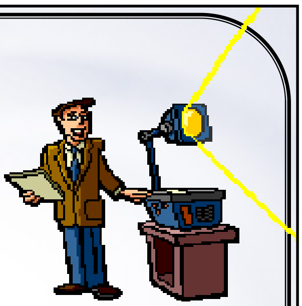
Biometric Authentication

Lecture 2

How to Design
Biometric
Systems



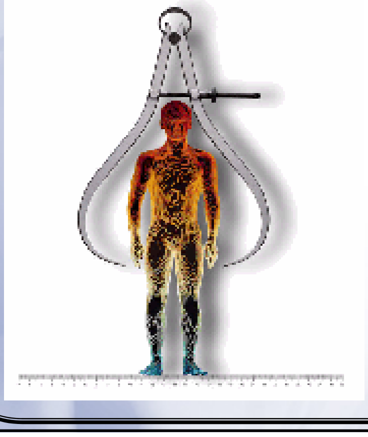
Outline

- Biometrics Definitions
- Biometrics Systems

Biometrics Definition

What?

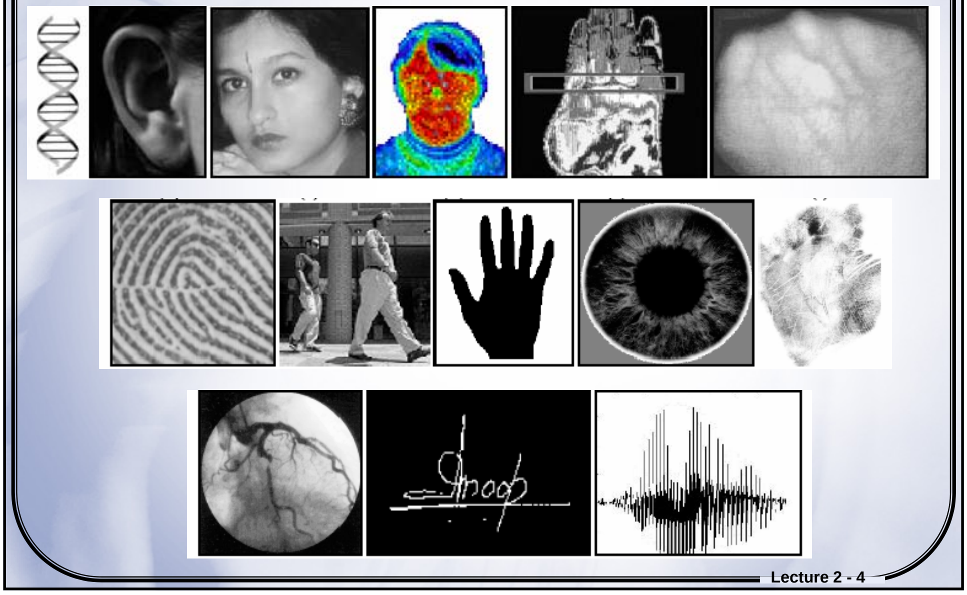
- ❑ Automated methods of recognizing individuals based on their traits

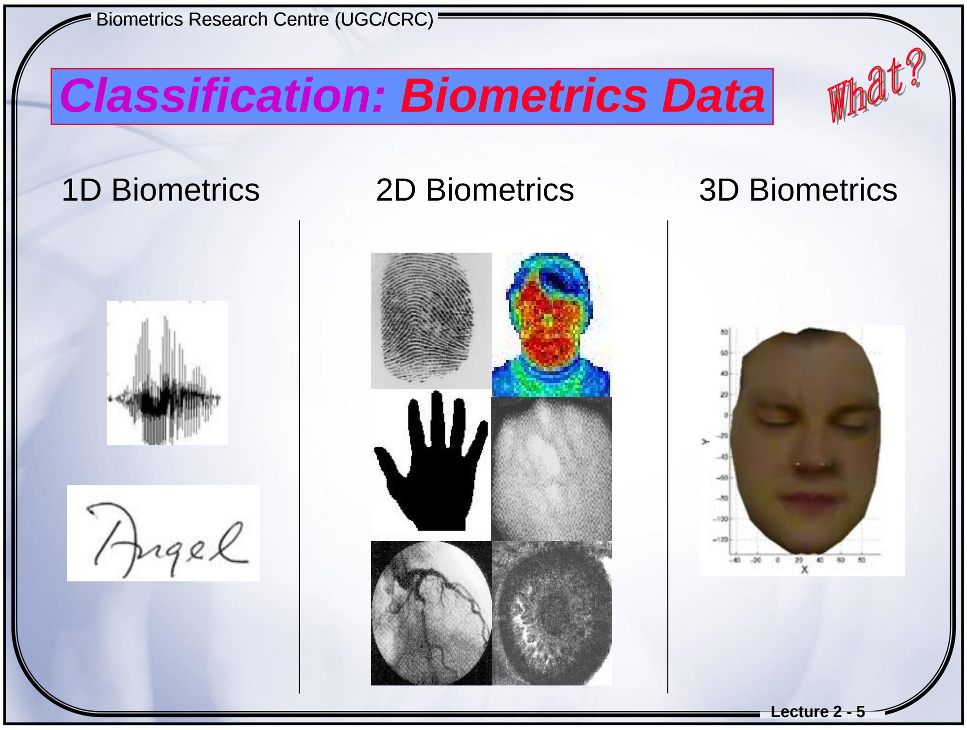


- ❑ A measurable *physical characteristics* or *personal behavioral trait* used to recognize the identity, or verify the claimed identity, of an enrollee

Examples of Biometrics

What?





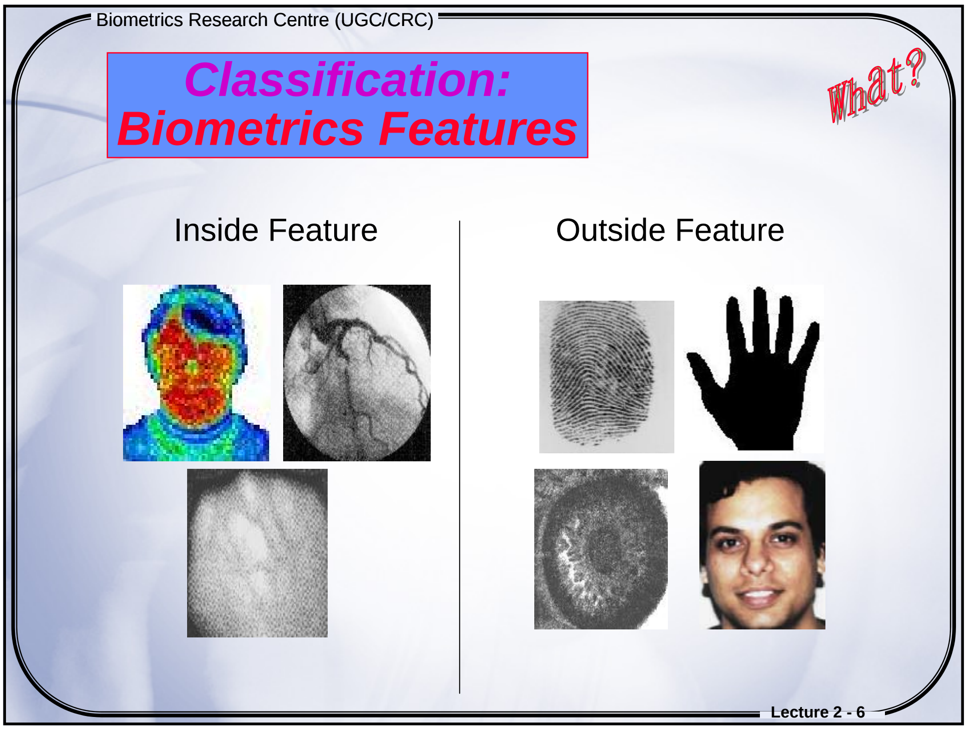
Classification: Biometrics Data

What?

1D Biometrics

2D Biometrics

3D Biometrics



Classification: Biometrics Features

What?

Inside Feature

Outside Feature

Biometrics Classification

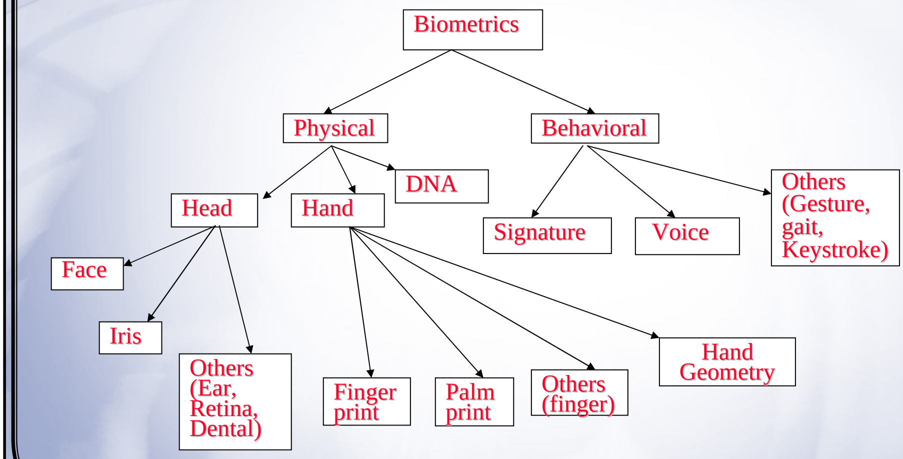
Two types of biometrics

- – Physiological: fingerprint, iris, hand geometrics, palmprint, etc
- – Behavioral: voice, signature, etc

- Selection of biometrics technology is *Application dependent*
- Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters

Taxonomy of Biometrics

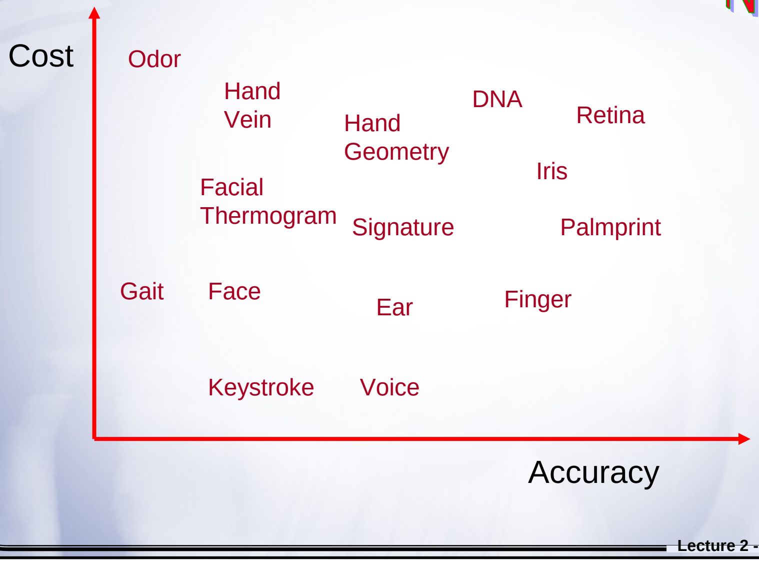
What?



Biometrics
Physical
Behavioral
Head
Hand
DNA
Face
Iris
Others (Ear, Retina, Dental)
Finger print
Palm print
Others (finger)
Hand Geometry
Signature
Voice
Others (Gesture, gait, Keystroke)

Our View of Biometric Evaluation

New



Cost

Accuracy

Odor

Hand Vein

Hand Geometry

DNA

Retina

Iris

Facial Thermogram

Signature

Palmprint

Gait

Face

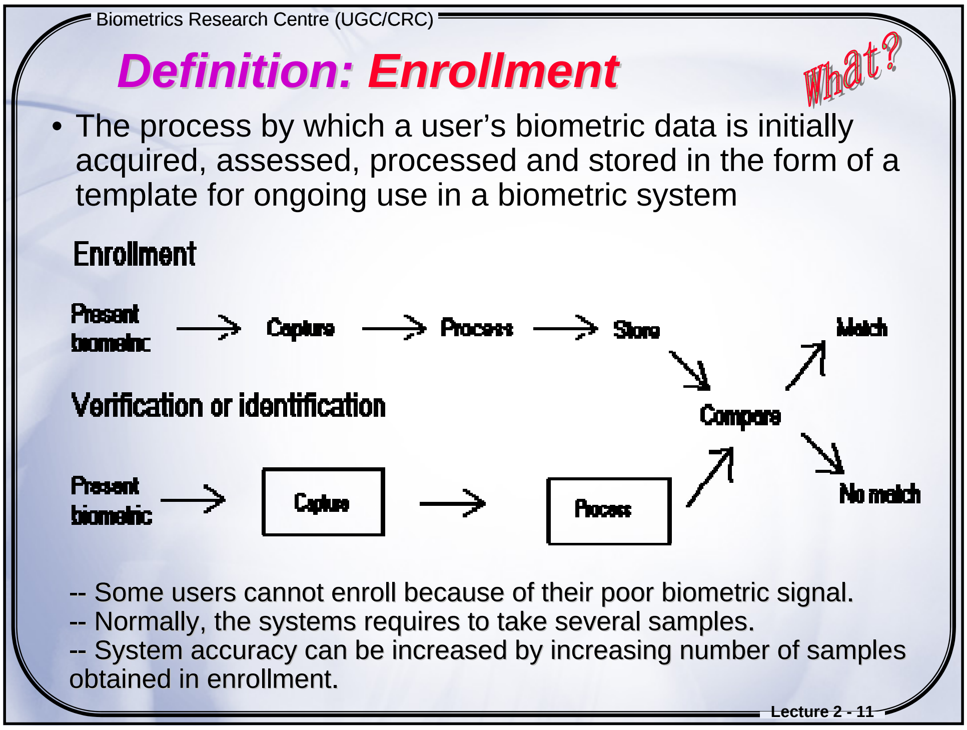
Ear

Finger

Keystroke

Voice

Biometrics Definitions



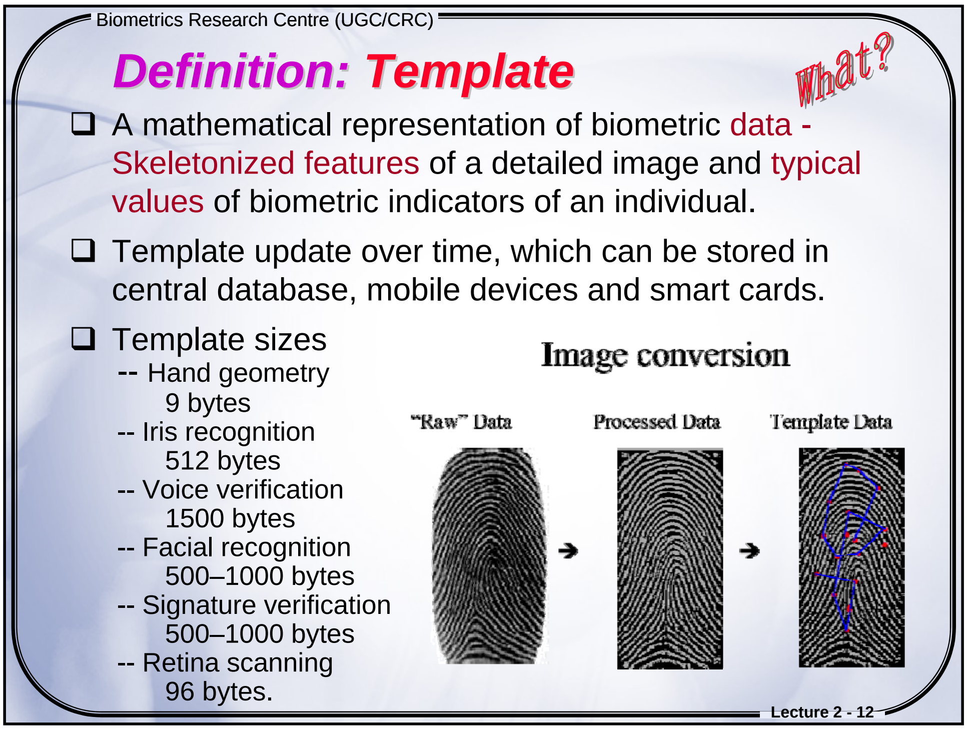
Definition: Enrollment

What?

- The process by which a user's biometric data is initially acquired, assessed, processed and stored in the form of a template for ongoing use in a biometric system

Enrollment
Present biometric
Capture
Process
Store
Match
Verification or identification
Compare
Present biometric
Capture
Process
No match

-- Some users cannot enroll because of their poor biometric signal.
-- Normally, the systems requires to take several samples.
-- System accuracy can be increased by increasing number of samples obtained in enrollment.



Definition: Template

What?

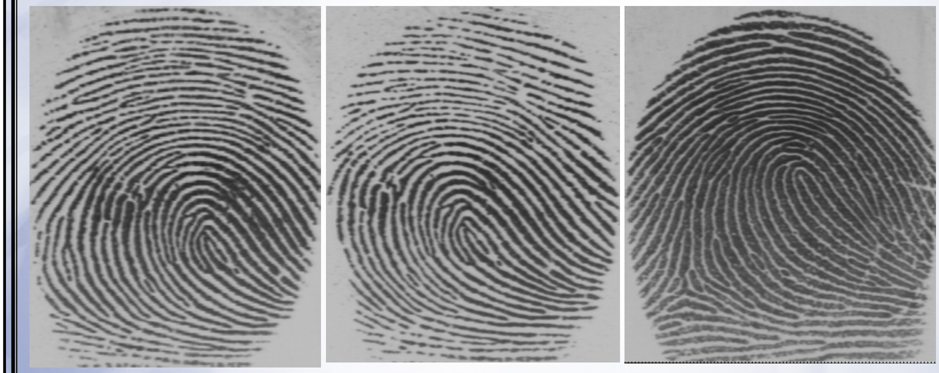
- ❑ A mathematical representation of biometric data - Skeletonized features of a detailed image and typical values of biometric indicators of an individual.
- ❑ Template update over time, which can be stored in central database, mobile devices and smart cards.
- ❑ Template sizes
  - -- Hand geometry
    9 bytes
  - -- Iris recognition
    512 bytes
  - -- Voice verification
    1500 bytes
  - -- Facial recognition
    500–1000 bytes
  - -- Signature verification
    500–1000 bytes
  - -- Retina scanning
    96 bytes.

Image conversion

Definition: Matching

What?

- ❑ Matching scores is the matching result between two templates.

