

Tutorial 1

Qu Xiaofeng, Teaching Assistant
quxiaofeng.at.polyu@gmail.com

COMP435p
Biometrics Authentication

January 16, 2012





Table of Contents

1 Problems

- Problem 1: Answer the following questions
- Problem 2: Biometric authentication system
- Problem 3: Compare
- Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC
- Problem 5: Evaluate FAR, FRR and ATV



Outline

1 Problems

- Problem 1: Answer the following questions
- Problem 2: Biometric authentication system
- Problem 3: Compare
- Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC
- Problem 5: Evaluate FAR, FRR and ATV



Problem 1.a

Understand the reasons why biometrics security in e-world.



Problem 1.a

Biometrics Research Centre (UGC/CRC)

Why Security in e-World

Why?

- We enter *the age of universal electronic connectivity* ⇒ *called e-World*:
 - ⇒ e-commerce ⇒ e-backing
 - ⇒ e-shop ⇒ e-purse
 - ⇒ e-phone ⇒ e-government
- In an e-world, the more and more activities are related to **INTERNET**.
- With Internet development, there exist some troubles and problems.
 - ⇒ *Viruses* ⇒ *Hackers*
 - ⇒ *Computer theft* ⇒ *Unauthorized access*

Why_security

e-Banking

Lecture 1 - 4



Problem 1.a

Biometrics Research Centre (UGC/CRC)

Security Solutions

Why?

- ❑ All these problems threaten the prosperity and productivity of corporations and individuals.
 - ⇒ Security is increasingly important.
 - ⇒ Two approaches:
 - “Make Water Clear” - “使水变清”
 - “Make Water Chaotic” - “把水搅混”
- ❑ One security solution: **Authentication**
 - ⇒ Verify message and user.
- ❑ In fact, there is an ever growing need to **identify individuals** in e-world.
 - Should this person be given **access** to a secure system?
 - Does this person have **authorization** to perform a given transaction?

Lecture 1 - 5



Problem 1.a

Biometrics Research Centre (UGC/CRC)

User Authentication Problem

Why?

- ❑ Every day, questions like “Who Are You?” that are related to establishing the identity of individuals are asked *millions times*.

PROBLEM 1: (Credit Card)

Each year, billions of dollars are lost through the fraudulent use of credit cards.

PROBLEM 2: (Benefit Care)

A lot of money losses due to the abuse of health care unemployment insurance benefits and welfare systems.

PROBLEM 3: (Immigration)

Many individuals illegally enter the country each year using falsified travel documents.

Lecture 1 - 6



Problem 1.a

Biometrics Research Centre (UGC/CRC)

User Authentication

- User authentication (identity verification)
 - Convince system of your identity
 - Before it can act on your behalf
- Sometimes also require that the computer verify its identity with the user
- User authentication: Three methods
 - What you know
 - What you have
 - What you are/do
- All then involve some validation of information supplied against a table of possible values based on users claimed identity

Lecture 1 - 7



Problem 1.a

Biometrics Research Centre (UGC/CRC)

Method 1: What You Know

- Passwords or Pass-phrases

- ⇒ Knowledge-based

- Use "something that you know"
- Examples: password, PIN

abc0123

Passwords/PINs

What you know

- Verify identity by checking that password is correct
- More often use a one-way function, whose output cannot easily be used to find the input value
 - either takes a fixed sized input (e.g., 8 chars)
 - or accept a variable sized input to create the value
- Important that passwords are selected with care to reduce risk of exhaustive search
- Other solution: One-shot (one-time) passwords

Lecture 1 - 8



Problem 1.a

Biometrics Research Centre (UGC/CRC)

Method 2: What You Have

⇒ **Token-based**

- Use “something that you have”
- Examples: credit card, smart card, keys

- Verify identity based on possession of some object, often also combined with a password
- Magnetic Card, Magnetic Key
 - possess item with required code value encoded in it
- Smart Card or Calculator
 - may interact with system
 - may require information from user
 - could be used to actively calculate
 - a time dependent password
 - a one-shot password

Keys Cards

What you have

Lecture 1 - 9

Problem 1.a

Biometrics Research Centre (UGC/CRC)

What Problems

- At the NY Times web site, about 1,000 people per week forget their passwords
- Common hacker tools can typically guess 30% or more of the passwords on a network
 - Some hackers claim 90% success
- Tedious, time-consuming, inefficient & expensive

Lost your Key ?

Forgot your Password ?

Lecture 1 - 10



Problem 1.a

Biometrics Research Centre (UGC/CRC)

Method 3: What You Are/Do

- Verify identity based on your **physical characteristics or behavioural patterns**, known as biometrics Flash
- Characteristics used include:
 - signature (usually dynamic)
 - fingerprint
 - hand geometry
 - face or body profile
 - speech
 - retina pattern
- Comparison: Biometrics
 - More security
 - More reliable



Lecture 1 - 11





Problem 1.b

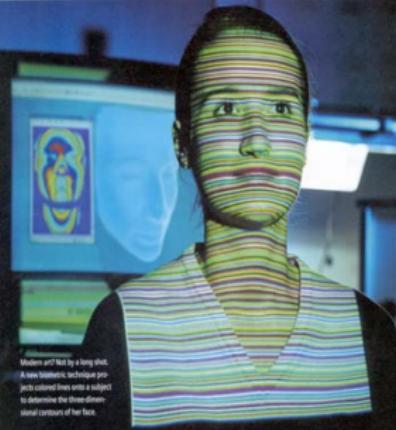
What is biometrics?



