Community and Public Health Nursing
Vol. 3 No. 3, September - December 2018
DOI: http://dx.doi.org/10.21088/cphn.2455.8621.3318.6

Biometrics: A New Era in Health Care

Jinu K. Rajan

Abstract

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. In the mid to late 90s there was often confusion like this in the media when "biometrics" was used by the security and the pharmaceutical/medical world. Biometrics covers a variety of technologies in which unique identifiable attributes of people are used for identification and authentication. These include (but are not limited to) a person's fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals seeking to control access to computers, airlines, databases and other areas which may need to be restricted. Every medium of authentication has its own advantages and shortcomings. With the increased use of computers as vehicles of information technology, it is necessary to restrict unauthorized access to or fraudulent use of sensitive/personal data. Biometric techniques being potentially able to augment this restriction are enjoying a renewed interest.

Keywords: Biometrics; Health Care; Technology.

Introduction

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioral traits.

- *Biometric identification* consists of determining the identity of a person. The aim is to capture an item of biometric data from this person. It can be a photo of their face, a record of their voice, or an image of their fingerprint. This data is then compared to the biometric data of several other persons kept in a database.

Author's Affiliations: Assistant Professor, Department of Nursing, College of Applied Medical Sciences, Majmaah University, Kingdom of Saudi Arabia.

Corresponding Author: Jinu K Rajan, Assistant Professor, Department of Nursing, College of Applied Medical Sciences, Majmaah University, Kingdom of Saudi Arabia.

E-mail: jinukrajan@rediffmail.com

Recived on 14.10.2018, **Accepted on** 31.10.2018

- *Biometric authentication* is the process of comparing data for the person's characteristics to that person's biometric "template" in order to determine resemblance. The reference model is first store in a database or a secure portable element like a smart card. The data stored is then compared to the person's biometric data to be authenticated. Here it is the person's identity which is being verified.

As technology becomes a pivotal part of our everyday lives, we are increasingly willing to provide personal information in exchange for a more effortless and interactive experience.

History

- The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing.
- Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago.

- Biometrics addresses a *longstanding concern* to be able to prove one›s identity, irrefutably, by making use of what makes one different. Going as far back as prehistoric times, man already had a feeling that certain characteristics such as the trace of his finger were sufficient to identify him, and he "signed" with his finger.
- In the second century B.C., the Chinese emperor Ts'In, was already authenticating certain seals with a fingerprint.
- In the 19th century, Bertillon took the first steps in scientific policing. He used measurements taken of certain anatomical characteristics to identify reoffending criminals, a technique which often proved successful, though without offering any real guarantee of reliability.
- This budding use of biometrics was then somewhat forgotten, only to be rediscovered by William James Herschel, a British officer, to be used for an entirely different purpose. Having been put in charge of building roads in Bengal, he had his subcontractors sign contracts with their fingerprints. An early form of biometric authentication and a sure way of being able to find them more easily if they defaulted.
- In the UK, the Metropolitan Police started the use of biometrics for identification in 1901.
- During World War II allied forces used the same method to identify senders and authentication messages they received.
- True biometric systems began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems. The nascent field experienced an explosion of activity in the 1990s and began to surface in everyday applications in the early 2000s.

Types of Biometrics

All biometric modalities are basically two types; physiological and behavioral. Physiological biometrics includes fingerprint, iris, face, palm vein recognition etc. Behavioral biometrics includes signature and voice recognition. However, the known types of biometrics are following:

1. Fingerprint Recognition

Fingerprint recognition technology has been done by taking a photograph of an individual's fingertips and record the characteristics including whorls, arches, and loops of the fingertip. It also captures the patterns of ridges, furrows, and minutiae for accurate analysis.

The process can be done in three ways:

- Minutiae based
- Correlation based
- Ridge feature based

The fingerprint is a very secured, reliable and stable biometric solution. Law enforcement agencies have been using this technology for decades to identify criminals. Currently, this technology is becoming popular in household security, banking, workforce management etc.