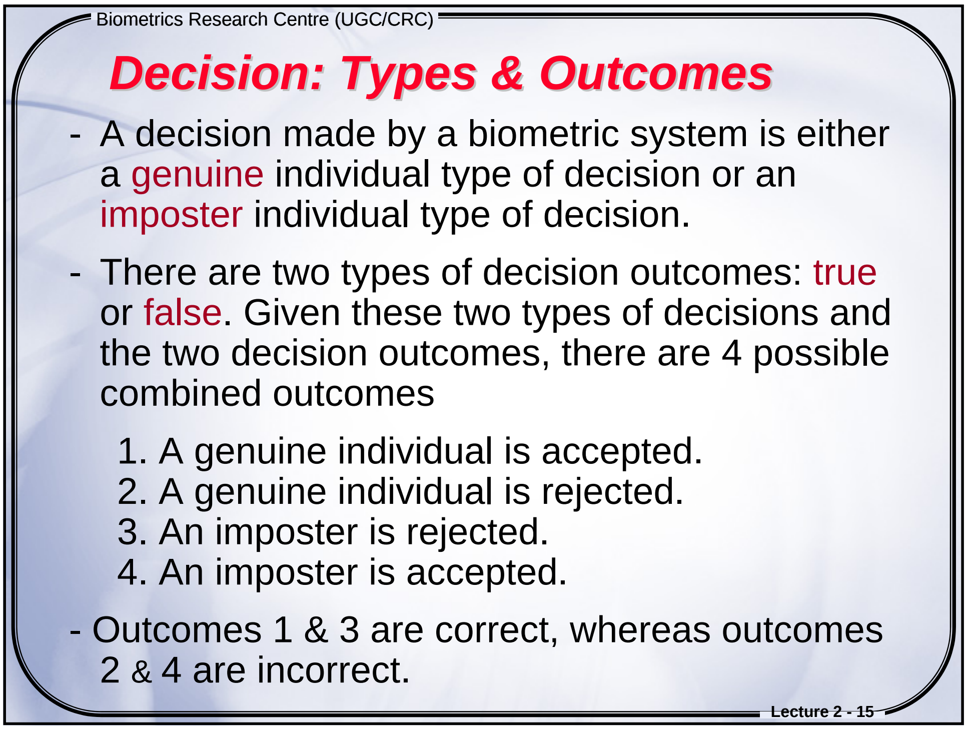


(a) (b) (c)

Matching Scores: $S_{ab} = 97$; $S_{bc} = 5$; $S_{ac} = 2$

Evaluation Method
Decision Introduction

- No single metric is sufficient to give a reliable and convincing indication of the identification accuracy of a biometric system.
- Let’s first look at describing the decision outcomes from a biometric system.
  - This is under normal operating conditions
  - No spoofing of the system considered.

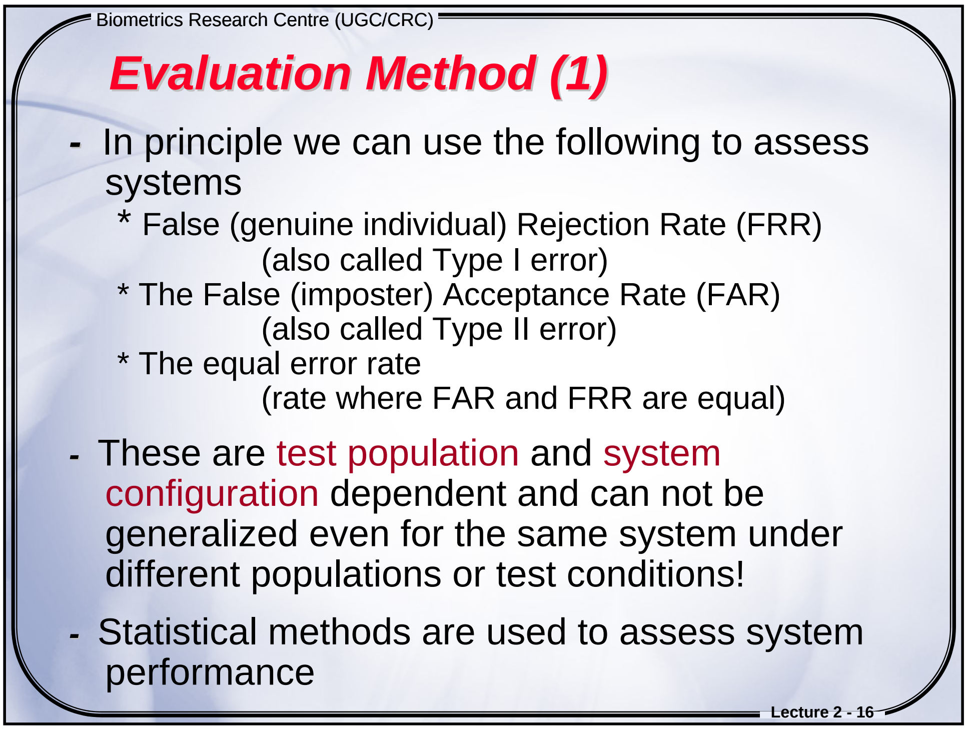


Decision: Types & Outcomes

- A decision made by a biometric system is either a genuine individual type of decision or an imposter individual type of decision.
- There are two types of decision outcomes: true or false. Given these two types of decisions and the two decision outcomes, there are 4 possible combined outcomes

  1. A genuine individual is accepted.
  2. A genuine individual is rejected.
  3. An imposter is rejected.
  4. An imposter is accepted.

- Outcomes 1 & 3 are correct, whereas outcomes 2 & 4 are incorrect.

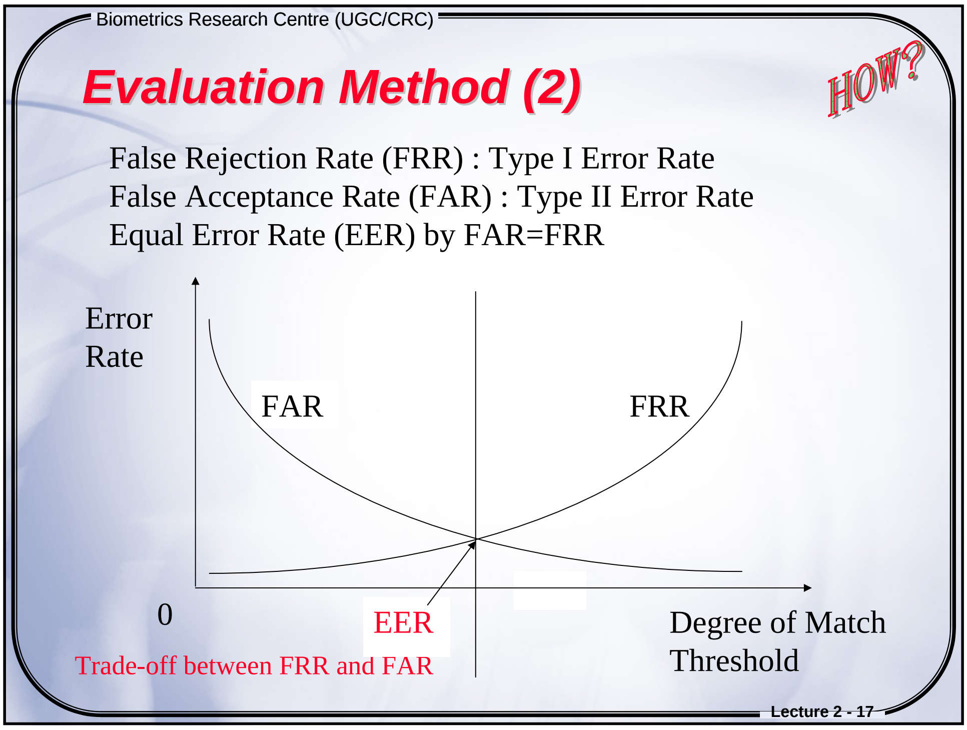


Evaluation Method (1)

- In principle we can use the following to assess systems

  * False (genuine individual) Rejection Rate (FRR)
  (also called Type I error)
  * The False (imposter) Acceptance Rate (FAR)
  (also called Type II error)
  * The equal error rate
  (rate where FAR and FRR are equal)

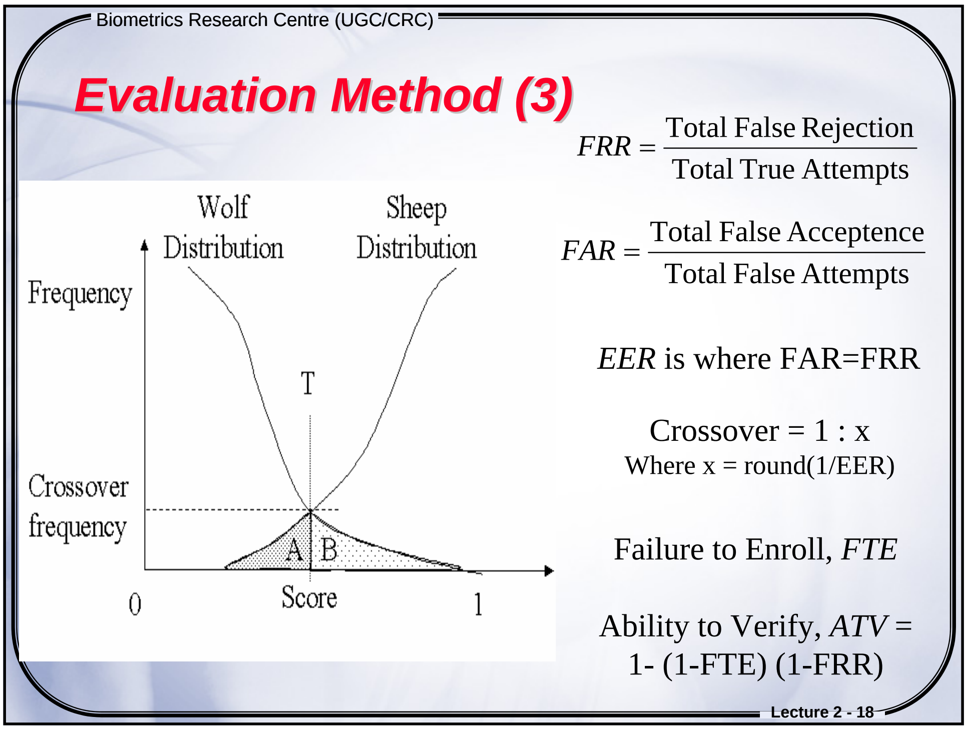
- These are test population and system configuration dependent and can not be generalized even for the same system under different populations or test conditions!
- Statistical methods are used to assess system performance



