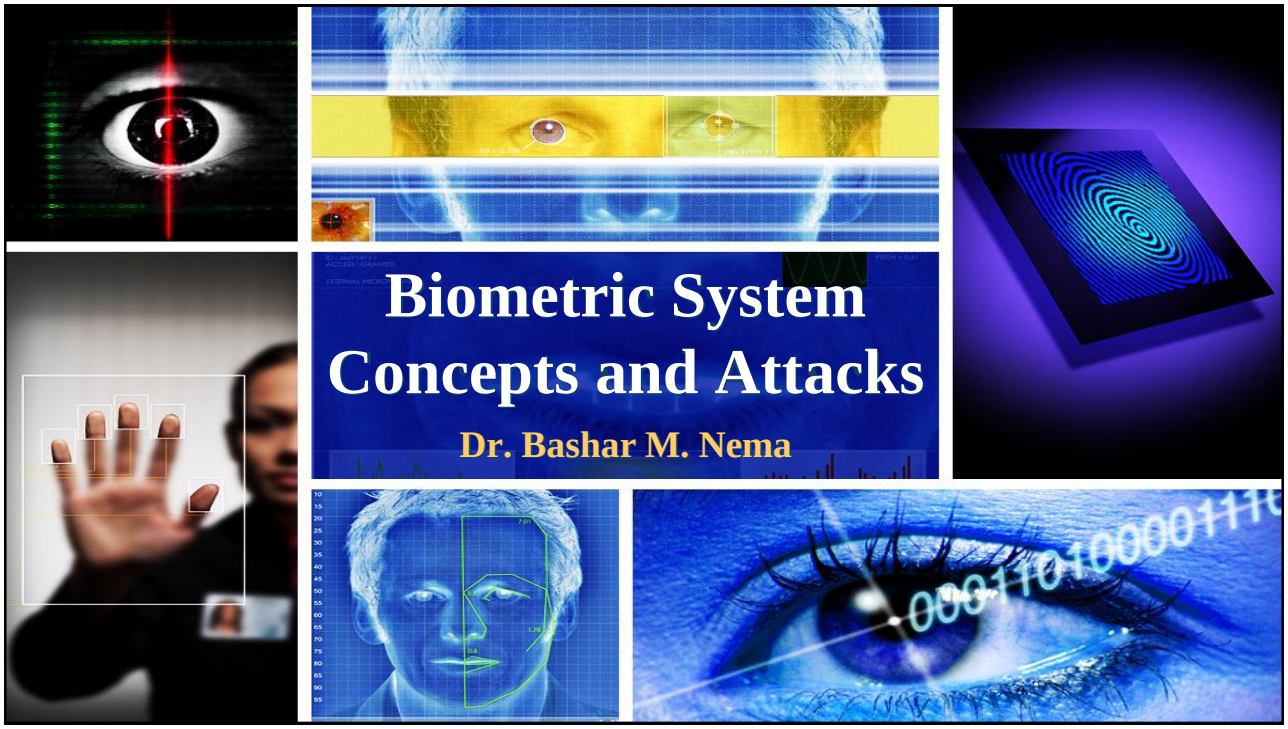
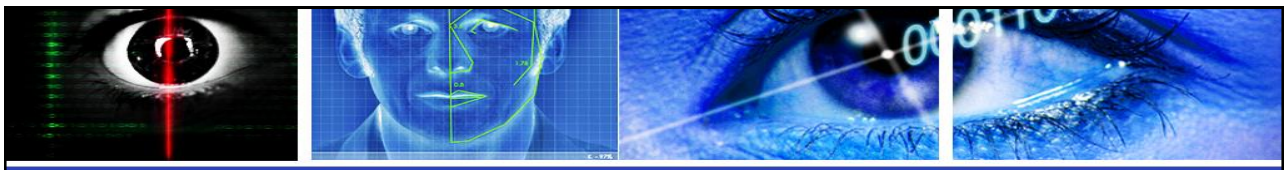


Biometric System Concepts and Attacks

Dr. Bashar M. Nema



OUTLINE

- What is Biometrics and Why need Biometrics
- Advantages of biometrics and Disadvantages of biometrics
- Biometrics Vs Privacy
- Types of biometrics
- Comparison of Biometrics
- Components of Biometric System
- Attack Points in a Biometric system
- Known Technologies To Resist the Attacks.

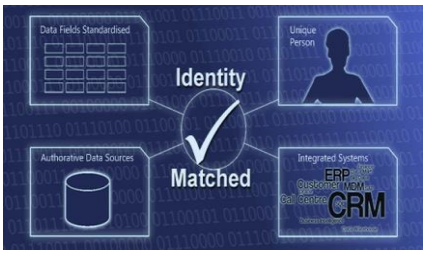
What is Biometrics

The term biometrics is derived from the Greek words bio meaning life and metric meaning to measure.

