Authentication, Identification and Access Control, Biometrics

March 2023

Dr. Dhiren R. Patel

Authentication

- Authentication
- Anonymity
- Identification
- Verification

Access Control

- □ Individual access (e-mail)
- □ Group access (e.g. Library subscription to IEEE)
- □ Quota (Printing, CPU/GPU limit per day, Storage)

Entity authentication techniques

- Something the user **knows**
- Something the user **has**
- Something the user **is**

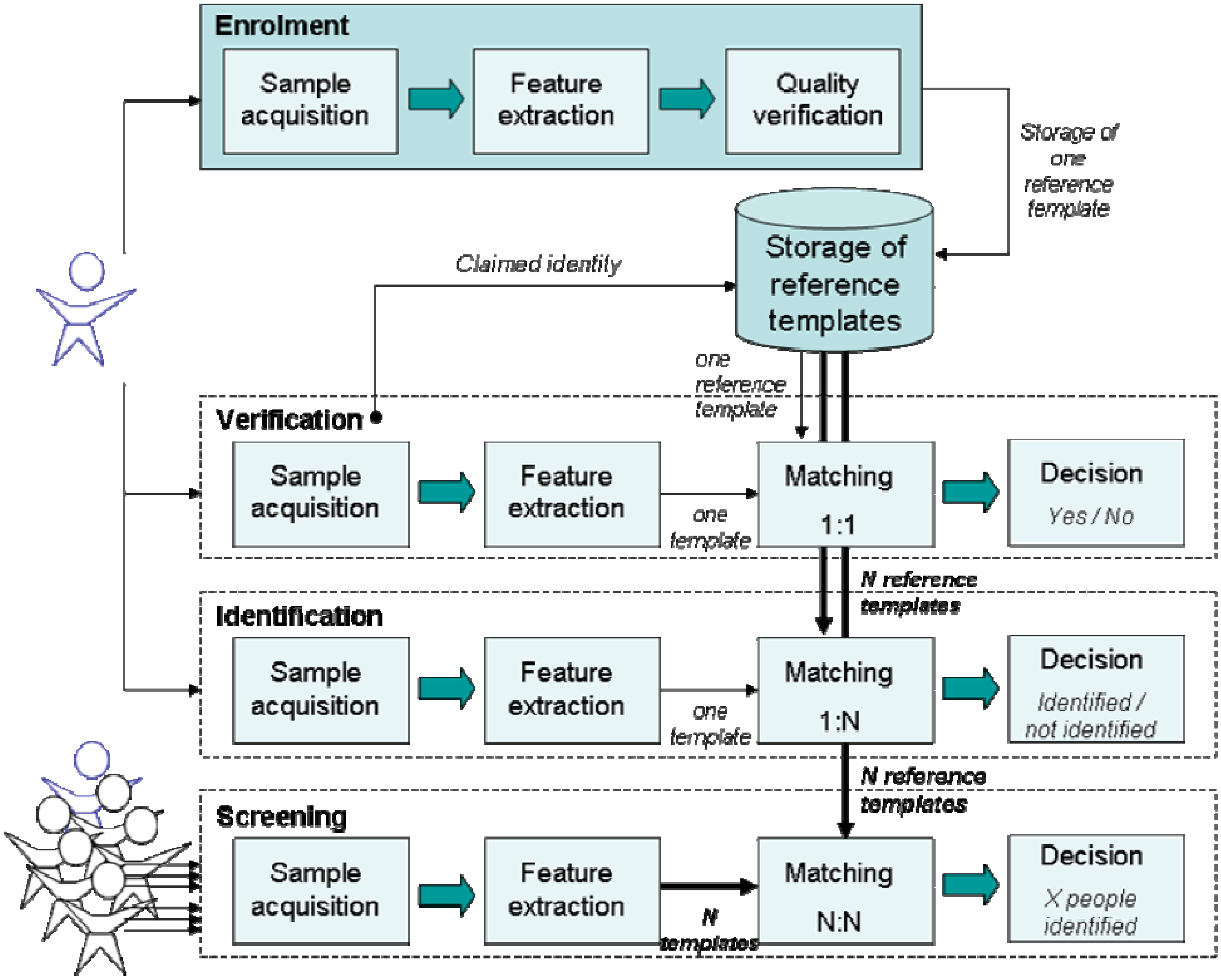
- **Discussion on merits and demerits of above systems**

Biometric techniques

- Biometric techniques are based on the features that cannot be lost or forgotten. It benefits users as well as system administrators because it avoids the problems and cost associated with lost, reissued, or temporary tokens, cards, and passwords
- It is almost impossible to lose or forget biometrics, since they are an intrinsic part of each person, and this is an advantage which they hold over keys, passwords or codes.

Technology

- Biometric technologies may be used in three ways:
- (a) to verify that people are who they claim to be,
- (b) to discover the identity of unknown people, and
- (c) to screen people against a watch-list.
- Biometric identification works in four stages: *enrolment*, *storage*, *acquisition* and *matching*.
- It cannot rely on secrecy, since most biometric features are either self-evident or easily obtainable.



Enrolment

Sample acquisition

Feature extraction

Quality verification

Storage of one reference template

Storage of reference templates

Claimed identity

one reference template

Verification

Sample acquisition

Feature extraction

one template

Matching 1:1

Decision *Yes / No*

N reference templates

Identification

Sample acquisition

Feature extraction

one template

Matching 1:N

Decision *Identified / not identified*

N reference templates

Screening

Sample acquisition

Feature extraction

N templates

Matching N:N

Decision *X people identified*

Process

- First, Individuals are enrolled, i.e. a record associating the identifying features with the individual is created. For example, an iris scan is performed and the result is labeled “Y. Singh”.
- Features extracted during enrolment and acquisition stages are often transformed (through a non-reversible process) into *templates* in an effort to facilitate the storage and matching processes.
- Templates or full samples thus acquired may then be held in storage that is either centralized (e.g. in a database) or decentralized (e.g. on a smart card or tokens). When identification is required, a new sample of the feature is acquired (e.g. a new iris scan performed).
- Finally, the newly acquired record is compared to the stored record. If they match, the individual has been identified.

Approaches

- Physiological approaches include fingerprints; iris and retina scans; shape of hand, finger prints, face, and ear geometry; hand vein and nail bed recognition; height, weight, body odour, DNA; palm prints etc.
- Biometric characteristics can be considered as a bridge between an identity record and the individual this record belongs to.
- Since biometric measurements are part of the body, they will always be present when needed
- In this way it establishes a ‘trusted’ method to strongly link the stored identity with the physical person it represents.

Complexity

- Biometric identification is a statistical process. Variations in conditions between enrolment and acquisition as well as bodily changes (temporary or permanent) mean that there is never a 100% match.
- For a password or a PIN, the answer given is either exactly the same as the one that has been stored, or it is not – the smallest deviation is a reason for refusal; for a biometric, there is no clear line between a *match* and a *non-match*.

Complexity

- A 90% probability of a match may or may not be considered acceptable, depending on the implementation of the biometric in question and the application security requirements (on the setting of the threshold). As a consequence of the statistical nature of the acquisition and matching stages, biometric systems are never 100% accurate.
- A false match occurs when an acquired template is erroneously matched to a template stored from enrolment, although the two templates are from two different persons.
- A false non-match occurs when an acquired template is not judged to match the template stored from enrolment, although both are from the same person.

Evaluation criteria

- Biometric features include various subsets of body characteristics, but not all such subsets are suitable for identification purposes. For example, a photograph of one particular body part (the face) is sufficient for many purposes, while a photograph of other body parts (say, elbows or feet) is useless.
- In functional terms the current uses of biometrics can be categorized under the following headings: *verification*, *identification* and *screening*.

Evaluation criteria

- 1. **Universality:** All human beings are endowed with the same physical characteristics - such as fingers, iris, face, DNA – which can be used for identification
- **2. Distinctiveness:** For each person these characteristics are unique, and thus constitute a distinguishing feature
- **3. Permanence:** These characteristics remain largely unchanged throughout a person's life
- **4. Collectability:** A person's unique physical characteristics need to be collected in a reasonably easy fashion for quick identification
- **5. Performance:** The degree of accuracy of identification must be quite high before the system can be operational
- **6. Acceptability:** Applications will not be successful if the public offers strong and continuous resistance to biometrics
- **7. Resistance to Circumvention:** In order to provide added security, a system needs to be harder to circumvent than existing identity management systems

Types of biometrics

There are 2 classifications of biometrics

- Behavioral – something that you do
- Physiological – something that you are

Biological

- Face
- Hand
- Finger
- Iris
- Vein
- Retinal Imaging
- Ear
- Odor

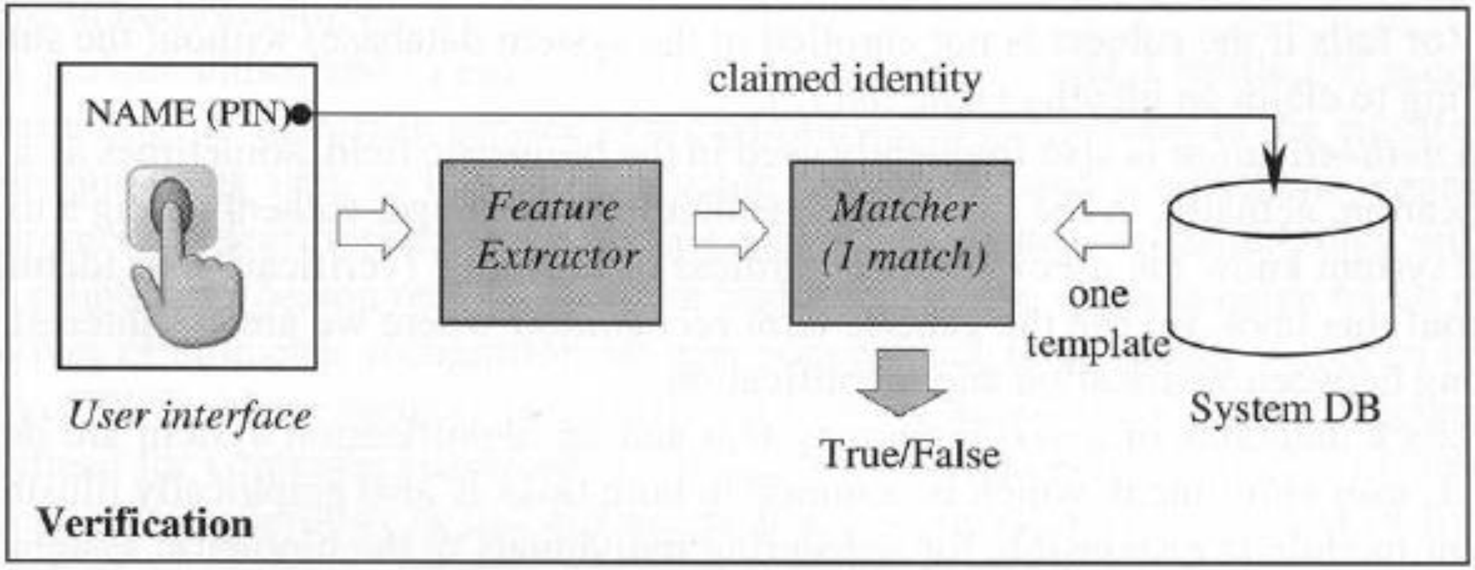
Behavioral

- Signature
- Keystroke
- Voice*
- Gait*

* Indicates has components that are behavioral and physiological

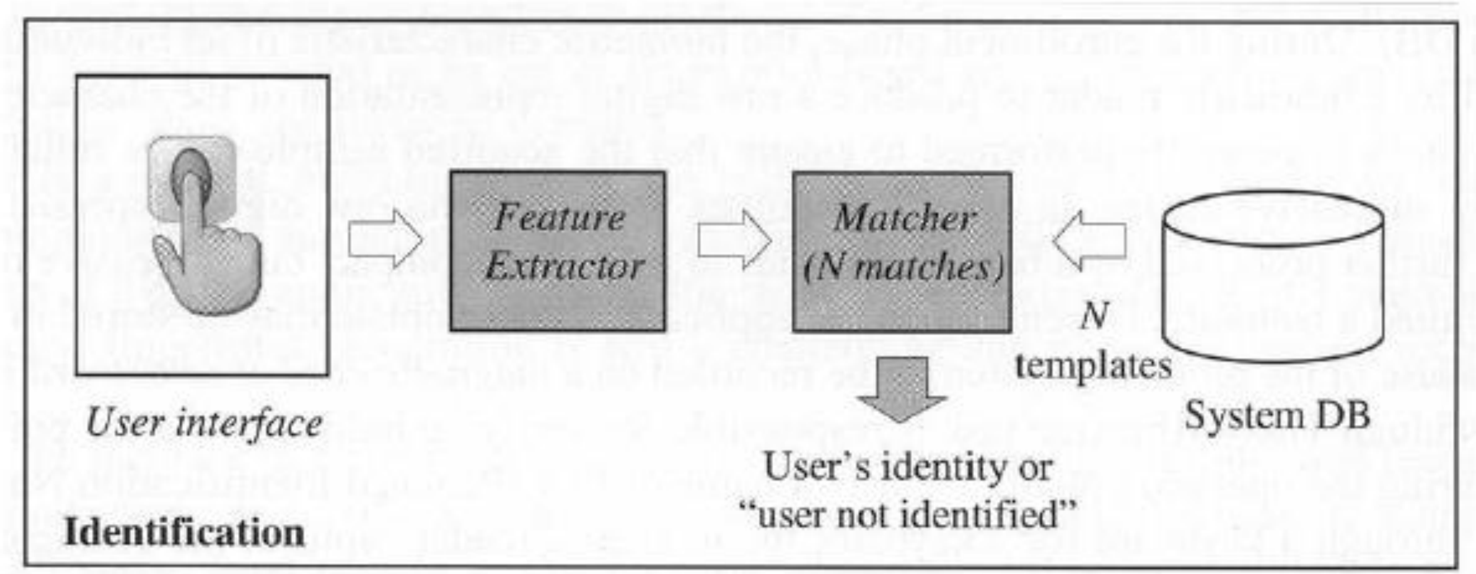
Verification

- a test to ensure whether person X is really who he or she claims to be.
- 1-to-1 matching



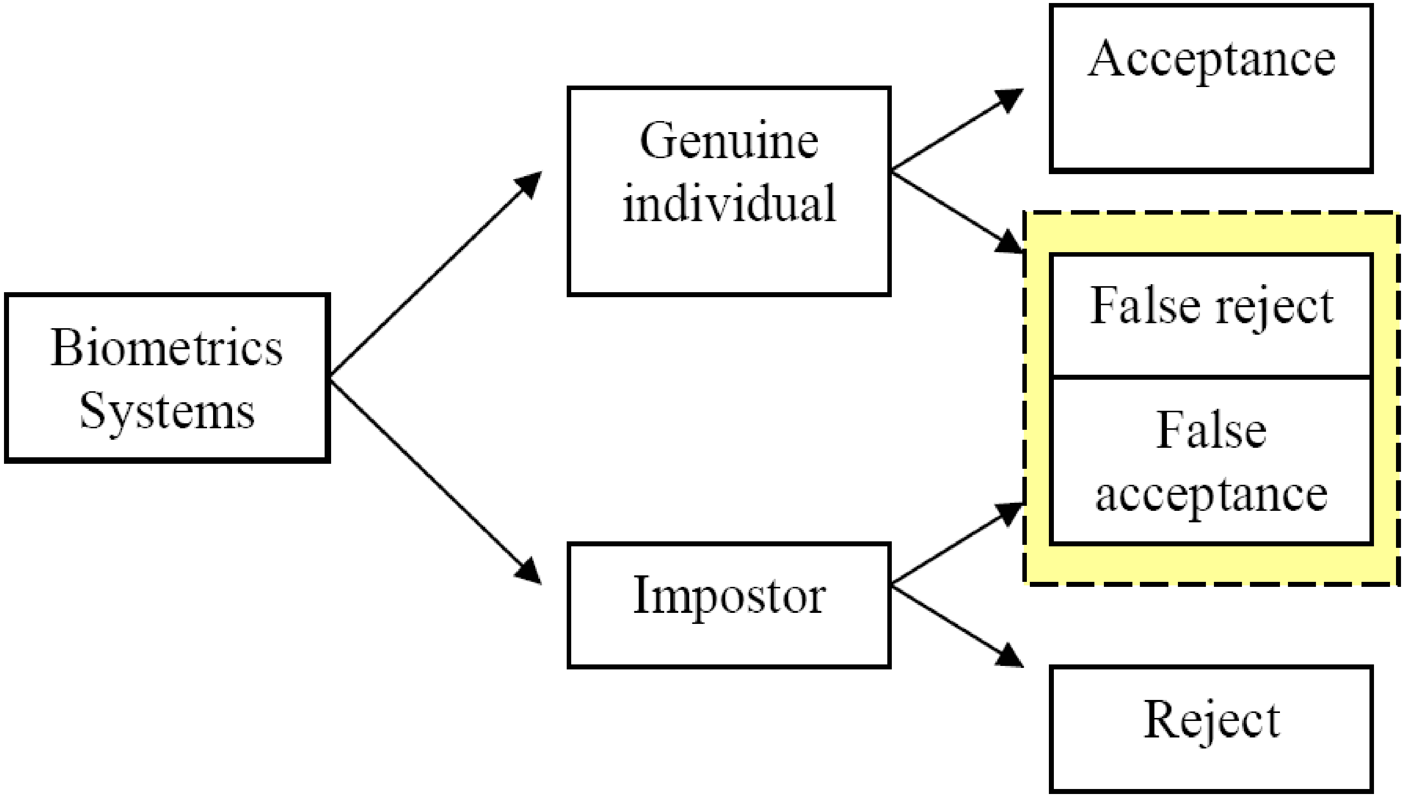
Identification

- (1-to-many matching)
- used to discover the identity of an individual when the identity is unknown (the user makes no claim of identity).
- a central database is necessary that holds records for all people known to the system.



