Biometric systems

Identification systems (IDFS)

Department of Telematics
Faculty of Transportation Sciences, CTU in Prague

Discussion

- What is **BIOMETRICS**?

- Identification / authentication
- Advantages / disadvantages

Biometrics – Definition

Definition:

- *General:* Biometrics is the science of measuring physical properties of living beings.
- *ISO/IEC:* Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics.

Discussion

- What is basic classification of biometric techniques
- What biometric techniques do you know – where they are used?

Biometric techniques

Standard

- Facial recognition
- Voice recognition
- Signature recognition
- DNA
- Retinal scanning
- Iris recognition
- Fingerprint
- Hand Geometry

Miscellaneous (esoteric)

- Finger geometry
- Palm geometry
- Wrist veins
- Locomotion
- shape of ear
- scent
- dynamics of keyboard typing

Behavioral vs. anatomic?

Biometric characteristic

Biometric characteristic	***Description of the features***
Fingerprint	Finger lines, pore structure
Signature (dynamic)	Writing with pressure and speed differentials
Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	Iris pattern
Retina	Eye background (pattern of the vein structure)
Hand geometry	Measurement of fingers and palm
Finger geometry	Finger measurement
Vein structure of hand	Vein structure of the back or palm of the hand or a finger
Ear form	Dimensions of the visible ear
Voice	Tone or timbre
DNA	DNA code as the carrier of human hereditary
Odor	Chemical composition of the one's odor
Keyboard strokes	Rhythm of keyboard strokes (PC or other keyboard)
Password	Sequence of letters and digits memorized in brain

Discussion

- **Which biometric characteristics are most constant over time?**
- What other characteristics SHALL biometrics characteristics / system have?

Biometrics – Characteristics

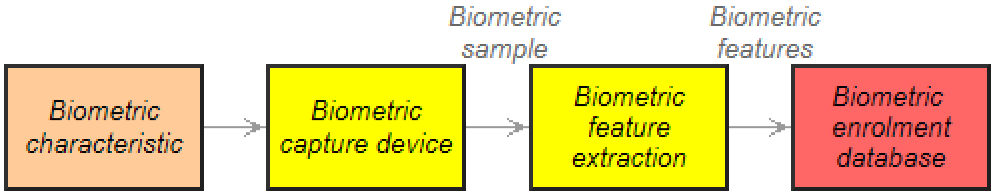
Characteristics:

- **Universality**: Every person should have the characteristic.
- **Uniqueness**: Generally, no two people have identical characteristics.
- **Permanence**: The characteristics should not vary with time.
- **Collectability**: The characteristics must be easily collectible and measurable.

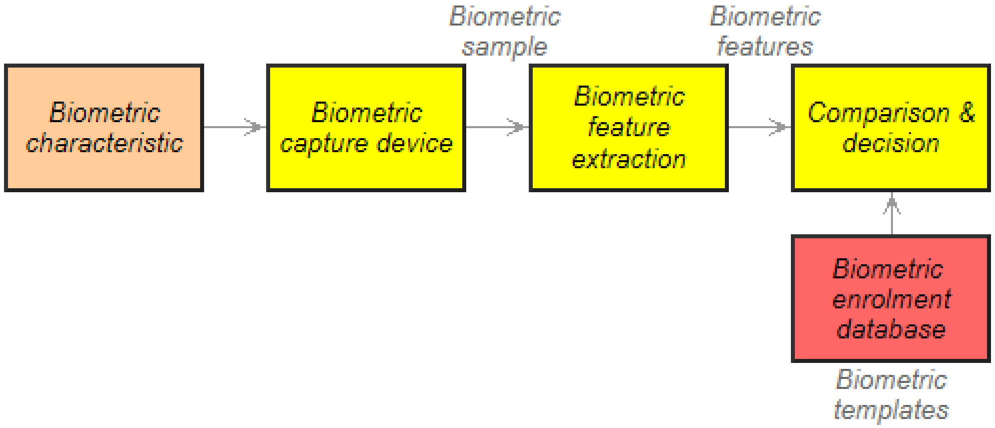
Method:

- **Performance**: The method must deliver accurate results under varied environmental circumstances.
- **Acceptability**: The general public must accept the sample collection routines.
- **Circumvention**: The technology should be difficult to deceive.

Biometrics – process



Typical internal enrolment process



Typical biometric recognition system

Discussion

- How you can compare biometric systems?

Biometric performance standards

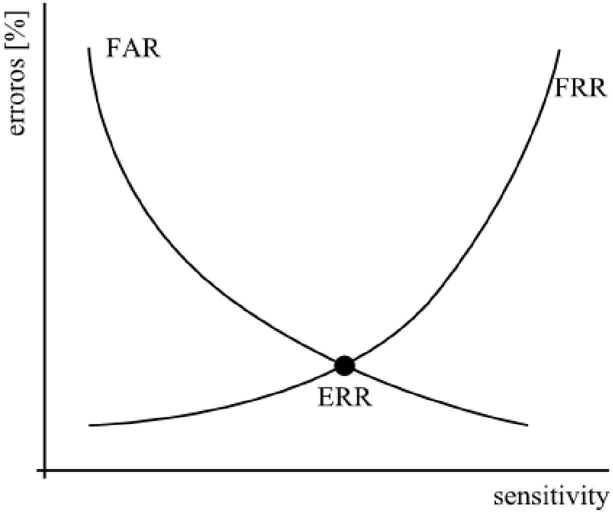
Measurement of efficiency of biometric systems

$$FAR = \frac{FA}{FA + TR}$$

$$FRR = \frac{FR}{FR + TA}$$

- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)
  - FA and TA are the number of false and true accepts
  - FR and TR are the number of false and true rejects, respectively.
- Failure to Enroll Rate (FTE, FER)
- Failure to Acquire (FTA)
- False Identification Rate (FIR)
  - wrong recognition attempts, FI, and the total number of recognition attempts, TI,