Evaluation Method (2)

False Rejection Rate (FRR) : Type I Error Rate
False Acceptance Rate (FAR) : Type II Error Rate
Equal Error Rate (EER) by FAR=FRR

Trade-off between FRR and FAR



Evaluation Method (3)

$$FRR = \frac{\text{Total False Rejection}}{\text{Total True Attempts}}$$

$$FAR = \frac{\text{Total False Acceptence}}{\text{Total False Attempts}}$$

EER is where FAR=FRR

Crossover = 1 : x
Where x = round(1/EER)

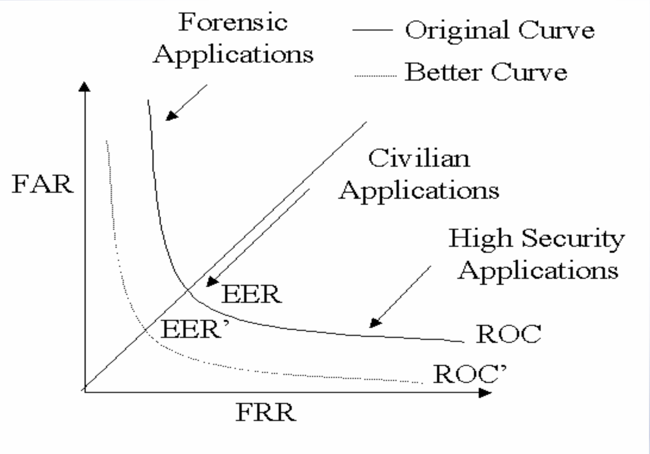
Failure to Enroll, *FTE*

Ability to Verify, *ATV* =
1- (1-FTE) (1-FRR)

Evaluation Method (4)

What?

- Receiver Operating Characteristic (ROC) curve is a plot of FRR (or the genuine acceptance rate, 100-FRR) against FAR for all possible operating points.



Requirement for an Ideal Biometric

- An automated biometric system uses biological, physiological or behavioral characteristics to automatically authenticate the identity of an individual based on a previous enrollment event.
- If a biological, physiological, or behavioral characteristic has the following properties…
  - ⇒ **Universality** (*Every person should possess this characteristic*)
  - ⇒ **Uniqueness** (*No two persons possess the same characteristic*)
  - ⇒ **Permanence** (*Does not change in time, i.e., it is time invariant*)
  - ⇒ **Collectability** (Can be quantitatively measured)

…. then it can potentially serve as a biometric *for a given application*.

Biometric Characteristics (1)

What?

- **Universality**

  (*Every person should possess this characteristic*)

  ⇒ In practice, this may not be the case

  ⇒ Otherwise, population of non-universality must be small < 1%

- **Uniqueness**

  (*No two persons possess the same characteristic*)

  -- Genotypical – Genetically linked
  (e.g. identical twins will have same biometric)

  -- Phenotypical – Non-genetically linked
  different perhaps even on same individual

  ⇒ Establishing uniqueness is difficult to prove analytically

Biometric Characteristics (2)

What?

- **Permanence**

  (*Does not change in time, i.e., it is time invariant*)

  -- At best this is an approximation

  -- Degree of permanence has a major impact on the system design and long term operation of biometrics. (e.g. enrollment, adaptive matching design, etc.)

  -- Long vs. short-term stability

- **Collectability**

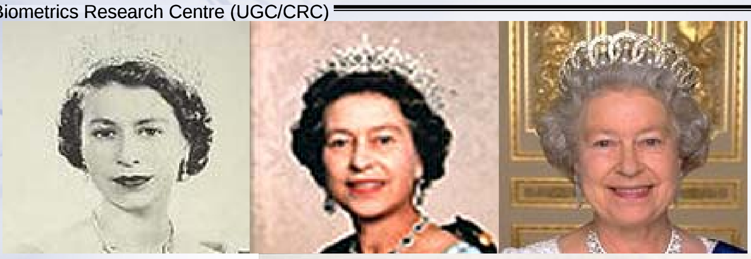
  (Can be quantitatively measured)

  ⇒ In practice, the biometric collection must be:

  -- Non-intrusive

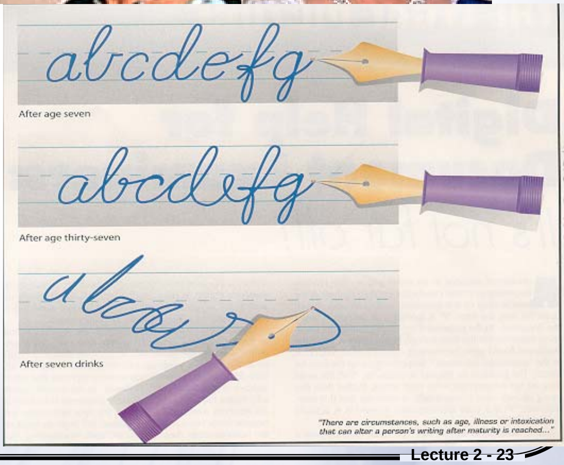
  -- Reliable and robust

  -- Cost effective for a given application



Uniqueness: *Intra-Class Variability*

⇒ The same person may have the different features


abcdefg
After age seven
abcdefg
After age thirty-seven
After seven drinks
"There are circumstances, such as age, illness or intoxication that can alter a person's writing after maturity is reached..."

Uniqueness : *Inter-Class Similarity*

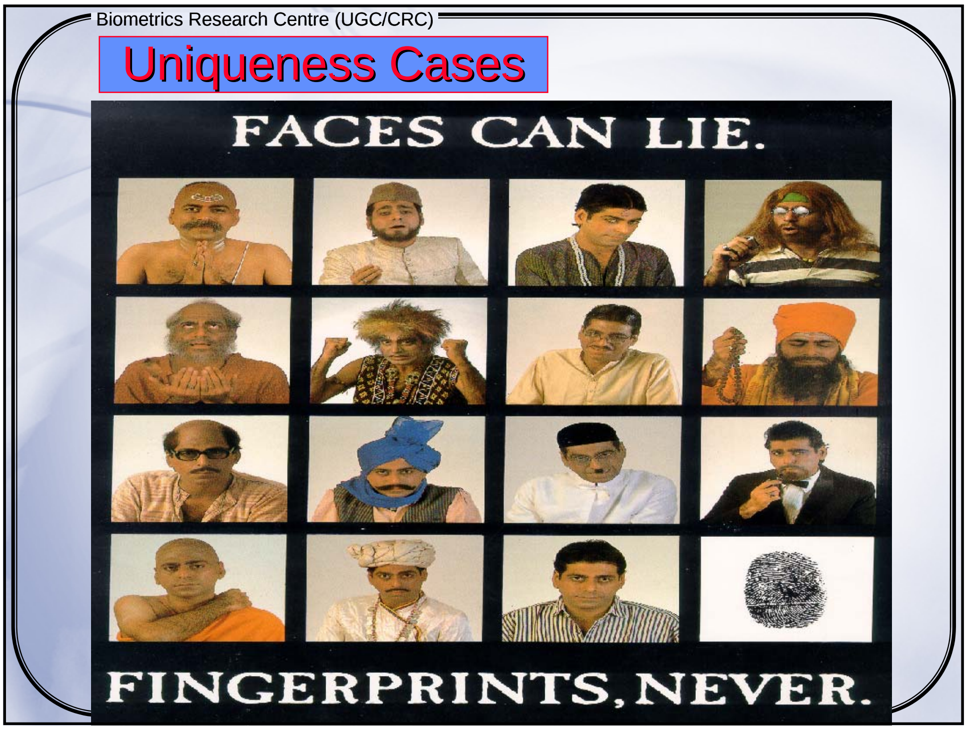
www.marykateandashley.com

Twins

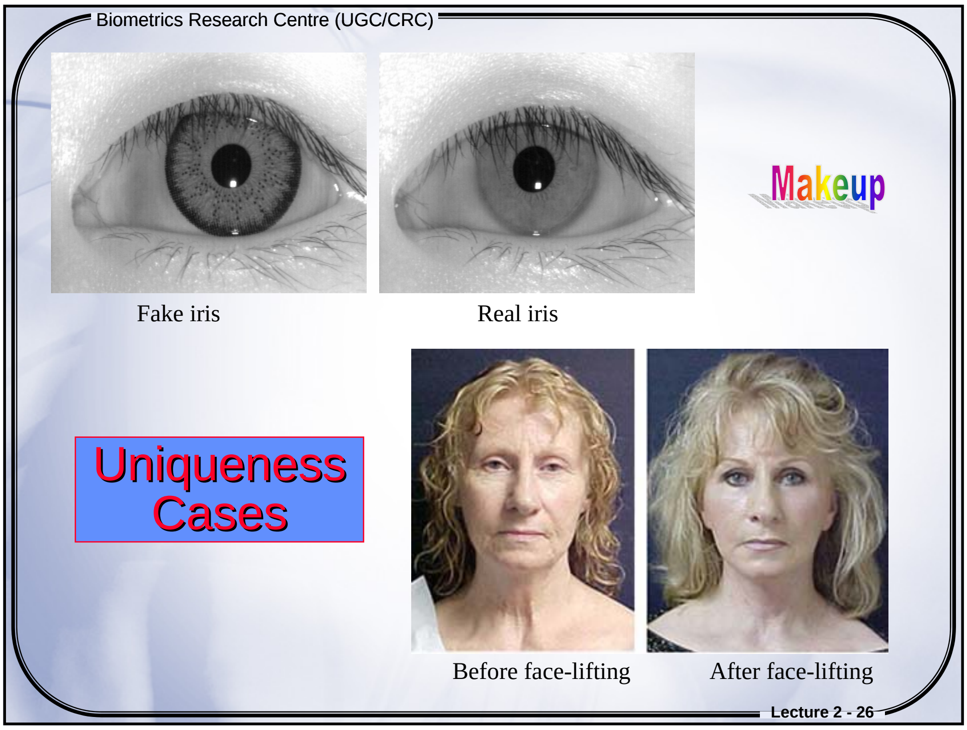
news.bbc.co.uk/hi/english/in_depth/americas/2000/us_elections