2. Iris Recognition

Many recognize Iris recognition as the best biometric technology for identification. It analyzes the iris characteristics including rings, furrows, freckles that is situated in the colored tissue around the pupil. The iris scanner that contains a video camera and works through glasses and contact lenses.

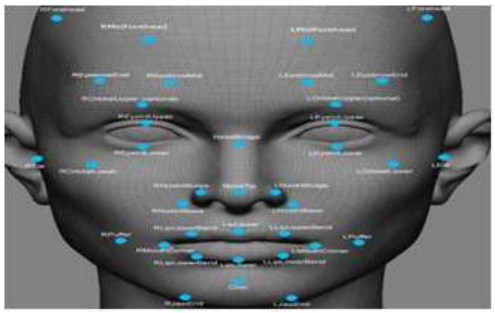
Generally, iris recognition can be done by two methods:

- Daugman System and
- Wildes System

Iris recognition is deployed by many countries in crucial places like border crossings, banking, private companies, institutes, law enforcement agencies etc.

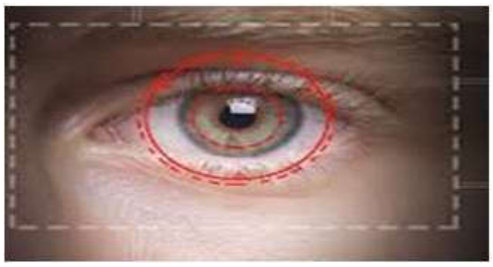
3. Face Recognition

Face recognition technique records face images through a digital video camera and analyses facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These measurements are broken into facial planes and retained in a database, further used for comparison.Then, the system creates a template on the database for that person to compare the data for further uses.



4. Retina Recognition

Retina recognition is a biometric modality that uses infrared technology to capture the unique patterns of an individual's retina blood vessels. As an internal organ of the eye and protected from external environments, retina recognition is recognized as a reliable biometric authentication system.

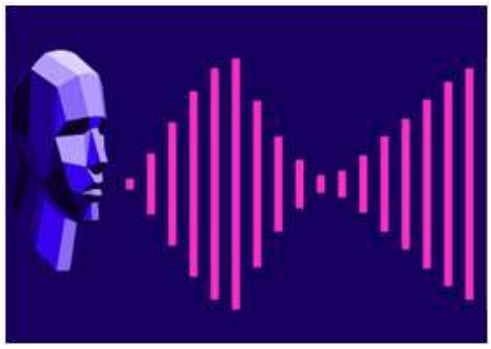


5. Hand Geometry

Hand geometry recognition works with the shape of a person's hand characteristics. The hand geometry reader measures an individual's hand in several dimensions. Then, it stores the data for further comparison and measurement. It is mostly popular for its comfort, easiness, and public acceptance. Nevertheless, this system isn't very unique as like face or fingerprint recognition.

6. Voice/Speech Recognition

Voice/speech recognition is a combination of physiological and behavioral biometrics. It works with speech patterns that capture by speech processing technology. This system analyzes the fundamental frequency, nasal tone, cadence, inflection, etc. to recognize a person's speech. It is also known as "automatic speech recognition" (ASR), "computer speech recognition", "speech to text" (STT) etc.



7. Palm Vein Recognition

Pam vein recognition is one of the physiological types of biometrics that analyzes the unique patterns of the vein in the palms of an individual's hand. As like other biometric technology, at first it captures an image of the individual's palm, then analyze and process the vein data and store it for further comparison.

8. Signature Recognition

Signature recognition is one of the behavior *types of biometrics.* It works in two ways, static and dynamic. In this recognition system, the way an individual signs his name is counted as the characteristic of that person. It is based on metrics like number of interior contours and number of vertical slope components.

9. Handwritten Biometric Recognition

Handwritten biometric recognition is close to signature recognition and undoubtedly a behavior type of biometrics. It is a system of recognizing a person by his handwriting procedure. As like signature recognition it can also be categorized in two parts, static and dynamic.