$$FIR = \frac{FI}{TI}$$



Discussion

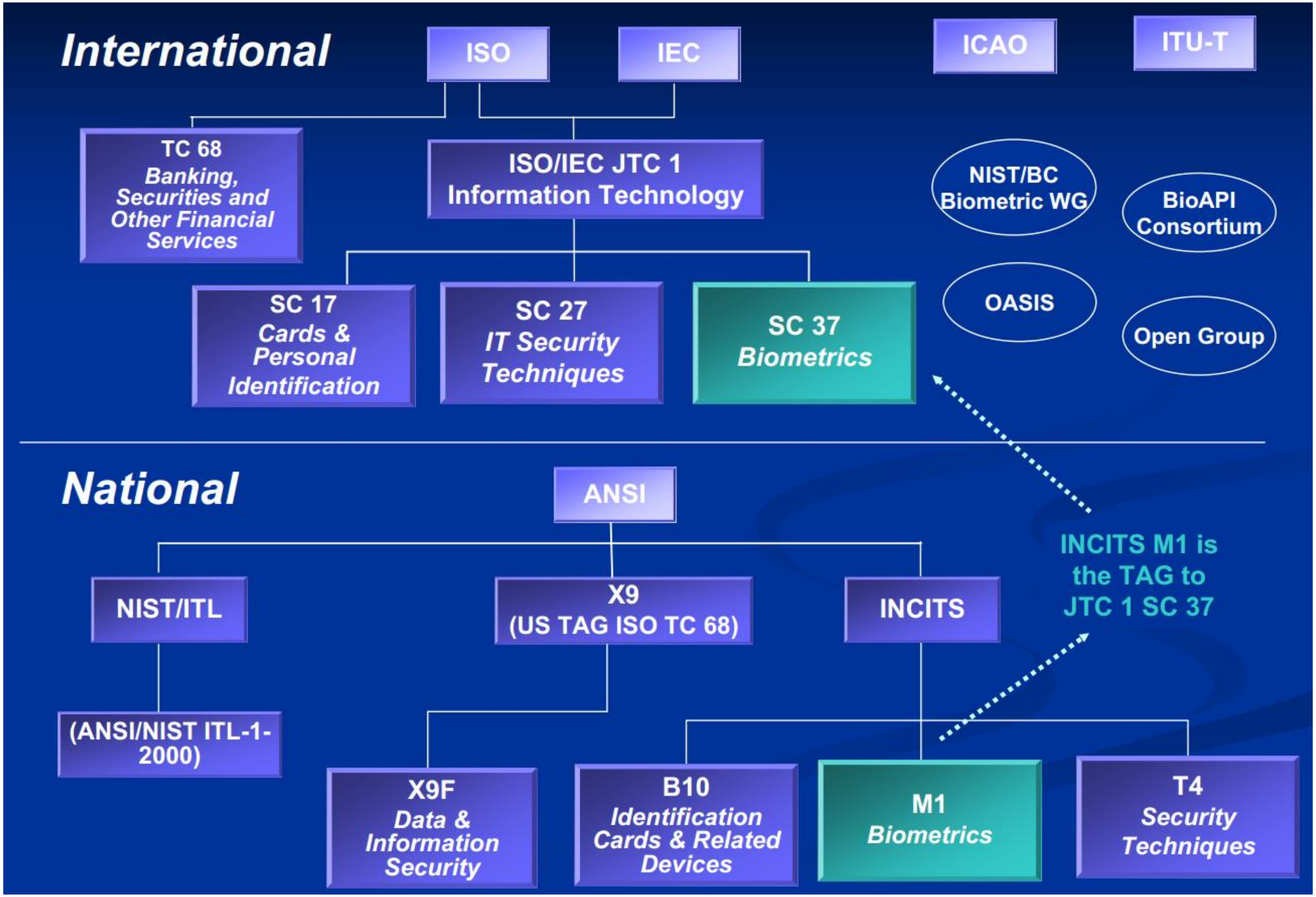
- Which biometric characteristics are most suitable for recognition purposes?

- Criteria:
  - **Comfort**: duration of verification and the ease of use
  - **Accuracy**: minimal error rates (clarity, consistency, measurability)
  - **Availability**: the portion of a potential user group who can use biometrics for technical recognition purposes (universal, measurable)
  - **Costs**: essentially due to the biometric capture device incl. sensors.

Biometric techniques - comparison

Biometric characteristic	***Comfort***	***Accuracy***	***Availability***	***Costs***
Fingerprint	**ooooooo**	**ooooooo**	**oooo**	**ooo**
Signature (dynamic)	**ooo**	**oooo**	**ooooo**	**oooo**
Facial geometry	**ooooooooo**	**oooo**	**ooooooo**	**ooooo**
Iris	**oooooooo**	**ooooooooo**	**oooooooo**	**oooooooo**
Retina	**oooooo**	**oooooooo**	**ooooo**	**ooooooo**
Hand geometry	**oooooo**	**ooooo**	**oooooo**	**ooooo**
Finger geometry	**ooooooo**	**ooo**	**ooooooo**	**oooo**
Vein Structure of the hand	**oooooo**	**oooooo**	**oooooo**	**ooooo**
Ear form	**ooooo**	**oooo**	**ooooooo**	**ooooo**
Voice	**oooo**	**oo**	**ooo**	**oo**
DNA	**o**	**ooooooo**	**ooooooooo**	**ooooooooo**
Odor	?	**oo**	**ooooooo**	?
Keyboard strokes	**oooo**	**o**	**oo**	**o**
Comparison: Password	**ooooo**	**oo**	**oooooooo**	**o**

Standardization



International

ISO

IEC

ICAO

ITU-T

TC 68
Banking, Securities and Other Financial Services

ISO/IEC JTC 1
Information Technology

NIST/BC
Biometric WG

BioAPI
Consortium

OASIS

Open Group

SC 17
Cards & Personal Identification

SC 27
IT Security Techniques

SC 37
Biometrics

National

ANSI

NIST/ITL

X9
(US TAG ISO TC 68)

INCITS

INCITS M1 is the TAG to JTC 1 SC 37

(ANSI/NIST ITL-1-2000)

X9F
Data & Information Security

B10
Identification Cards & Related Devices

M1
Biometrics

T4
Security Techniques

Facial recognition

Voice recognition

Signature recognition

DNA

Retinal scanning

Iris recognition

Fingerprint

Hand Geometry

BIOMETRIC TECHNIQUES

Facial recognition

- Face recognition technologies analyze the unique shape, pattern and positioning of facial features.
- The face is **natural biometric** because it is a key component in the way we humans remember and recognize each other.

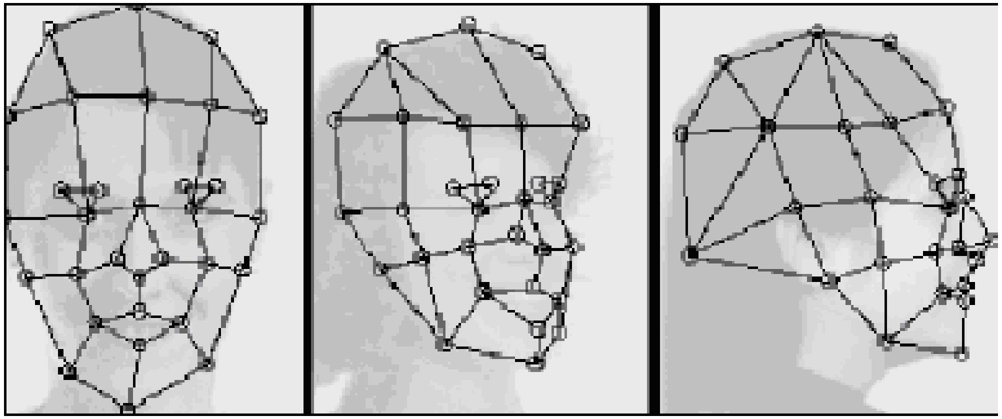
Problem:

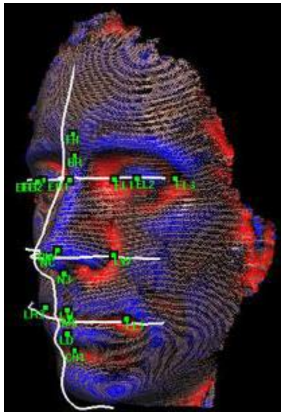
- people do change over time; **wrinkles, beard, glasses and position of the head** can affect the performance considerably.
- To **increase the accuracy and adapt** to these changes some kind of machine learning has to be implemented.
- There are essentially two methods of capture:
  - **using video or**
  - **thermal imaging.**

Facial recognition

Capture on video:

- The precise position and angle of the head and surrounding lightning conditions may affect the system's performance.
- The complete facial image is usually captured and a number of points on the face can then be mapped, position of the eyes, mouth and nostrils as a example. **Three-dimensional map** of the face which multiplies the possible measurements can be made.