Problem 1.b

Biometrics Research Centre (UGC/CRC)

Body Language: Biometrics



Modern art? Not by a long shot.
A new biometric technique projects colored lines onto a subject to determine the three-dimensional visual contours of her face.

- No two people are the same.
- With this in mind, we can use the methods that enable **the unique characteristics** of eyes, faces and voices to be converted into **data keys** that enhance **security** and **convenience**.

Lecture 1 - 13



Problem 1.b

Biometrics Research Centre (UGC/CRC)

Biometrics Authentication: Security and Privacy Concerns

- ❑ Biometrics can overcome some of the limitations, hence it offers *greater security and convenience* than traditional methods.
- ❑ In some applications, biometrics can **replace** or **supplement** the existing technology. In others, it is **the only viable approach**.
- ❑ Biometrics-based identification is emerging as the most reliable method.



Lecture 1 - 14



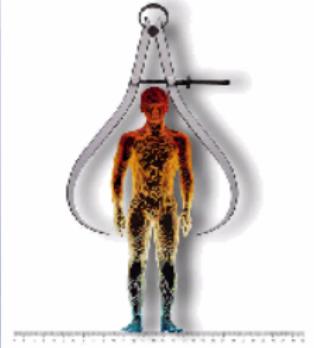
Problem 1.b

Biometrics Research Centre (UGC/CRC)

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



Lecture 2 - 3



Problem 1.b

Biometrics Research Centre (UGC/CRC)

Examples of Biometrics

What?

Lecture 2 - 4



Problem 1.b

Biometrics Research Centre (UGC/CRC)

Classification: Biometrics Data

What?

1D Biometrics

Angel

2D Biometrics

3D Biometrics

Lecture 2 - 5



Problem 1.b

Biometrics Research Centre (UGC/CRC)

Classification: Biometrics Features

What?

Inside Feature	Outside Feature

Lecture 2 - 6





Problem 1.c

Understand two types of biometrics and give some examples respectively.



Problem 1.c

Biometrics Research Centre (UGC/CRC)

Biometrics Classification

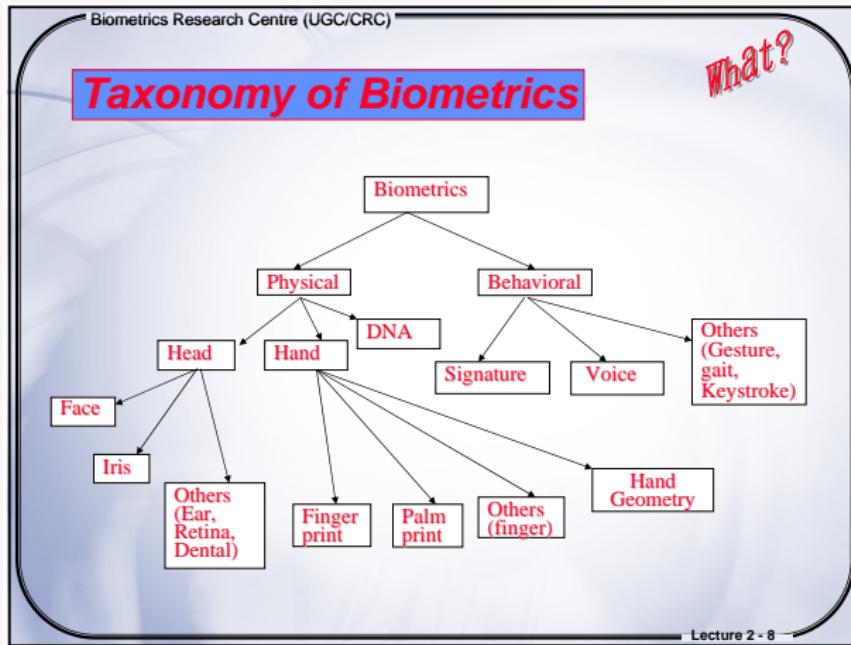
Two types of biometrics

- **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

Lecture 2 - 7



Problem 1.c





Problem 1.d

The definition of enrollment, template and matching in a biometrics system.

Problem 1.d

Biometrics Research Centre (UGC/CRC)

Definition: Enrollment

• 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

Verification or identification

Present biometric → Capture → Process

Match

Compare

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.

Lecture 2 - 11

Problem 1.d

Biometrics Research Centre (UGC/CRC)

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

The diagram shows three stages of image processing:

- "Raw" Data: A grayscale fingerprint image.
- Processed Data: The same fingerprint image with skeletonized features highlighted in blue.
- Template Data: The processed data with specific points of interest marked by red dots.

Lecture 2 - 12



Problem 1.d

Biometrics Research Centre (UGC/CRC)

Definition: Matching

Matching scores is the matching result between two templates.

What?

(a) (b) (c)

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

Lecture 2 - 13





Problem 1.e

What are the requirements of a biometric feature used for authentication purposes?