Biometrics is a multidisciplinary field concerned with

- **Representing,**
- **Measuring and**
- **Statistical analysis**

of unique physical and behavioural characteristics e.g. fingerprints, face, palm veins, etc. to be used as an individualized code for recognition.



Why need Biometrics

The need and the complexity of recognition of humans has never been in this great in our history as it is now, so that, the need for fast and accurate new technology is increasing day by day, Which are used in Verification (control access systems), or Identification (surveillance systems).

The first use of biometrics was to link between identity documents and their holders through a face photos as in a passport.

Today the Authentication by biometric verification is becoming increasingly common and an indispensable tool to overcome the difficulties being faced in security systems.

Advantages and Benefits of biometrics

- Hard to fake or steal, unlike passwords or Key.
- Fast Verify a large number of individuals in short time.
- Fast Identify the individual from a very huge number of people.
- Ease of use and convenience (Nothing to forget or lose it).
- Simple change along the user's life.(long life)
- Non-transferrable from one to another.
- Templates take up less storage space.
- Continuous authentication in behavioural identifiers.

Disadvantages of Biometrics

- It is costly to get up a biometric system and running it.
- If the system fails to capture all of the biometric data, it can lead to failure in identifying the person required.
- Databases holding biometric data can still be hacked.
- If a user gets injured or burn, then a biometric authentication system may fail to identify them.
- Errors such as false rejects can still happen.

Biometrics Vs Privacy

- Using biometrics can help to protect privacy by combating identity fraud, But it is also can reveal an element of personal privacy.
- The biometrics are not usually ‘secret’, and cannot be easily changed, destroyed or declared invalid in case it was stolen, this prevent using it again.

TWO SIDES OF A COIN

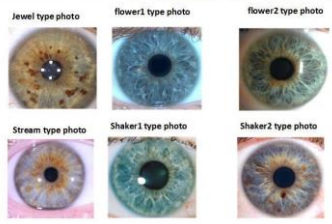
Types of Biometrics

The two main types of biometric identifiers depend on either **physiological** characteristics or **behavioural** characteristics.

- **Physiological identifiers**

relate to the unique composition of the user, include:

- **Face recognition.**
- **Fingerprints.**
- **Iris recognition.**
- **DNA matching.**

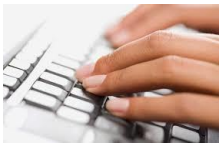


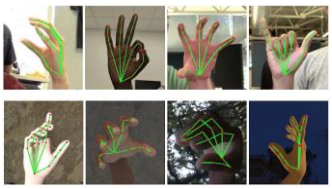
Types of Biometrics

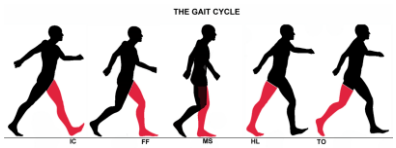
- **Behavioural identifiers**

It's the unique ways in which individuals act, including

- **Handwriting**
- **keystroke**
- **Voice recognition**
- **Walking speed**
- **Gestures.**







Comparison of Biometrics

Table 1. Comparison of biometrics

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

* The large number of factors involved makes a simple cost comparison impractical.

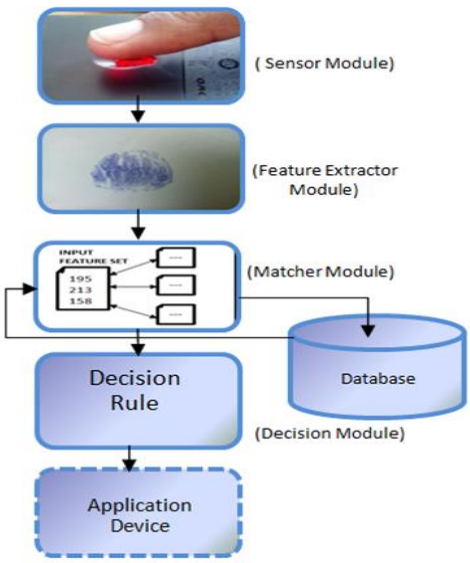
- **Verify Whether or not the Biometric is capable of verification.** Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be.
- **ID Whether or not the Biometric is capable of identification.** Identification is the process where an input is compared to a large data set previously recorded from many people to see which person the user is.
- **Accuracy How well the Biometric is able to tell individuals.** This is partially determined by the amount of information gathered as well as the number of possible different data results.
- **Reliability How dependable the Biometric is for recognition purposes.**
- **Security Level The highest level of security that this Biometric is capable of working at.**
- **Long-term Stability How Biometric continues to work without data updates over long of time.**
- **User Acceptance How willing the public is to use this Biometric.**
- **Ease of Use How easy this Biometric is for both the user and the personnel involved.**
- **Low Cost Whether or not there is a low-cost option for this Biometric to be used.**
- **Hardware Type and cost of hardware required to use this Biometric.**

Components of Biometric System

The Biometric systems have four basic modules which are:

- **Sensor module,**
- **Feature extractor module,**
- **Matcher module,**
- **Decision module.**

These four modules are necessary in any biometric system to acquire and process raw biometric data and convert it into some useful information. The block diagram of biometric system is shown in figure.