Father and son

⇒ Different persons may have very similar appearance



Uniqueness Cases



Fake iris

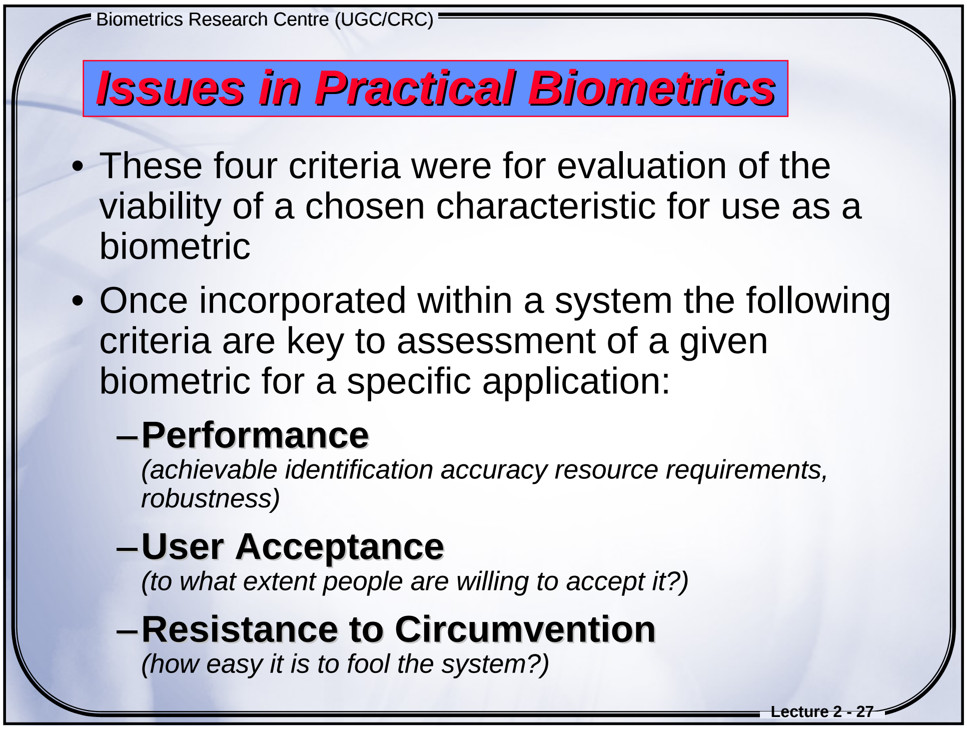
Real iris

Makeup

Uniqueness Cases

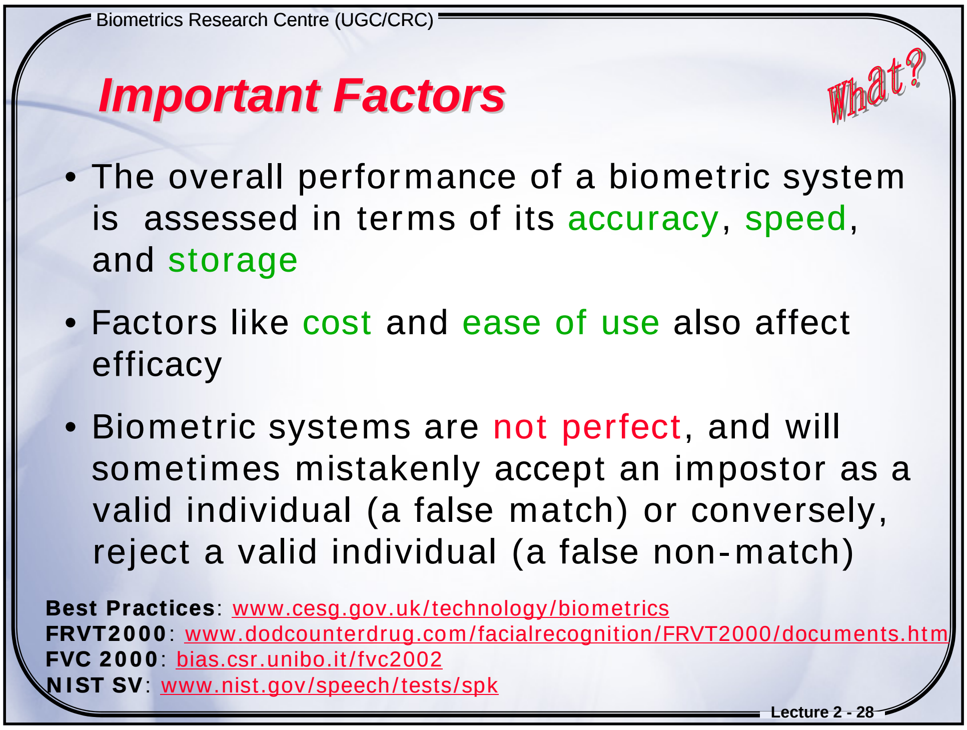
Before face-lifting

After face-lifting



Issues in Practical Biometrics

- These four criteria were for evaluation of the viability of a chosen characteristic for use as a biometric
- Once incorporated within a system the following criteria are key to assessment of a given biometric for a specific application:
  - **Performance**
    (achievable identification accuracy resource requirements, robustness)
  - **User Acceptance**
    (to what extent people are willing to accept it?)
  - **Resistance to Circumvention**
    (how easy it is to fool the system?)



Important Factors

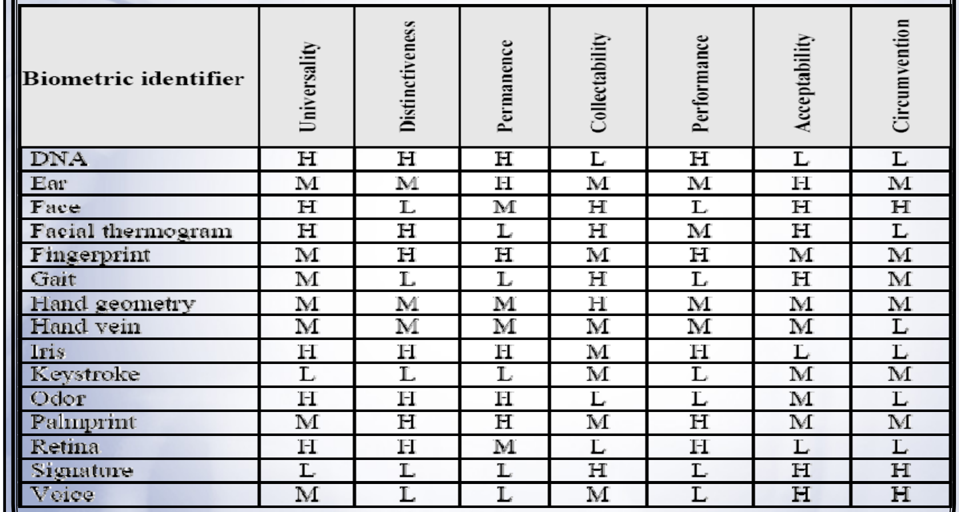
What?

- The overall performance of a biometric system is assessed in terms of its accuracy, speed, and storage
- Factors like cost and ease of use also affect efficacy
- Biometric systems are not perfect, and will sometimes mistakenly accept an impostor as a valid individual (a false match) or conversely, reject a valid individual (a false non-match)

Best Practices: www.cesg.gov.uk/technology/biometrics
FRVT2000: www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.htm
FVC 2000: bias.csr.unibo.it/fvc2002
NIST SV: www.nist.gov/speech/tests/spk