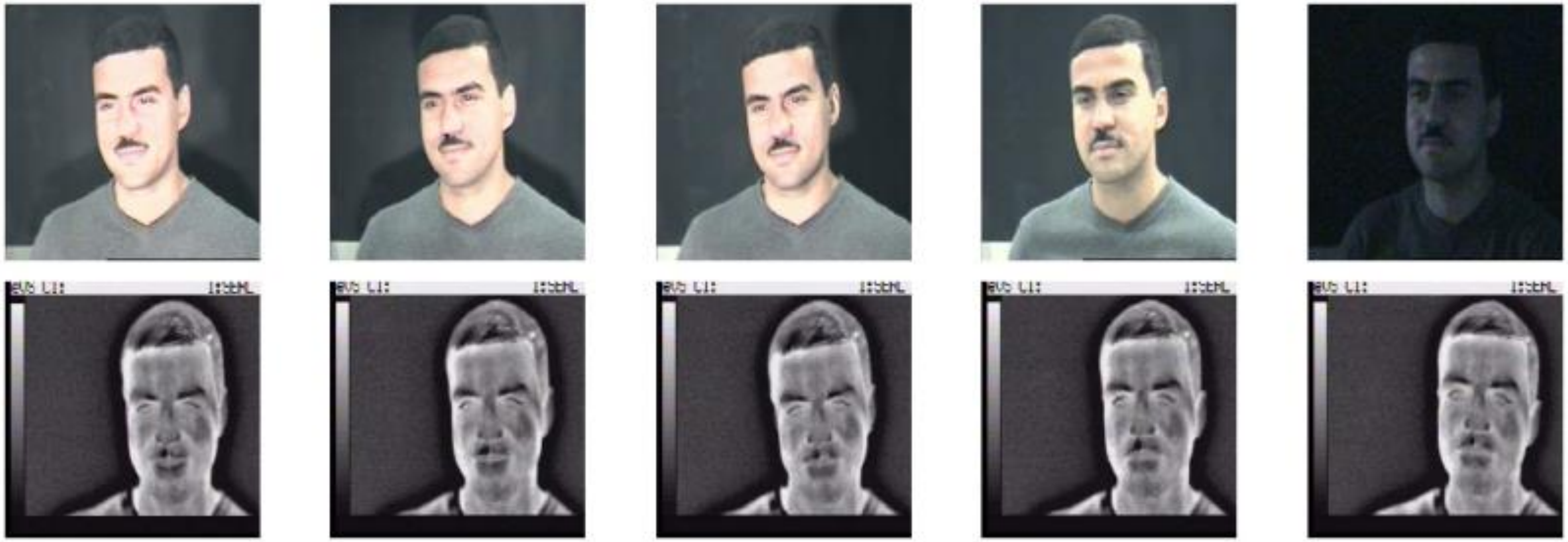




Facial recognition

Capture on thermal camera:

- has better accuracy as it uses facial temperature variations caused by vein structure as the distinguishing trait.
- systems can capture images despite the lighting conditions, even in the dark. The drawback is cost, thermal cameras are **significantly more expensive** than standard video.



Facial recognition

Facial recognition:

- Advantages:
  - Non intrusive
  - Cheap technology. (in case of normal camera)
- Disadvantages
  - 2D recognition is affected by changes in lighting, the person’s hair, the age, and if the person wear glasses.
  - Requires camera equipment for user identification; *thus, it is not likely to become popular until most PCs include cameras as standard equipment.*

Contents

- Definition, Characteristics and Biometrics process
- Biometric techniques
  - **Standard**
    - Facial recognition
    - **Voice recognition**
    - Signature recognition
    - DNA
    - Retinal scanning
    - Iris recognition
    - Fingerprint
    - Hand Geometry
  - Esoteric

Voice recognition

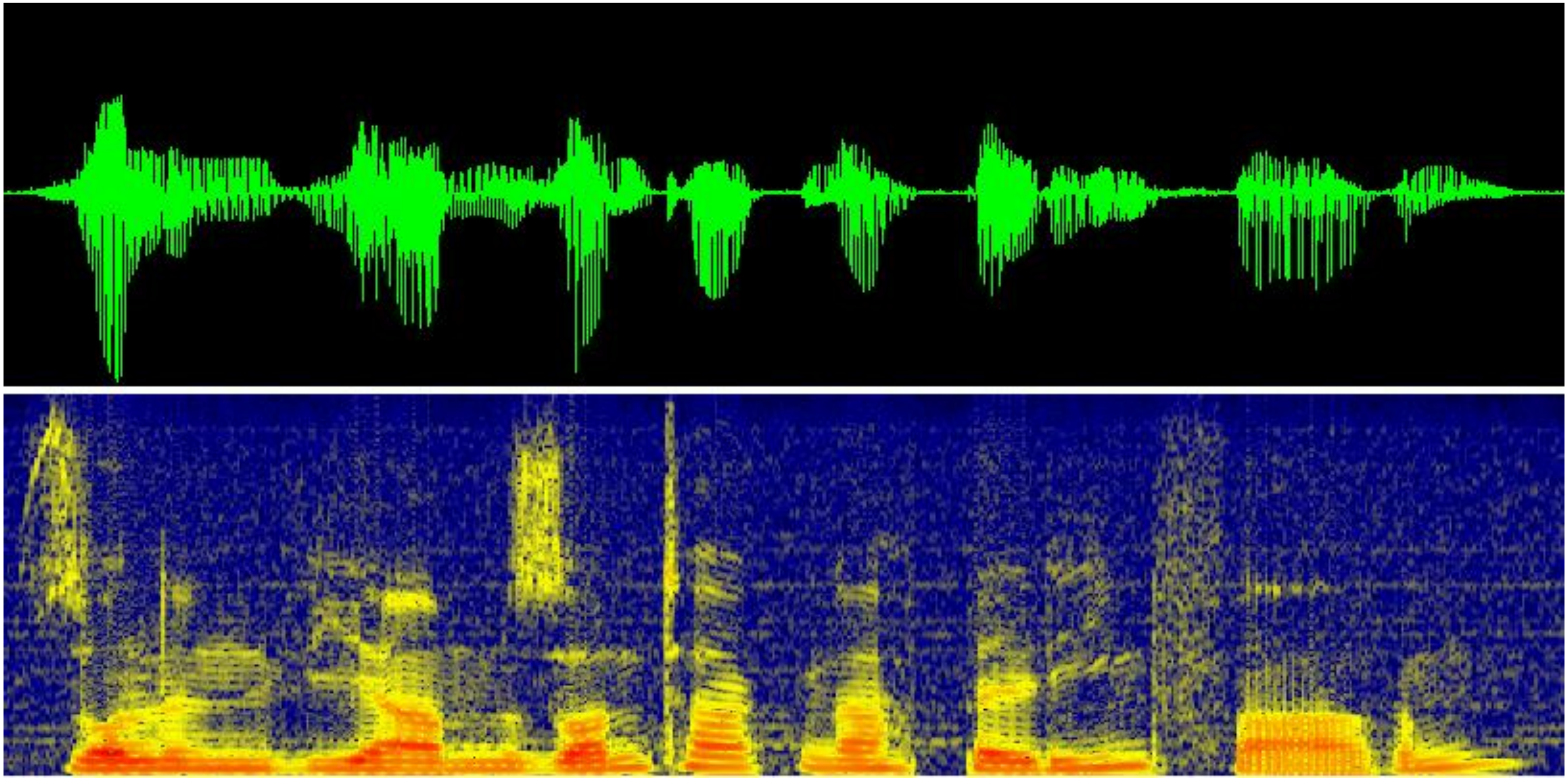
- unique patterns of an individual’s voice - as produced by the vocal tract is examined. it has to be **distinguished from speech recognition**.

Capture:

- speaker identification evaluates the input with models stored in a database to determine the speaker's identity.
- The technique of measuring the voice may use either **text dependent or text independent**.
    - Speech templates are made from a number of words or phrases which are trained in the system.
    - Voice is analyzed as syllable, phoneme, triphone or more fine-grained part at a time so on the recognition phase speaker doesn't have to use specific words.

Voice recognition

- Example



Voice recognition

Voice recognition:

- Advantages:
  - Non intrusive. High social acceptability.
  - Verification time is about *five seconds*.
  - Cheap technology.
- Disadvantages:
  - A person’s voice can be easily recorded and used for unauthorized PC or network.
  - Low accuracy.
  - An illness such as a cold can change a person’s voice, making absolute identification difficult or impossible.