System

- Identification may result in one of two types of error described previously: i.e. a false match or a false reject.



Data Capture: Scan

Data capture involves the presentation of the biometric to the sensor by the user

- Encompasses the Human-Biometric Sensor Interaction (HBSI)
- Must consider issues of usability
  - What must your user do to interact?
  - When should the user interact?
- Data capture occurs for enrollment and each verification/identification attempt

Signal Processing

Signal Processing is broken down into 3 tasks:

1. Segmentation
2. Feature Extraction
3. Quality Control
    - Enrollment
        - If quality is high, the sample can be processed as a template
            - Templates are a binary representation of the sample
            - Templates are sent to an enrollment database for storage
            - If the quality is low the user will be asked to present their biometric again
    - Verification/Identification
        - Samples of good quality are sent for comparison to template(s)

Data Storage

Enrollment database contains stored templates

- When an individual makes a claim to an identity for verification, the enrollment template for that identity is used for comparison
- For identification, the submitted sample is compared to all enrolled templates

Matching & Decision

Comparison is made between template and sample and a similarity score is calculated

- Similarity score is an indicator of how close the template and sample are to each other

Decision is made whether or not the sample and the template is a match

- Based on a threshold value

Biometric System Decision Errors

- False Match – Deciding that two biometric samples are from the same individual, when they are from different individuals
- False Non Match – Deciding that two biometric samples are from different individuals, when they are from the same individual

Table 1: Decision Error Table

Score	Genuine Match (Correct Sample)	Imposter Match (Incorrect Sample)
Score ≥ threshold	Correct Match	False Match
Score < threshold	False Non-Match	Correct Non-Match

Match

- What constitutes a match between the biometric presented—the "bid sample"—and the enrolled template?
- The system should not require a perfect match because the bid sample and enrolled template most likely will not be identical. For example, in the case of a fingerprint, the samples will differ based on the fingertip area that any particular scan covers and the degree of compression of the ridges that results from varying pressure during the scan.
- Acceptable degree of difference
- false acceptance rate (FAR), the fraction of access attempts by an unenrolled individual that are nevertheless deemed a match; and
- false rejection rate (FRR), the fraction of access attempts by a legitimately enrolled individual that are nevertheless rejected.

Performance Measures

Error Rates

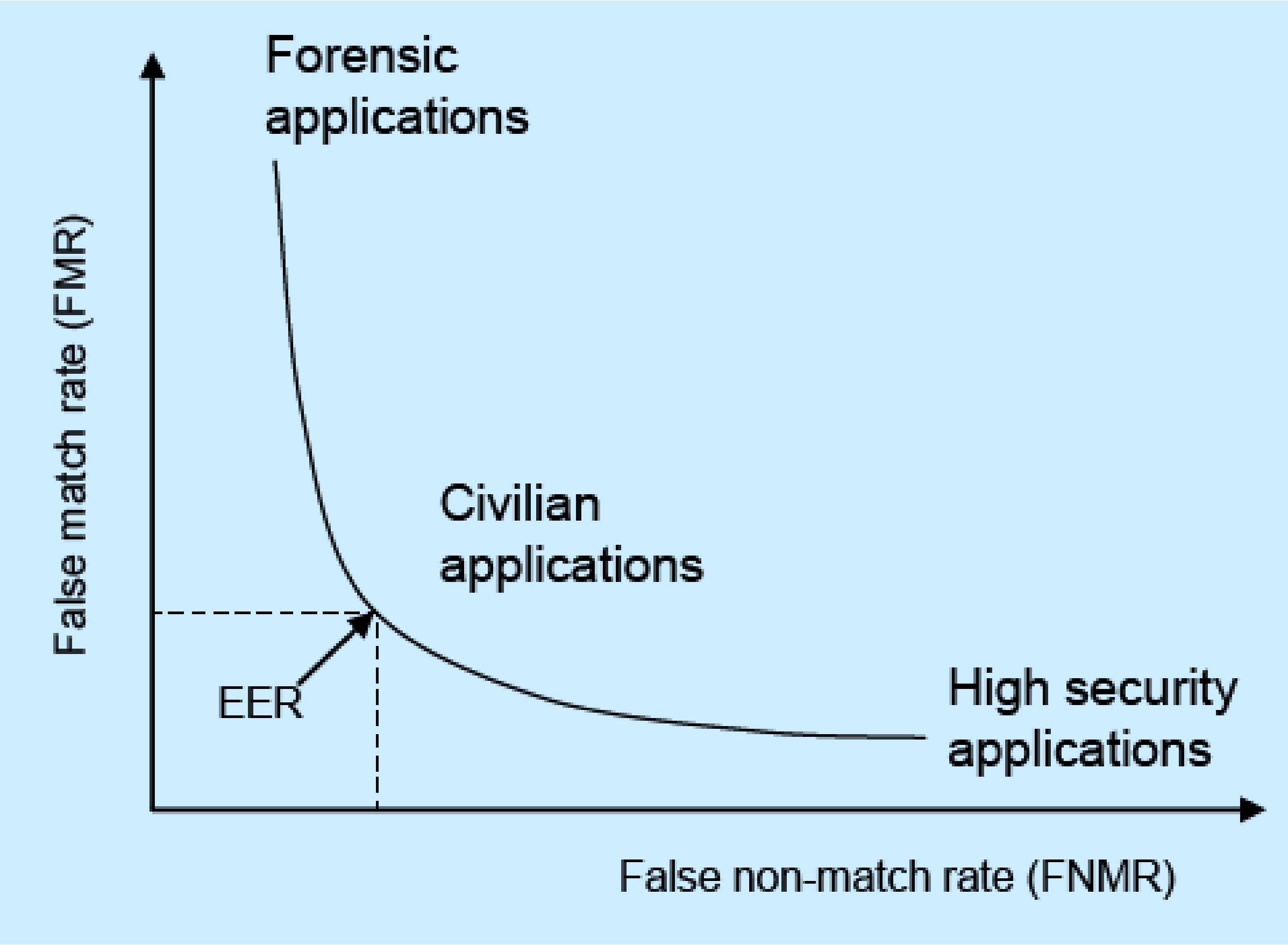
- False Match Rate (FMR)
    - Probability that a sample will be falsely declared to match a single randomly-selected imposter template
- False Non-Match Rate (FNMR)
    - Probability that a sample will be falsely declared not to match a template of the same user supplying the sample

Accuracy of biometric system

- in the case of a verification system there are two possible types of error:
- false non-match (also known as false negative or false rejection, i.e. rejection of a legitimate user) and
- false match (also known as false positive or false acceptance, i.e. acceptance of an impostor).
- The corresponding error rates are the **false rejection rate (FRR)** which is equivalent to false non-match rate (FNMR) and the false acceptance rate **(FAR)** which is equivalent to **false match rate (FMR)**.
- global error rate also includes the **failure to enroll rate (FTE)**, the **failure to acquire rate (FTA)** and also the **binning error rate -**To improve efficiency in systems requiring a one-to-many search of the enrolled database, some systems may partition template data to separate "bins".

Receiver operating characteristic (ROC) curve

different trade-offs between the false match rate and false non-match rate (FMR and FNMR).



DET Curve

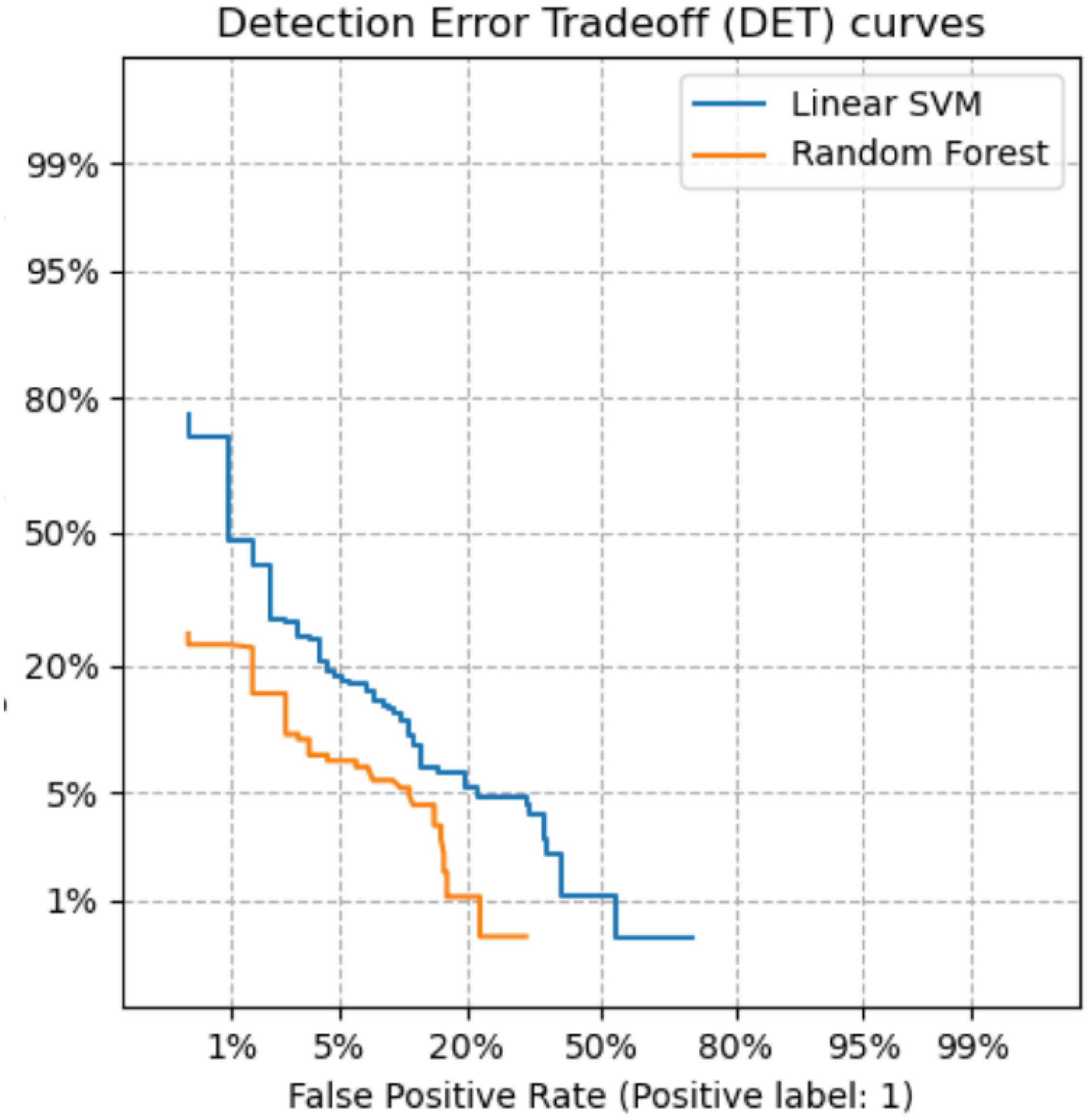
DET: Detection Error Trade-off

□ DET is a modified ROC (Receiver Operating Characteristic) curve that plots errors on both axes

□ DET plots false matches on the x-axis and false non matches on the y-axis

□DET curves give direct feedback of the detection error tradeoff to aid in operating point analysis. The user can then decide the FNR they are willing to accept at the expense of the FPR (or vice-versa).

DET (T) = (FMR (T), FNMR (T)) where T is the threshold


Detection Error Tradeoff (DET) curves
Linear SVM
Random Forest
99%
95%
80%
50%
20%
5%
1%
1%
5%
20%
50%
80%
95%
99%
False Positive Rate (Positive label: 1)

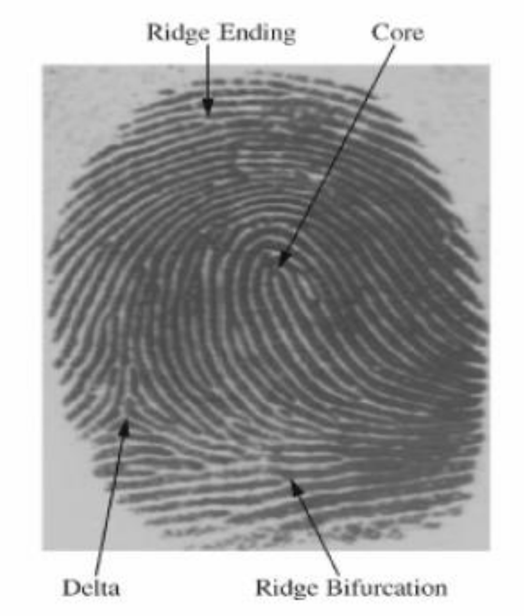
Finger print – as Biometric ID

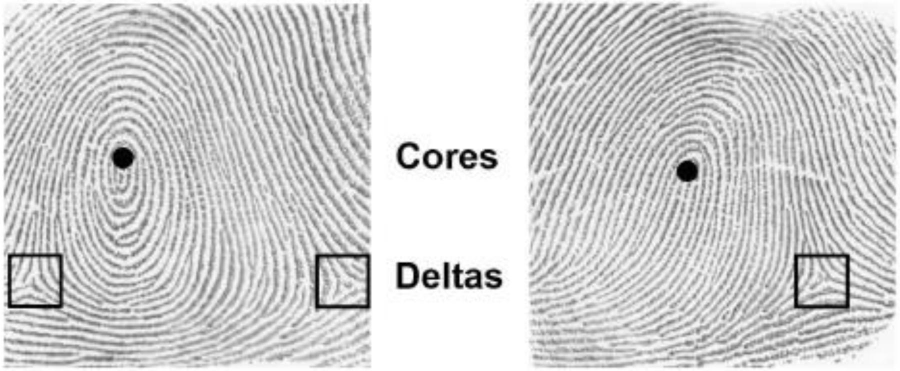
- Nearly every human being possesses fingerprints (*universality*) with the exception of hand-related disabilities.
- Fingerprints are also *distinctive* and the fingerprint details are *permanent*, although they may temporarily change due to cuts and bruises on the skin or external conditions (e.g. wet fingers).
- Live-scan fingerprint sensors can capture high-quality images (*collectability*).
- The deployed fingerprint-based biometric systems offer good *performance* and fingerprint sensors have become quite small and affordable.