10. DNA Recognition

DNA biometric is quite different from standard biometric modalities. It requires tangible physical sample and couldn't be done in real time. It is a recognition technology with very high accuracy.

11. Ear Biometrics

Ear biometrics is one of the most accurate types of biometrics to authenticate a person. Some believe that it provides more accurate result than fingerprint and will be the future of biometrics.

12. Gait Recognition

Gait recognition is a biometric technology method that analyzes an individual by how the way they walk like saunter, swagger, sashay etc. This technology is highly suitable for surveillance analysis.

13. Odour Recognition:

A quite strange biometric method compare to fingerprint or face recognition system. It works with the body odor of an individual for verification and identification.

14. Typing/ Keystroke Recognition:

Typing or keystroke recognition is one of the behavioral types of biometrics. It analyzes the way a person press the keys to type something. The keystroke dynamics uses the data of the manner and the rhythm an individual types on a keyboard.

15. Finger Vein Recognition

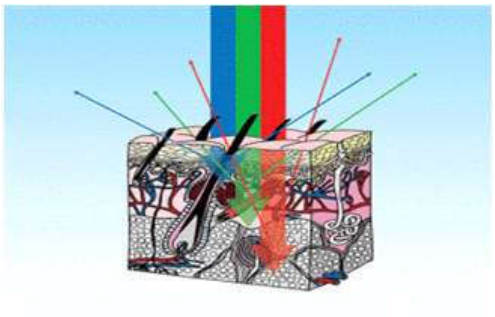
Finger vein recognition is a method of biometric identification that works with the patterns of finger vein underneath the skin's surface. It matches with the vascular pattern of an individual's finger to previously acquired data.

16. Eye Vein Recognition

Eye vein recognition is a type of biometric method that helps pattern-recognition techniques to video images of the veins of an individual's eye. The veins are complex and unique that makes it one of the most accurate biometric authentication systems.

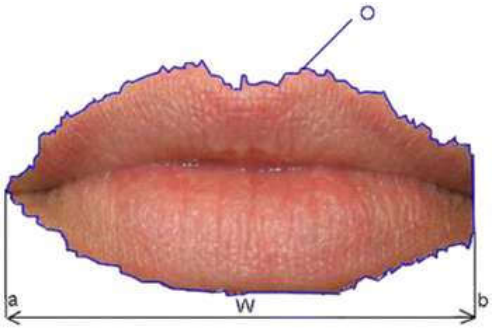
17. Skin Reflection

Skin reflection biometric is quite uncommon biometric modality. In this system, several LEDs send light at various wavelengths into the human skin and photodiodes read the scattered light that is analyzed to perform the authentication.



18. Lip Motion

Lip motion technology analyzes a person's lip motions and creates a password according to the activity. Then it verifies the data with previously stored data with new lip motion data. Compared to other biometric modalities lip motion technology is quite a new modality.

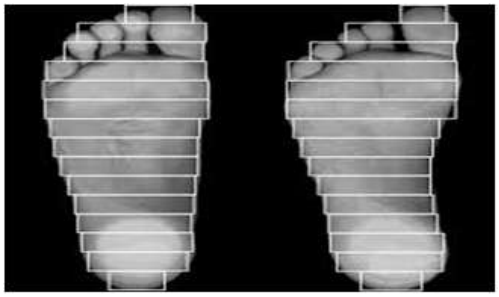


19. Brain Wave Pattern

Brainwave recognition is a unique and surprising biometric modality. It measures the signals given by the brain to create a unique individual feature set on the database. Some researchers believe that it is a hundred percent accurate biometric identification process.

20. Footprint And Foot Dynamics

As like fingerprint, finger vein, palm vein, iris and retina recognition, footprint can also be a unique physiological type of biometric identification. It is relatively new biometric identification system compares to other modalities. This system captures the footprint based biometric identification characteristics of an individual, then store the data in a database for further comparison to verify the person.