Problem 1.e

Biometrics Research Centre (UGC/CRC)

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*.

Lecture 2 - 20



Problem 1.e

Biometrics Research Centre (UGC/CRC)

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

Lecture 2 - 21



Problem 1.e

Biometrics Research Centre (UGC/CRC)

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

Lecture 2 - 22



Problem 1.e

Biometrics Research Centre (UGC/CRC)

The slide features three photographs of Queen Elizabeth II. The first is a black and white portrait from her younger years. The second is a color portrait from her middle years. The third is a color portrait from her later years, showing significant hair loss and wrinkles. Below the photos is a blue box containing the text "Uniqueness: Intra-Class Variability". To the right is a graphic illustrating handwriting variability. It shows three rows of cursive handwriting: "abcdefg" at age seven, "abcdefg" at age thirty-seven, and "abegf" after seven drinks. Each row includes a purple fountain pen and a small caption below it. A small note at the bottom right states: "There are circumstances, such as age, illness or intoxication, that can alter a person's writing after which it is no longer unique." The slide is labeled "Lecture 2 - 23" at the bottom right.

**Uniqueness:
Intra-Class
Variability**

⇒ The same person may have the different features

After age seven

After age thirty-seven

After seven drinks

There are circumstances, such as age, illness or intoxication, that can alter a person's writing after which it is no longer unique.

Lecture 2 - 23



Problem 1.e

Biometrics Research Centre (UGC/CRC)

Uniqueness : *Inter-Class Similarity*



www.marykateandashley.com

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

Twins

Father and son

⇒ Different persons may have very similar appearance

Lecture 2 - 24



Problem 1.e

Biometrics Research Centre (UGC/CRC)

Uniqueness Cases

FACES CAN LIE.

FINGERPRINTS, NEVER.



Problem 1.e

Biometrics Research Centre (UGC/CRC)

Fake iris Real iris

Uniqueness Cases

Before face-lifting After face-lifting

Makeup

Lecture 2 - 26



Problem 1.e

Biometrics Research Centre (UGC/CRC)

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?)

Lecture 2 - 27



Problem 1.e

Biometrics Research Centre (UGC/CRC)

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

Lecture 2 - 28





Problem 1.f

Which difference between identification and verification?



Problem 1.f

Biometrics Research Centre (UGC/CRC)

Systems Architecture

• **Architecture Dependent on Application:** *System*

- 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.

Lecture 2 - 35

Problem 1.f

Biometrics Research Centre (UGC/CRC)

Two Types of Biometric Systems Verification & Identification

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

Identification **Vs.** **Verification**

One-to-Many One-to-One

Lecture 2 - 36



Outline

1 Problems

- Problem 1: Answer the following questions
- **Problem 2: Biometric authentication system**
- Problem 3: Compare
- Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC
- Problem 5: Evaluate FAR, FRR and ATV

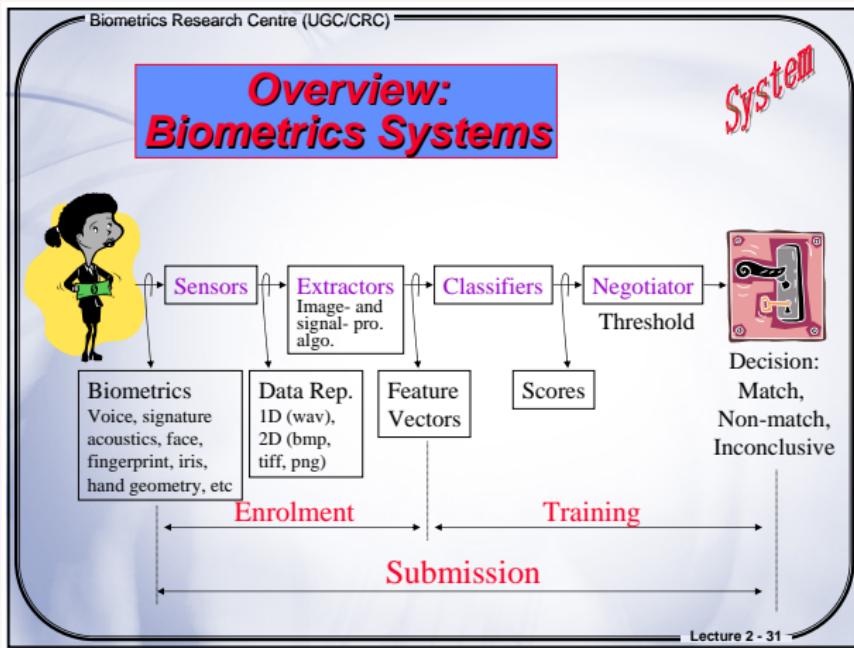


Problem 2: Biometric authentication system

What makes up a biometric authentication system? Please give an example to explain them.