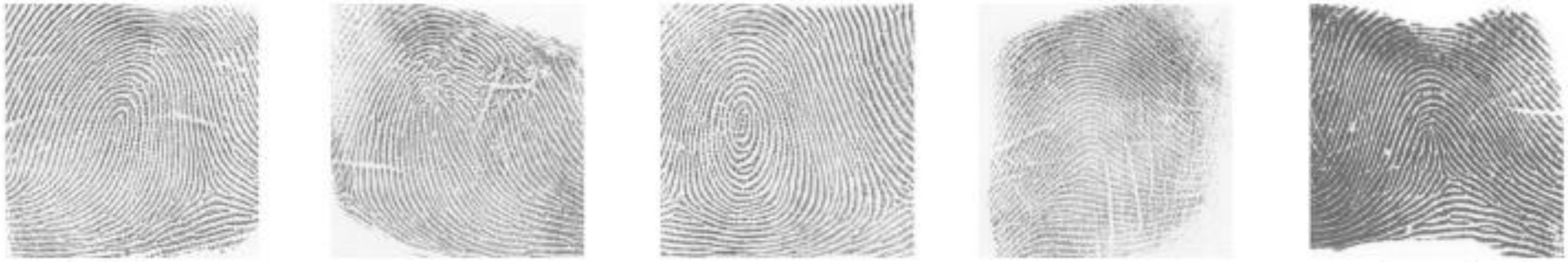
fingerprint

- By combining the use of multiple fingers, cryptographic techniques and liveness detection, fingerprint systems are becoming quite difficult to *circumvent*.
- A fingerprint consists of the features and details of a fingertip.
- There are three major fingerprint features: the arch, loop and whorl. Each finger has at least one major feature.
- The minor features (or minutiae) consist of the position of ridge ends (ridges are the lines that flow in various patterns across fingerprints) and of ridge bifurcations (the point where ridges split in two).

fingerprint

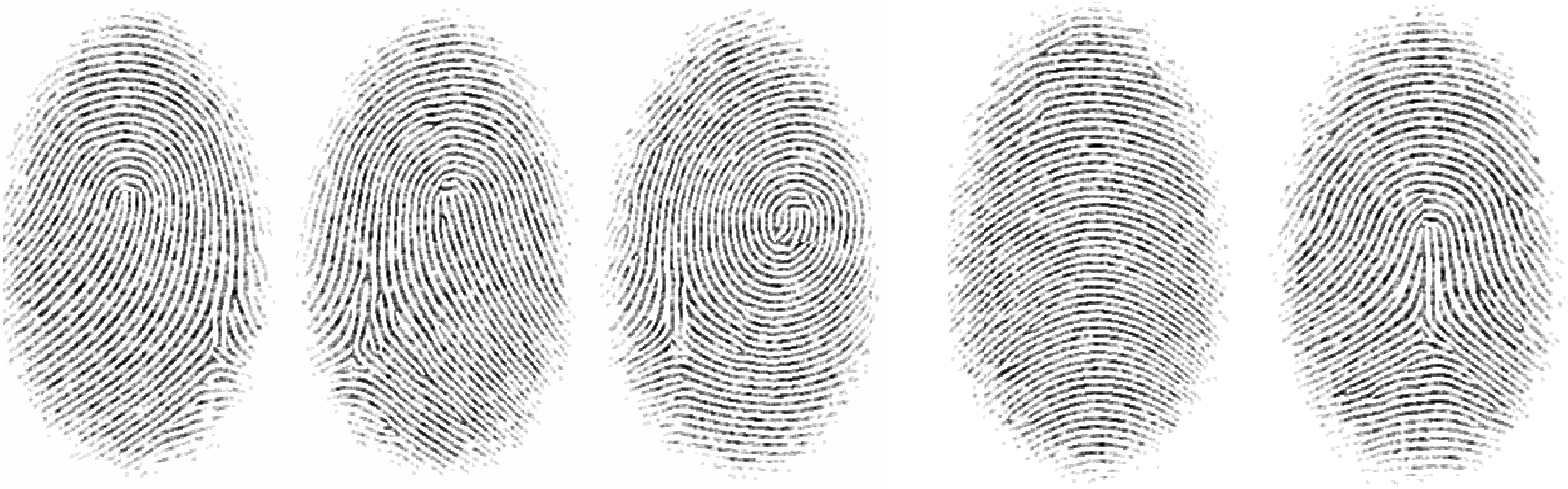






Left Loop Right loop Whorl Simple arch Tented arch

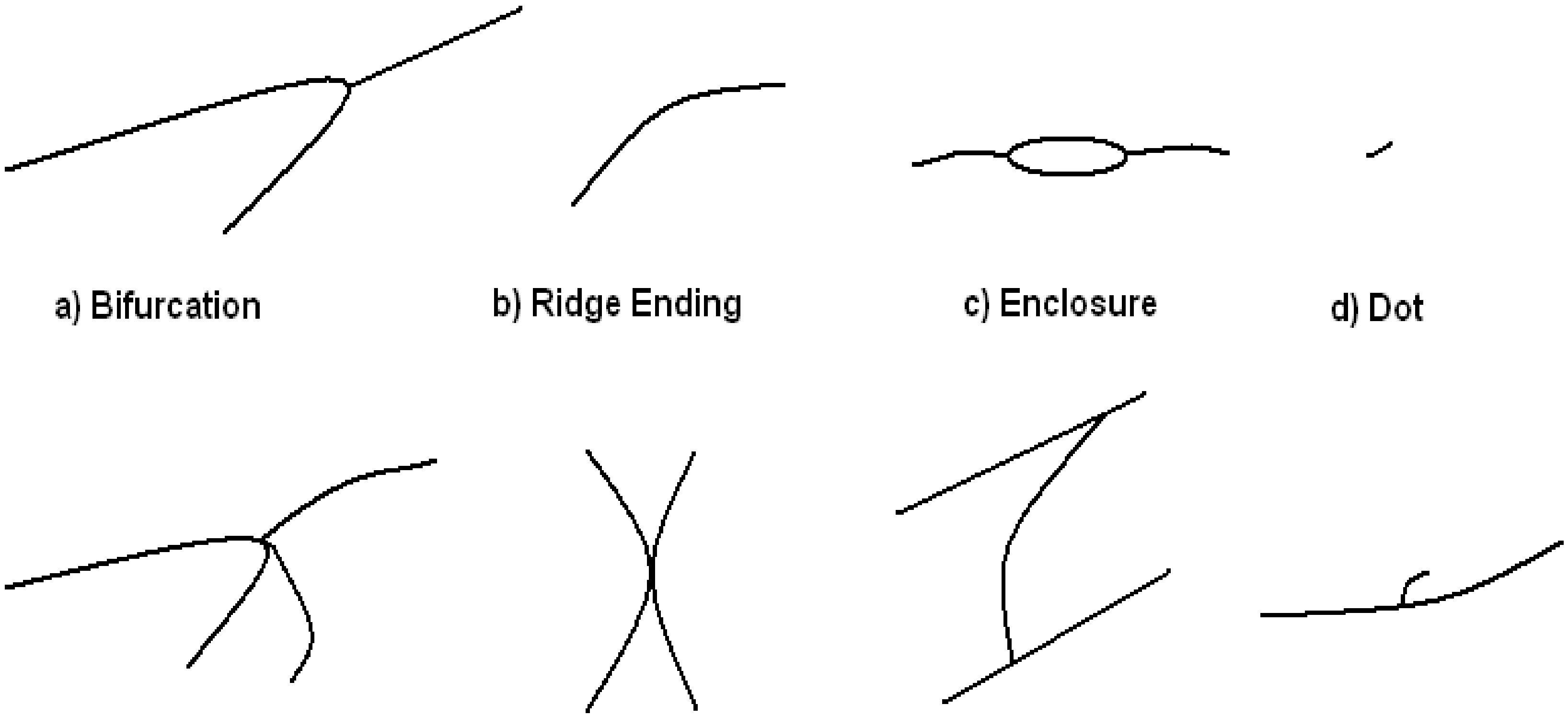
Henry System



Left Loop Right Loop Whorl Arch Tented Arch

Henry Classifications

Galton Features



a) Bifurcation

b) Ridge Ending

c) Enclosure

d) Dot

e) Trifurcation

f) Crossover

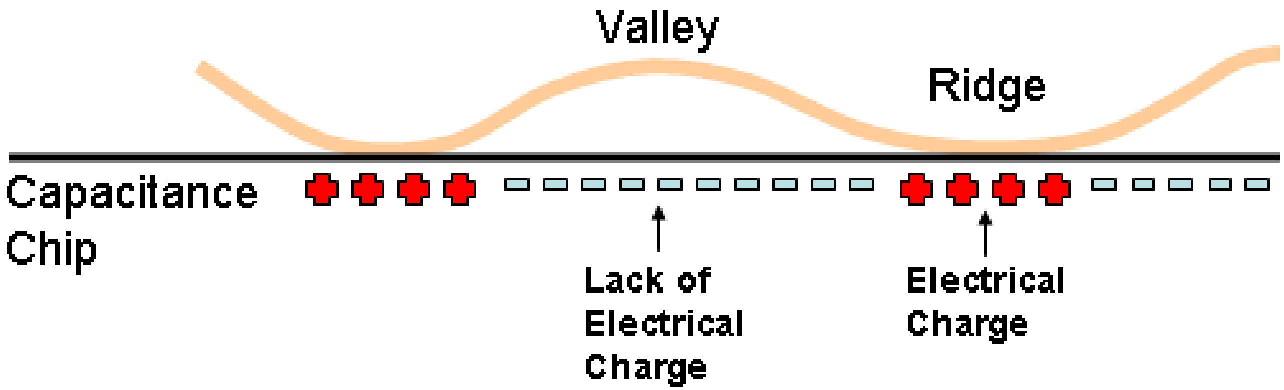
g) Bridge

h) Hook

Acquisition Technologies

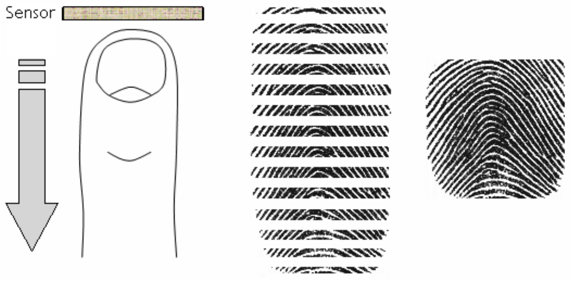
- Capacitance
- Optical
- Thermal
- Ultra-Sound
- Piezoelectric
- Touchless

Capacitance Touch & Swipe



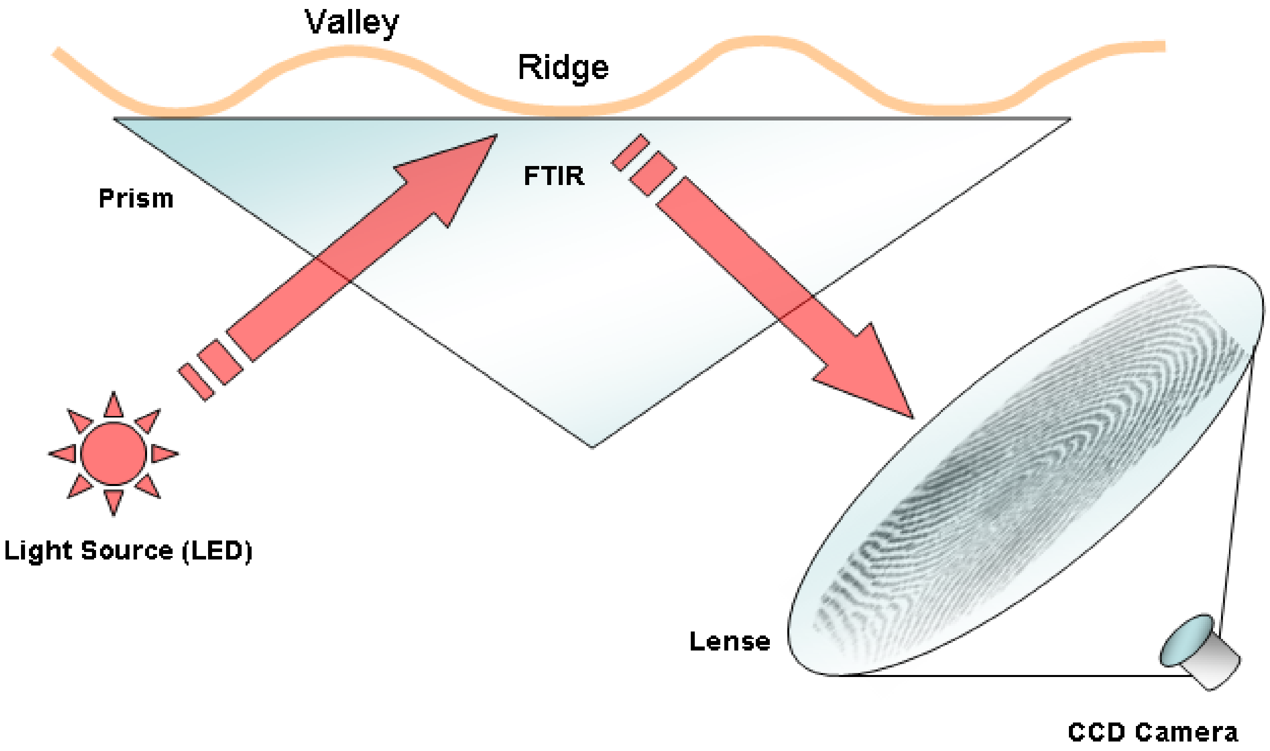
Electrical charge across finger skin

Swipe sensor



Stitching of capacitance image from a swipe sensor

Sensor Technology - Optical



Optical sensing diagram

Sensor Technology - Thermal

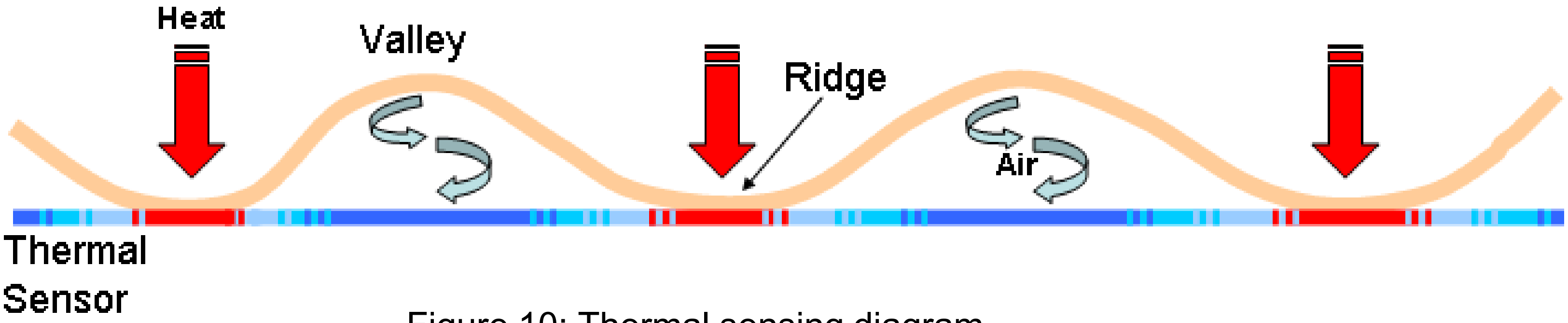
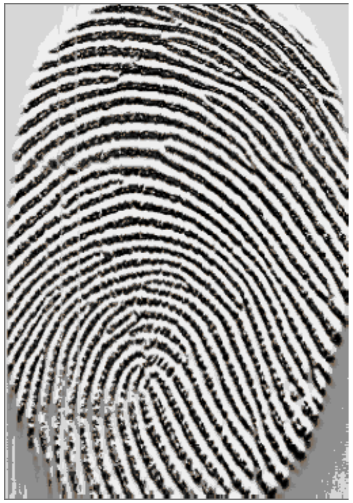


Figure 10: Thermal sensing diagram



Example print from a thermal sensor

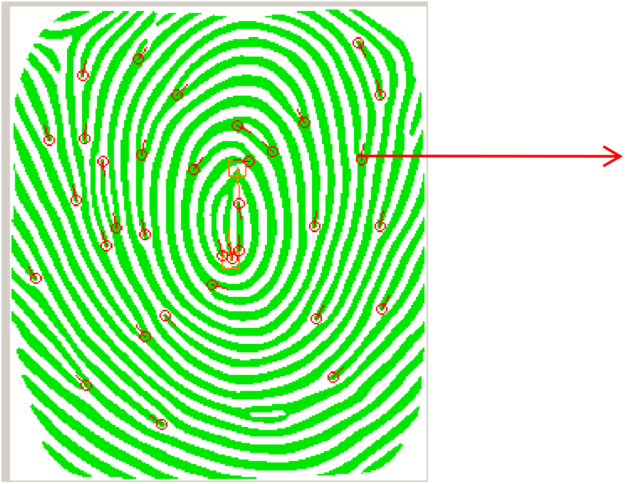
Extraction and Matching Algorithms

There are 3 categories for fingerprint matching:

1. Minutiae Based
2. Pattern Based
3. Hybrid

Minutiae Points

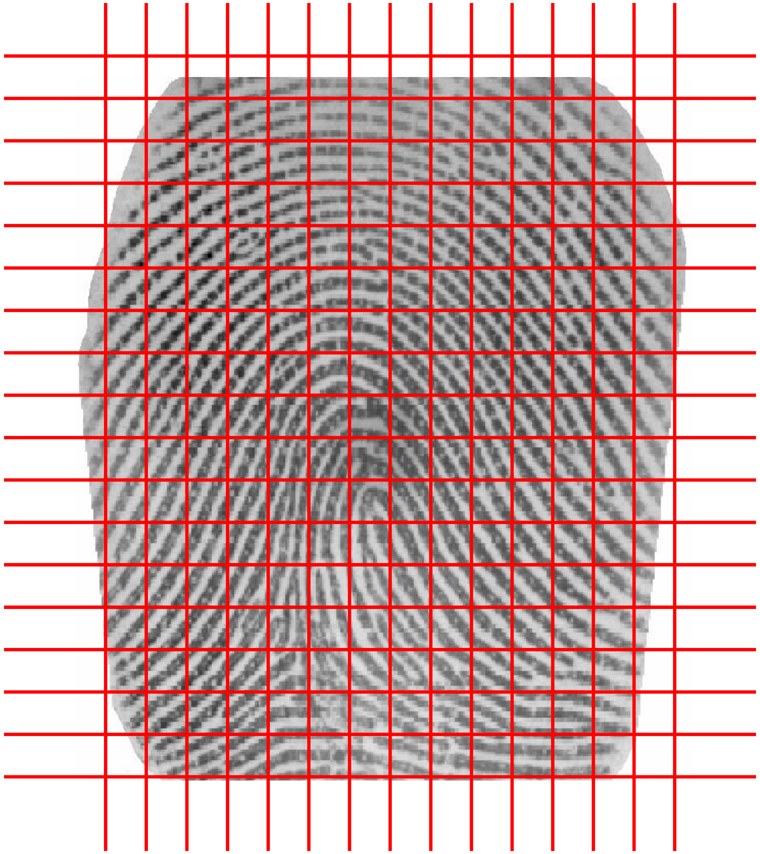
- The discontinuities in flow of ridges are called minutiae points
- The pattern of these minutiae points is used for fingerprint recognition in minutiae based matchers



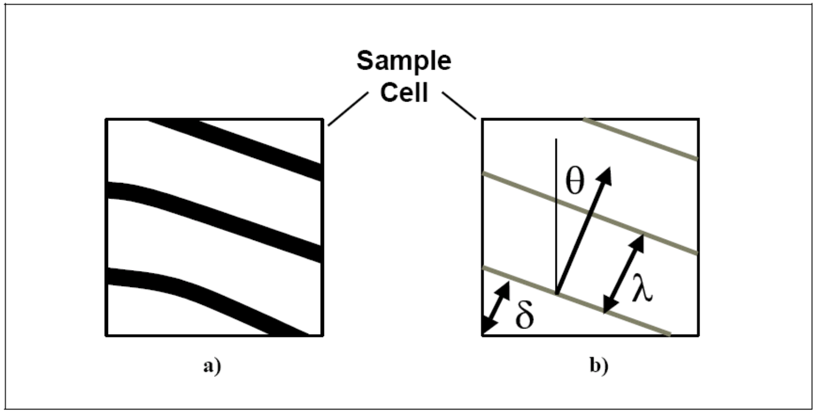
(x ,y ,θ, type)

Template with identified minutiae points

Image Processing – Pattern Based



Pattern recognition approach



Sample Cell

Analyze cells:

1. Overall shape
2. ridge counting
3. direction phase
4. pitch

question of interoperability

- Fingerprint recognition normally consists of a closed system that uses the same sensors for enrolment and acquisition, the same algorithms for feature extraction and matching and clear standards for the template and for instance, the enrolment procedure. (except for a large project - UIDAI)
- Different sensors using the same technology (e.g. solid state) produce different fingerprint raw image data, in the same way as sensors using different technologies (e.g. optical and solid state) deliver raw images that are significantly different.

Applications

- liveness detection procedures (e.g. 3-dimensional imaging, temperature measuring)
- to prevent fraudulent enrolment for benefits
- integration of fingerprints (with other biometrics) on travel documents and passports.
- Fingerprint identification of criminals for law enforcement

Iris - as BioID

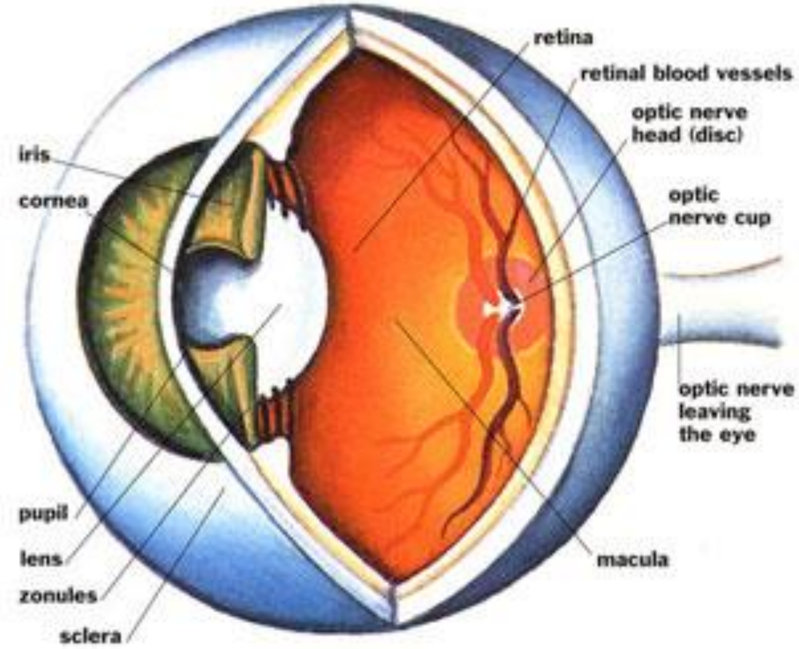
- □ externally-visible, coloured ring around the pupil
- □ Iris patterns are both highly complex and unique (the chance of two irises being identical is estimated at 1 in 10^78) making them very well-suited for biometric identification.
- □ An iris ‘scan’ is a high-quality photograph of the iris taken under near-infrared (near-IR) illumination.
- □ use narrow-angle cameras and ask the user to position their eyes correctly in the camera’s field of view

Introduction

- Iris, by definition, is the colored part of the eye that controls the amount of light that enters into the eye and is located between the pupil and the sclera
  - 1 in 10^{78} chance of someone having a

The eye is comprised of the pupil, lens, cornea, retina, and optic nerve

- Approximately 11mm in size
- Iris characteristics: multiple collagenous fibers, coronas, contraction furrows, crypts, color, serpentine, vasculature, striations, freckles, rifts, and pits.
- Blue irises signify an absence of melanin



Anatomy of Human Eye

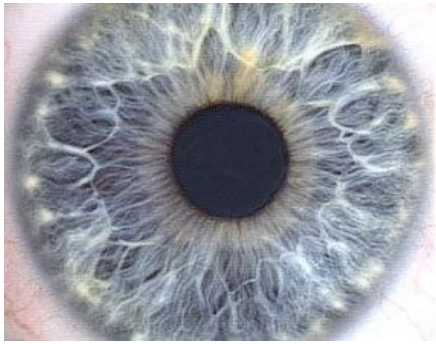
Acquisition - Illumination Effects

Normal light

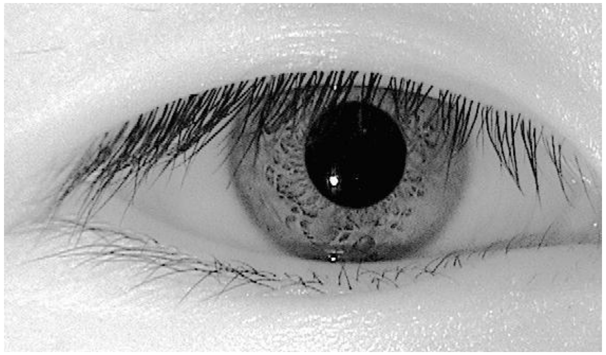
- Visible layers
- Less texture info
- Light absorbed by melanin

Infrared light

- More texture info
- Light reflected by melanin

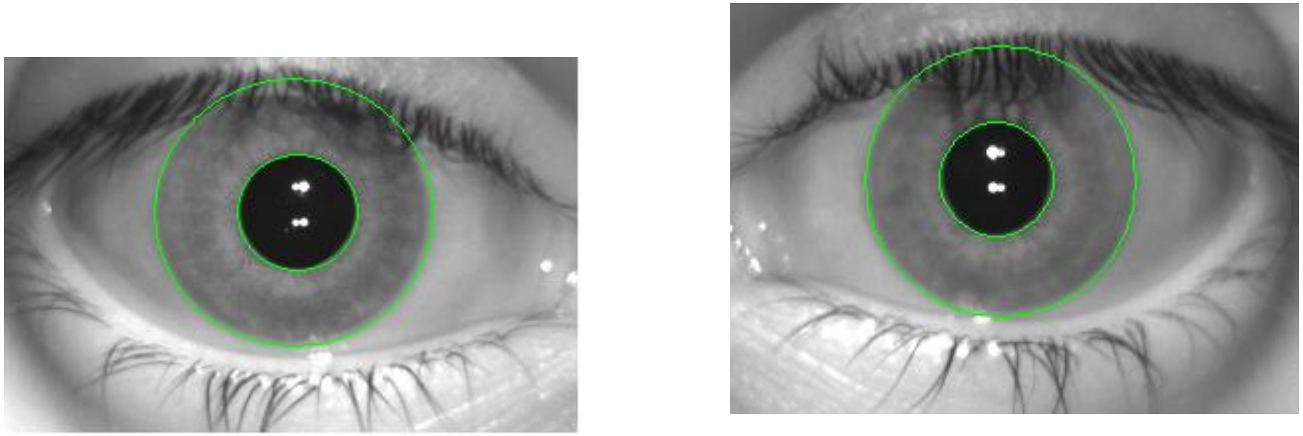


Normal Light Iris Image

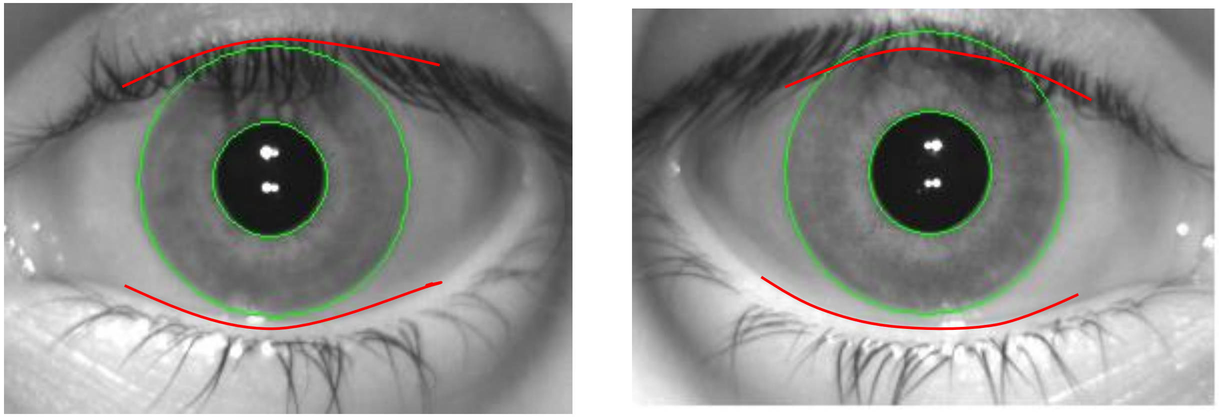


Infrared Illuminated Iris Image

Segmentation – Iris and Pupil Boundary & Eyelid Boundary

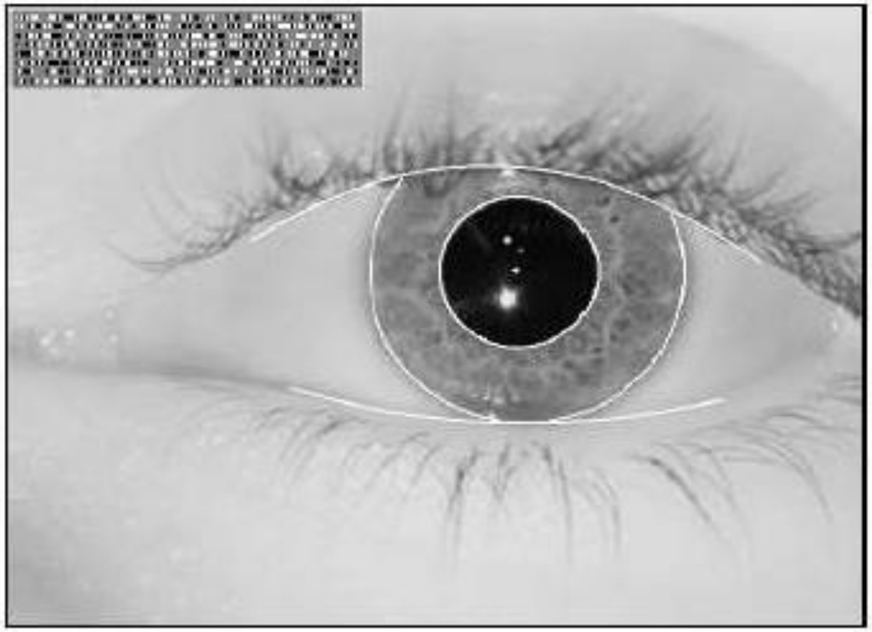


Pupil & Iris Boundary



Eyelid Boundary

resulting photograph is analyzed using algorithms to locate the iris and extract feature information, in order to create a biometric template or ‘IrisCode



iris

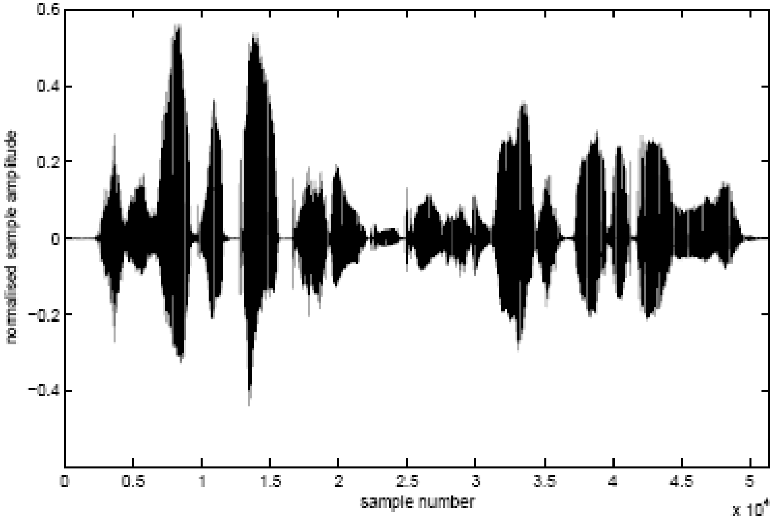
- All humans (including blind people) possess irises (*universality*) with some exceptions
- The patterns are also *permanent* from infancy to old age with the exception of the effects of some eye diseases. Existing sensors can capture high-quality images (*collectability*)
- The iris recognition system offers excellent *performance* even in identification mode with huge databases of enrolled users
- relatively small size of the template (512 bytes) .
- It is also extremely efficient in verification applications (physical access control, time and attendance control)