Contents

- Definition, Characteristics and Biometrics process
- Biometric techniques
  - **Standard**
    - Facial recognition
    - Voice recognition
    - **Signature recognition**
    - DNA
    - Retinal scanning
    - Iris recognition
    - Fingerprint
    - Hand Geometry
  - Esoteric

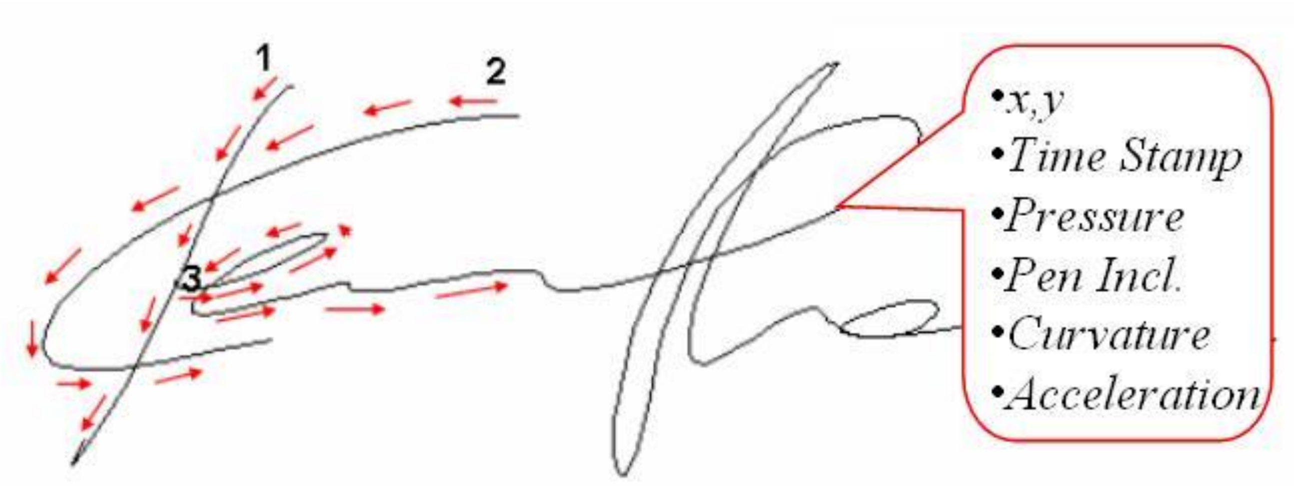
Signature recognition

- Signature is one of the most accepted methods of asserting ones identity. In digitized form the static geometry of signature is not enough to ensure the uniqueness of its author.
- Signature biometrics = **dynamic signature verification** (DSV) and look at the way we sign our names.
- a number of characteristics can be extracted from the physical signing process.
  - the **angle** of the pen is held,
  - the **time** taken to sign,
  - **velocity** and **acceleration** of the tip of the pen,
  - number of **times** the pen **is lifted** from the paper.
- it is very hard to forge and replicate.

Signature recognition

Capture:

- via a special sensitive tablet or pen, or both.
- Because of the behavioral nature of signature, more than one signature enroll is needed so that the system can build a profile of the signing characteristics.



source: http://biometrics.sabanciuniv.edu/signature.html

Signature recognition

Signature recognition:

- Advantages:
  - Non intrusive.
  - Fast verification (about five seconds).
  - Cheap technology.
- Disadvantages:
  - Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names **in a consistent manner may have difficulty** enrolling and verifying in signature verification.
  - Error rate: 1 in 50.
- More info: http://www.cccure.org/Documents/HISM/053-055.html

DNA

From wikipedia:

- **DNA profiling** (also called **DNA testing**, **DNA typing**, or **genetic fingerprinting**) is a technique employed by forensic scientists to assist in the identification of individuals by their respective DNA profiles.
- **DNA profiles** are encrypted sets of numbers that reflect a person's DNA makeup, which can also be used as the person's identifier. DNA profiling **should not be confused with full genome sequencing**. It is used in, for example, parental testing and criminal investigation.

DNA

DNA:

- Advantages:
  - Very high accuracy.
  - It impossible that the system made mistakes.
  - It is standardized.
- Disadvantages:
  - Extremely intrusive.
  - Very expensive.

Retinal scanning

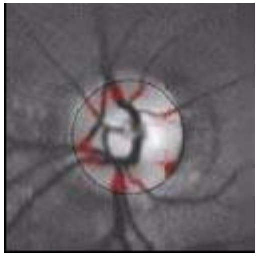
- the layer of blood vessels situated at the back of the eye.
- forms a unique pattern and begins to decay quickly after death.
- are (along iris) to be the most accurate of all the biometrics.

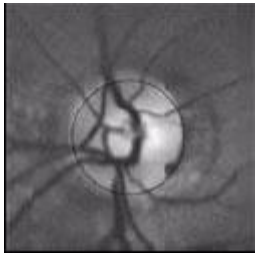
Capture:

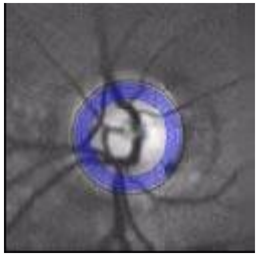
- the most inconvenient for end users.
- user must position the eye approximately **three inches** from an eyepiece, stabilize head movement and **focus on a green dot**
- Then the system uses a beam of light to capture the unique characteristics in the area known as fovea, situated in the center of retina.

Retinal scanning

- Because of the high accuracy, the retina biometrics are usually to be found in high security applications where preventing false acceptance is extremely important.
- Partly this is achieved by setting high threshold for accepting the scanned biometric.







Retinal scanning

Retinal scanning:

- Advantages:
  - Very high accuracy. There is no known way to replicate a retina.
  - The eye from a dead person would deteriorate too fast to be useful, sure that the user is a living human being.
- Disadvantages:
  - Very intrusive, Very expensive.
  - It has the stigma of consumer's thinking it is potentially harmful to the eye.
  - Comparisons of template records can take upwards of 10 seconds, depending on the size of the database.
- More info: http://www.cccure.org/Documents/HISM/050-053.html

Contents

- Definition, Characteristics and Biometrics process
- Biometric techniques
  - **Standard**
    - Facial recognition
    - Voice recognition
    - Signature recognition
    - DNA
    - Retinal scanning
    - **Iris recognition**
    - Fingerprint
    - Hand Geometry
  - Esoteric

Iris recognition

- Internal organ of the eye, behind the cornea and the aqueous humour. Visually examined iris is the **colored ring of textured tissue** that surrounds the pupil of the eye.
- Each iris is a unique structure, featuring a complex system which is stable and unchanging throughout life.

Analysis:

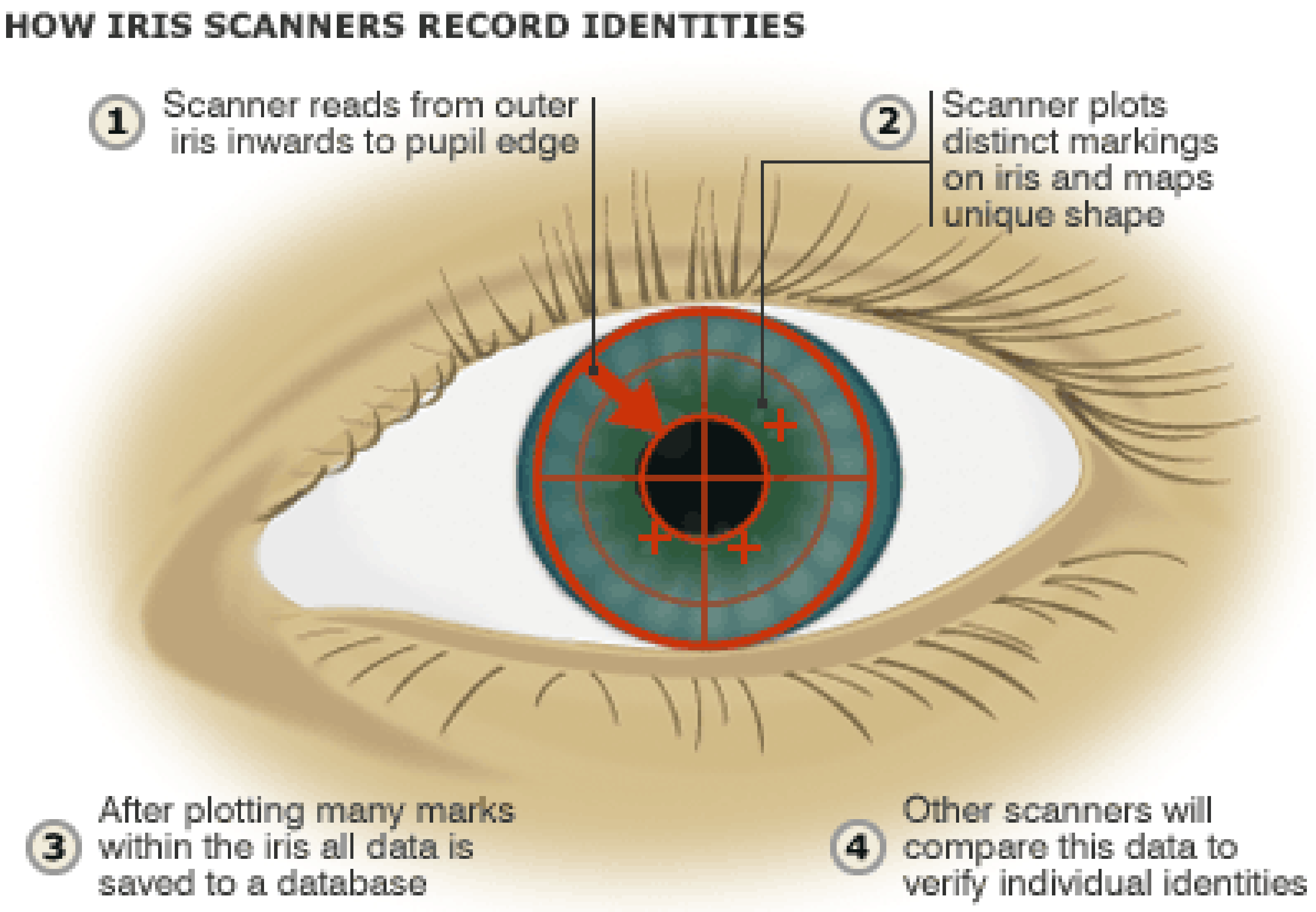
- information density of iris patterns is roughly **3.4 bits / mm^2** and complexity has about 266 degrees of freedom.
- one of the first parts of the body to **decay after death**. -> use of a dead eye for fraudulent purposes is very difficult.
- Tests against eye replicas include **testing the natural pupillary motion** and refractions to different infrared light sources.

Iris recognition

Capturing:

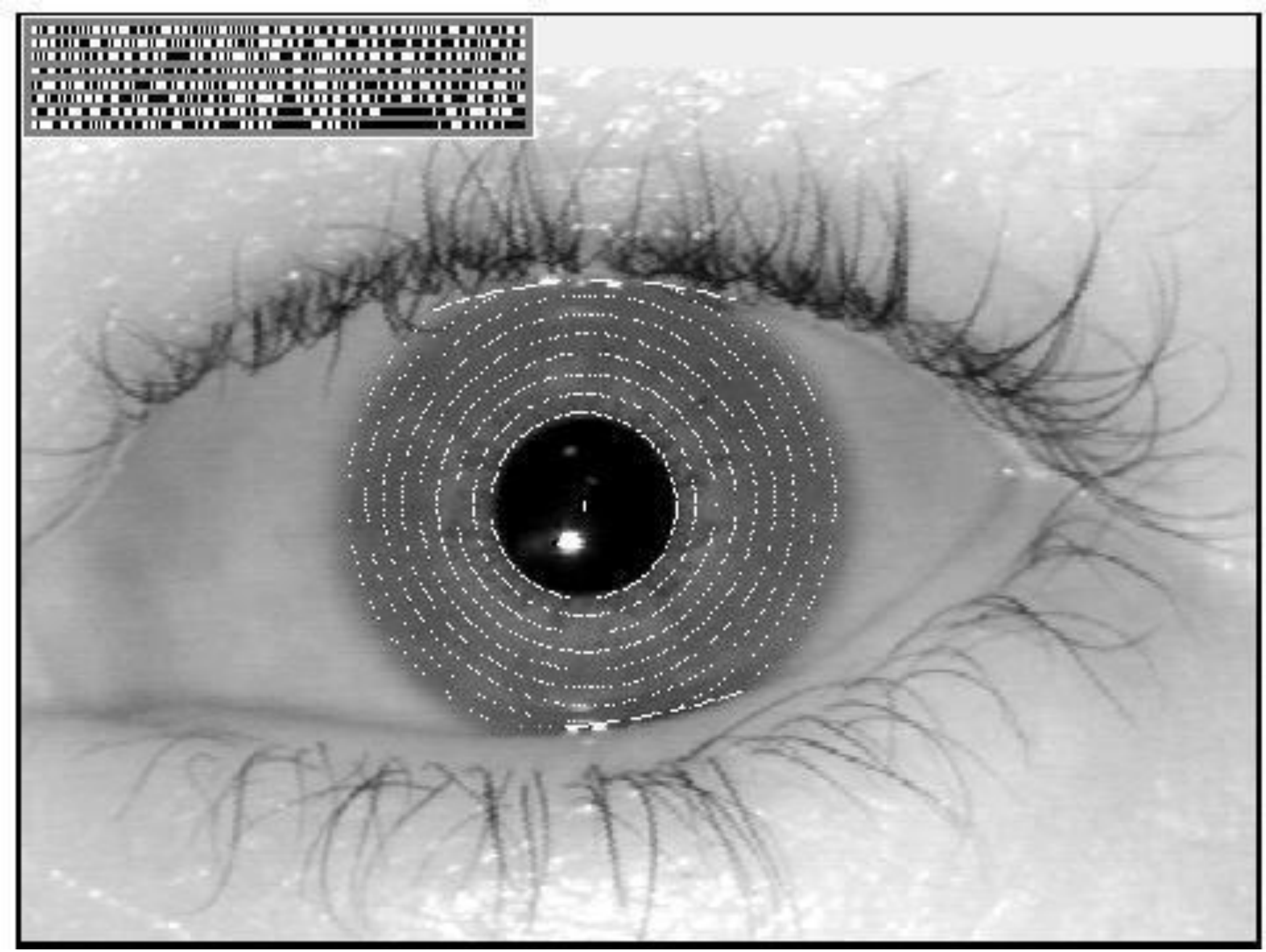
- with a black and white video camera in a well lit environment.
- The pattern is extracted after elastic deformations, such as dilation and constriction, mapped to pseudo polar coordinate
- method called complex valued 2D Gabor wavelets used to extract a bit stream of typically 256 bytes of information
- The amount and uniqueness of extracted information make the False Accept probability lowest of all known biometrics.
- The scanning can be made from the distance of few meters so the user does not feel the process intrusive.