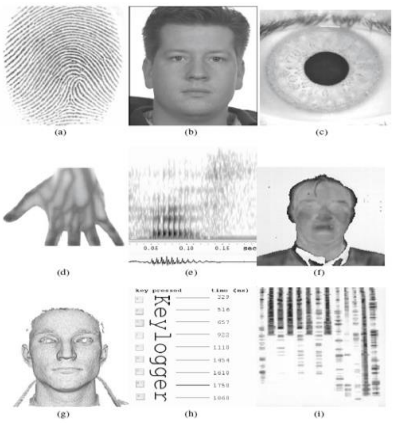


Components of Biometric System

1- Sensor Module

In this type of *module raw biometric data* is captured by the sensor and it scans the biometric trait to *convert it into digital form*.

After converting it to digital form, this module transmits the data to feature extraction module.

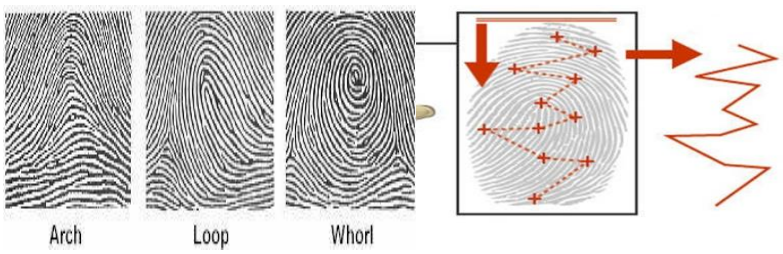


Components of Biometric System

2- Feature Extraction Module

It processes the raw data captured by sensor and generate a biometric template. It extracts the necessary features from the raw data which needs much attention because essential features must be extracted in an optimal way.

It basically removes noise from the input sample and transmits the sample to the matcher module.

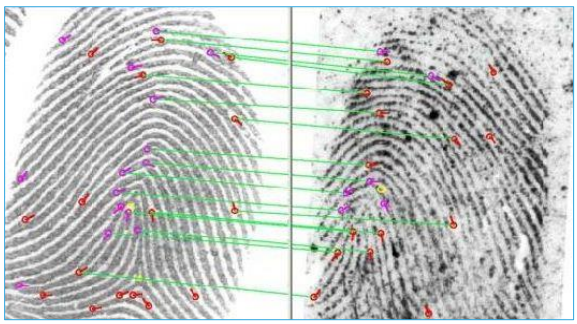


Components of Biometric System

3- Matcher Module

This module compares the input sample with the templates being stored in the database using matching algorithm and produces match score.

The Resulting Match Score is transmitted to the decision module.

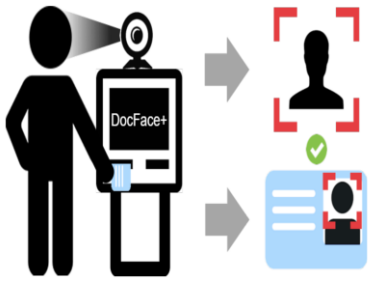


Components of Biometric System

4- Decision Module

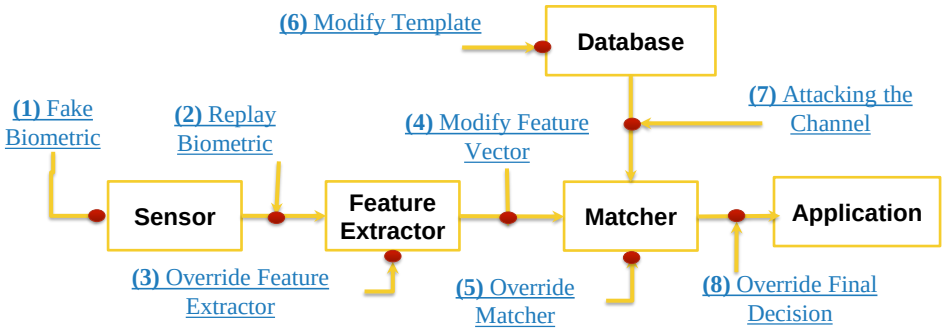
After accepting the match score from matcher module, it compares the matching score against the predefined security threshold.

If ***match score*** is greater than predefined security threshold it will accept the individual otherwise reject it.



