Introduction to Biometrics

Dr.M.Prabukumar
Associate Professor
mprabukumar@vit.ac.in 9894699058
SJT (Annex201G)

Agenda

- SWE1015-Biometric Systems
- Assessment modes and the rubrics
- Introduction of Biometrics
- Operations of Biometric system
- Advantages of Biometrics
- Applications of Biometrics
- Terminology
- Q & A

Assessment modes and the rubrics

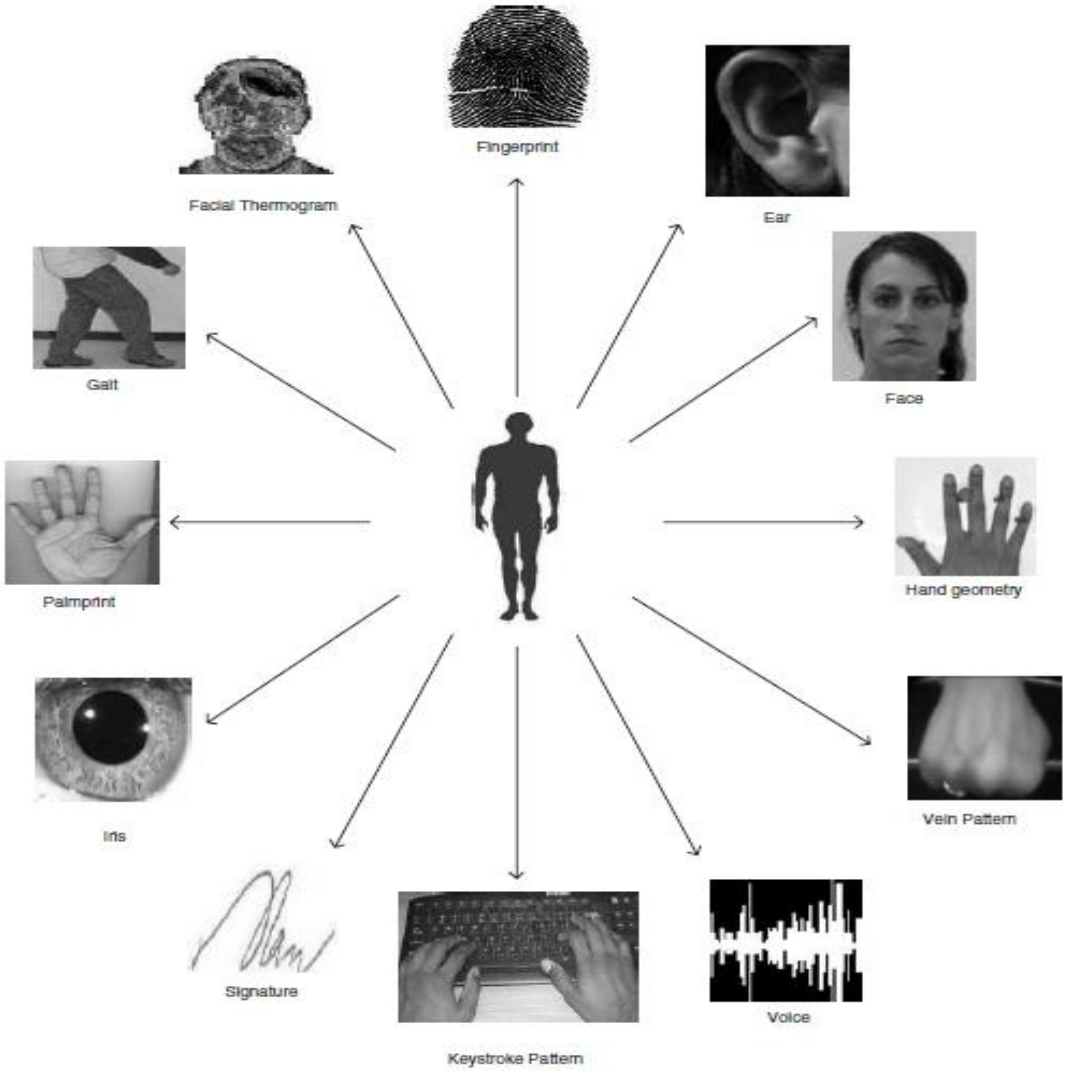
Assessment type	Max. Marks	Weightage
Quiz 1	10	10
Quiz 2	10	10
Assignment	10	10
CAT – I	50	15
CAT – II	50	15
FAT	100	40

What are Biometrics?

