - – Low accuracy

Choosing the biometrics

- Does the application need identification or authentication?
- Is the collection point attended or unattended?
- Are the users used to the biometrics?
- Is the application covert or overt?

Choosing the biometrics

- Are the subjects cooperative or non-cooperative?
- What are the storage requirement constraints?
- How strict are the performance requirements?
- What types of biometrics are acceptable to the users?

Time for a break…

State of the Art in Biometrics

13th October 2003
IC3
Scarlet Schwiderski-Grosche

Outline

- Application domains for biometric products
- Overview of biometric products
- How good are biometrics today?

Application domains (I)

- Access control
  - To devices
    - Cellular phones
    - Logging in to computer, laptop, or PDA
    - Cars
    - Guns, gun safes
  - To local services
    - Debitting money from cash dispenser
    - Accessing data on smartcard
  - To remote services
    - E-commerce
    - E-business

Application domains (II)

- Physical access control
  - To high security areas
  - To public buildings or areas
- Time & attendance control
- Identification
  - Forensic person investigation
  - Social services applications, e.g. immigration or prevention of welfare fraud
  - Personal documents, e.g. electronic drivers license or ID card

Fingerprint recognition: overview

- Sensors
  - Optical sensors
  - Ultrasound sensors
  - Chip-based sensors
  - Thermal sensors
- Integrated products
  - For identification – AFIS systems
  - For verification

Fingerprint recognition: sensors (I)

Optical fingerprint sensor
[Fingerprint Identification Unit
FIU-001/500 by Sony]

Electro-optical sensor
[DELSY® CMOS sensor modul]

Capacitive sensor
[FingerTIP™ by Infineon]

Fingerprint recognition: sensors (II)

E-Field Sensor
[FingerLoc™ by Authentec]

Thermal sensor
[FingerChip™ by ATMEL
(was: Thomson CSF)]

Fingerprint recognition: integrated systems (I)

Physical Access Control System
[BioGate Tower by Bergdata]

[BioMouse™ Plus by American Biometric Company]

[ID Mouse by Siemens]

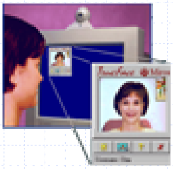
Fingerprint recognition: integrated systems (II)

[TravelMate 740 by Compaq und Acer]

System including fingerprint sensor, smartcard reader and display by DELSY

Keyboard [G 81-12000 by Cherry]

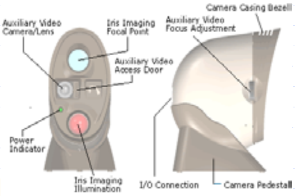
Face recognition



Face recognition system
[TrueFace Engine by Miros]

Face recognition system
[One-to-One™ by Biometric Access Corporation]

Iris recognition



System for passive iris recognition by Sensar

System for active iris recognition by
IrisScan

Iris recognition system at Heathrow airport

- Large-scale trial of iris recognition system at Heathrow Airport for immigration control (no passports)
- http://news.bbc.co.uk/1/hi/uk/1808187.stm

Retinal recognition

Retinal recognition system [Icam 2001 by Eyedentify]

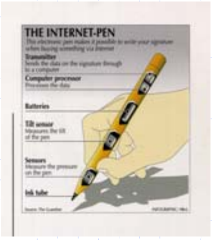
Hand geometry reading

Hand geometry reader for
two finger recognition by BioMet Partners

Hand geometry reader by Recognition Systems

Dynamic signature verification (I)

Electronic pen [LCI-SmartPen]


THE INTERNET-PEN
This electronic pen makes it possible to write your signature when buying something via Internet
Transmitter
Sends the data on the signature through to a computer
Computer processor
Processes the data
Batteries
Tilt sensor
Measures the tilt of the pen
Sensors
Measure the pressure on the pen
Ink tube
Source: The Guardian

Dynamic signature verification (II)

Digitising tablet by Wacom Technologies

Digitising tablet [Hesy Signature Pad by BS Biometric Systems GmbH]

Multimodal biometric systems

- Combination of biometric technologies, e.g.
  - Fingerprint and face recognition
  - Face recognition and lip movement
  - Fingerprint recognition and dynamic signature verification
- → Increase the level of security achieved by the system
- → Enlarge the user base

Which biometric method / product is best?

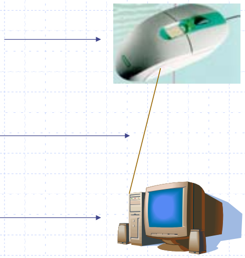
- Depends on the application
  - ✓ reliability
  - ✓ security
  - ✓ performance
  - ✓ cost
  - ✓ user acceptance
  - ✓ life detection
  - ✓ users that are unsuitable
  - ✓ size of sensor

How good are biometric products?