Iris recognition



HOW IRIS SCANNERS RECORD IDENTITIES
1
Scanner reads from outer iris inwards to pupil edge
2
Scanner plots distinct markings on iris and maps unique shape
3
After plotting many marks within the iris all data is saved to a database
4
Other scanners will compare this data to verify individual identities

Iris recognition



Iris recognition

Iris recognition:

- Advantages:
  - Very high accuracy. minimally invasive, requiring an individual only to look into a reader
  - The eye from a dead person would deteriorate too fast to be useful, sure that the user is a living human being.
  - Iris scanning has the lowest false-accept rate of all biometrics
- Disadvantages:
  - Intrusive.
  - A lot of memory for the data to be stored.
  - Very expensive

Contents

- Definition, Characteristics and Biometrics process
- Biometric techniques
  - **Standard**
    - Facial recognition
    - Voice recognition
    - Signature recognition
    - DNA
    - Retinal scanning
    - Iris recognition
    - **Fingerprint**
    - Hand Geometry
  - Esoteric

Fingerprint

History

- Fingerprints have been found on ancient Babylonian clay tablets, seals, and pottery also been found on the walls of Egyptian tombs and on Minoan, Greek, and Chinese pottery
- By **246 BC**, Chinese officials were impressing their fingerprints into the clay seals used to seal documents
- **1247–1318**, Persian physician Rashid-al-Din Hamadani refers to practice of identifying via fingerprints commenting: "Experience shows that no two individuals have fingers exactly alike”
- **1684**, the English physician Nehemiah Grew published the first scientific paper to describe the ridge structure of the skin covering the fingers and palms

Fingerprint

- most commercially successful biometric technologies today
- systematic classification of fingerprints started in the 1800's.
- positive user response in the enrolled pilot projects, drawbacks and disappointments have occurred trough the years.

Analysis:

- small unique marks of the finger image known as minutiae are used. Minutiae points such as finger image ridge endings or bifurcations, branches made by ridges.
- The relative position of minutiae is used for comparison, and according to empirical studies, two individuals will not have eight or more common minutiae

Fingerprint

Capture:

- a typical live-scan fingerprint will contain 30-40 minutiae
- not immune to environmental disturbance.

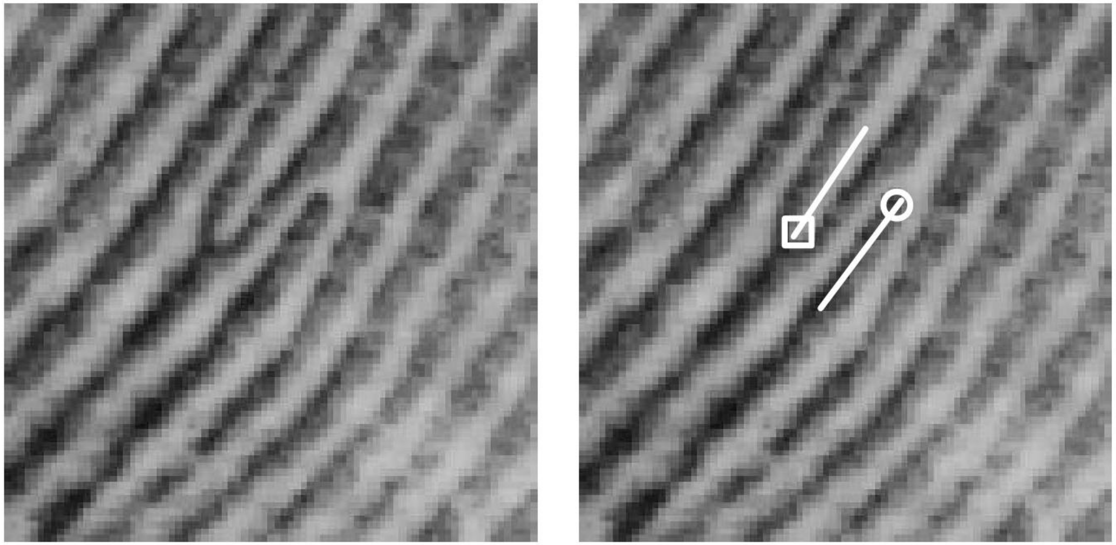
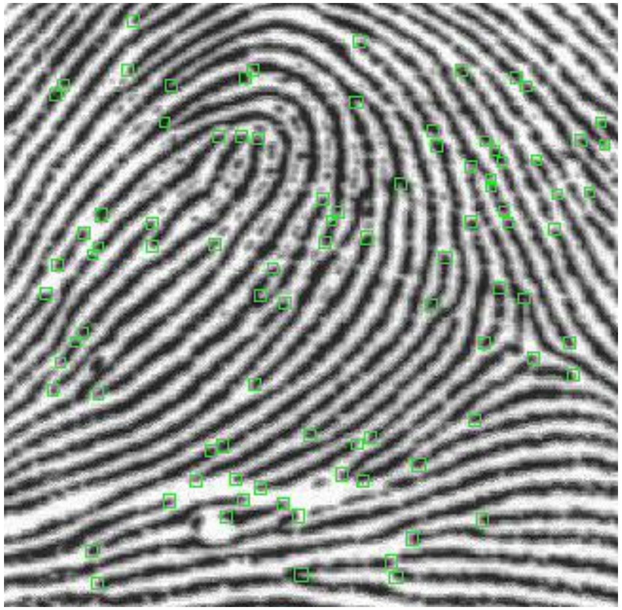


Figure 5. Minutiae: bifurcation (square marker) and ridge ending (circle marker).



- Interesting resource http://www.youtube.com/watch?v=IrpTqKkgygA, http://www.youtube.com/watch?v=Ry8920R7bxs

Fingerprint

Capturing techniques (4):

- Optical image capture typically involves a light source which is refracted trough a prism. Users place a finger on a glass surface known as platen. Light shines on the parts of the fingertip touching the glass and the formed image is captured.
- Tactile or thermal techniques use sophisticated silicon chip sensitive to pressure or heat to capture the finger image.
- Capacitance silicon sensors measure electrical charges and give an electrical signal from the areas where the finger ridges are touching the sensor surface.
- Ultrasound image capture.

Fingerprint

Fingerprinting systems

- AFIS systems predominantly used by law enforcement organizations around the world.
- developed for rapid and automatic comparison of single finger images with a large database of known images. For example FBI database contains approximately 70 million fingerprints (1998).
- It is impossible to reconstruct a fingerprint from the biometric template file, still that itself does not prevent using it to fraud purposes.
- How it is stored? www.c3.lanl.gov/~brislawn/FBI/FBI.html

Fingerprint

Summary

- Criminology has been using finger printing procedures since the early 20th century
- Comparison of papillae and dermal ridges of the fingertips
- When used for personal identification (entrance procedures) -> special fingertips reader required
  - The system calculates data record from the pattern it has read and compares that with stored pattern
- Modern fingerprint ID systems – half a second to recognize
  - Preventing frauds, it can recognize whether the placed fingertip is that of a living person

Fingerprint

Fingerprint:

- Advantages:
  - Very high accuracy.
  - Is the most economical biometric authentication technique.
  - it is one of the most developed biometrics, easy to use.
  - Small storage space required for the biometric template, reducing the size of the database memory required
- Disadvantages:
  - related to criminal identification = lowers social acceptability
  - It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age.
- More info: http://www.cccure.org/Documents/HISM/046-048.html

Contents

- Definition, Characteristics and Biometrics process
- Biometric techniques
  - **Standard**
    - Facial recognition
    - Voice recognition
    - Signature recognition
    - DNA
    - Retinal scanning
    - Iris recognition
    - Fingerprint
    - **Hand Geometry**
  - Esoteric