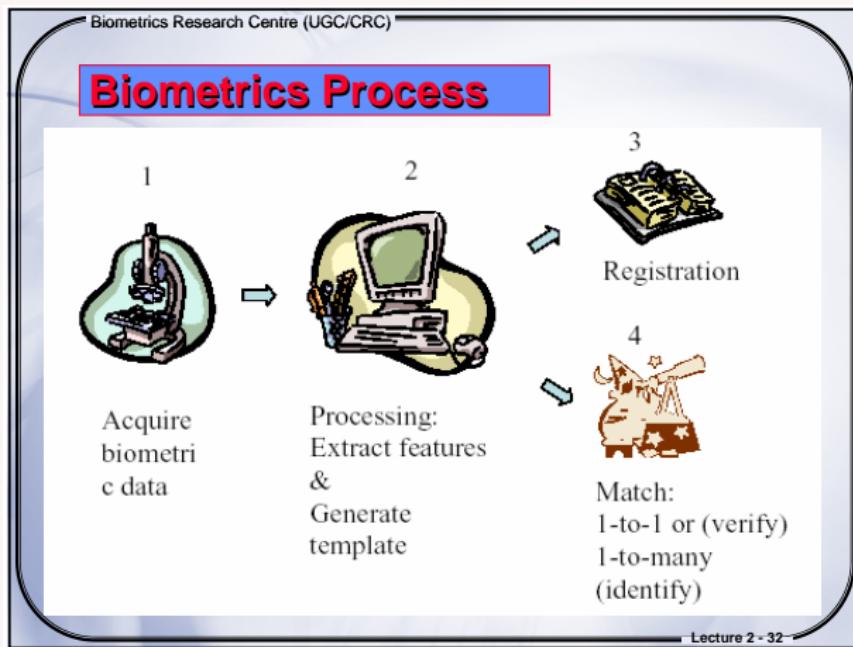


Problem 2: Biometric authentication system





Problem 2: Biometric authentication system





Problem 2: Biometric authentication system

Biometrics Research Centre (UGC/CRC)

Four Stage Procedure

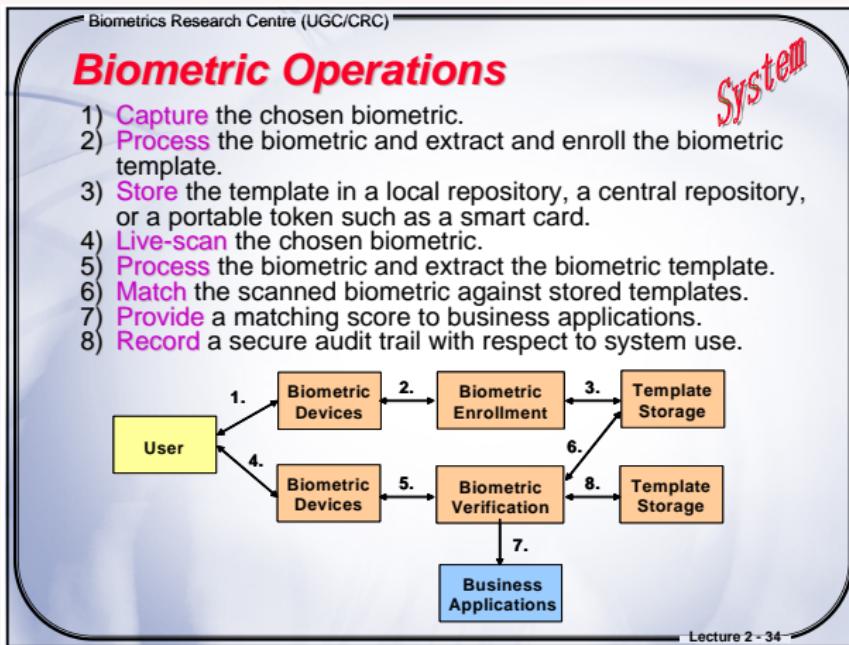
System

- 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

Lecture 2 - 33

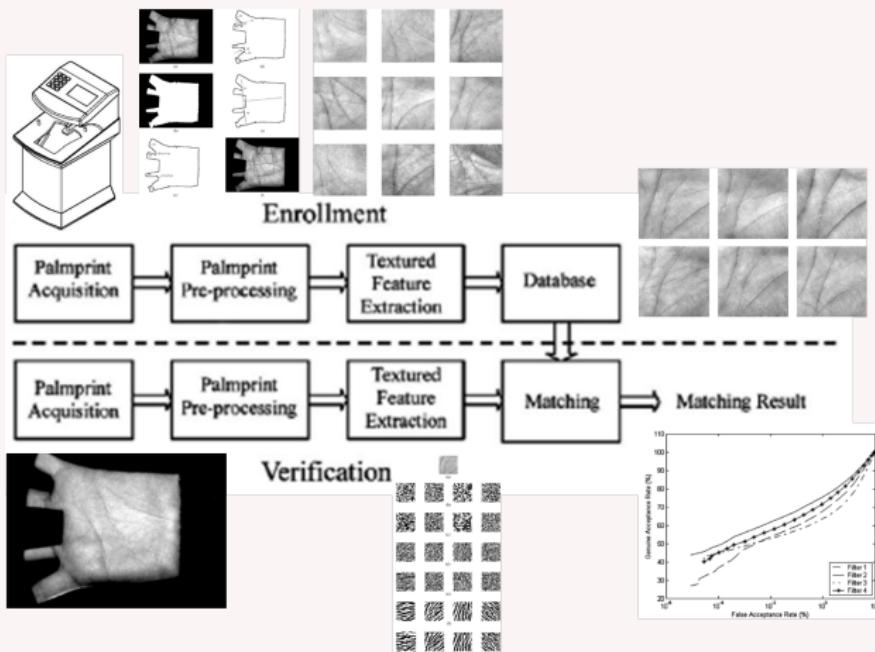


Problem 2: Biometric authentication system





A palmprint biometrics system





Outline

1 Problems

- Problem 1: Answer the following questions
- Problem 2: Biometric authentication system
- **Problem 3: Compare**
- Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC
- Problem 5: Evaluate FAR, FRR and ATV