21. Thermography Recognition:

Facial thermography uses Infrared cameras to capture the flow of blood beneath the skin of an individual. Then, the underlying pattern generates a robust biometric characteristic for positive identification.

- This technology can be used to test "liveness" of an individual.
- These are the common types of biometrics available right now.
- As researchers are working hard to find more and more accurate biometric modalities to make this system more comfortable for the users, we are going to get a lot more solutions in coming future.

Components of biometric devices include

- A reader or scanning device to record the biometric factor being authenticated.
- Software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data
- A database to securely store biometric data for comparison.
- Biometric data may be held in a centralized database, although modern biometric implementations often depend instead on gathering biometric data locally and then cryptographically hashing it, so that authentication or identification can be accomplished without direct access to the biometric data itself.

Uses of biometrics in today's society

Companies and government agencies are increasingly using biometrics systems in a variety of applications including identification, personalized experiences or surveillance. The uses for biometrics are vast and benefit not only commercial organizations, but also governmental agencies and service providers. These groups are turning to biometrics for identification or surveillance purposes

- These applications are predominantly introduced by national authorities, as the biometric enrollment and management of a population›s biometric data call for a tightly regulated legal and technical framework.
- Law enforcement biometrics is referring to applications of biometric systems which support law enforcement agencies. This category can include criminal ID solutions such as Automated Fingerprint (and palm print) Identification Systems (AFIS). They process, store, search and retrieve, fingerprint images and subject records.
- Today Automated Biometric Identification Systems (ABIS) can create and store biometric information that matches biometric templates for face, finger, and iris.
- Live face recognition - the ability to do face identification in a crowd in real-time or post-event - is also gaining interest for homeland security – in cities, airports and at borders.
- Biometrics and border control-This application has been most widely deployed to date is the electronic passport (e-passport), particularly with the second generation of such documents also known as biometric passports, on which two fingerprints are stored in addition to a passport photo.
- Biometrics provides irrefutable evidence of the link between the document and its holder.
- Biometric authentication is done by comparing the fingerprint(s) read with the fingerprints in the passport micro-controller. If both biometric data match, authentication is confirmed.

- Identification, if necessary, is done with the biographic data in the chip and printed.
- Another advantage of this solution is that it speeds up border crossing through the use of scanners, which use the principle of recognition by comparison of the face and/ or fingerprints.
- In addition, many countries have set up biometric infrastructures to *control migration flows* to and from their territories.
- Fingerprint scanners and cameras at border posts capture information that help identify travelers entering the country in a more precise and reliable way. In some countries, the same applies in consulates to visa applications and renewals.
- Data acquisition requires reliable equipment to ensure optimum capture of photos and fingerprints, essential for precision during comparison and verification.
- Healthcare and subsidies-The health insurance card is used in hospitals, pharmacies and clinics, to check social security rights whilst protecting the confidentiality of personal data. Checks are performed using terminals with fingerprint sensors.
- Civil Identity, population registration and voter registration-AFIS databases (Automated Fingerprint Identification System), often linked to a civil register database, ensure the identity and uniqueness of the citizen in relation to the rest of the population in a reliable, fast and automated way. They can combine digital fingerprints, a photo and an iris scan for greater reliability.
- Civil identity and population registration-India's Aadhaar **project** is emblematic of biometric registration. It is by far the world's largest biometric identification system and the cornerstone of strong identification and authentication in India.
- Voter registration-Biometrics can also be key for the "one person, one vote" principle. To know more on this aspect please visit our web dossier on biometric voter registration

Why is biometrics controversial?

- Biometrics offer many advantages (to strongly authenticate and identify) but is not without controversy. This is linked to privacy and citizen's ability to really control information about him/her.
- The use of biometric data to **other ends** than those agreed by the citizen either by service providers or fraudsters. As soon as biometric data is in the possession of a third party, there is always a risk that such data may be used for purposes different to those to which the person concerned has given their consent
- There may thus be cases of unwanted end use if such data is interconnected with other files, or if it is used for types of processing other than those for which it was initially intended.
- The risk on the biometric database and data presented for biometric check. The data can be captured during their transmission to the central database and fraudulently replicated in another transaction.
- The result is a person losing control over their own data which poses major risks in terms of privacy.
- In practice, data protection authorities seem to give preference to solutions which feature decentralized data devices.

