Biometric Recognition

How it works

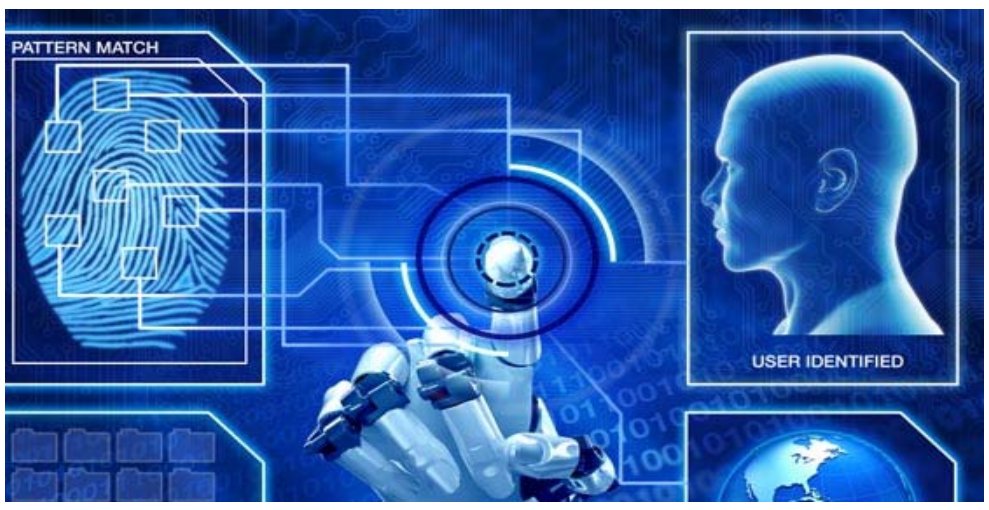
- ✓ Dedicated hardware, using provider's fingerprint or recorded voice sample to register the visit
- ✓ Hardware installed in the member's home
- ✓ Automated method of recognizing a person based on certain characteristics
- ✓ Can securely verify that a provider was on site

Advantages

+ Can securely verify that a provider was on site
+ Accurate identification and accountability
+ Convenient and versatile

Challenges

— Biometric devices are costly
— Each member must have a dedicated biometric device installed
— May be an inconvenience by the member
— Unable to verify the services provided during a visit
— Unable to document services provided
— Lacks data to optimize care delivery and coordination
— Two types of errors:
  — False Acceptance Rate (FAR)
  — False Rejection Rate (FRR)
— Unable to track individual caregiver locations in the field



Biometrics

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic if it meets the following requirements:

THESE CHARACTERISTICS MUST BE:

UNIVERSAL + **UNIQUE** + **INVARIABLE** +

so that everybody can use them | to unequivocally distinguish between different persons | to ensure they can be used throughout a person's lifetime

RECORDABLE + **MEASURABLE**

so they can be collected and stored | to enable comparisons

- ✓ ***UNIQUE-Distinctiveness*:** any two persons should be sufficiently different in terms of the characteristic.
- ✓ ***INVARIABLE-Permanence*:** the characteristic should be sufficiently invariant (with respect to matching)over time.
- ✓ ***RECORDABLE & MEASURABLE:*** *Collectability*: the characteristic can be measured quantitatively.

Additionally, other issues that should be considered are:

- ✓ ***Performance*:**
  - achievable recognition accuracy and speed
  - the resources required to achieve the desired recognition accuracy and speed
  - operational and environmental factors that affect the accuracy and speed
- ✓ ***Acceptability:***
  - which indicates the extent to which people are willing to accept a particular identifier
- ✓ ***Circumvention*:**
  - reflects how easily the system can be fooled using fraudulent methods.