Comparison of Biometrics

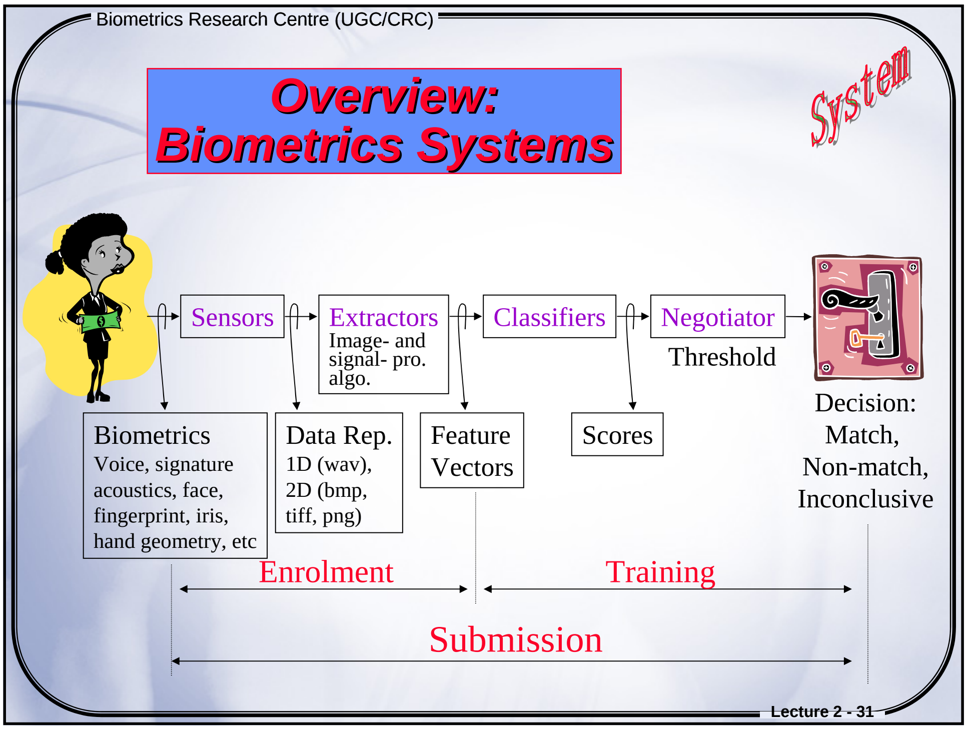
New



Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

*A.K. Jain, et al., “An Introduction to Biometric Recognition”, *IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, January, 2004.*

Biometrics Systems



Overview: Biometrics Systems

Sensors → Extractors (Image- and signal- pro. algo.) → Classifiers → Negotiator → Decision: Match, Non-match, Inconclusive

Threshold

Biometrics
Voice, signature acoustics, face, fingerprint, iris, hand geometry, etc

Data Rep.
1D (wav), 2D (bmp, tiff, png)

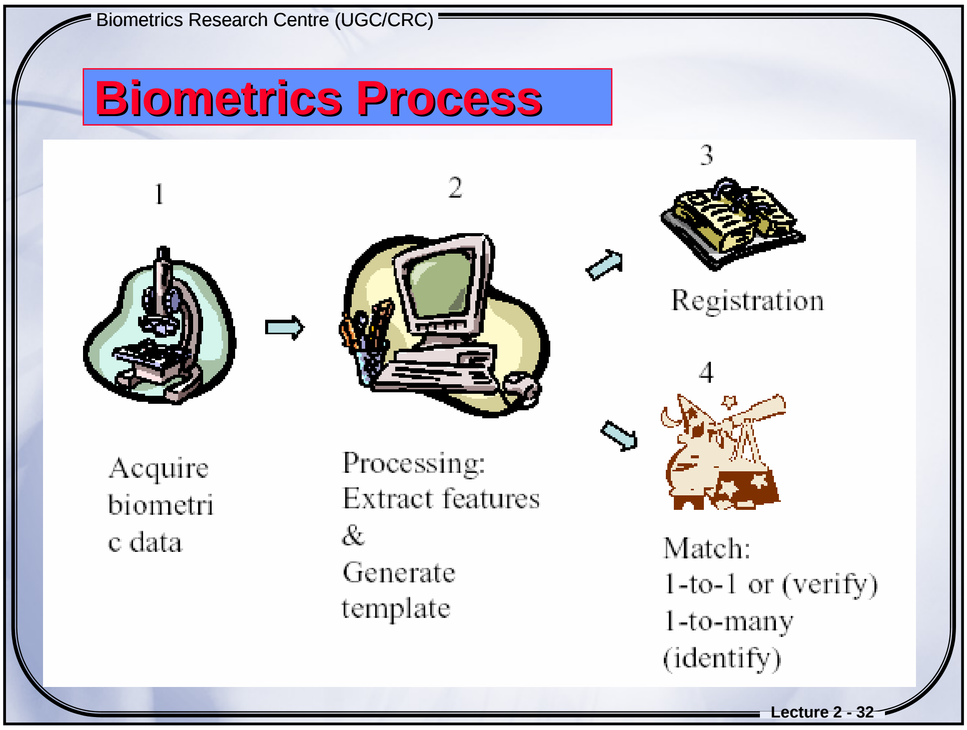
Feature Vectors

Scores

Enrolment

Training

Submission



Biometrics Process

1 Acquire biometri c data

2 Processing: Extract features & Generate template

3 Registration

4 Match: 1-to-1 or (verify) 1-to-many (identify)

Four Stage Procedure

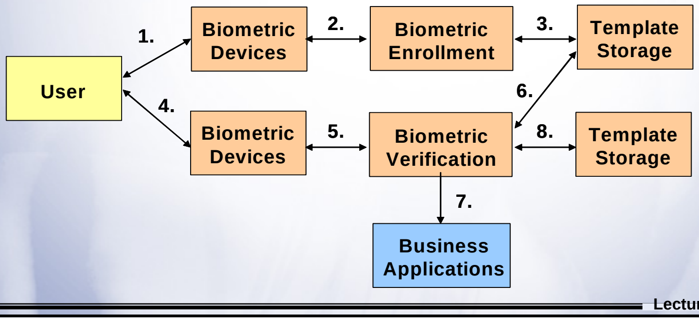
System

- All biometric technology systems operate using the following four-stage procedures:
  - Capture – a physical or behavioral sample is captured during enrollment, identification or verification process
  - Extraction – unique data is extracted from the sample and a template is created
  - Comparison – the template is compared to new sample
  - Match/Non-Match – system then decides if the features extracted from the new sample are a match or non-match

Biometric Operations

System

1) Capture the chosen biometric.
2) Process the biometric and extract and enroll the biometric template.
3) Store the template in a local repository, a central repository, or a portable token such as a smart card.
4) Live-scan the chosen biometric.
5) Process the biometric and extract the biometric template.
6) Match the scanned biometric against stored templates.
7) Provide a matching score to business applications.
8) Record a secure audit trail with respect to system use.



Systems Architecture

System

- **Architecture Dependent on Application:**
  - ❑ Identification: Who are you?

    One to Many **(millions) match (1:Many)**

    One to "Few" **(less than 500) (1:Few)**

    Who does this fingerprint belong to?
  - ❑ Verification: **Are you who you say you are?**

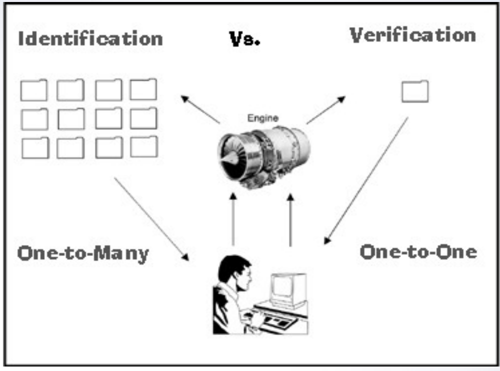
    One to One **Match (1:1)**

    Does this fingerprint belong to Joe Smith?

Identification is *a much harder problem* than verification *because an identification system must perform a large number of comparisons.*

- When the database size increases, the accuracy of the system decreases and computation time increases.

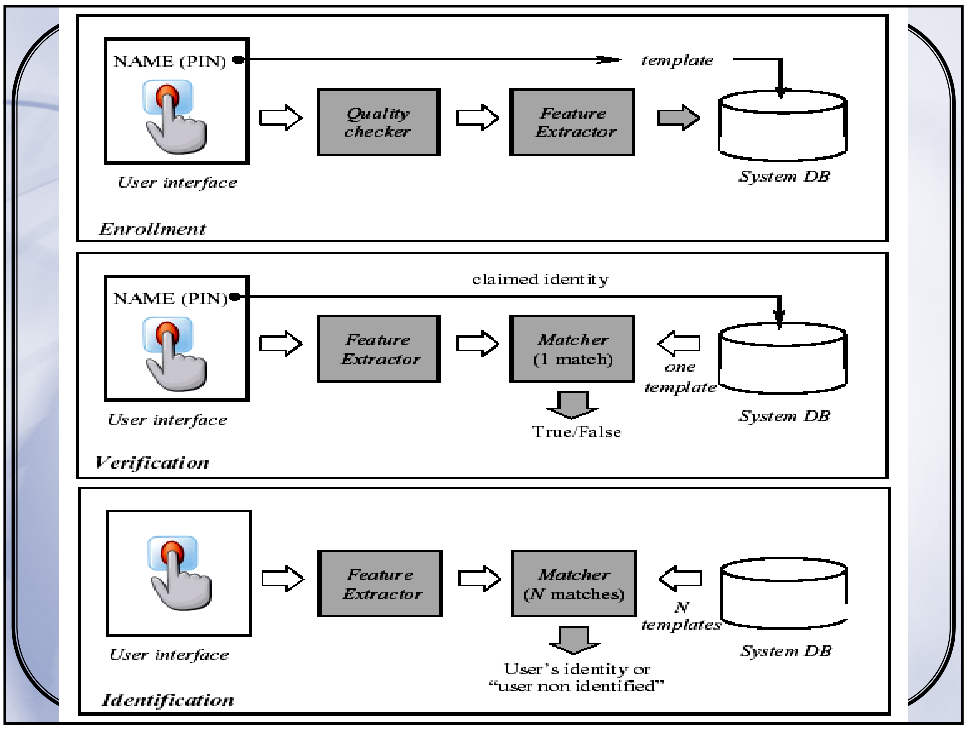
Two Types of Biometric Systems **Verification & Identification**