Benefits of using biometrics in hospitals and healthcare

Increase patient safety

Secure identification through biometric devices brings patient safety to a higher level. Errors are eradicated in the identification of the patient thus avoiding the appearance of adverse events of all types for this cause. Biometric identification through fingerprint scanner can also save lives, as it allows finding out the ailments or allergies of certain patients in cases of emergency.

More comfort for the patient

The patient can access health services in a much more comfortable way than before since he does not need to carry anything physical with him or memories the data that is necessary for his identification. In turn, the patient does not have to permanently wear uncomfortable bracelets that can cause skin irritations or other inconveniences.

Greater satisfaction with the service

Improved care processes (for example, reducing the time of all processes requiring patient identification) and more efficient and error-free information management, the quality of service

provided to the patient is improved, and patients who perceive favorable change increase their degree of service satisfaction.

More confidence and peace of mind

Patients welcome the use of the biometric system as a way to protect themselves against fraud and safeguard their identity. The new identification system guarantees the total privacy of access to the patient's confidential information respects his rights and complies with current legislation that supports the patient. The patient gains in tranquility and increases his level of confidence in the security of his personal data and the treatment of the same by the institution and the staff.

Improve your quality of life

By receiving better medical care free of medical errors and inconsistencies in the Electronic Medical History, the patient receives more successful treatments and, consequently, improves his quality of life.

Increased safety for health personnel

All health personnel benefit from greater security in the processes that require their unequivocal identification, both in the control of physical access to the facilities and in the logical access to the implanted information systems. Biometric machine eliminates the possibility of theft or fraudulent use of your passwords, as well as the possible loss of your identification cards.

- *More comfort in identification for health personnel*

Healthcare personnel do not need to memorise their passwords or carry identification cards to access hospital facilities or hospital management systems and patient information. Whenever you need to identify a patient, you can do it with great convenience, speed and agility through fingerprint scanner. Administrative staff can more quickly process such as filiation, admission or discharge of the patient.

Conclusion

The future portends a new era of biometrics. Advances to the technologies will make them more attractive to healthcare organizations. Decreasing costs will make biometrics a more palatable move. Other technologies like artificial intelligence will, in turn, also give biometrics a boost. But mainstreaming biometrics faces a variety of challenges. These include privacy, people, cost and interoperability. There's a lot of ground to cover in so experts at biometrics technology vendors, consulting firms and healthcare provider organizations shared their views on the road ahead. Biometrics can be used by various organizations to increase security levels and protect their data and patents. Biometrics although interdisciplinary, it is not the eventual choice of the masses due to its high cost and legal considerations like privacy issues. Without doubt the age of biometrics is here and the technology will directly affect everyone over the next few years.

References

1. Davide Maltoni, Durio Maio, Anil K. Jain, Salil Prabhakar, Handbook of Fingerprint Recognition, 2002.
2. http://www.oemupdate.com/experts-column/top-7-benefits-of-using-biometrics-in-healthcare-centre/.
3. https://biometrictoday.com/types-of-biometrics/.
4. https://blogs.thomsonreuters.com/answerson/biometrics-technology-convenience-data-privacy/.
5. https://searchsecurity.techtarget.com/definition/biometrics.
6. https://www.biometricsinstitute.org/definition-of-biometrics.
7. https://www.biometricsinstitute.org/types-of-biometrics.
8. https://www.biometricupdate.com/201205/biometric-terms-and-technique-classifications.
9. https://www.gemalto.com/govt/inspired/biometrics.
10. https://www.healthcareitnews.com/news/biometrics-entering-new-era-healthcare.
11. J.G. Daugman. High confidence visual recognition of persons by a test of statistical impedance. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993 Nov;15(11):1148-61.
12. Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha.