Biometrics Recognition Technology

A. H

lec.1-selected topics

Biometric Recognition

- Biometric recognition is the science of establishing the identity of a person based on physical or behavioral attributes.
- It is a rapidly evolving field with applications ranging from securely accessing one's computer to gaining entry into a country.
- While the deployment of large-scale biometric systems in both commercial and government applications has increased the public awareness of this technology,

Biometric Technologies

- Biometric technologies are fetching the establishment of an extensive array of extremely safe recognition and personal authentication solutions.
- As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometric-based solutions are proficient to offer for confidential financial transactions and personal data privacy.
- The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications

Biometric Recognition

- Utilized biometrics alone or integrated with other technologies such as smart cards, encryption keys and digital signatures.
- Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs).
- This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

Properties of Biometric

The properties of biometric use can be divided into two main categories:

1- Physiological link

2- Behavioral link

Physiological related to body shape and examples:

Fingerprints, facial recognition, DNA, hand geometry and iris.

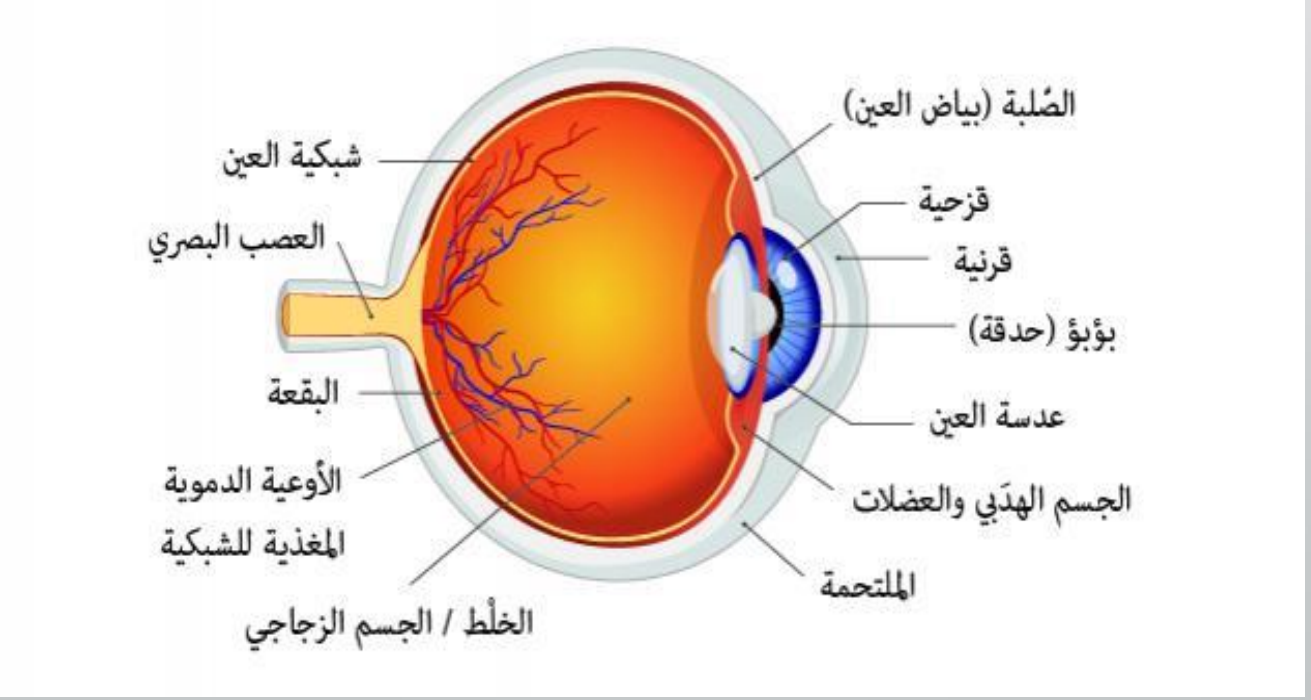
Behavioral and similar to it: writing rhythm, gait and sound.