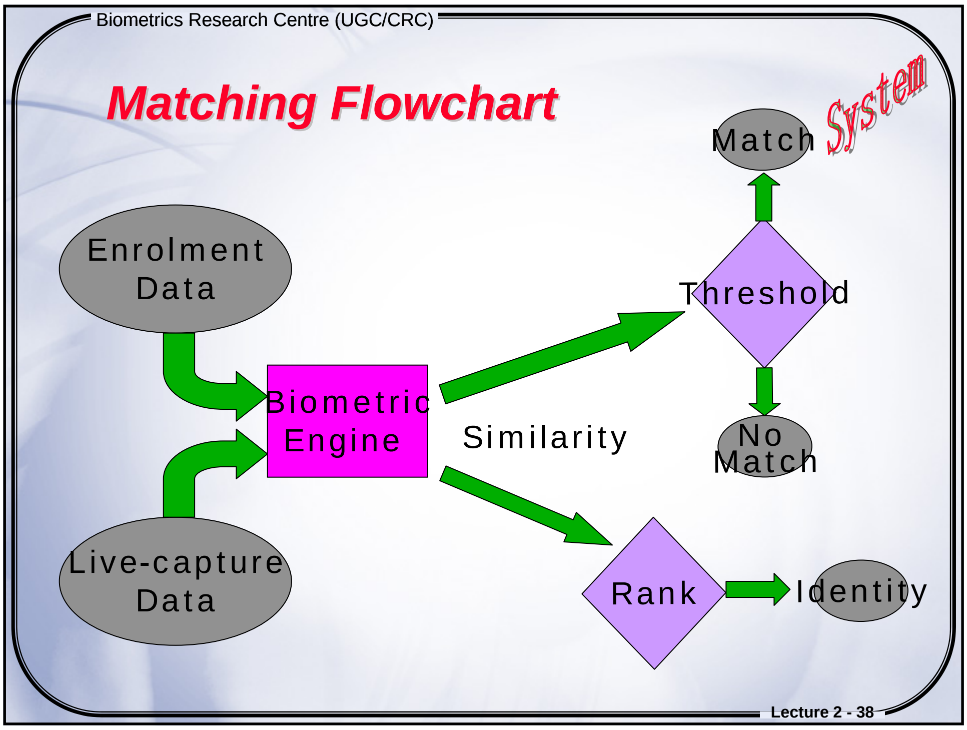


Identification:

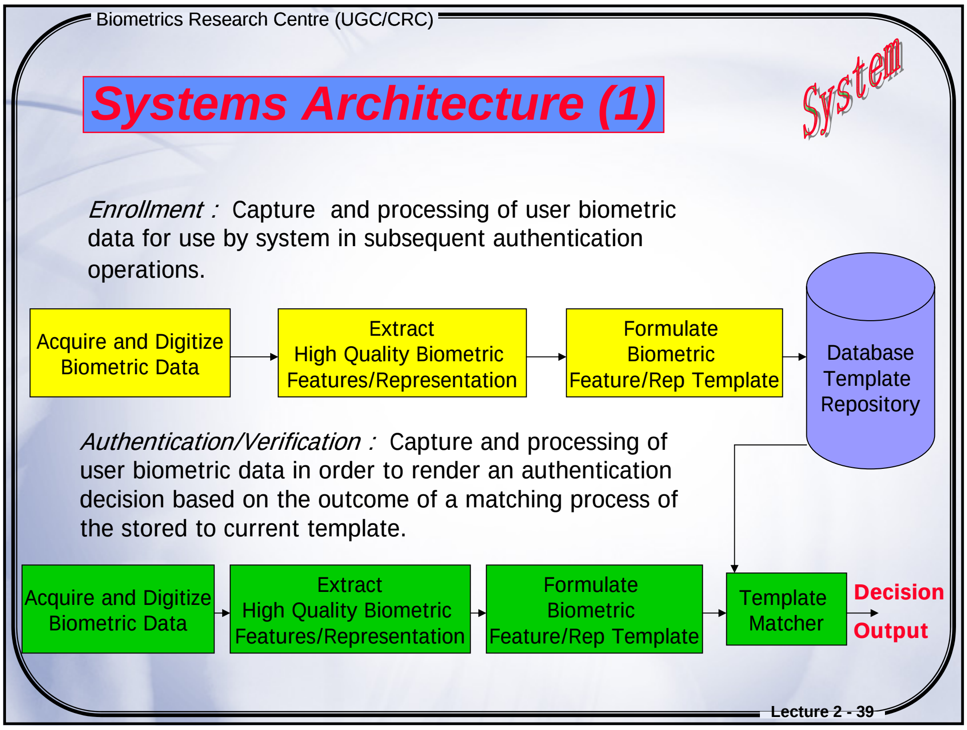
Some systems use hierarchical or classification methods to speed up the searching.

- Hierarchical approach uses some simple features and fast matching algorithm to retrieve a small set of templates for further recognition by using complex algorithm.
- Classification approach cuts down the database in several (fuzzy/ non-fuzzy) groups. The input feature is classified to one/several group(s).
- Hierarchical/classification would introduce errors.





Matching Flowchart



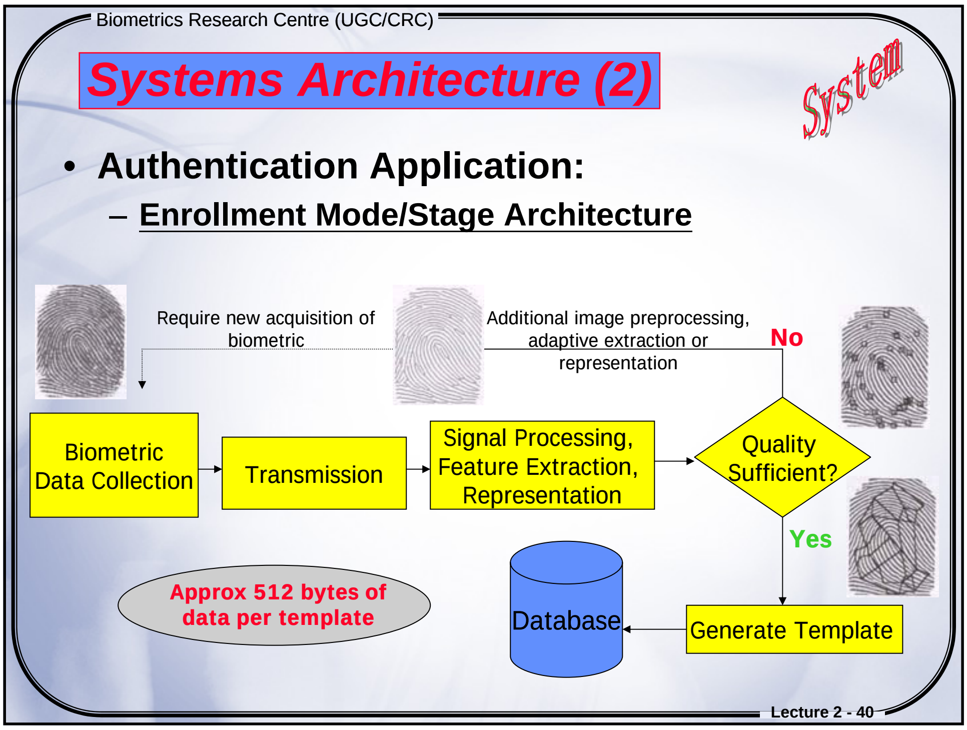
Systems Architecture (1)

Enrollment : Capture and processing of user biometric data for use by system in subsequent authentication operations.

Acquire and Digitize Biometric Data → Extract High Quality Biometric Features/Representation → Formulate Biometric Feature/Rep Template → Database Template Repository

Authentication/Verification : Capture and processing of user biometric data in order to render an authentication decision based on the outcome of a matching process of the stored to current template.

Acquire and Digitize Biometric Data → Extract High Quality Biometric Features/Representation → Formulate Biometric Feature/Rep Template → Template Matcher → Decision Output



Systems Architecture (2)

- **Authentication Application:**
  - **Enrollment Mode/Stage Architecture**

Biometric Data Collection → Transmission → Signal Processing, Feature Extraction, Representation → Quality Sufficient?

Additional image preprocessing, adaptive extraction or representation

No

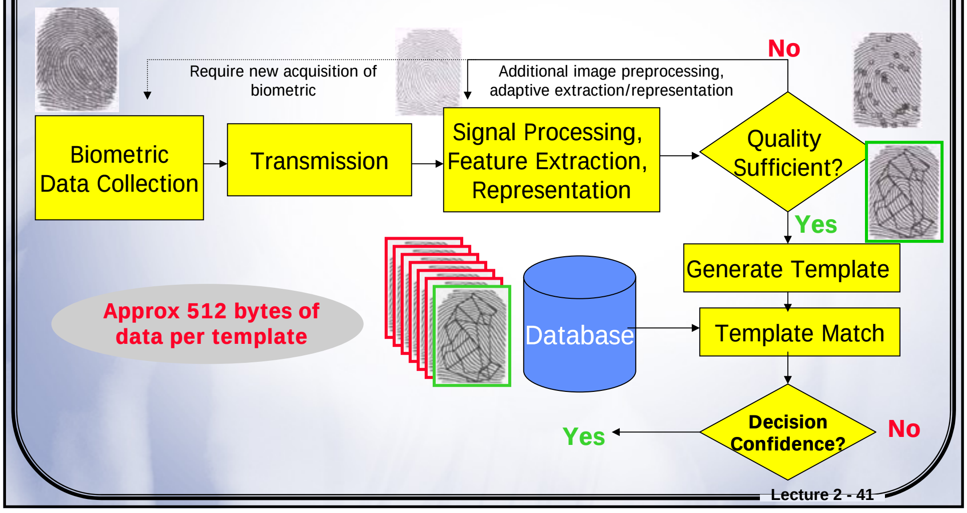
Require new acquisition of biometric

Yes → Generate Template → Database

Approx 512 bytes of data per template

Systems Architecture (3)

- **Authentication Application:**
  - **Verification/Authentication Mode/Stage Architecture**



Require new acquisition of biometric

Additional image preprocessing, adaptive extraction/representation

No

Biometric Data Collection

Transmission

Signal Processing, Feature Extraction, Representation

Quality Sufficient?