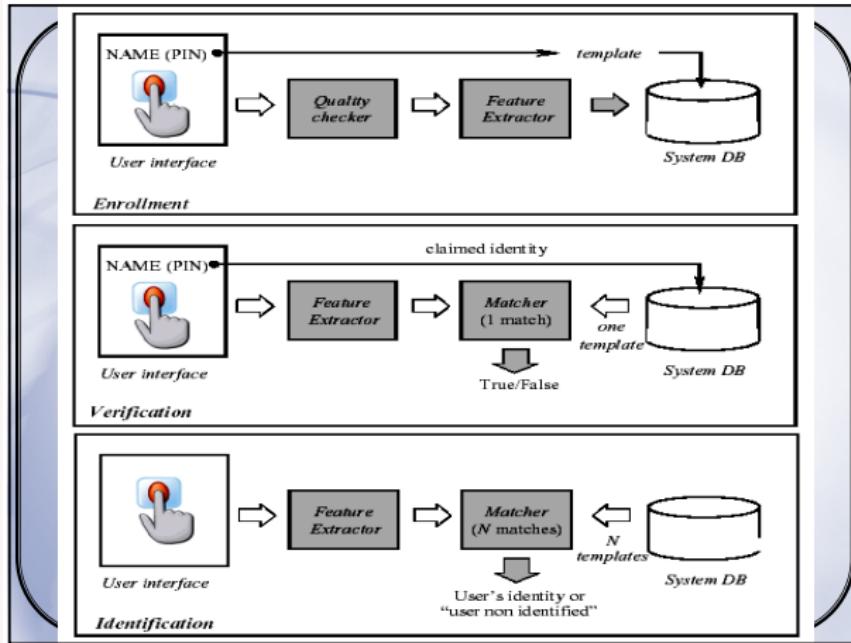


Problem 3: Compare

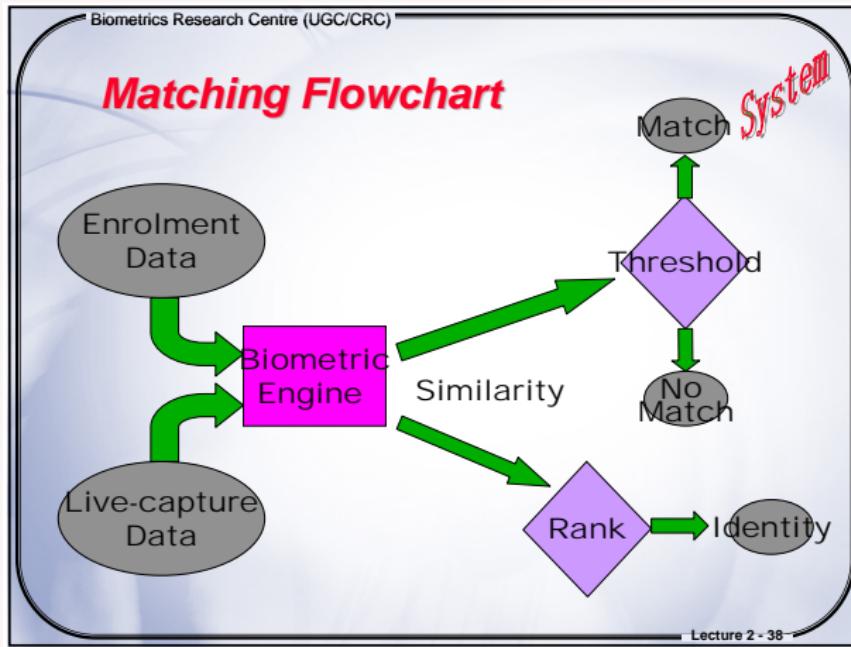
Compare enrollment mode and authentication/verification mode.



Problem 3: Compare



Problem 3: Compare





Outline

1 Problems

- Problem 1: Answer the following questions
- Problem 2: Biometric authentication system
- Problem 3: Compare
- **Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC**
- Problem 5: Evaluate FAR, FRR and ATV

Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC

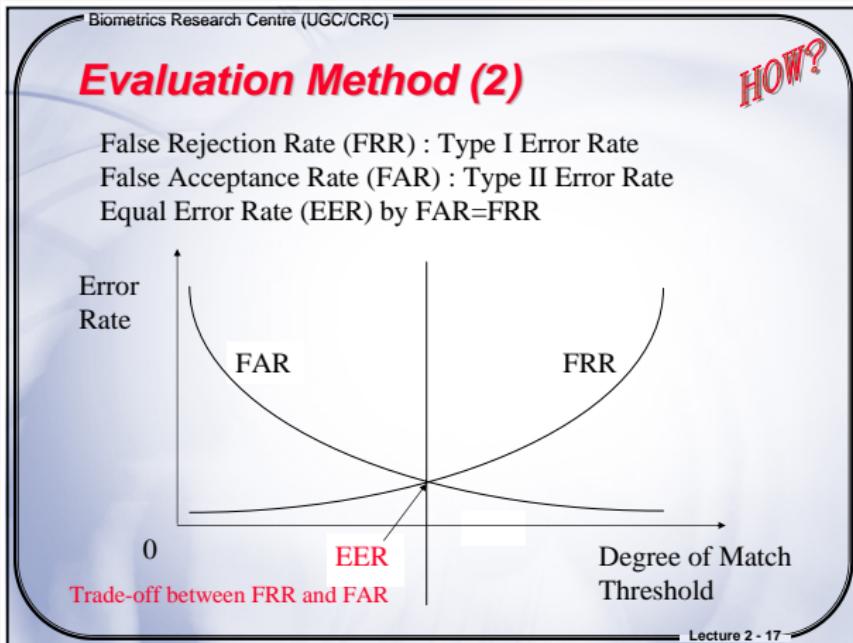


What are FRR, FAR, EER, Crossover, FTE, ATV and ROC?

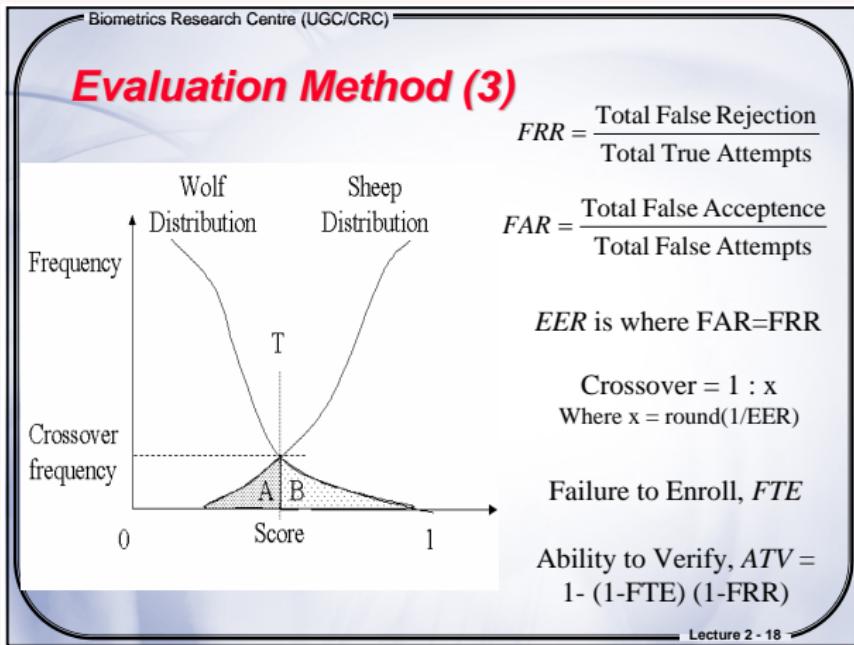
Now there are two FAR-FRR diagrams and one ROC curve.

Give the EER respectively. When FRR=0.1, how about FAR and Crossover, respectively? If the corresponding FTE are all equal to 0.05, then how about ATV?

Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC terms



Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC terms



Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROCterms

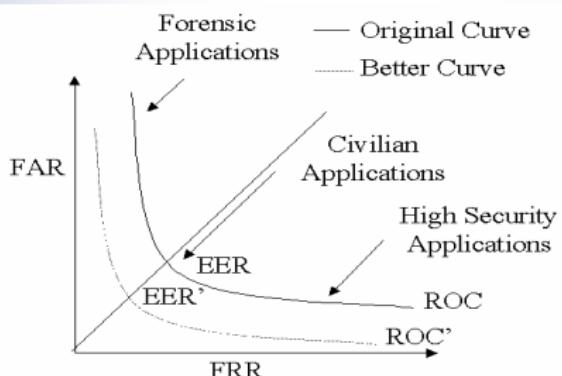


Biometrics Research Centre (UGC/CRC)

Evaluation Method (4)