iris

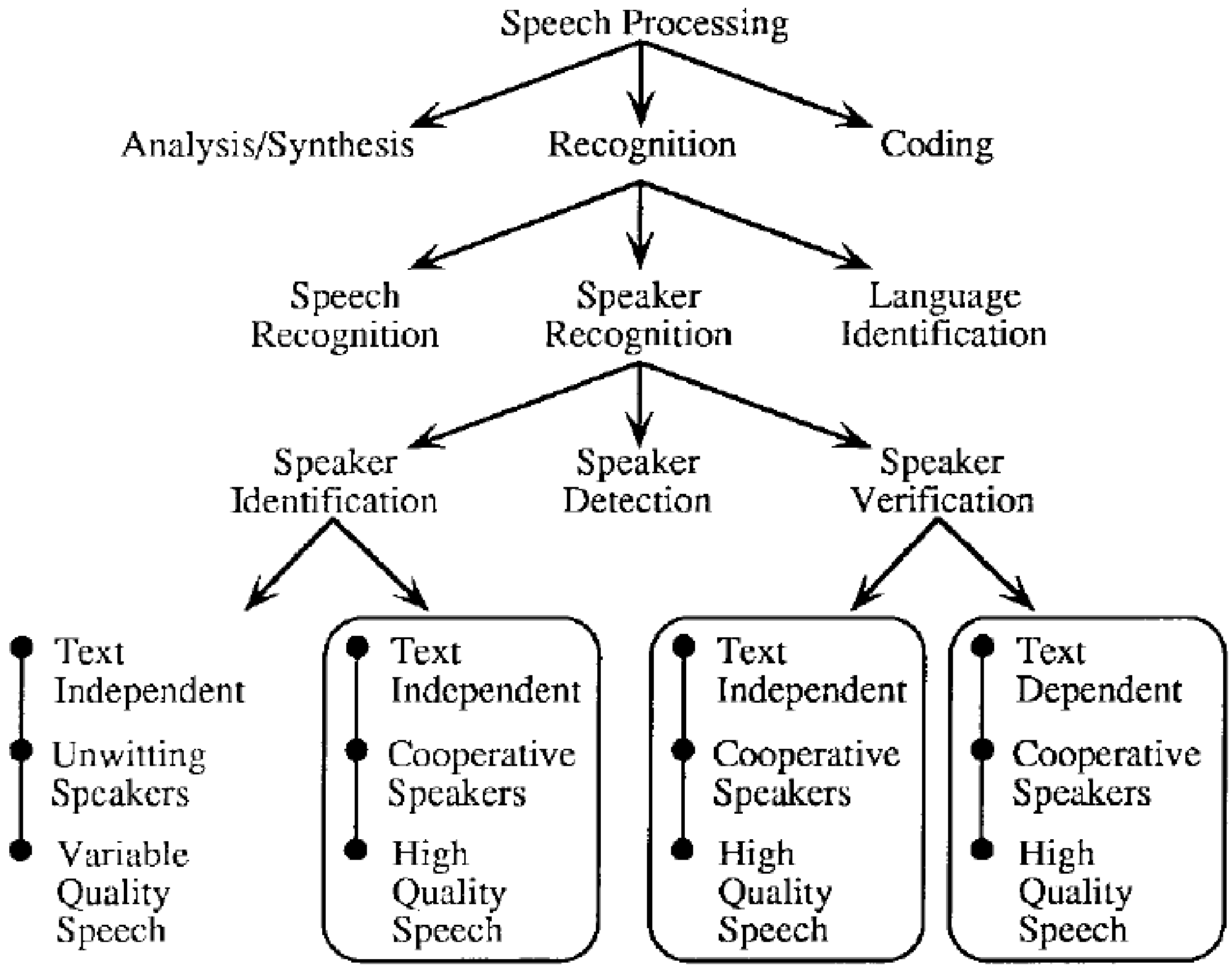
- major applications of iris recognition currently are: immigration control/border crossing (using verification, identification or watch-lists), aviation security, controlling access to restricted areas/buildings/homes, database/login access.
- automobile entry/ignition, forensic and police applications
- 17 border entry points (air, land and sea ports) of the United Arab Emirates (UAE)
- Immigration Control checks all incoming passengers against an enrolled database of about 420000 IrisCodes of persons who were expelled from the UAE
- The *acceptability* of iris recognition is relatively low

Voice as BioID

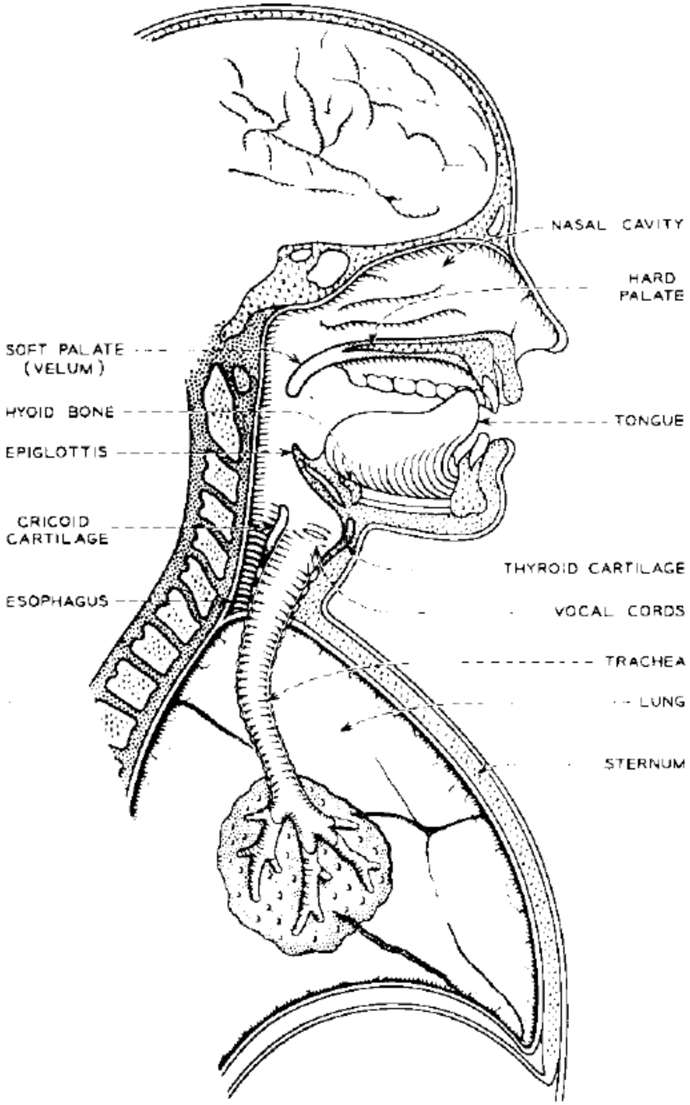
- Perhaps the least invasive of the biometric recognition technologies and the most natural to use - speech matching
- Voice as *BioID* offers an ability to provide positive verification of identity from an individual's voice characteristics



Speech Processing



Vocal tract shape is an important physical distinguishing factor of speech

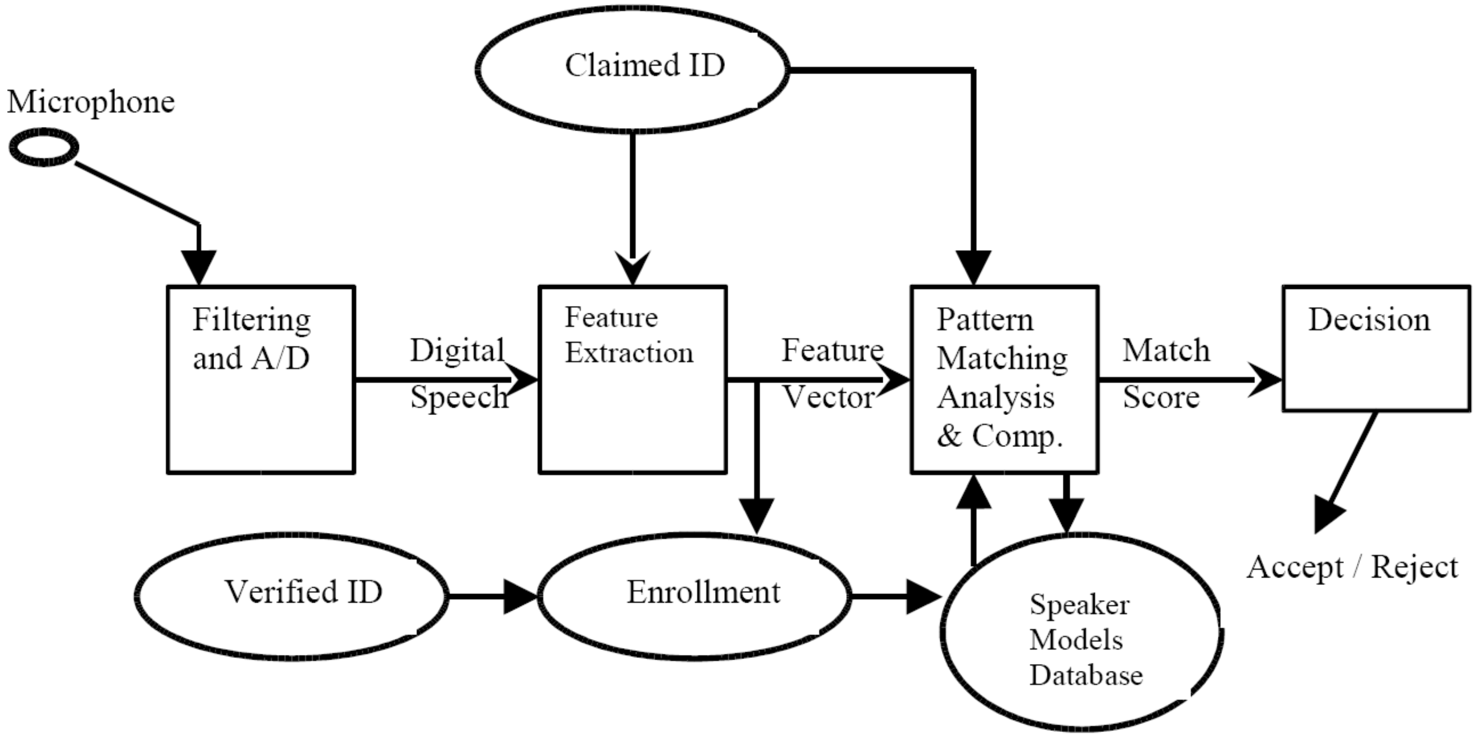


System

- As the acoustic wave passes through the vocal tract, its frequency content (spectrum) is altered by the resonances of the vocal tract. Vocal tract resonances are called *formants*.
- Phonated excitation (phonation) occurs when air flow is modulated by the vocal folds.
- The frequency of oscillation is called the fundamental frequency, and it depends upon the length, tension, and mass of the vocal folds.
- the speech signal can be represented by a sequence of *feature vectors*

Generic Speaker Verification System

- Speaker recognition systems can be used in two modes:
- to identify a particular person or to verify a person's claimed identity



System

- The pattern-matching task of speaker verification involves computing a match score, which is a measure of the similarity of the input feature vectors to some model.
- To authenticate a user, the matching algorithm compares/scores the incoming speech signal with the database model of the claimed user
- Replay attack
- Smart System

Voice Recognition - Types

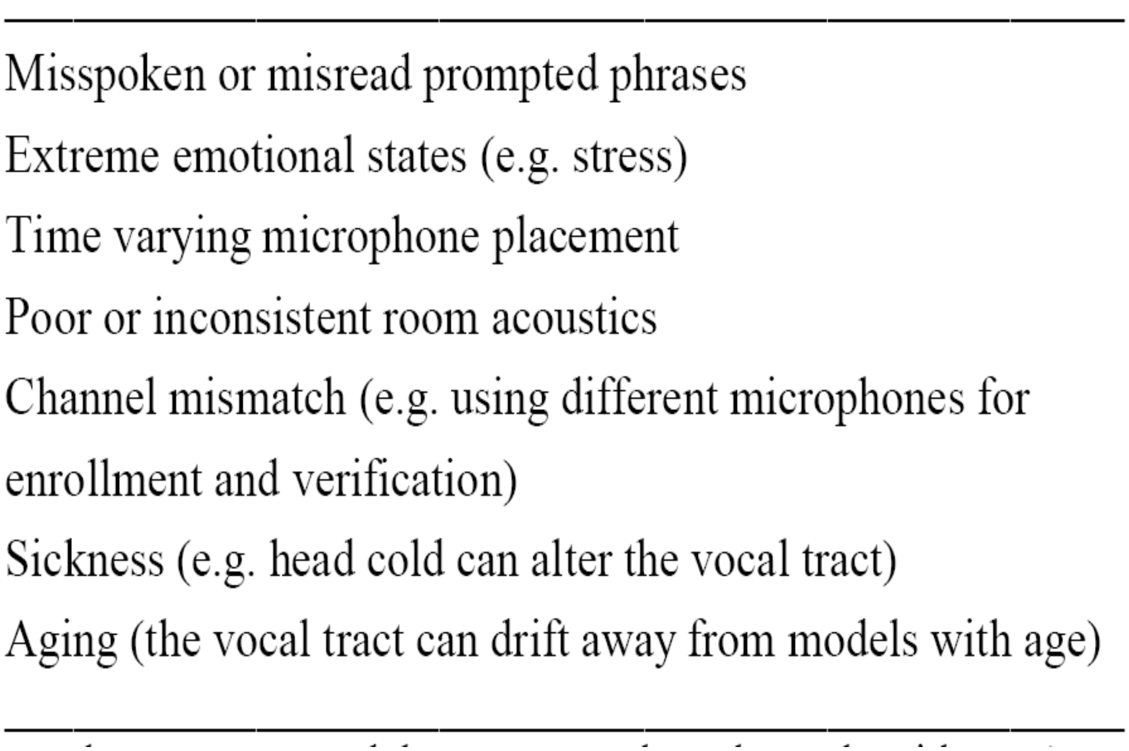
Text Dependent

- User is required to utter a specific phrase, or sequence of characters or numbers
- Based on training or enrollment of predefined words or phases

Text Independent

- Recognition is not constrained by what the user is saying
- Require individuals to train or enroll a comprehensive collection of words or phrases

Voice BioID - ERRORS



Misspoken or misread prompted phrases

Extreme emotional states (e.g. stress)

Time varying microphone placement

Poor or inconsistent room acoustics

Channel mismatch (e.g. using different microphones for enrollment and verification)

Sickness (e.g. head cold can alter the vocal tract)

Aging (the vocal tract can drift away from models with age)

Voice Recognition – Factors Affecting Performance

- Duration of segment
- Pitch
  - Cold or emotional stress during training or testing conversation
- Handset Differences
  - Variation in telephone handsets was a major factor
- Handset Type
  - Most handset microphones are of carbon-button or electret type
  - Microphone types affect performance
- Landline vs. Cellular

Face – as BioID

- higher level of user acceptance
- chosen as the primary biometric identifier for travel documents
- The image of the face is captured using a scanner and then analyzed in order to obtain a biometric “signature”
- 2D, 3D and infra-red (IR) facial scans

Image Processing – Face Localization & Eye Localization

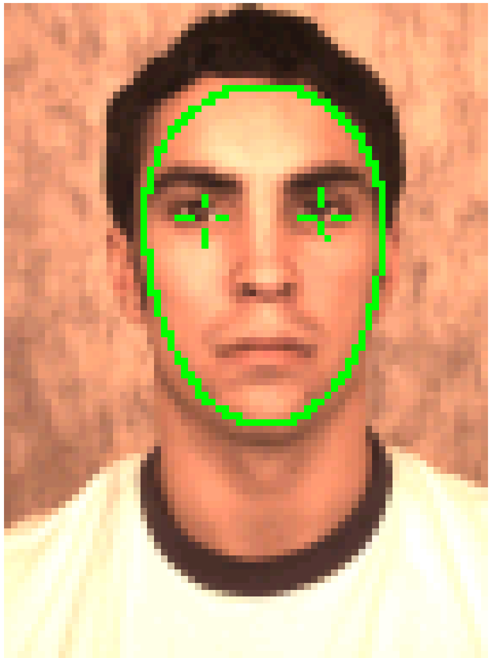
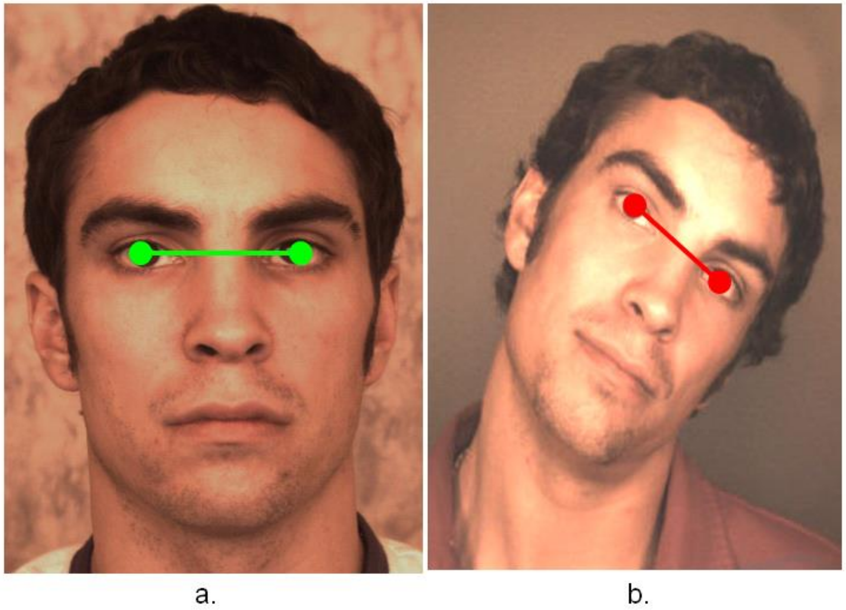
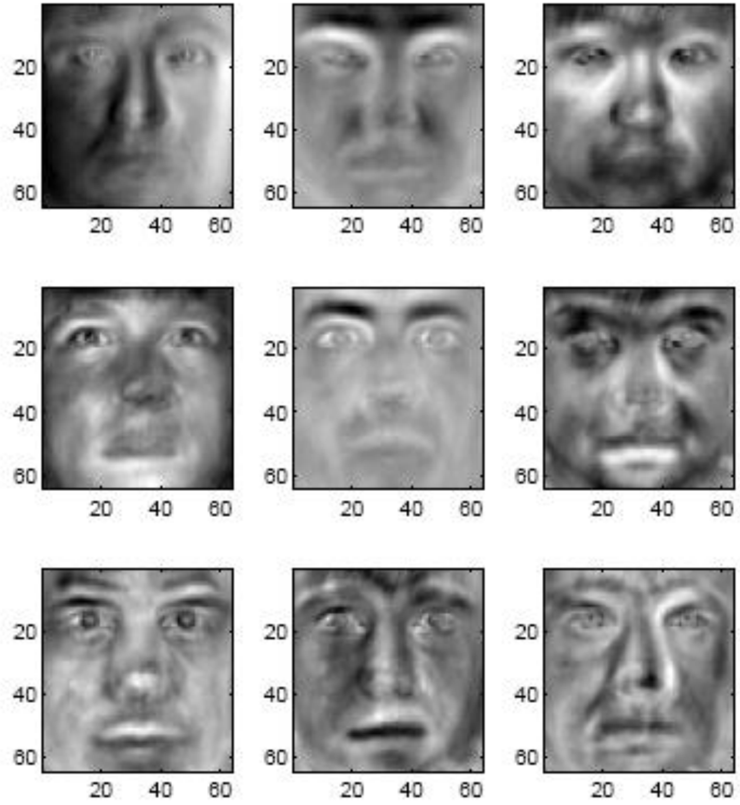


Figure 2: Image that has the face and eyes localized



In image b. subject has too large of a roll angle and is not compliant so image cannot be localized.