Yes

Generate Template

Approx 512 bytes of data per template

Database

Template Match

Yes

Decision Confidence?

No

Architecture Subsystems

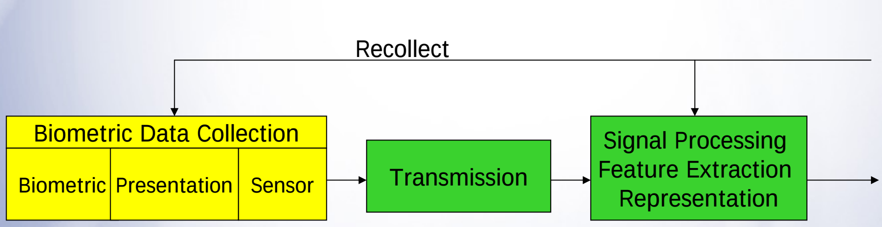
- **Data Collection**
- **Transmission**
- **Signal Processing/Pattern Matching**
- **Database/Storage**
- **Decision**

- **What comprises these subsystems and how do they interact with other elements (what are their interface and performance specifications?)**

Architecture Subsystems (1)

System

- Data Collection Module
  - Biometric choice, presentation of biometric, biometric data collection by sensor and its digitization.



Recollect

Biometric Data Collection

Biometric | Presentation | Sensor

Transmission

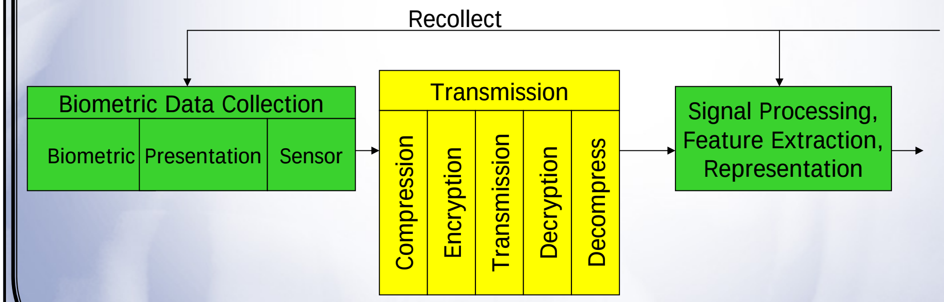
Signal Processing
Feature Extraction
Representation

Architecture Subsystems (2)

System

- Transmission Module

  Compress and encrypt sensor digital data, reverse process.



Recollect

Biometric Data Collection

Biometric | Presentation | Sensor

Transmission

Compression | Encryption | Transmission | Decryption | Decompress

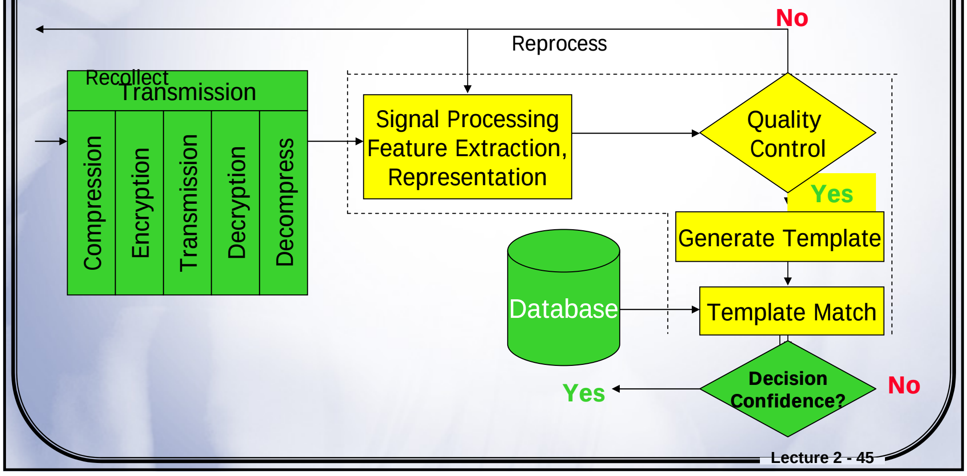
Signal Processing,
Feature Extraction,
Representation

Architecture Subsystems (3)

System

- **Signal Processing/Matching Module**

Be aware of potential transmission prior to match



No

Reprocess

Recollect

Transmission

Compression

Encryption

Transmission

Decryption

Decompress

Signal Processing Feature Extraction, Representation

Quality Control

Yes

Generate Template

Database

Template Match

Decision Confidence?

Yes

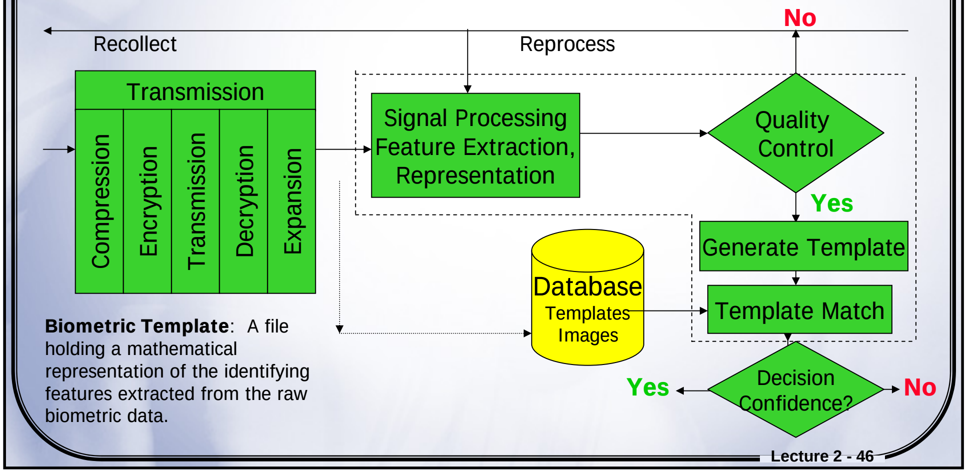
No

Architecture Subsystems (4)

System

- **Database module**

In what form is biometric stored? Template or raw data?



No

Recollect

Reprocess

Transmission

Compression

Encryption

Transmission

Decryption

Expansion

Signal Processing Feature Extraction, Representation

Quality Control

Yes

Generate Template

Database

Templates

Images

Template Match

Yes

Decision Confidence?

No

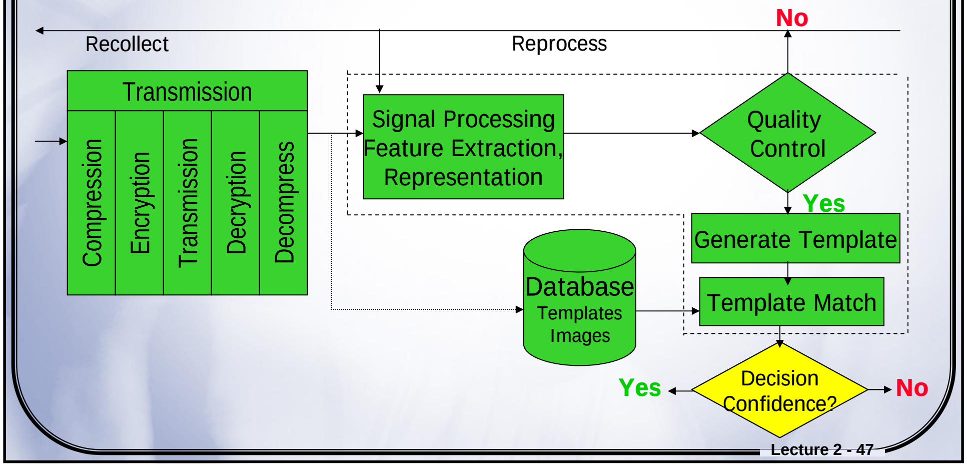
Biometric Template: A file holding a mathematical representation of the identifying features extracted from the raw biometric data.

Architecture Subsystems (5)

System

- Decision module

  Is there enough similarity to the stored information to declare a match with a certain confidence ?



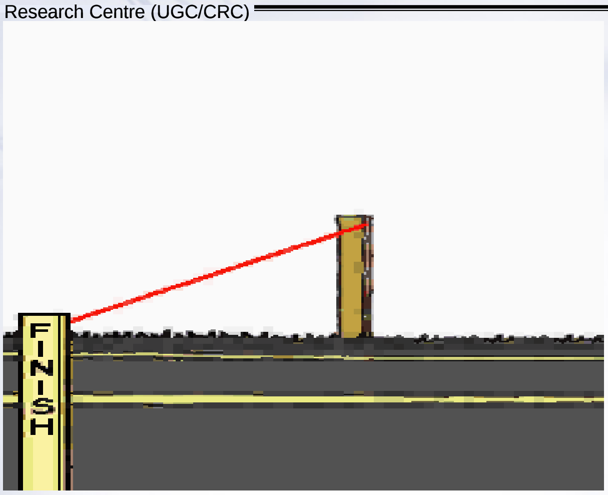
Questions?

1. Given both FRR and FAR, how to change these two curves into one in ROC?

2. Data collection is the first part in a biometrics system. Do you have any idea how to capture some useful data from human body? What kind of methods could you adopt?

3. Do you think what main problems are happened in the current biometrics system? For your opinion, which one is more serious?

4. Which difference between Verification & Identification? How about their applications?



END