A biometric system must:

1. provide adequate accuracy *2. provide adequate recognition speed*
3. meet resource requirements *4. be harmless to the users*
5. accepted by intended audience *6. resistant to system attacks*

ADVANTAGES		CHALLENGES	
ACCURACY	SECURITY	PHYSICAL TRAITS ARE UNCHANGABLE	ERROR RATE
ACOUNTABILITY	AUTHENICATION	COST	DELAY
STORAGE/RECORD MATENANCE	CONVENIENT	COMPLEXITY	UNHYGIENIC
SCALABLE	FLEXIBLE	SCANNING DIFFICULTY	PYHSICAL DISABILITIES
TRUSTIBLE	MONEY SAVING	ENVIRONMENT & USEAGE MATTERS	ADDITIONAL HARDWARE INTEGRATION

How Tech Devices Can Read Your Body

Facial Recognition
- 3D infrared scanning in future products
- 2D face-scanning appears in some devices

Iris Scanning
- Based off unique vascular patterns
- Some current smartphones have it

Ear Scanning
- Like fingerprints, enduring and unique
- Available for enterprise

Voice Recognition
- Could recognize speech patterns
- Used by some financial companies

Heartbeat Monitoring
- Electrodes on watch detect heartbeat
- Banks have shown interest

Vein Mapping
- Maps unique configuration of veins in arm
- Requires active blood flow

Fingerprint Sensor
- Common in modern smartphones

Gait Analysis
- Could be used to identify thief
- Relatively innacurate, currently in development

science FRIDAY

FINGERPRINT RECOGNITION

Advantages

- Fingerprints have been used for personal identification and the matching accuracy is very high
- A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, formed during the first seven months of fetal development.
- Fingerprint biometric recognition has become affordable and adequate to verify an individual.
- Multiple fingerprints of a person provides an even higher level of recognition and verification since no 2 finger prints are the same even those of identical twins.

Challenges

- Current fingerprint recognition systems require a large amount of computational resources, especially when operating in the identification mode.
- Fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

IRIS RECOGNITION

- Is an automated method of biometric identification that uses mathematical pattern-recognition techniques on images video of one or both of the irises of an individual's eyes,
- The complex patterns are unique, stable, and the detail-rich, intricate structures of the iris which are visible externally can be seen from some distance .
- The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation.

Caution: ***Retinal scanning is a different, ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition.***

Advantages

- The iris is the colored part of the eye, behind the cornea.
- It is formed before birth and its appearance changes very little during a person's life.
- A person's right iris is as different from the left iris as it is from another person's iris. And the irises of identical twins are as different from each other as are the irises of two persons chosen at random. This distinction makes iris recognition a very reliable identification technique. even if the person concerned is wearing glasses or contact lenses.
- Additionally, besides its speed of matching and its extreme resistance to false matches, is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

- The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound.
- These physiological characteristics change over time due to age, medical conditions (such as a common cold), and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification.

ADVANTAGES

- Speech **recognition** is the ability to recognize spoken words only and not the individual **voice** characteristics
- The software behind **voice recognition** analyzes data from actual interactions to improve its performance. ...
- Most **voice** systems are more than 97 percent accurate in identifying individual words.
- Voice modules are harder to hack
- In a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

CHALLENGES

- Speech features are sensitive to a number of factors such as background noise.
- Speaker recognition is most appropriate in phone-based applications
- Voice signal over phone is typically degraded in quality by the microphone and the communication channel.

IDEMIA WEBSITE (HTTPS://WWW.IDEMIA.COM)

Facial Recognition

✓ A facial recognition system is a technology capable of identifying or verifying a person from a digital image a video frame from a video source.

✓ There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database.

✓ Facial recognition is a Biometric Artificial Intelligence based application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape.

✓ It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

Advantage

- Facial recognition software is capable of identifying an individual according to facial morphology
- The system is designed to identify individuals among the crowds in airports, multiplexes, and other public places without passers-by even being aware of the system.

Challenges

- Its effectiveness depends on several key factors. including the quality of the captured image, the power of the identification algorithms (which compare, for example, spacing between the eyes)
- Reliability of the databases is dependent on the size of the database used (for example: the bigger the database, the greater the probability of identifying a person)
- Face recognition may not be the most reliable and efficient because of the following:
- Quality measures are very important in facial recognition systems as large degrees of variations are possible in face images
- Factors such as illumination, expression, pose and noise during face capture can affect the performance of facial recognition systems
- It has the highest false acceptance and rejection rates
- Questions have been raised on the effectiveness of face recognition software in cases of railway and airport security.

Some final thoughts about potential privacy violations: Civil rights right organizations (i.e. Electronic Frontier Foundation, Big Brother Watch and the ACLU) express concern that privacy is being compromised by the use of surveillance technologies and that it could lead to a "total surveillance society,"