Attack Points in a Biometric system

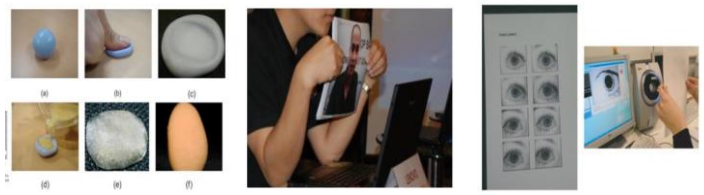
Biometric systems provide great advantages over traditional systems but they are vulnerable to attacks. There are eight attack points in biometric system which can be attacked as shown in the figure below.



Attack Points in a Biometric system

(1) Fake Biometric

In this type of attack a ***fake biometric*** such as a fake finger or image of the face is presented at the sensor.



(2) Replay Biometric

Biometric Signals In this mode of attack a recorded signal is replayed to the system bypassing to the sensor.

Attack Points in a Biometric system

(3) Override Feature Extractor

The feature extractor is forced to produce feature sets chosen by the attacker, instead of the actual values generated from the data obtained from the sensor.

(4) Modify Feature Vector

The features extracted using the data obtained from the sensor is replaced with a different fraudulent feature set.

(5) Override Matcher

The matcher component is attacked to produce pre-selected match scores regardless of the input feature set.

Attack Points in a Biometric system

(6) Modify Template

Modifying one or more templates in the database, which could result either in authorizing a fraud or denying service to the person, associated with the corrupted template.

(7) Attacking the Channel

Data traveling from the stored template to the matcher is intercepted and modified in this form of attack.

(8) Override Final Decision

Here the final match decision is overridden by the hacker disabling the entire authentication system.

Known Technologies To Resist the Attacks

1- Liveness Detection Mechanisms

Liveness detection can be used to thwart the attacks at attack **point 1** (attacking the sensor). Liveness detection refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artifact. Using extra hardware to acquire life signs like:

1- pulse detection

2- blood pressure

2- thermal measurement;

4- head, face, eye and pupil movement

Known Technologies To Resist the Attacks

2- Steganographic and Watermarking Techniques

Steganographic and Watermarking techniques are used to resist attacks at the attack **points 2 and 7** (Channel between the sensor and feature extractor and also the channel between the stored template and the matcher).

3- Soft biometrics

Soft biometrics can be used to thwart attacks at attack **points 1 and 8** (attacks on the sensor and decision-maker). Soft Biometric traits are those characteristics that provide some information about the individual but lack the distinctiveness or permanence to sufficiently differentiate any two individuals (gender, ethnicity, age, height, weight, etc).

Known Technologies To Resist the Attacks

4- Multi-modal Biometric Systems

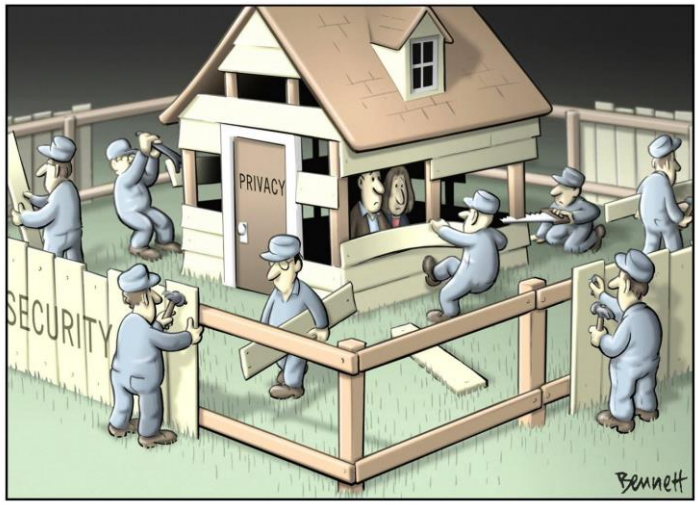
Multi-modal biometric systems can be used to resist spoofing attacks (attacks at **point 1**). Multi-modal Biometric systems use multiple representations of a single biometric, a single biometric with multiple matchers or multiple biometric identifiers.

The next table gives a comparison of the advantages and drawbacks of the different techniques to prevent attacks.

Table : Advantages and drawbacks of the different protection techniques.

Technique	Advantages	Drawbacks
Liveness Detection	Resists spoofing attacks.	Increased cost for the extra hardware and software, user inconvenience and increased acquisition time.
Watermarking	Prevents replay attacks and provide integrity of the stored templates.	Problem of image degradation and lack of algorithms to deal with it.
Soft Biometrics	Provides improved performance through filtering and tuning of parameters.	Lack of techniques for automatic extraction of soft biometric techniques.
Multi-modal Biometrics	Improves performance, resists spoofing and replay attacks and provides high population coverage.	Increased system complexity, computational demands and costs.

The last word



The last word

The last word

The last word