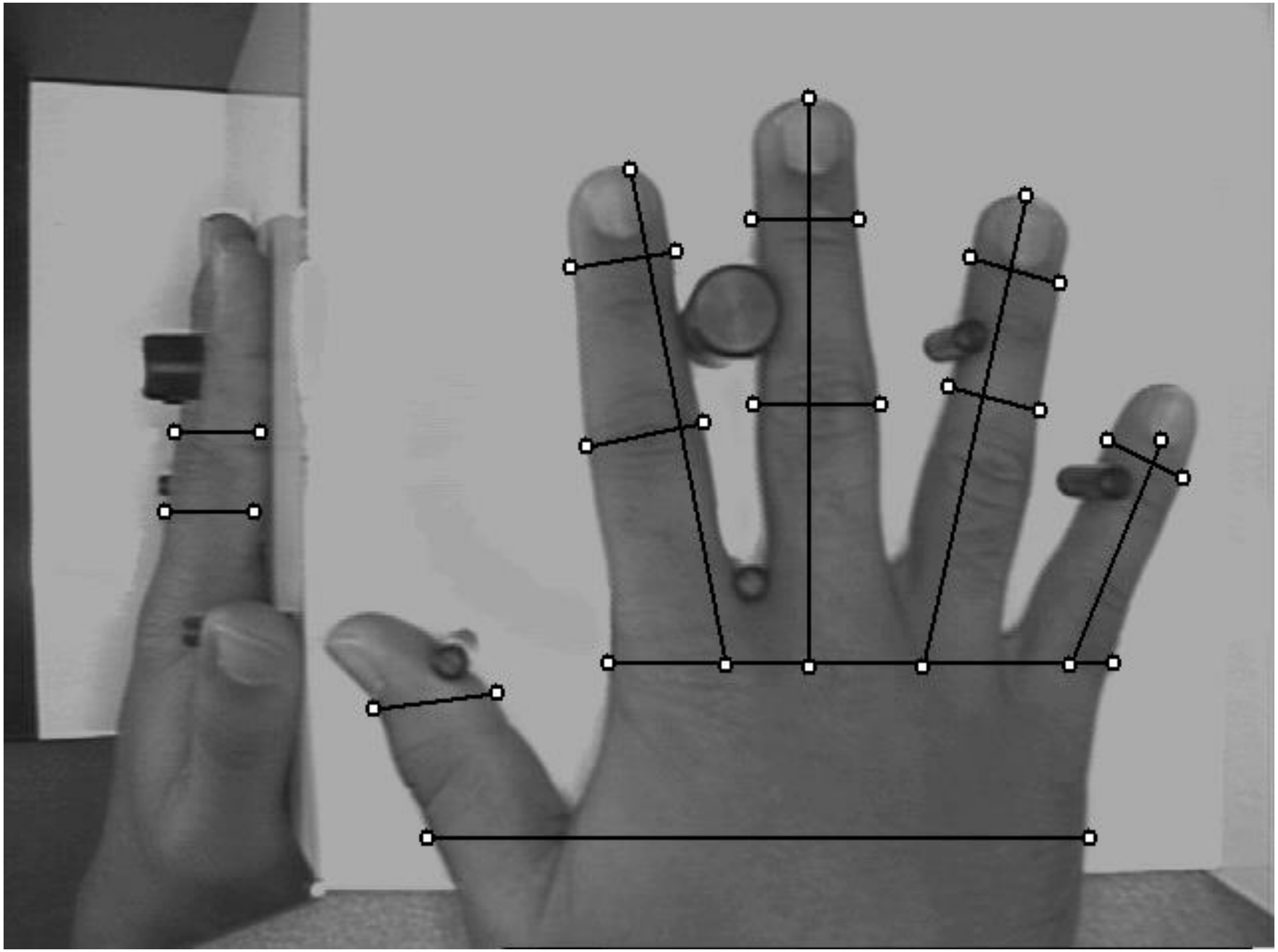
Hand geometry

- 3D image of the hand is taken and the shape and length of fingers and knuckles are measured.
- In use for many years in various applications, predominantly for access control. The technology does not achieve the highest levels of accuracy but it is convenient and fast to use.

Capture:

- a user places a hand on the reader, aligning fingers with guides. Cameras, positioned on above and on the side of hand capture images from which measurements are taken at selected points.
- Not unique, it cannot be used as accurate identification.
- Because of its user-friendliness it is well suited to id verification

Hand geometry



Hand geometry

Hand Geometry:

- Advantages:
  - – easy integration into other devices or systems.
  - – It has no public attitude problems as it is associated most commonly with authorized access.
  - – The amount of data required to uniquely identify a user in a system is the smallest by far.
- Disadvantages:
  - – Very expensive, Considerable size.
  - – It is not valid for arthritic person, since they cannot put the hand on the scanner properly.
- More info: http://www.cccure.org/Documents/HISM/048-050.html

Contents

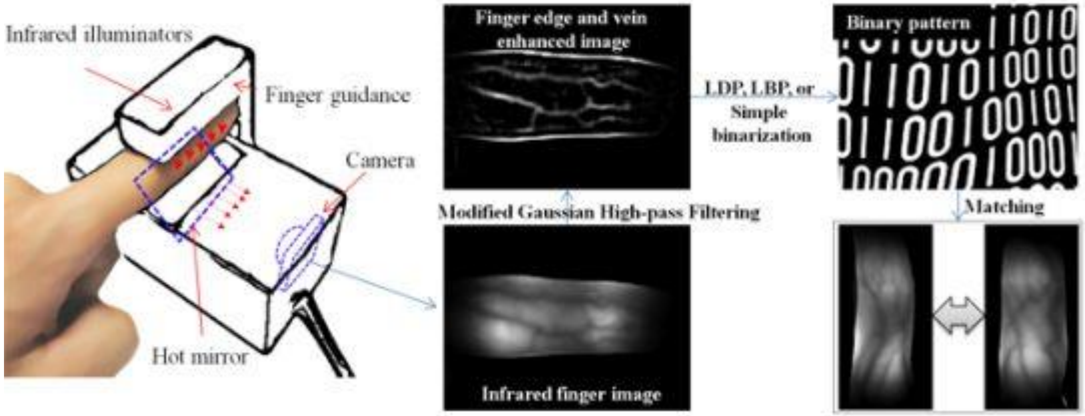
- Definition, Characteristics and Biometrics process
- Biometric techniques
  - Standard
  - **Esoteric**
    - Finger geometry
    - Palm geometry
    - Wrist veins
    - Locomotion
    - Shape of ear
    - scent
    - dynamics of keyboard typing

Finger geometry

- is very closely related to hand geometry. The use of just one or two fingers means more robustness, smaller devices and even higher throughput.

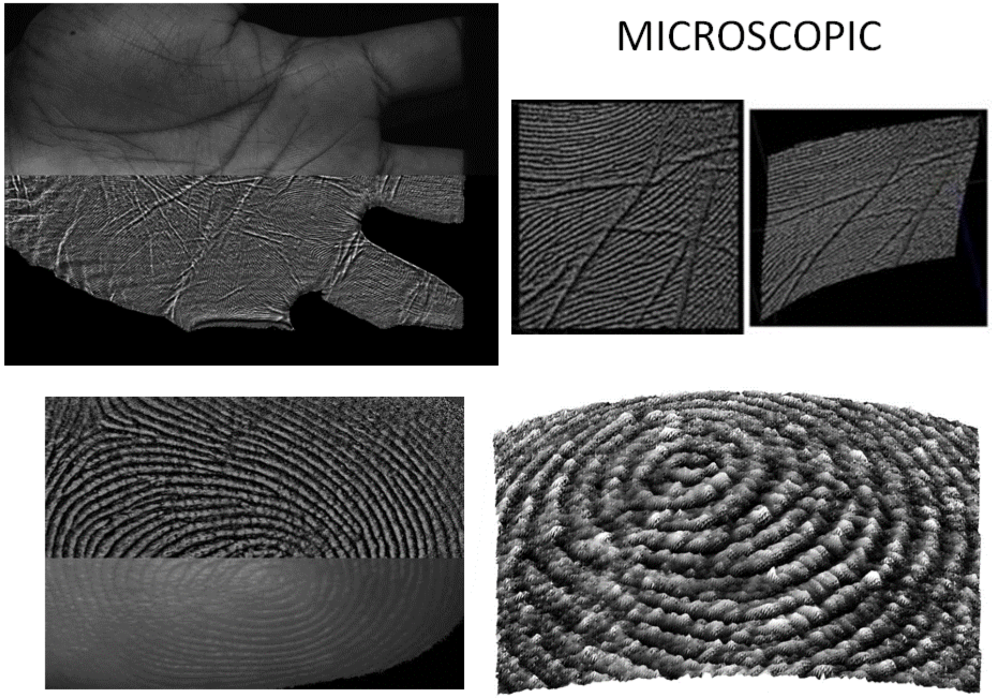
Capture (2 tech):

- first being similar to hand geometry presented above.
- second technique requires the user to insert a finger into a tunnel so that 3D measurements of the finger can be made.