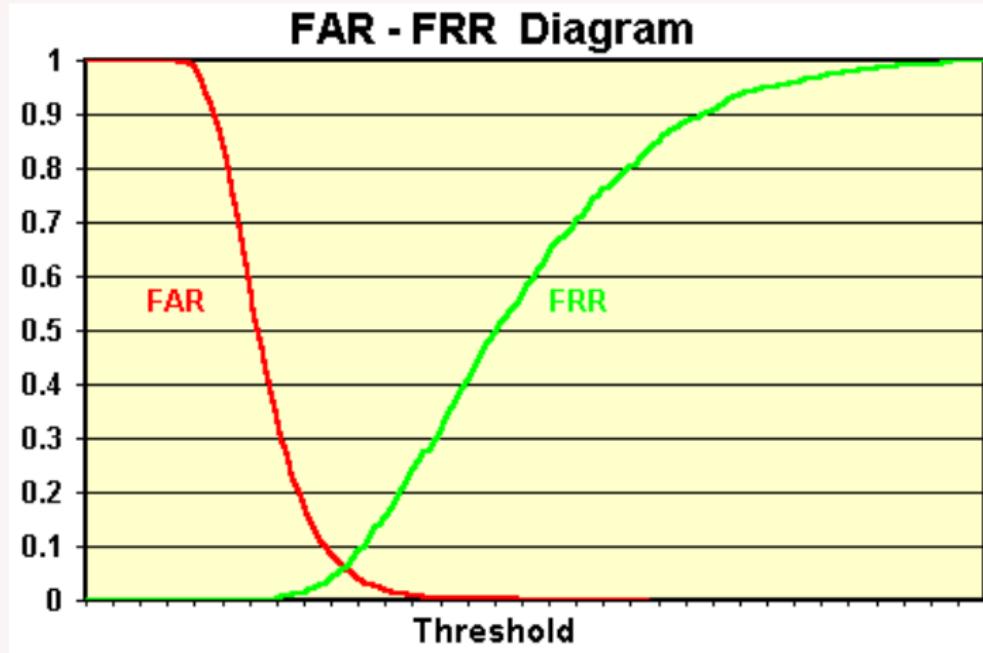
What?