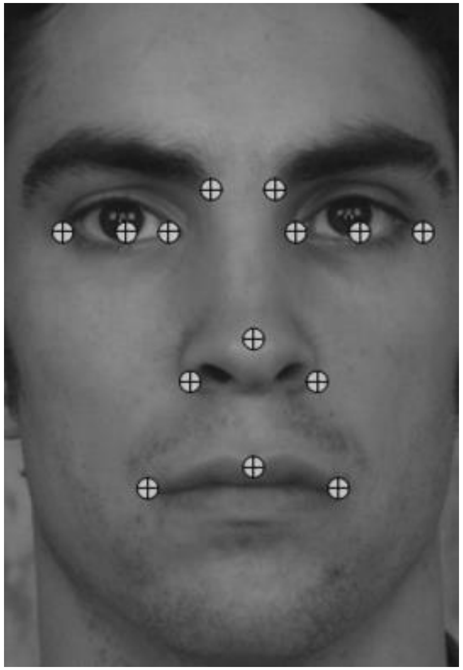
Face Recognition



Feature Extraction - 2D Features

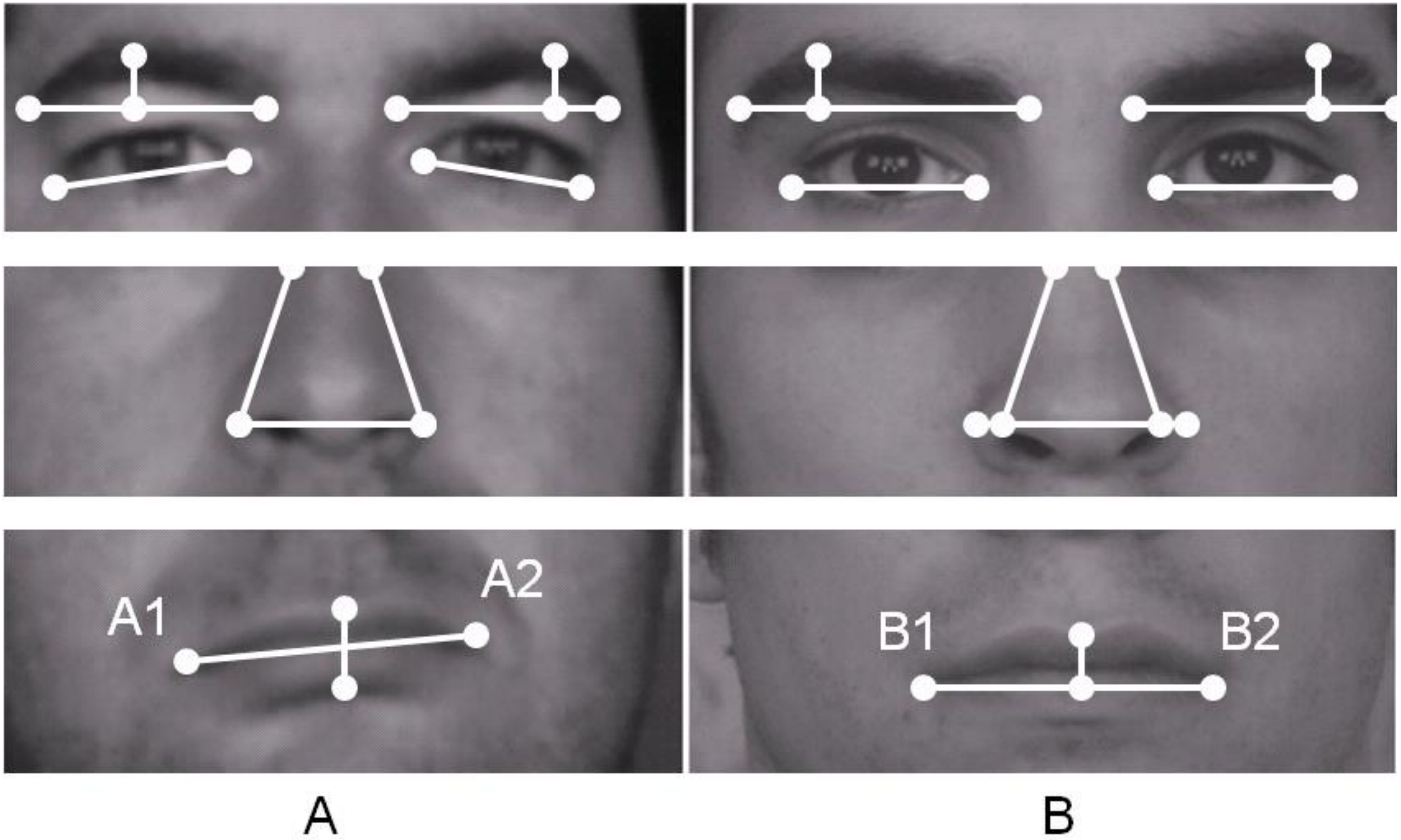
Some features/distances include:

- Eye center locations
- Distance between the eyes
- Location of the eyebrows
- Thickness of the eyebrows
- Nose position
- Nose width
- Locations of the nostrils
- Position of the mouth
- Lip width
- Distance between the upper lip and nose tip
- Distance between the nose tip and eyes

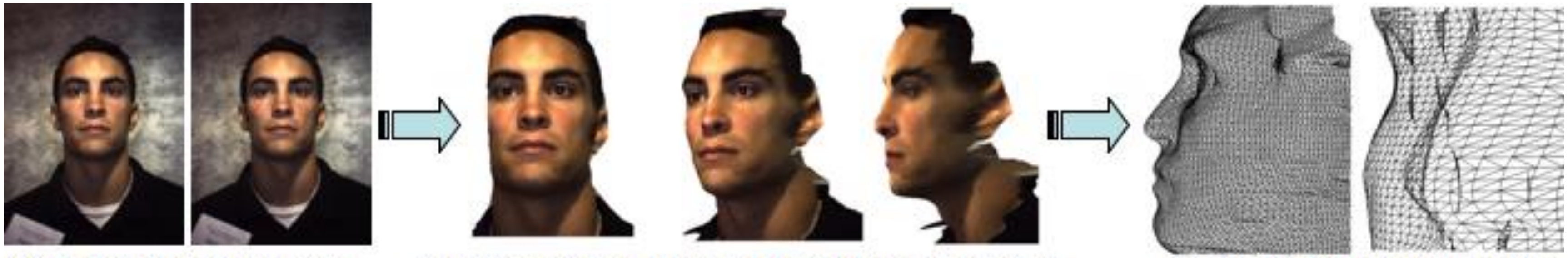


Common facial points

2D Feature Based Matching



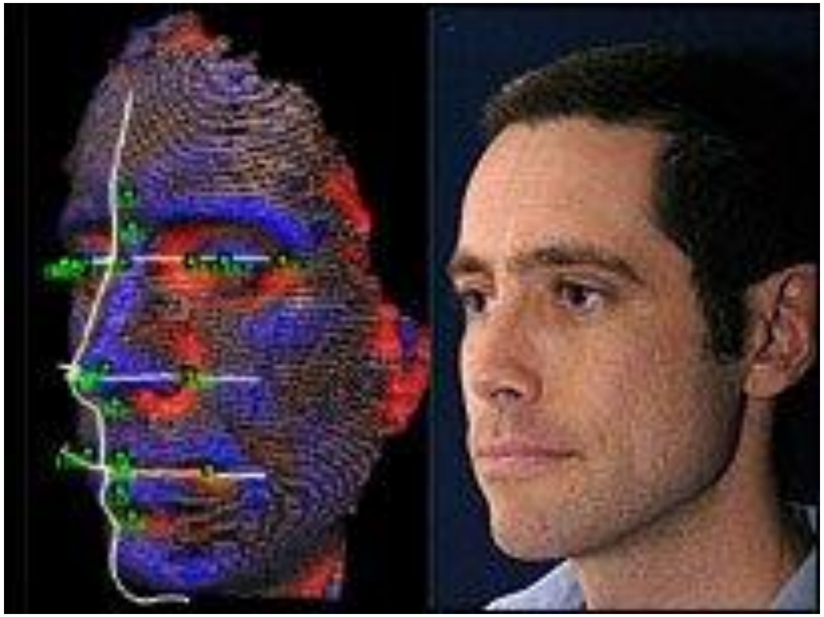
3D Face RecognitionTechnology

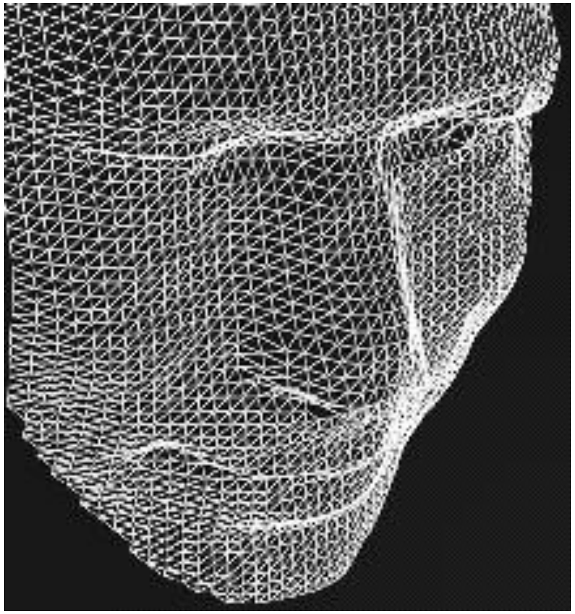


A) 2 photographs collected by passive stereo cameras.

B) Rotated 3D texture model based on images in A.

C) Profile 3D mesh model and an off-centered model of the nose region.

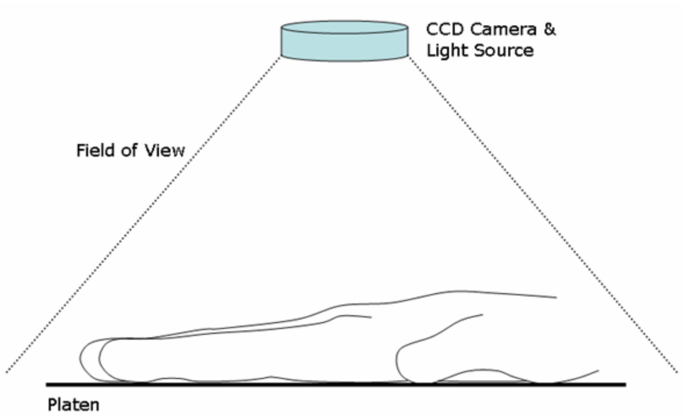




Face Recognition

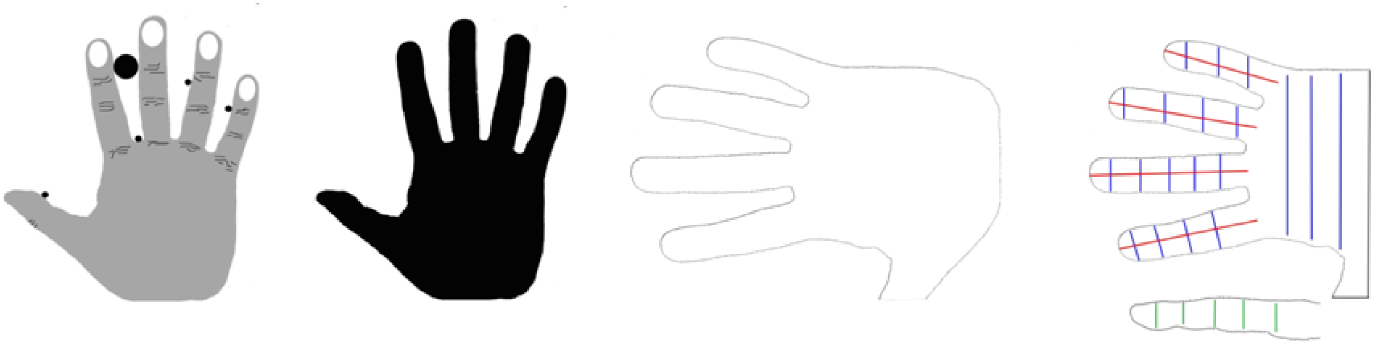
- Face recognition does well in the areas of universality (everybody has a face),
- collectability (2D face recognition uses a photograph, which is easy to acquire)
- acceptability (people are accustomed to the idea of using the face for identification and the technique is non-intrusive).
- It struggles with distinctiveness (the patterns of faces show less variation compared to fingerprints or irises for example),
- permanence (faces change significantly over time),
- performance (currently face recognition has much lower accuracy rates than the other featured biometric technologies).