Infrared illuminators
Finger guidance
Camera
Hot mirror
Finger edge and vein enhanced image
LDP, LBP, or Simple binarization
Binary pattern
Modified Gaussian High-pass Filtering
Matching
Infrared finger image

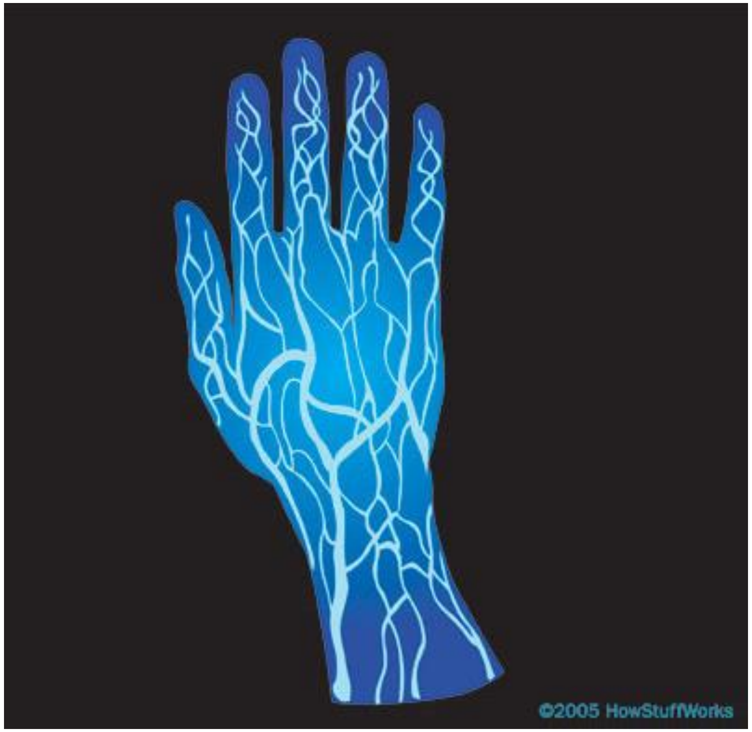
Palm geometry

- Palm biometrics is close to finger scanning and in particular AFIS technology.
- Ridges, valleys and other minutiae data are found on the palm as with finger images.



Wrist veins

- One of the latest method – first commercial system in 2000
- Joseph Rice is the originator of this technology where a low cost B&W CCD camera with near infrared LED array is used to read the veins beneath the skin



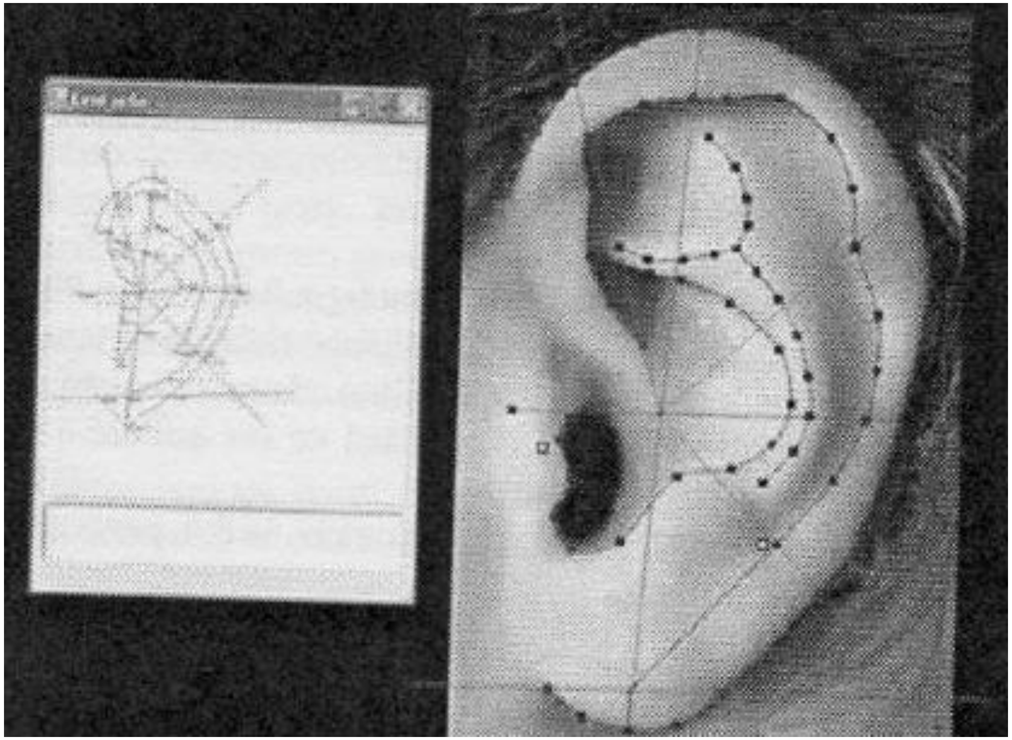
©2005 HowStuffWorks

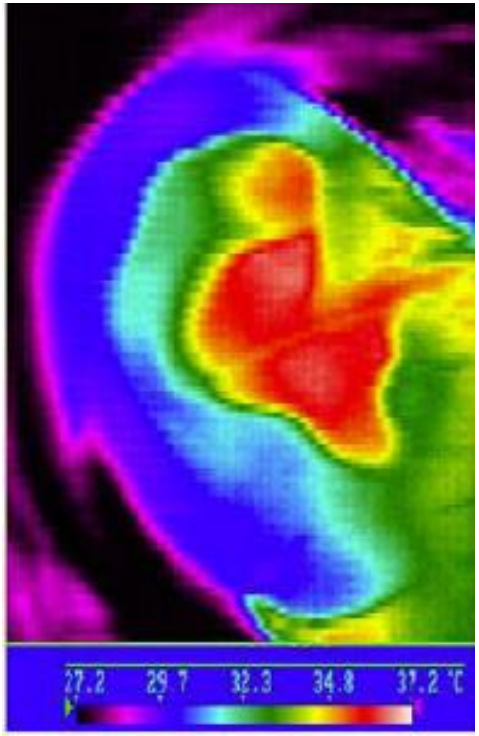
Locomotion

- Analysis of a movement
- Sophisticated forensic technique

Shape of ear

- By optical sensor 0,5 - 1 m from ear or security camera
- Geometry and special markers (forensic)
- Infrared / heat sensors used for partially obscured ears (by hair)





scent

- used in forensic as indirect proof
- 30 chemicals, unique in intensity or absent
- content of scent can change due to emotional or hormonal disbalance

dynamics of keyboard typing

- Keystroke recognition works by examining the unique way in which an individual types on a computer keyboard.
- Variables include typing speed, the length of time that keys are held down, and the time taken between consecutive keystrokes.

References

- **Encyclopedia of Biometrics: I - Z., Volume 2**
- http://www.bromba.com/faq/biofaqe.htm#Biometrie
- http://biometrics.nist.gov/cs_links/standard/archived/workshops/workshop1/presentations/Podio-M1-SC37.pdf
- http://fingerchip.pagesperso-orange.fr/biometrics/types.htm
- Advantages and disadvantages of technologies, http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

(TLG)Hades
NWS 2000/2
29/10/2000 02:21
nwsnet.de