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



Lecture 2 - 19

Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC.a





Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC.a

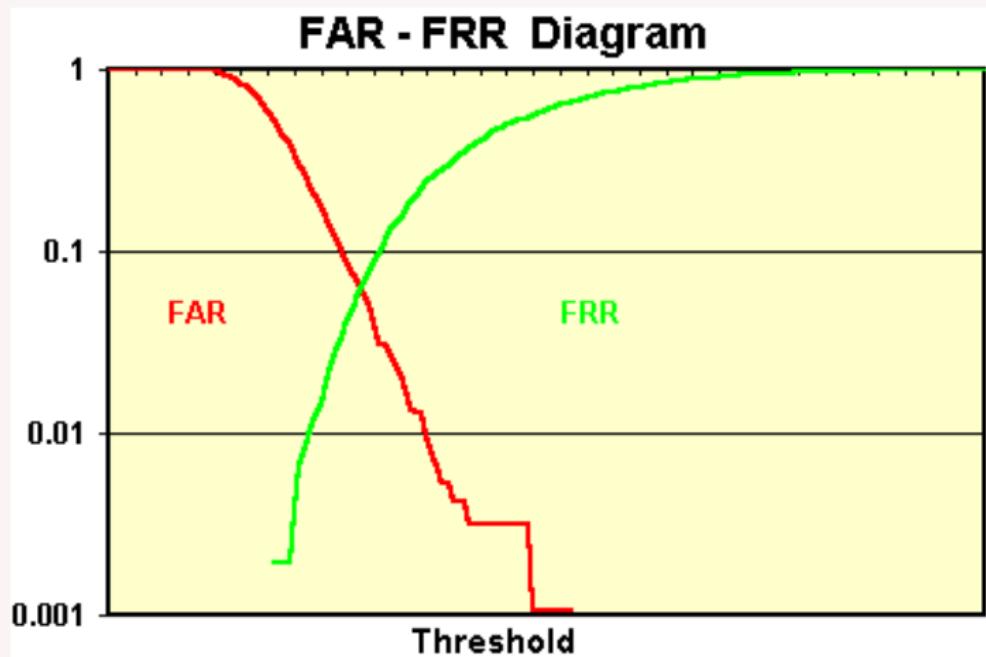
$$EER = 0.06$$

$$FAR = 0.03$$

$$\text{Crossover} = 1 : \text{round}(1/EER) = \frac{1}{17}$$

$$ATV = (1 - FTE)(1 - FRR) = (1 - 0.05) \times (1 - 0.1) = 0.855$$

Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC.b



Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC.b



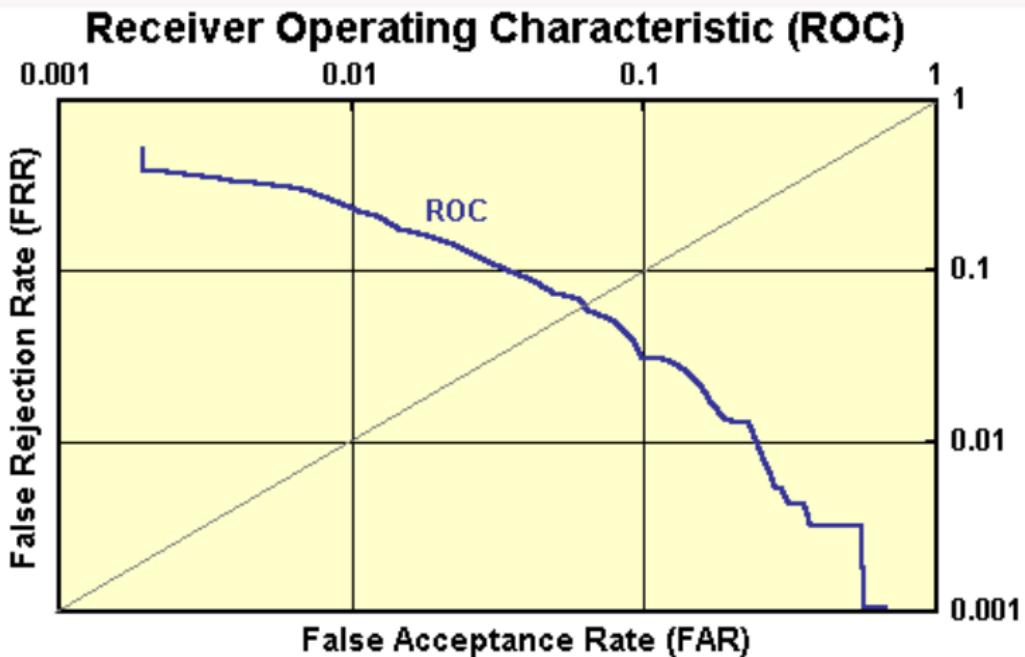
$$EER = 0.09$$

$$FAR = 0.07$$

$$\text{Crossover} = 1 : \text{round}(1/EER) = \frac{1}{11}$$

$$ATV = (1 - FTE)(1 - FRR) = (1 - 0.05) \times (1 - 0.1) = 0.855$$

Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC.c



Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC.c



$$EER = 0.08$$

$$FAR = 0.05$$

$$\text{Crossover} = 1 : \text{round}(1/EER) = \frac{1}{13}$$

$$ATV = (1 - FTE)(1 - FRR) = (1 - 0.05) \times (1 - 0.1) = 0.855$$





Outline

1 Problems

- Problem 1: Answer the following questions
- Problem 2: Biometric authentication system
- Problem 3: Compare
- Problem 4: FRR, FAR, EER, Crossover, FTE, ATV and ROC
- **Problem 5: Evaluate FAR, FRR and ATV**



Problem 5: Evaluate FAR, FRR and ATV

100 individuals try to use a biometric system. There are 38 genuine individuals are accepted, 8 genuine individuals rejected, 44 imposter rejected and 10 imposter accepted. Please evaluate the biometric system by giving the FAR and FRR. If $FTE=0.05$, then how about ATV?



Problem 5: Evaluate FAR, FRR and ATV

Biometrics Research Centre (UGC/CRC)

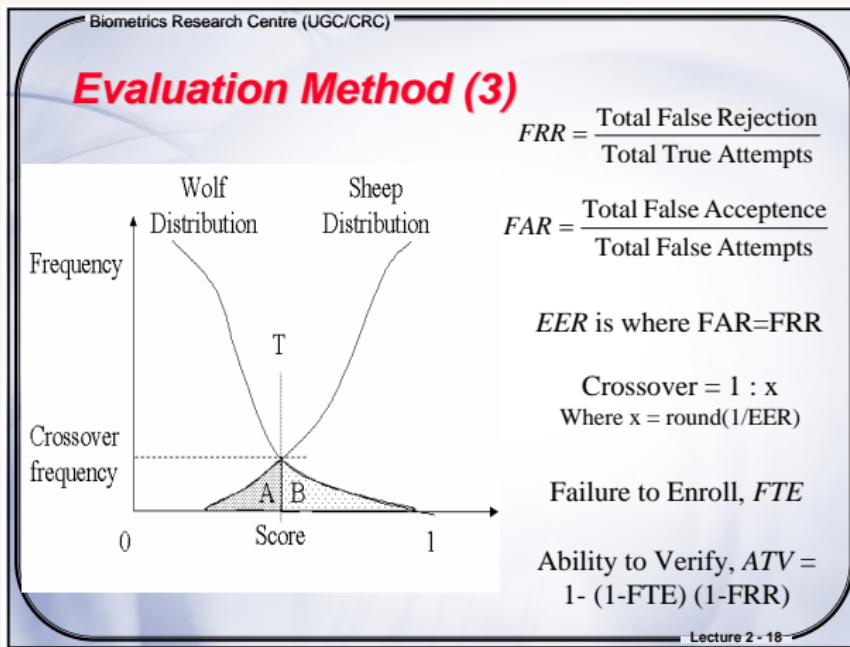
Decision: Types & Outcomes

- A decision made by a biometric system is either a **genuine** individual type of decision or an **impostor** 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.

Lecture 2 - 15



Problem 5: Evaluate FAR, FRR and ATV





Problem 5: Evaluate FAR, FRR and ATV

Individuals	Accepted	Rejected
Genuine	I_1	I_2
Imposter	I_4	I_3

$$FAR = \frac{I_4}{I_3 + I_4}$$

$$FRR = \frac{I_2}{I_1 + I_2}$$



Problem 5: Evaluate FAR, FRR and ATV

Individuals	Accepted	Rejected
Genuine	38	8
Imposter	10	44

$$FAR = \frac{I_4}{I_3 + I_4} = \frac{10}{44 + 10} = 0.19$$

$$FRR = \frac{I_2}{I_1 + I_2} = \frac{8}{38 + 8} = 0.17$$

$$ATV = (1 - FTE)(1 - FRR) = (1 - 0.05) \times (1 - 0.17) = 0.79$$





Problems

Any questions?