Biometrics: Human Body as a Password

Shriya Jain*
Ruby Dhaiya**
Ashi Chauhan***

Abstract

This paper examines biometry as an evolving technology. It explains the basic biometric system and their working. The characteristics of a biometric trait and the various techniques that can be used in a biometric system have also been elaborated upon. The paper also provides a comparison between the major techniques and elaborates on the applications of biometrics, specifically in India through the Aadhaar project.

Keywords: Aadhaar, Biometry, Identification, Verification, Comparison.

I. Introduction

Biometrics is the science of automatically identifying and/or verifying a person based on their physical, chemical and behavioural characteristics. It is a very convenient and almost fool proof method of ensuring the identity of a person, as biometric traits are unique to each individual and cannot borrowed, stolen or forged.

A biometrics system can be used for two purposes, namely: Identification (One to One) and Verification (One to Many). A biometrics system can be used to identify an individual with or without their knowledge. The system compares the captured biometric data of the user with the stored template of the user in the database, to verify his/her identity. It is a one to one process as a single template is compared with a single set of captured data. For example, it can be used by the government to find and individual by scanning security feeds using facial recognition or they can be used by nefarious parties to identify citizens unknowingly. A biometric system may also be used to verify the identity of an individual. It can be used by anyone to ensure that the person is exactly who they say they are. The system uses already stored templates in the database to search for a possible match among many samples. Thus it is a one to many approach. For example, usage of palm prints to grant access to secure locations or activating/deactivating locks with speech recognition.

Physiological biometric traits include retina, iris, facial characteristics, ear, palm geometry, fingerprint and DNA. Behavioural biometric traits include gait, signature, odour, voice patterns and keystroke.

Shriya Jain*
Student, Institute of Information Technology and Management, New Delhi, India

Ruby Dhaiya**
Department of IT, Institute of Information Technology and Management, New Delhi, India

Ashi Chauhan***
Student, Institute of Information Technology and Management, New Delhi, India

II. Characteristics of Biometrics Traits

For a trait to be used as biometric recognition technique, a personal trait must have some attributes that ensure that it is apt to be used in a biometric system. These characteristics are:

A. Acceptable

Taking samples of the attribute should be acceptable to the public and must not violate their dignity in any manner.

B. Comparable

The biometric trait should be able to provide a sample that can be effectively compared with other samples of the data without ambiguity.

C. Constant

For an attribute to act as an effective biometric trait, it must be invariant. The attribute should not change over time, location or chronic diseases.

D. Inimitable

The trait should be such that it cannot be forged. It is one of the most important characteristic as it ensures the security of the biometric system. The trait should not be reproducible.

E. Not violate privacy

The attribute should not violate the privacy of anyone in any manner. For the attribute to be accepted worldwide and have co-operating participants it must respect the privacy of users.

F. Quantifiable

The attribute should be capable of being measured so as to be useful in comparison of samples. It should not be an infinite or abstract value.

G. Reducible

The trait should be such that it can be reduced to a series of data that can be stored on files and used for analysis.

H. Reliable

The trait should be difficult to manipulate and prove to be a reliable source of identification.

I. Uniqueness

Each instance of the attribute must be singular to the individual. It should not be found in any other individual and should have enough unique properties to be distinguishable from the sample of other individual.

J. Universal

The trait should be possessed by each and every individual. It rules out any special features that only a select number of people may have, for example a sixth finger.

III. Operation of Biometric Systems

Although each biometric system is configured according to the biometric trait(s) it uses, the general working and operations of a biometric system remain the same. There are four main modules involved in the working of a biometric system, namely: Sensor Module, Feature Extraction Module, Comparison Module and Decision Making Module. Sensor module consists of the physical hardware or sensors that capture the biometric data from the user. For example, the iris scanner or the voice recorder. The Feature Extraction Module deduces a specified feature set from the data captured by the Sensor Module. Each individual set of biometric data needs to be able to provide the specified feature set for the data to be accepted as a valid sample. The comparison or matching module compares the features extracted by the previous module with the ones already stored in the database. This module only provided the hard facts about the similarities or the differences between the template and data. It does not provide any decisions. Based on the comparison done by the Matching Module, Decision Making module passes the final verdict on whether to accept or reject the user. All biometric system work on the same basic principle of capturing biometric data, identifying the salient feature set and storing the values into the database. When a user inputs some biometric data, the salient features are identified again and the samples are compared with the values in the database.

The two main operations performed in a biometric system are Enrolment and Comparison (which includes Identification and Verification).

Enrolment -This is the basic operation needed for both identification and verification purposes. This operation involves the capturing of user data for the first time. The user can enter their personal details such as name, age, designation etc. as well as provide the sample of the specific biometric trait. The quality of this sample is then checked and if found appropriate the features are extracted from the sample and stored in the database as a template. If the sample does not pass the quality check, the user needs to provide the data again.

Comparison -After enrolment when the user logs into the system, the user provides his/her biometric sample to the system. The system compares the current sample with the template in the database and passes the verdict stating whether the person is who they claim to be or not.

IV. Techniques of Biometric Sytems

A. DNA

According to Oxford Dictionary, deoxyribonucleic acid, a self-replicating material which is present in nearly all living organisms as the main constituent of chromosomes. It is the carrier of genetic information. Although a major percentage of the DNA is same for each human being, 0.10 percent of the DNA is unique for every person and can be used to identify the person. The DNA is easy to acquire and can therefore be used for nefarious purposes. There is also the fact that DNA

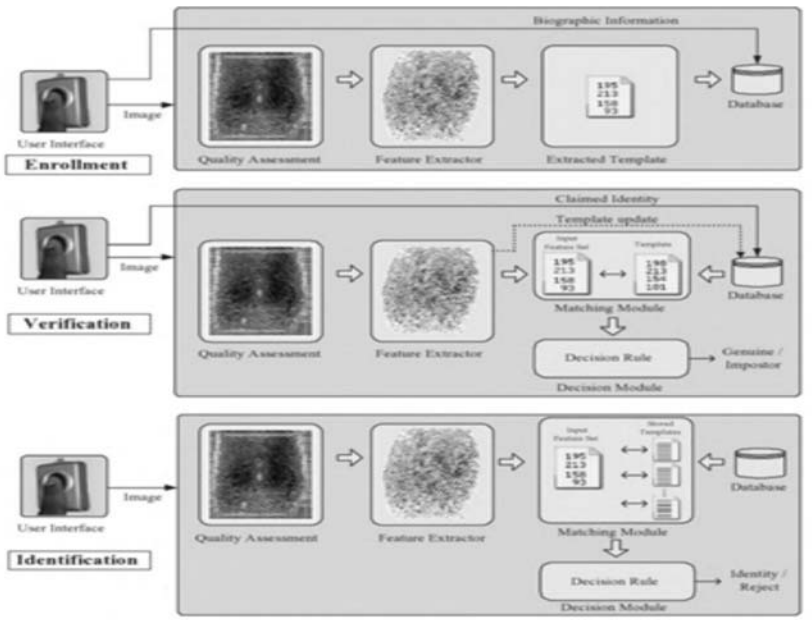

Fig. 1: Simple Biometric System

Source: Anil Jain, Patrick Flynn, Arun A. Ross. Handbook of Biometrics. Springer Science & Business Media, 2007, pp. 1-170.

is the same for identical twins thus they cannot be distinguished on a biometric system.

B. Face

Looking at a person's face is the most common way of identifying a person and is used predominantly by humans. It is one of the most non-intrusive methods of biometric detection and are therefore one of the most widely used techniques. The face recognition techniques mainly uses the location and relative position of the facial features to determine a match.

C. Fingerprint

Fingerprints have long been used as an acceptable measure of a person's identity. They are still used to identify illiterate people in many countries like India. This is therefore one of the most developed biometric technology and has proved to be quite reliable and accurate. Fingerprints are different for each individual so much so that each person has a different pattern on each of the ten fingers. It is also one of the cheapest methods and most widely used, for example it is present in laptops as well.

D. Gait

Gait, according to Oxford Dictionary, is a person's manner of walking. It is a very non-intrusive method of detection and can be used to identify an individual without his/her consent. The biometric systems using gait extract a silhouette of the human body and track it as a combination of moving points. This trait, however, is not very consistent as the way a person walks is greatly affected by his/her choice of footwear, the ground s/he is walking upon and the physical condition of their legs.

E. Hand Geometry

This technique analyses the hand in detail for things like the length and width of fingers, the gap between each finger, the shape of the palm etc. to create a template. It is an easy to use trait that is non-intrusive and not easy affected by external factors. The drawback, however, is the fact that hand geometry is not a proven distinctive feature. Compared to other traits, hand geometry is more likely to be same for two people.

F. Iris

The iris is a flat and ring-shaped membrane behind the cornea of the eye with an adjustable circular opening in the centre called a pupil. Together with the pupil, the iris is responsible for regulating the amount of light that gets into the eye[6]. The iris is a distinctive feature and is different even for identical twins.Two people cannot have the same iris pattern

Fig. 2: Face Recognition Pattern

Source: Katie Collins. (2013, July 19). Hacker gives Google Glass facial recognition using his own OS. [Online]. Available: http://www.wired.co.uk/news/archive/2013-07/19/google-glass-facial-recognition.

and there is also technology to detect natural iris from the fake contact lenses. It is one of the most effective although a little expensive technology.

G. Odour

Body odour is a distinctive smell that can be used as biometric trait. Thesis an ancient method as it has been used by the police in tracking criminals by scent using bloodhounds. Finding people by scent could usually be done be done only by animals who have a highly developed sense of smell, like dogs. Now as technology evolves odour can also be tracked by computer systems. It is a relatively new technology hence it is not very developed as sensors have yet to achieve the accuracy of a dog's sense of smell.

H. Signature

Signatures have long been used to determine the identity of an individual by authenticating the person,

Table 1: Comparison of Various Biometric Techniques

Quality / Technique	Acceptability	Comparability	Constancy	Inimitability	Non Violating	Quantifiably	Reducibility	Reliability	Uniqueness	Universality
DNA	High	High	High	High	Low	High	High	High	High	High
Face	High	Low	Low	Medium	High	Medium	Medium	Low	Low	High
Fingerprint	High	Medium	High	Medium	High	High	High	Medium	High	Medium
Gait	Low	Low	Low	Low	High	Low	Low	Low	Low	Medium
Hand Geometry	Medium	Low	Medium	Medium	High	Medium	Medium	Medium	Medium	Medium
Iris	Medium	Medium	High	High	Medium	High	High	High	High	High
Keystroke	High	Low	Low	Low	High	Medium	Medium	Low	Low	Low
Odour	Low	Low	Low	Medium	Low	Low	Low	Low	Low	Medium
Signature	High	Medium	Low	Low	High	Medium	Medium	Low	Low	Medium
Voice	High	Medium	Low	Medium	Medium	Medium	Low	Medium	Medium	High

be it on legal documents or attendance registers. The same principle can also be applied to biometrics where the signature of a person can be scanned and stored as a template that can be further compared to other samples to determine identity. However, professional forgers may be able to replicate the signature and fool the system. Signatures also change over time and are influenced by the physical and emotional state of the signatory.

I. Voice

Humans can often distinguish each other by voice; so can computers. Voice recognition is another widespread technology that is implemented in mobiles, laptops, TVs and security systems. Voice and speech recognition are cheap but forgeable traits as one can easily replicate voice via technological means. Also the fact that voice can be altered due to ailments such as sinus, make voice an inconsistent trait.

V. "Aadhar Project" Application of Biometric Systems in India

The use of biometric systems has drastically increased in the last few years as people across the globe pay more attention to security. Almost all countries have ongoing research projects on biometry to make things more secure.

The biggest application of biometry in India is the "Aadhaar" project. It is the world's largest biometric identification system with the Unique Identification Authority of India (UIDAI) issuing nearly 82 crore cards [9].The "Aadhaar" is our nation's bid to provide a unique identification to each of its citizens. An Aadhaar card is an irrefutable proof of identity for any resident of India, verifiable online anywhere, any time. While creating an Aadhaar card, a person is required to provide his/her fingerprints and iris scan. These biometric scans solidify the individual's identity ensuring that one person cannot have more than one Aadhaar card.

VI. Conclusion

Biometrics has emerged has a rapidly growing field of study today. As the security becomes more important each day and gets harder to achieve, biometrics seem to offer a viable solution. There are numerous techniques or traits that are already used as a biometric identifier and more are to come.

There are infinite areas in which biometrics can be used and has already started being used, defence, government, police, personal security are just a few examples. Although biometric systems have been researched on for quite a while now, theiruse has yet to be widespread due to their considerable disadvantages like intrusiveness and expensive technology. However, the field of biometryshows a strong promise of evolving and forever changing the outlook of data security.

References

1. Anil Jain, Patrick Flynn, Arun A. Ross. Handbook of Biometrics. Springer Science & Business Media, 2007, pp. 1-170.
2. Anil Jain, ýRuud Bolle, ýSharath Pankanti. Biometrics: Personal Identification in Networked Society. Springer Science & Business Media, 2006, pp. 2-15.
3. Anil K. Jain, Arun Rossand Salil Prabhakar. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, VOL. 14, NO. 1, 2004, January.
4. Chien Le. (2011, November 28). A Survey of Biometrics Security Systems. [Online]. Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/.
5. Filip Orság Martin Drahanský. Biometric Security Systems: Fingerprint and SpeechTechnology. Faculty of Information Technology Department of Intelligent Systems. Czech Republic.
6. Healthline Medical Team(2015, January 28). Iris [Online]. Available: http://www.healthline.com/human-body-maps/iris-eye.