- How can we find out, how good a biometric product is?
  - Empirical tests of the product
- In the past year, there were two independent test series of biometric products
  - in Japan
  - in Germany

Different threat scenarios

1. Regular biometric sensor using artificially generated biometric data
2. Replay attack of eavesdropped biometric data
3. Manipulation of stored biometric reference data



Test in Japan

- Tsutomu Matsumoto, a Japanese cryptographer working at Yokohama National University
- 11 state-of-the-art fingerprint sensors
- 2 different processes to make gummy fingers
  - from live finger
  - from latent fingerprint
- → Gummy fingers fooled all 11 fingerprint sensors 80% of the time

Test in Germany (I)

- Computer magazine c't (see http://www.heise.de/ct/english/02/11/114/)
- 11 biometric sensors
  - 9 fingerprint sensors,
  - 1 face recognition system, and
  - 1 iris scanner
- Fingerprint sensors –
  - Reactivate latent fingerprints (optical and capacitive sensors)
  - Apply latex finger (thermal sensor)

Test in Germany (II)

- Face recognition system –
  - Down- (up-)load biometric reference data from (to) hard disk
  - No or only weak life detection
- Iris recognition –
  - Picture of iris of enrolled person with cut-out pupil, where a real pupil is displayed

→ All tested biometric systems could be fooled, but the effort differed considerably

Conclusions

- Biometric technology has great potential
- There are many biometric products around, regarding the different biometric technologies
- Shortcomings of biometric systems due to
  - Manufacturers ignorance of security concerns
  - Lack of quality control
  - Standardisation problems

- Biometric technology is very promising
- Manufacturers have to take security concerns serious

References

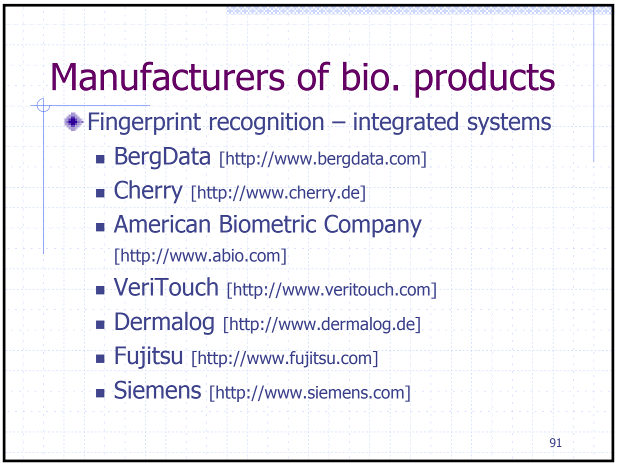
- ANSI X9.84-2003: Biometric Information Management and Security for the Financial Services Industry.
- Scheuermann, Schwiderski-Grosche, and Struif, Usability of Biometrics in Relation to Electronic Signatures, GMD Report 118, Nov 2000.
- Jain et al., Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers.

References (cont.)

- Nanavati et al., Biometrics: Identity Verification in a Networked Society, Wiley.
- The Biometric Consortium: http://www.biometrics.org/
- Thalheim et. al., Body Check, c't 11/2002, http://www.heise.de/ct/english/02/11/114/
- T. Matsumoto et. al., Impact of Artificial Gummy Fingers on Fingerprint Systems, Proc. Of SPIE Vol. 4677, 2002.

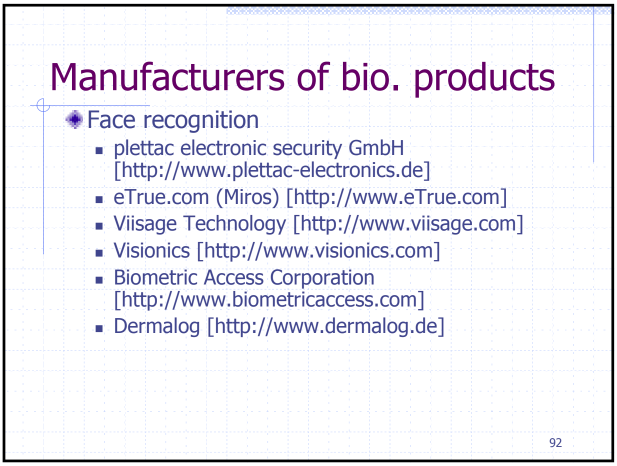
Manufacturers of bio. products

- Fingerprint recognition – sensors
  - American Biometric Company [http://www.abio.com]
  - Biometric Access Corp. (BAC) [http://www.biometricaccess.com]
  - Sony [http://www.sony.com]
  - UltraScan [http://www.ultra-scan.com]
  - Infineon [http://www.infineon.com]
  - Veridicom [http://www.veridicom.com]
  - Authentec [http://www.authentec.com]
  - DELSY [http://www.delsy.de]
  - Who?Vision [http://www.whovision.com]
  - ATMEL [http://www.atmel-grenoble.com]



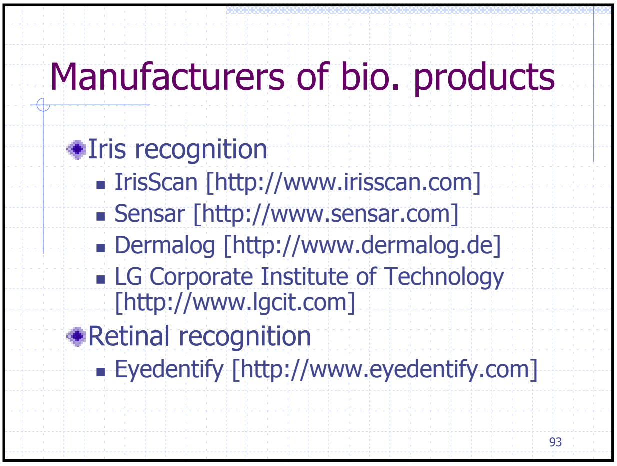
Manufacturers of bio. products

- Fingerprint recognition – integrated systems
  - BergData [http://www.bergdata.com]
  - Cherry [http://www.cherry.de]
  - American Biometric Company [http://www.abio.com]
  - VeriTouch [http://www.veritouch.com]
  - Dermalog [http://www.dermalog.de]
  - Fujitsu [http://www.fujitsu.com]
  - Siemens [http://www.siemens.com]



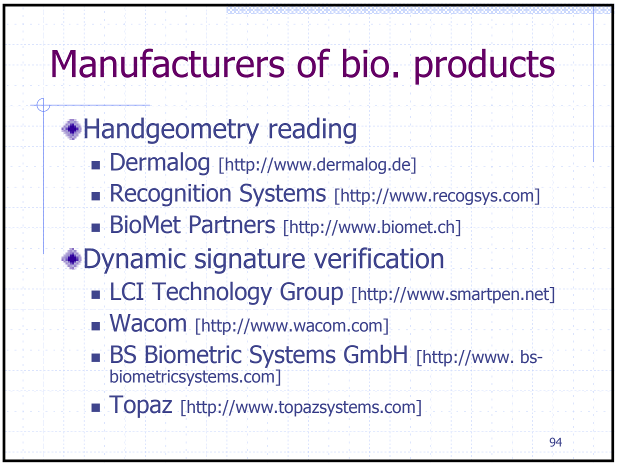
Manufacturers of bio. products

- Face recognition
  - plettac electronic security GmbH [http://www.plettac-electronics.de]
  - eTrue.com (Miros) [http://www.eTrue.com]
  - Viisage Technology [http://www.viisage.com]
  - Visionics [http://www.visionics.com]
  - Biometric Access Corporation [http://www.biometricaccess.com]
  - Dermalog [http://www.dermalog.de]



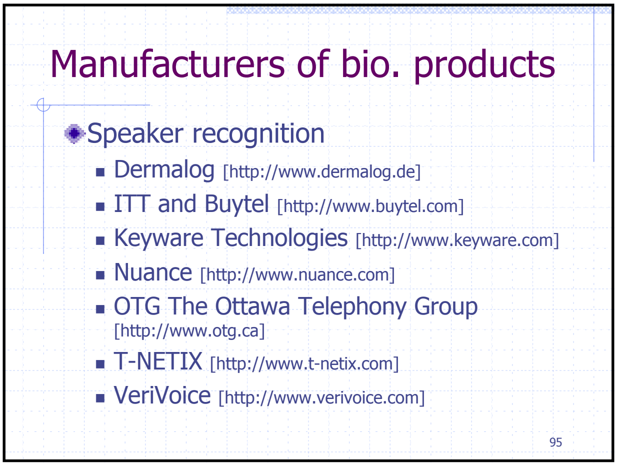
Manufacturers of bio. products

- Iris recognition
  - IrisScan [http://www.irisscan.com]
  - Sensar [http://www.sensar.com]
  - Dermalog [http://www.dermalog.de]
  - LG Corporate Institute of Technology [http://www.lgcit.com]
- Retinal recognition
  - Eyedentify [http://www.eyedentify.com]



Manufacturers of bio. products

- Handgeometry reading
  - Dermalog [http://www.dermalog.de]
  - Recognition Systems [http://www.recogsys.com]
  - BioMet Partners [http://www.biomet.ch]
- Dynamic signature verification
  - LCI Technology Group [http://www.smartpen.net]
  - Wacom [http://www.wacom.com]
  - BS Biometric Systems GmbH [http://www. bs-biometricsystems.com]
  - Topaz [http://www.topazsystems.com]



Manufacturers of bio. products

- Speaker recognition
  - Dermalog [http://www.dermalog.de]
  - ITT and Buytel [http://www.buytel.com]
  - Keyware Technologies [http://www.keyware.com]
  - Nuance [http://www.nuance.com]
  - OTG The Ottawa Telephony Group [http://www.otg.ca]
  - T-NETIX [http://www.t-netix.com]
  - VeriVoice [http://www.verivoice.com]