- The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).
- Biometrics is the science of recognizing the identity of a person based on the physical, chemical or behavioural attributes of the person.
- Biometric systems use a variety of physical or behavioral characteristics including fingerprint, face, hand/finger geometry, iris, retina, signature, gait, palm print, voice pattern, ear, hand vein, the DNA information.
- In the literature, these biometric characteristics are referred to as traits, indicators, identifiers or modalities
- These characteristics are unique to individuals hence can be used to verify or identify a person.

Examples of Different Biometrics

- Face
- Fingerprint
- Voice
- Palmprint
- Hand Geometry
- Iris
- Retina Scan
- Voice
- DNA
- Signatures
- Gait
- Keystroke



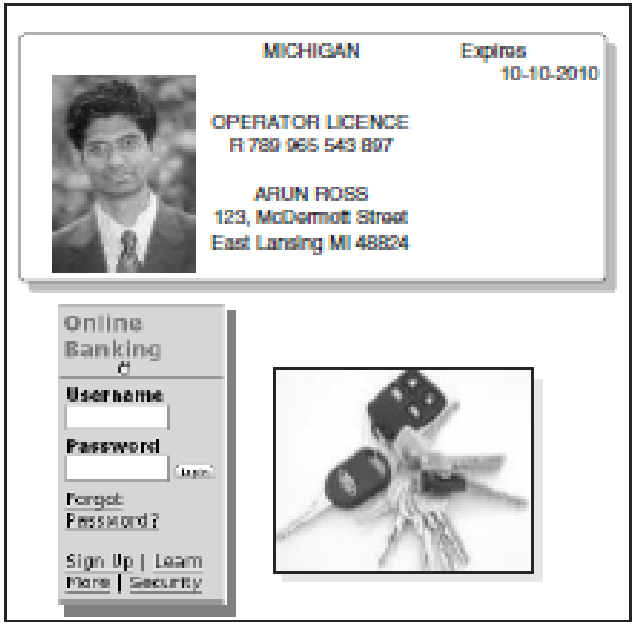
Operation of a biometric system

four main modules:

- a sensor module
- a quality assessment and feature extraction module
- a matching module
- a database module

Problems with current security systems

- Based on Passwords, or ID/Swipe cards



- Can be Lost.

- Can be forgotten.

- Worse! Can be stolen and used by a thief/intruder to access your data, bank accounts, car etc….

Some statistics on User/Passwords

- Case Study: Telesis Community Credit Union(CA), a California based financial services provider that manages $1.2 billion in assets.

- The VP of IT, lead a team to run a network password cracker as part of an enterprise security audit to see if employees were following Telesis' password policies.

- In fact within **30 seconds** the team was able to identify 80% of people's passwords!

Some statistics on User/Passwords

- The team asked employees to change their passwords and comply with password policies.

- A few days later, the IT team run their password cracking exercise again….

- This time they still were able to crack 70% of the passwords!

Problems with current security systems…

- With increasing use of IT technology and need to protect data, we have multiple accounts/passwords.

- We can only remember so many passwords, so we end up using things we know to create them (birthdays, Relation/boyfriend/girlfriend name, dog, cat…)

- Its is easy to crack passwords, because most of our passwords are weak!

- If we create strong passwords (that should be meaningless to us) we will forget them! And there is no way to remember multiple such passwords