Eye Print

- It is one of the best security methods to verify the identity of people as it is the easiest to apply to people from other types of fingerprints.
- The eye has a fingerprint where there are no similar eyes in all, where the eye is taken by looking at the lens of the device, which in turn take a picture of the retina.
- Type of a eye print

  1-fingerprint iris

  2-fingerprint retina



Iris

- Iris based biometric, involves analyzing features found in the colored ring of tissue that surrounds the pupil.
- Iris scanning, undoubtedly the less intrusive of the eye related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader.

Retina

- Retina based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina.
- Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device.

Advantages of fingerprint iris

1. Fixed does not change for life.

2. In the human eye, there are no identical probes even in identical twins.

3. The individual does not need to be close to the lens because he can only look at the camera Thirty centimeters away.

4. High accuracy with ease of use.

Disadvantages of iris

- 1. It can not be applied to individuals who are blind or infected in their eyes.
- 2. Can not be easily included in personal tools such as mobile phone or car
- 3. Not being able to easily use them in forensic evidence if they do not leave an impact.

Advantages of the retina

1. Not sensitive to environmental factors.
2. Easy and quick to use.
3. Safe.
4. Low cost

Disadvantages of the retina

1. the eye position is very close to the lens of the device
2. Looking directly at the lens.
3. Focus on light in terms of capturing the retinal camera through the pupil

Fingerprint

- Fingerprint looks at the patterns found on a fingertip.
- There are a variety of approaches to fingerprint verification.
- Some emulate the traditional police method of matching minutiae;
- others use straight pattern-matching devices;
- and still others are a bit more unique, including things like patterns and ultrasonic.
- Some verification approaches can detect when a live finger is presented; some cannot.

Hand Geometry

- Hand Geometry involves analyzing and measuring the shape of the hand. This biometric offer a good balances of performance characteristics and is relatively easy to use
- Organizations are using hand geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular.
- Ease of integration into other systems and processes, coupled with ease of use, and makes hand geometry an obvious first step for many biometric projects.

Voice Authentication

- Voice authentication is not based on voice recognition but on voice to- print authentication, where complex technology transforms voice into text.
- Voice biometrics has the most potential for growth, because it requires no new hardware — most PCs already contain a microphone.
- However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement.
- voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.

Fingerprint Sensing

- The acquisition of fingerprint images has been historically carried out by spreading the finger with ink and pressing it against a paper card. The paper card is then scanned, resulting in a digital representation. This process is known as off-line acquisition and is still used in law enforcement applications.
- Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as online acquisition.

There are three families of electronic fingerprint sensors based on the sensing technology

1- Solid-state or silicon sensors:

- These consist of an array of pixels, each pixel being a sensor itself. Users place the finger on the surface of the silicon, and four techniques are typically used to convert the ridge/valley information into an electrical signal: capacitive, thermal, electric field and piezoelectric.
- Since solid-state sensors do not use optical components, their size is considerably smaller and can be easily embedded.
- On the other hand, silicon sensors are expensive, so the sensing area of solid state sensors is typically small.

2-Optical sensors :

- The finger touches a glass prism and the prism is illuminated with diffused light. The light is reflected at the valleys and absorbed at the ridges. The reflected light is focused onto a CCD or CMOS sensor.
- Optical fingerprint sensors provide good image quality and large sensing area but they cannot be miniaturized because as the distance between the prism and the image sensor is reduced, more optical distortion is introduced in the acquired image.

3- Ultrasound sensors :

- Acoustic signals are sent, capturing the echo signals that are reflected at the fingerprint surface.
- Acoustic signals are able to cross dirt and oil that may be present in the finger, thus giving good quality images.
- On the other hand, ultrasound scanners are large and expensive,

  and take some seconds to acquire an image.

live scan devices

- A new generation of touch less live scan devices that generate a 3D representation of fingerprints is appearing.
- Several images of the finger are acquired from different views using a multi camera system, and a contact-free 3D representation of the fingerprint is constructed.
- This new sensing technology overcomes some of the problems that intrinsically appear in contact-based sensors such as improper finger placement, skin deformation, sensor noise or dirt.