Hand Recognition – Bio ID



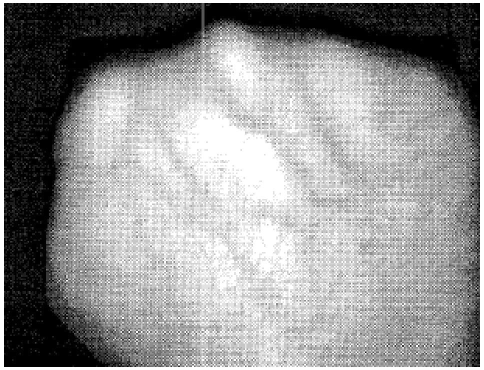
Components of a hand geometry system

- Several geometric features of the hand are extracted from the processed image
- Width, length, thickness, and surface area
- These features show a very high level of correlation
  - Methods such as Principal Component Analysis (PCA) are often used to transform these features into non-correlated feature sets

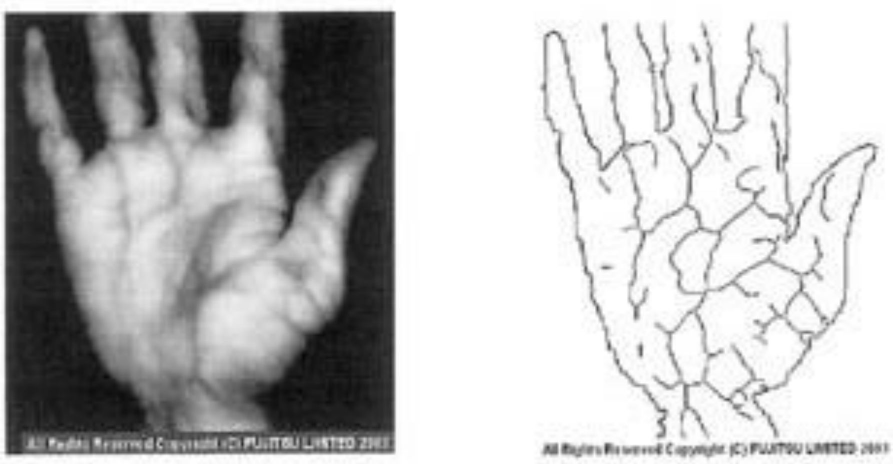


Hand Geometry Image Processing Steps

Vein Recognition – Bio ID



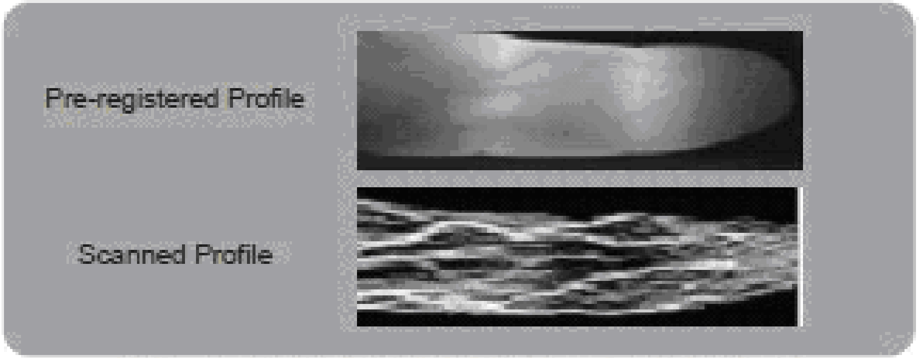
Back of hand image obtained with infrared light



All Rights Reserved Copyright (C) FUJITSU LIMITED 2003

All Rights Reserved Copyright (C) FUJITSU LIMITED 2003

Captured palm vein image (left) & skeletonized palm vein image (right)



Authentication is achieved by matching pre-registered and scanned vein pattern profiles

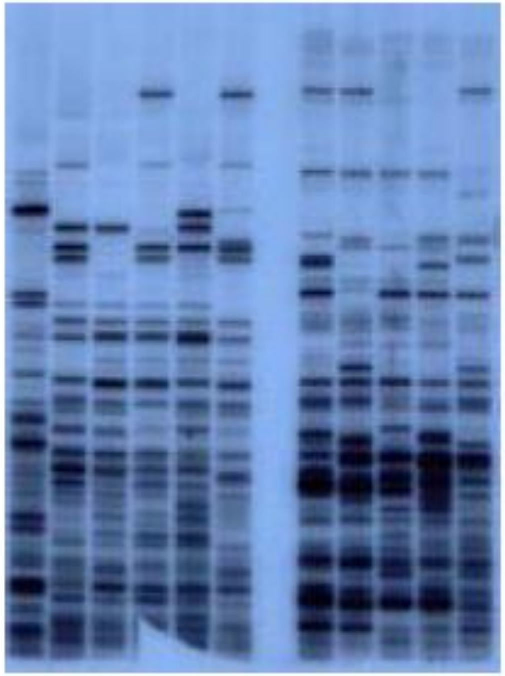
DNA – Bio ID

- DNA (deoxyribonucleic acid) is the well-known double helix structure present in every human cell.
- A DNA sample is used to produce either a DNA fingerprint or a DNA profile.
- Only a small amount of tissue - like blood, hair, or skin - is needed
- DNA does not change throughout a person's life
- DNA testing is a technique with a very high degree of accuracy

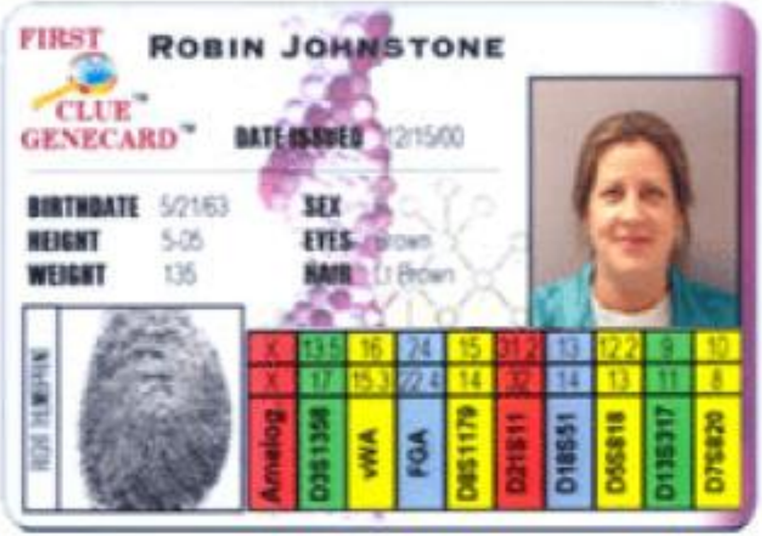
DNA

- The procedure to make DNA fingerprint is composed of the following steps,
- i.e. isolation of DNA;
- denaturalization of DNA (cutting, sizing and sorting); transfer and probing.
- DNA fingerprint is built by using several probes (5-10 or more) simultaneously.
- Progress in DNA testing will come in two areas: current techniques will improve, offering more automation, precision and faster processing times, and new techniques will be developed

DNA



DNA fingerprint image



FIRST CLUE™ GENECARD™

ROBIN JOHNSTONE

DATE ISSUED 12/15/00

BIRTHDATE 5/21/63
HEIGHT 5-05
WEIGHT 135

SEX
EYES Brown
HAIR Lt Brown

Amelog	D3S1358	vWA	FGA	D8S1179	D21S11	D18S51	D5S818	D13S317	D7S820
X	13.5	16	24	15	31.2	13	12.2	9	10
X	17	15.3	22.4	14	32	14	13	11	8

DNA profile representation

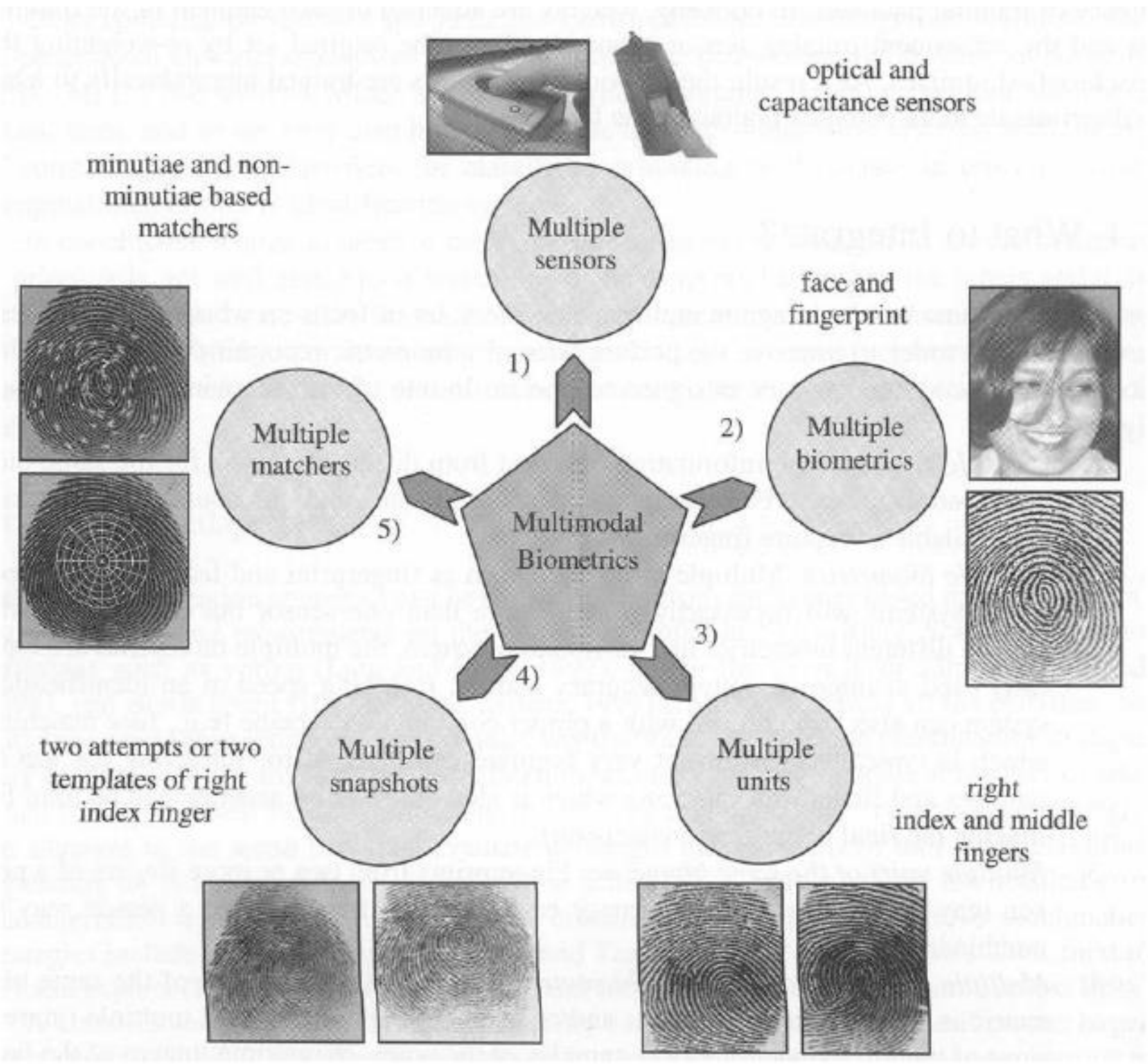
Problems

- The main problem with DNA is that it includes sensitive information related to genetic and medical aspects of individuals. So any misuse of DNA information can disclose information about: (a) hereditary factors and (b) medical disorders.
- If sample collection is not supervised however, an impostor could submit anybody’s DNA.
- problems with the security of DNA system (access rights, use of information only for the overriding purpose),
- and the implementation of security mechanisms in order to ensure for instance a high level of confidentiality and the security of DNA database (access rights, length of information retention).

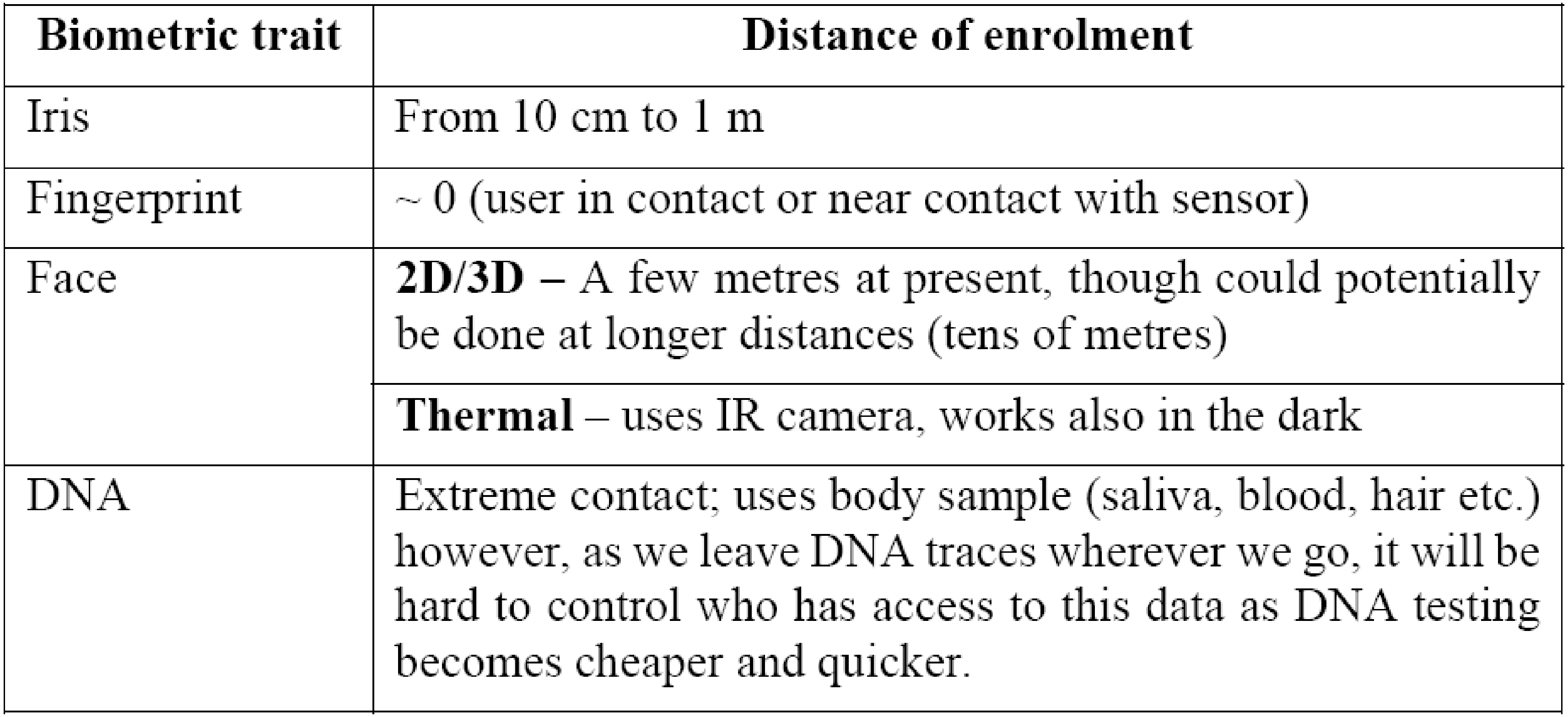
Multimodal Biometric systems

- by combining more than one modality, enhanced performance reliability and even increased user acceptance could be achieved
- Unimodal biometric systems can be subject to many types of errors
- due to *noise* associated with the acquired data
- by sensor performance
- by user behaviour/status
- ‘liveness’ attacks

combinations



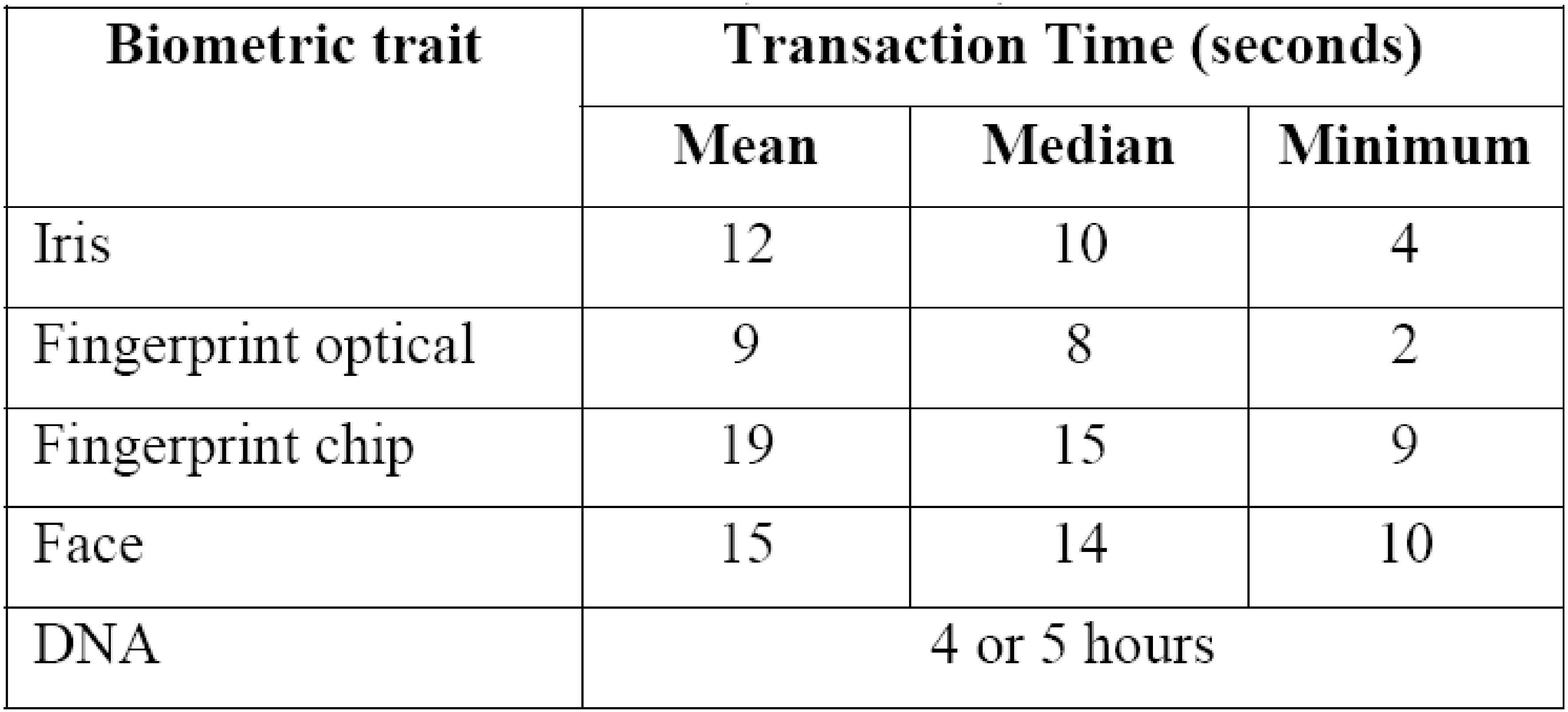
Bio ID – capturing distance



Biometric trait	Distance of enrolment
Iris	From 10 cm to 1 m
Fingerprint	~ 0 (user in contact or near contact with sensor)
Face	**2D/3D –** A few metres at present, though could potentially be done at longer distances (tens of metres)
	Thermal – uses IR camera, works also in the dark
DNA	Extreme contact; uses body sample (saliva, blood, hair etc.) however, as we leave DNA traces wherever we go, it will be hard to control who has access to this data as DNA testing becomes cheaper and quicker.