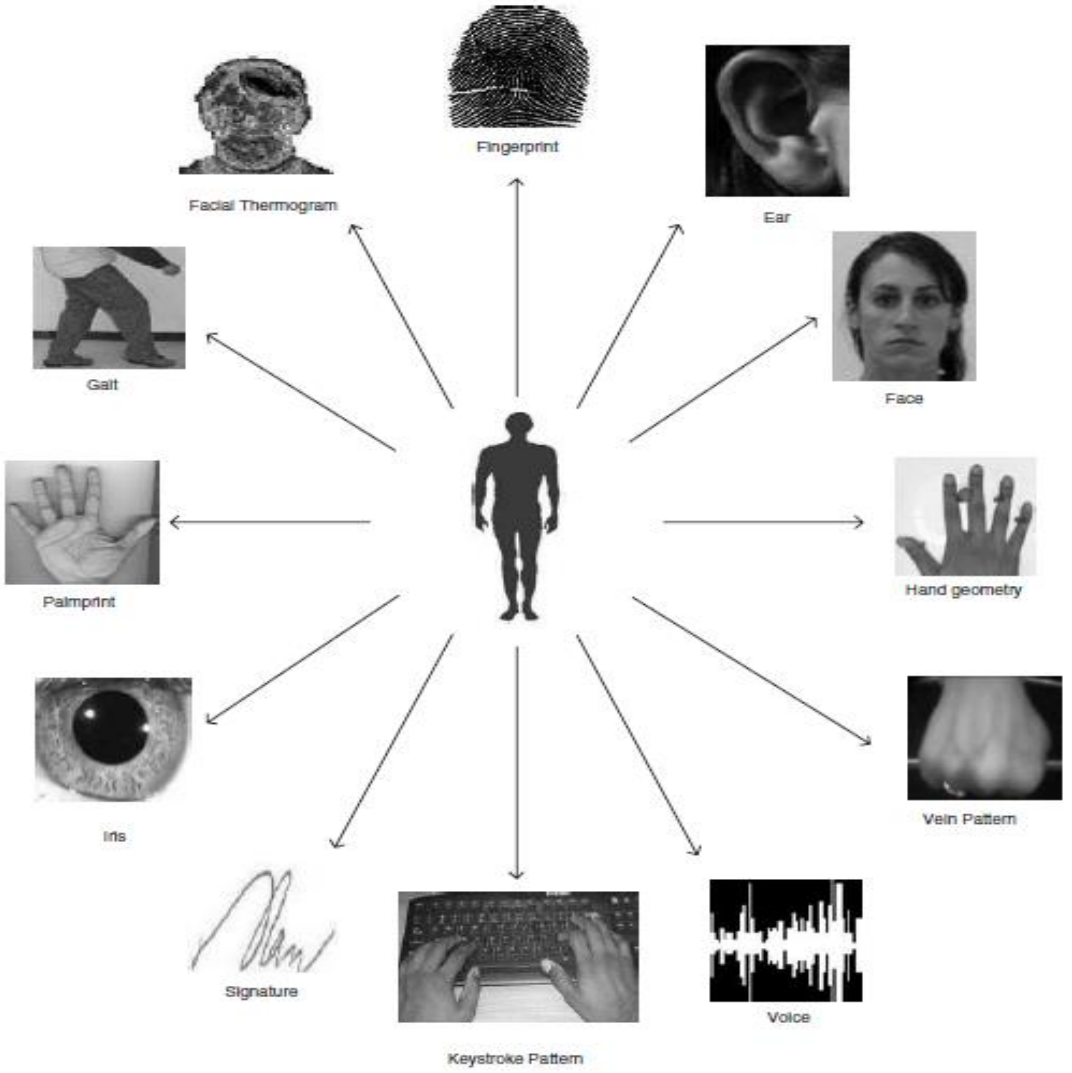
Many problems with current security authentication systems…

ANSWER:

USE BIOMETRIC TECHNOLOGY

Examples of Different Biometrics

- Face
- Fingerprint
- Voice
- Palmprint
- Hand Geometry
- Iris
- Retina Scan
- Voice
- DNA
- Signatures
- Gait
- Keystroke



Biometrics Advantages

- Biometrics offers certain advantages such as negative recognition and non-repudiation.

Negative recognition is the process by which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it.

Non-repudiation is a way to guarantee that an individual who accesses a certain facility cannot later deny using it (e.g., a person accesses a certain computer resource and later claims that an impostor must have used it under falsified credentials).

Terminology

- **Identification**:

– Match a person's biometrics against a database to figure out his identity by finding the closest match.

– Commonly referred to as 1:N matching

– 'Criminal Watch-list' application scenarios

Terminology Cont…

- **Verification**:

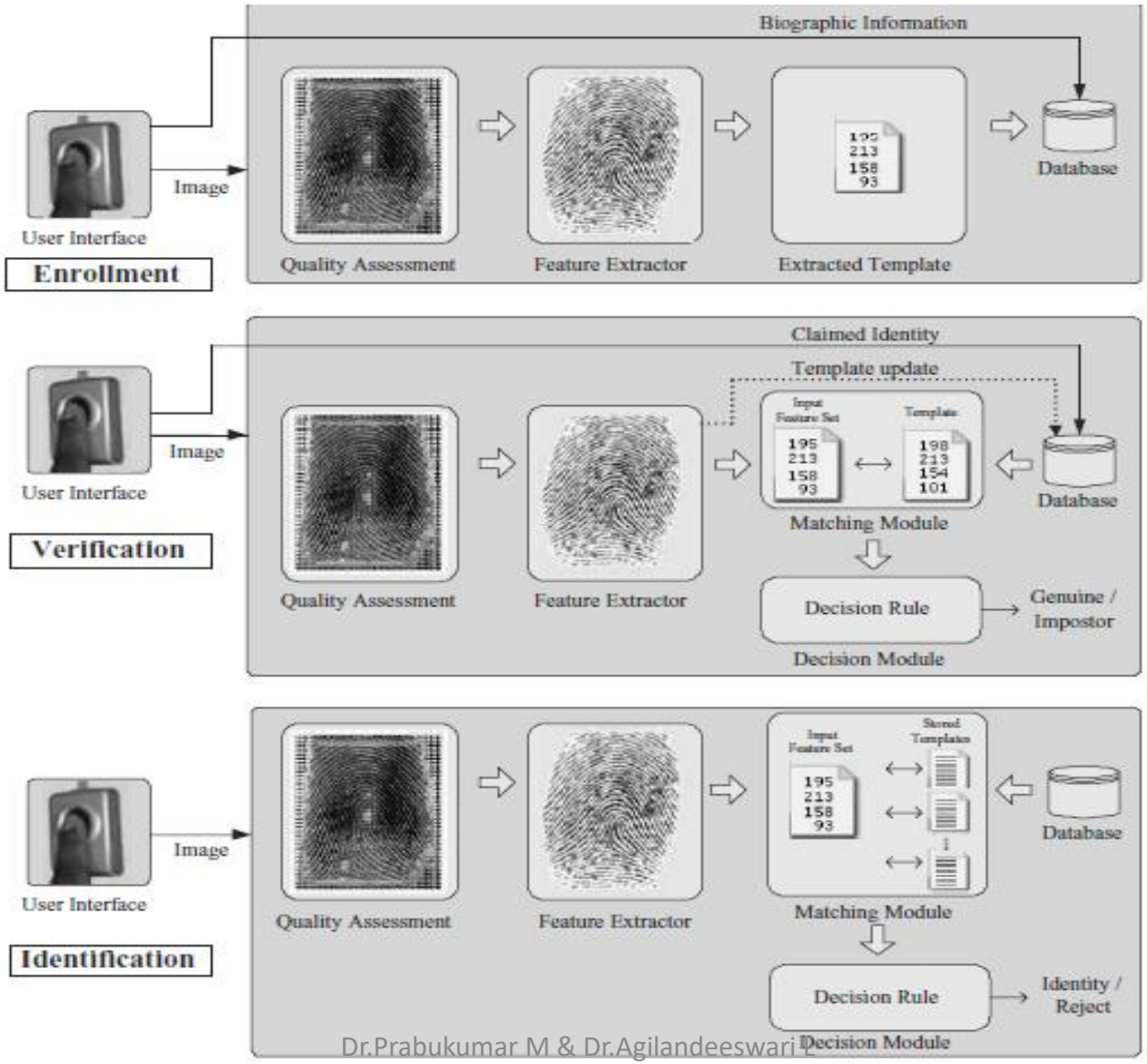
– The person claims to be ‘John’, system must match and compare his/hers biometrics with John’s stored Biometrics.

– If they match, then user is ‘verified’ or authenticated that he is indeed ‘John’

– Access control application scenarios.

– Typically referred as 1:1 matching.

Terminology Cont…



Applications

FORENSICS	GOVERNMENT	COMMERCIAL
Corpse identification	National ID card	ATM
Criminal investigation	Drivers license; voter registration	Access control; computer login
Parenthood determination	Welfare disbursement	Mobile phone
Missing children	Border crossing	E-commerce; Internet; banking; smart card

Q &A

Summary

- Introduction of Biometrics
- Operations of Biometric system
- Advantages of Biometrics
- Applications of Biometrics
- Terminology

Text Book & Reference Books

- Shimon K. Modi, Biometrics in Identity Management: Concepts to Applications, Artech House,2011
- G.R. Sinha, Sandeep B. Patil, Biometrics: Concepts and Applications ,Wiley , 2013.
- James L. Wayman, Anil Jain, DavideMaltoni, Dario Maio , Biometric Systems: Technology, Design and Performance Evaluation, Springer 2010.
- Anil Jain, Patrick Flynn, Arun Ross, Handbook of Biometrics, Springer,2008.