Bio IDs – typical transaction times

(historical data – improved by manifold today)

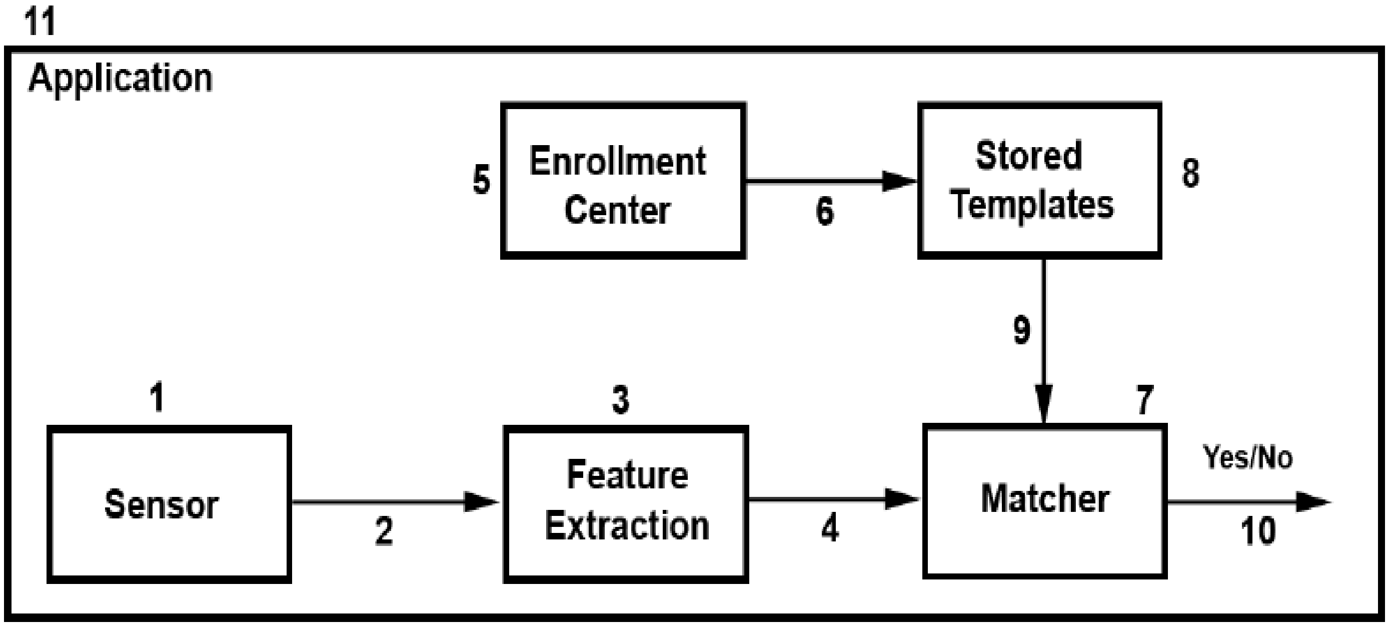


Biometric trait	Transaction Time (seconds)		
	Mean	Median	Minimum
Iris	12	10	4
Fingerprint optical	9	8	2
Fingerprint chip	19	15	9
Face	15	14	10
DNA	4 or 5 hours		

Operational mechanism - Screening

- makes use of a database or *watch-list*
- Everyone who passes the screening process provides a biometric sample, which is checked for matches against the watch-list.
- In the case of a match, a human operator decides on further action.
- Screening can take place overtly or covertly, for example at border control or such as scanning a crowd with the use of security cameras.

Biometric System - Vulnerability points?



Privacy & Interoperability

Biometric identification and verification generates digital data.

More delicately, it creates a machine-readable trace every time identification is performed.

From a data protection point of view, it therefore raises the usual questions: what data are stored, how are they stored (centrally in a database or decentralized on smart cards), who has access to the data, for what purposes can the data be accessed, etc. ???????

- As for any emerging technology, interoperability plays an important role for the development of biometrics.
- For example, the more widely a memory device carrying biometric identification can be read, the more useful it is.

Biometric System Test Methods

3 types of test methods:

1. Technology
   - Goal: to compare competing algorithms from a single technology
2. Scenario
   - Goal: to determine the overall system performance in a prototype or simulated application
3. Operational
   - Goal: to determine the performance of a complete biometric system in a specific application environment with a specific target population

Technology Test

- The testing of algorithm is carried out on a standardized database collected by “universal” sensor
- Sample data may be distributed for developmental or tuning purposes before the test, but the actual testing must be done with new data that has not been previously seen by the developers
- Testing is carried out using offline processing
  - Offline: pertaining to execution of enrollment and matching separately from image or signal submission

The results of the technology tests are repeatable

Scenario Test

- The testing of the algorithm is carried out on a complete system in a real-world model environment
- Each system will have its own acquisition sensor so it will receive slightly different data that will come from the same environment with the same population
- Testing might be a combination of offline and online comparisons, depending on the storage capabilities of each device
  - Online: pertaining to execution of enrollment and matching at the time of image or signal submission

Operational Test

□ Test results obtained by monitoring a live biometric system deployment

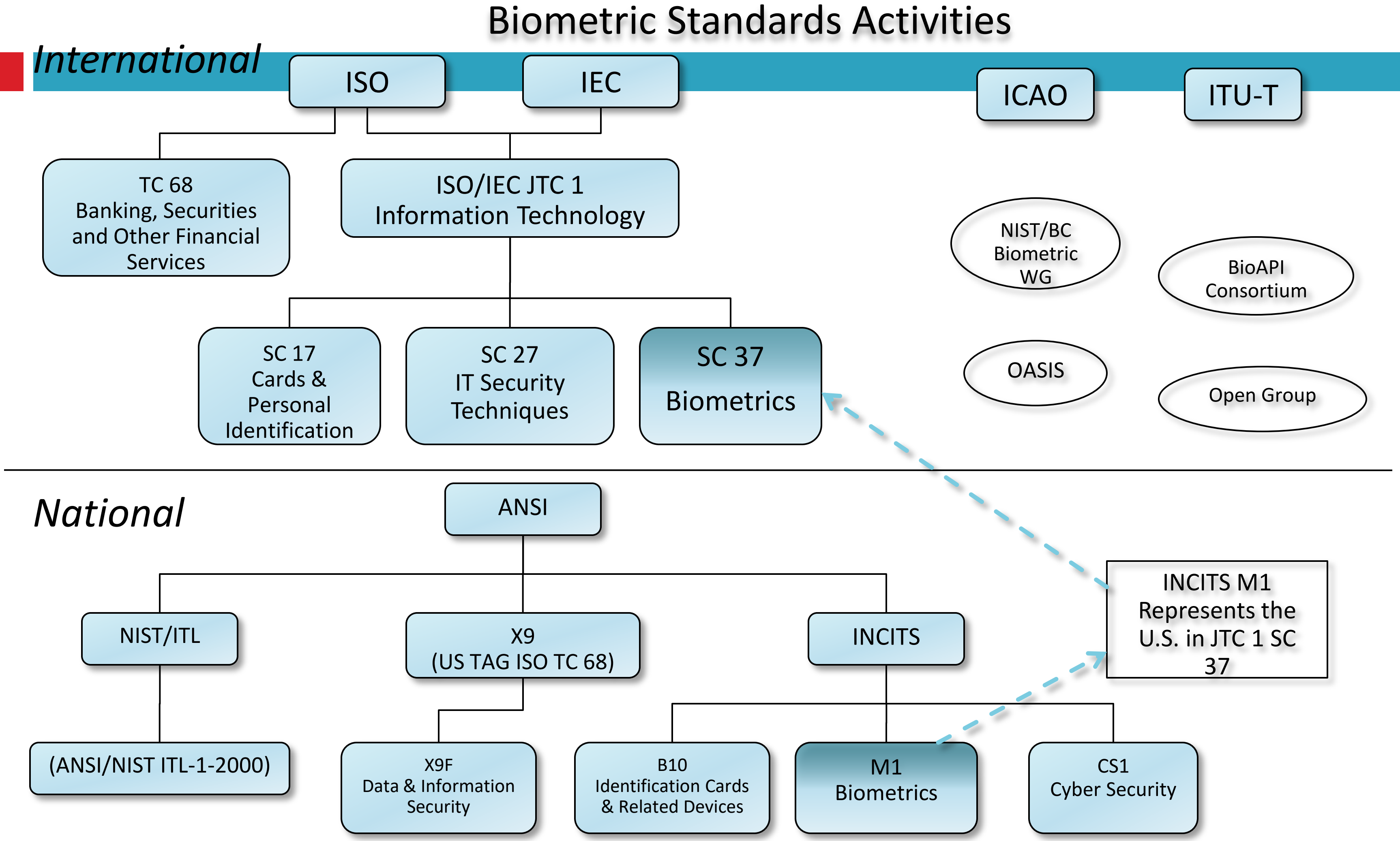
□ Offline testing might not be possible depending on the storage capabilities of each device

□ This type of evaluation will not be repeatable because of the unknown and the undocumented differences between operational environments

Match Acceptance Threshold

- The acceptance or rejection of biometric data is dependent on the match score being greater or less than the threshold
- The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric
- Threshold is required to be set for every biometric system

Biometrics Standards Bodies



Biometric Standards Bodies

Usability Issues!!!

Why support the user in a biometric system?

- Effectiveness
  - for operator/end user
- Efficiency
  - for operator/end user
- Accessibility
  - for (partially, multiply) disabled
- Cultural accessibility
  - reduce dependency on written instructions
- Reduction of ‘User discomfort’
  - in unfamiliar/stressful/encumbered situations

Context of animation

Identification:	what is this?
Transition:	where have I come from or am going to?
Orientation:	where am I?
Choice:	what do I do now?
Demonstration:	what can I do with this?
Explanation:	how can I do this?
Feedback:	what is happening?
History:	what have I done?
Interpretation:	why did that happen?
Guidance:	what should I do now?

Project Aadhar (India) challenges… (UIDAI)

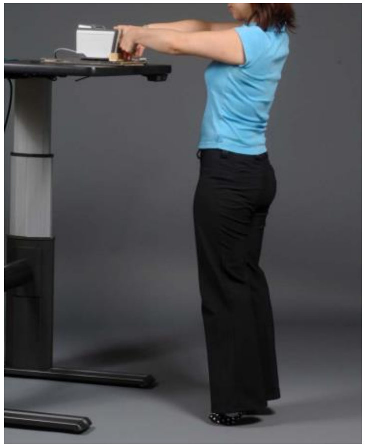
- Capturing Biometric data for such a large population
- with different Environment,
- variable usability education,
- and biometric conditions (bad/missing finger, eye disease/blind) in India and computing templates with score normalization

Devices from different vendors

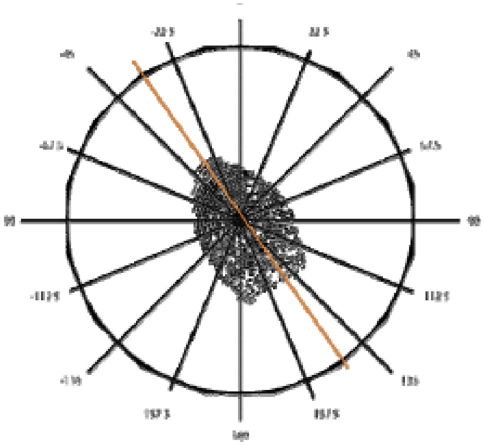
Usability of Devices: Acquisition Challenges

Physical characteristics

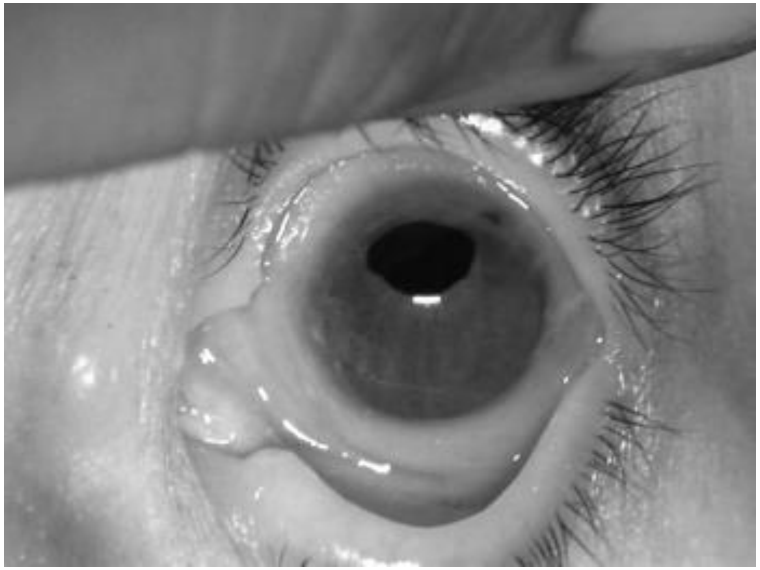
- ■ Dimensions of device
- ■ Interfaces
- ■ Environmental conditions
- ■ Context of use



- □ Placement – angle, height, contact area
- □ Usage directives



Acquisition Challenges



Challenges: Face recognition

- Height
- Problems with eyes (e.g. infections)
- Wearing items such as glasses, hats, sunglasses
- Variations in hairstyle
- Time taken to enrol/verify

Challenges: Fingerprints

- Poor quality fingerprints (e.g. due to manual labour or accidents)
- Finger placement (e.g. just the tip of finger on sensor)
- Removing finger before image capture is complete

Data - Challenges

- Conversion
- Normalization
- Secure storage and retrieval
- Compromise!!

ISO/IEC WD 24779: Pictograms, Icons and Symbols for Use with Biometric Systems

- Recognition Scenarios:
  - Verification, Identification: Yes
  - Enrolment: No
    - in general, this is supervised
- Required symbols:
  - General use of biometric device and its type/modality
    - eg. Facial recognition or fingerprints
  - Where to stand, look or to place finger.
  - Wait (or hold steady): for process to complete
  - Success: process complete
  - Failure
  - Re-try (the same characteristic)
  - Try another finger or eye
  - *CDN: Seek human assistance*
  - Give up
- ISO standardisation for ICONS

Privacy issues

- Privacy matters for acceptance.
- Biometrics are unique identifiers, but they are not secrets!!! i.e. the information is not secret in the first place!
- **We need to address non-secret nature of biometrics..**

Privacy matters for biometrics

- □ governed by privacy laws and regulations
- □ in some places, regulators are putting strict requirements on systems, such as requiring encryption, ensuring single use, no match to latents, strict access controls, separate storage of personal information, etc.

Different Rules!

- Biometric data is owned by the data subject, who principally have the right for self-determination

- Biometric data is owned by the organization that processed the data

Interoperability

- Integration of technology from various vendors.
- Data minimization
- Protected templates should be stored efficiently, with a minimum of information required for
- reliable verification.
- Architecture flexibility
- Both on-line verification and off-line verification should be supported.

Policies

- **Policies affect daily lives, and we usually have to live with policy decisions for a long time….**
- complex challenges of identity policies
- about the data sharing
- National Identity Register
- In spite of all these challenges, UIDAI is the most successful biometric project of the Globe!!!

Summary

- Generally, when trying to match the right authentication solution with a specific application, the following should be considered:
- User Environment -- Convenience/Ease of use, Robustness / Reliability, Portability
- Application Environment --Application Security Requirements, Secure Identity Management Extensibility, Ease of Management and Administration
- Business Requirements - Acquisition Costs, Deployment Costs, On-going Costs (including maintenance and support), Integration Costs

- Ref: Dhiren Patel; **Information Security: Theory and Practice**, PHI – April 2008