International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Biometric: Types and its Applications

Shilpa Shrivastava[1]

[1]M.Tech (Information Security)
Disha Institute of Management and Technology, Nardaha, Raipur(C.G)
shilpas71991@gmail.com

Abstract: ***The term Biometrics is becoming highly important in computer security world. The human physical characteristics like fingerprints, face, hand geometry, voice and iris are known as biometrics. These features are used to provide an authentication for computer based security systems. By using biometrics a person could be identified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows" (password, PIN).In this paper, the main focus is on the various biometrics and their applications.***

Keywords: Biometrics, Biometric System, Security, Characteristics, Physiological, Behavioral.

1. Introduction

The term biometric comes from the Greek words bios (life) and metrikos (measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. It is the study of physical or behavioral characteristics used for the identification of a person [1].

The identification of a person is becoming highly important as the ID cards, punch, secret password and PIN are used for personal identification [2] .The ID can be stolen; passwords can be forgotten or cracked. The biometric identification overcomes all the above. Additional security barriers can be provided using any one of the biometrics features [3]. The features like fingerprints, face, hand geometry, voice, and iris. These biometrics features can be used for authentication purpose in computer based security systems.

For many applications of biometric, the system uses the password as well as biometrics for authentication. The biometric characteristics have been used in different applications. According to the requirement (Universal, Uniqueness, Permanence, Collectability, Performance, Acceptability, Circumvention) of the application suitable biometric can be selected. In this paper, we have presented the different types of biometrics, their applications, advantages and disadvantages.

2. Biometrics

"Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometric identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities.

2.1 Biometric System

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.[4] Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

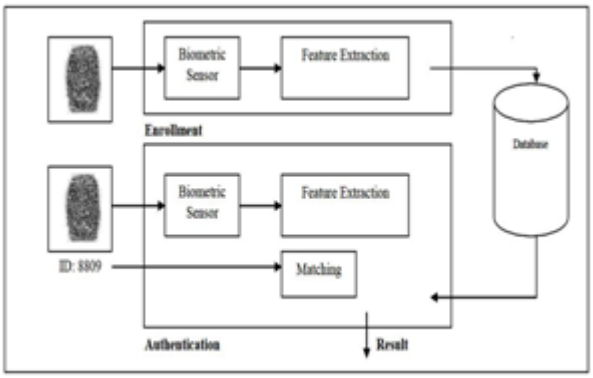

Figure 1: General Biometric System [5]

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

3. Biometric Types

Biometrics measures biological characteristics for identification or verification purposes of an individual. Since IDs and passports can be forged, more sophisticated methods needed to be put into place to help protect companies and individuals.

There are two types of biometric methods. One is called Physiological biometrics used for identification or verification purposes. Identification refers to determining who a person is. This method is commonly used in criminal investigations.

Behavioral biometrics is the other type. It is used for verification purposes. Verification is determining if a person is who they say they are. This method looks at patterns of how certain activities are performed by an individual.

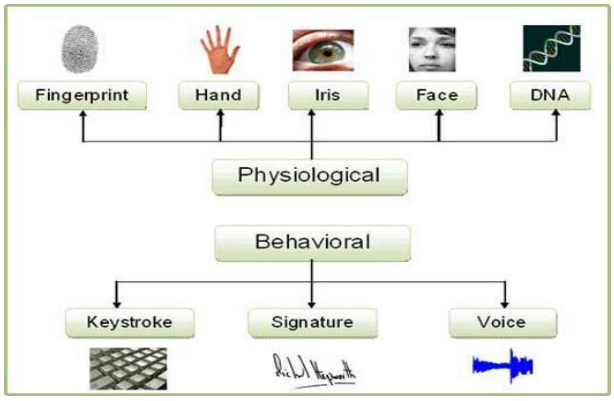

Figure 2: Biometric Classification

3.1 Physiological Type of Biometric

The physical characteristics of a person like finger prints, hand geometry, iris, face and DNA are known as biometrics. Each biometric trait has its strengths and weaknesses.

3.1.1 Fingerprints

A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [6]. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. This method is traditional and it gives accuracy for currently available Fingerprint Recognition Systems for authentication.

3.1.2 Hand Geometry

Hand geometry systems produce estimates of certain measurements of the hand such as the length and the width of fingers. Various methods are used to measure the hand. These methods are most commonly based either on mechanical or optical principle. The latter ones are much more common today. The hand geometry is used for identification and recognition of a person.

3.1.3 Iris

The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarets [7]. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away. Responses of the iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage.

3.1.4 Face

Facial recognition is the most natural means of biometric identification. The approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. As this technique involves many facial elements; these systems have difficulty in matching face images [8].

3.1.5 DNA

DNA(Deoxyribonucleic Acid) sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. As soon as the technology advances so that DNA can be matched automatically in real time, it may become more significant. At present DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being.

3.2 Behavioral type of Biometric

Behavior methods of identification pay attention to the actions of a person, giving the user an opportunity to control his actions. Biometrics based on these methods takes into consideration high level of inner variants (mood, health condition, etc), that is why such methods are useful only in constant use. It includes keystroke, signature and voice.

3.2.1 Keystroke

Keyboard- is the part that helps us to communicate with computer. People use keyboard in different ways. Some people type fast, some slow. The speed of the typing also depends on the mood of a person and a time of a day. Biometric keystroke recognition – is a technology of recognizing people from the way they are typing. It is rather important to understand that this technology does not deal with “what” is written but “how” it is written.

3.2.2 Signature

The way a person signs his or her name is known to be characteristic of that individual.Signature is a simple, concrete expression of the unique variations in human hand geometry. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

3.2.3 Voice

The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state. Voice recognition techniques are generally categorized according to two approaches: 1) Automatic Speaker Verification (ASV) and 2) Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario.

Speaker identification attempts to use voice to identify who an individual actually is.

4. Biometric Characteristic's Requirements

Physical and Behavioral characteristics should meet some requirements in order to be used as biometrics methods. These requirements are either theoretical or practical. There are basically seven theoretical requirements which includes:[9]

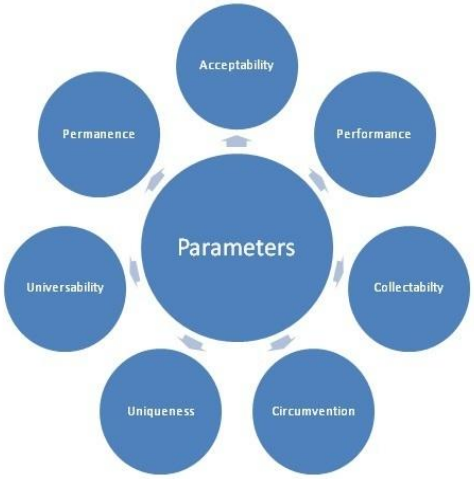

Figure 3: Biometrics requirements

4.1 Universality

Each person should have biometric characteristics. There are mute people, people without fingers or with injured eyes. It is really difficult to get 100% coverage.

4.2 Uniqueness

This means that no two persons should be the same in terms of the biometric characteristics. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users.

4.3 Permanence

It is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This means that the characteristics should be invariant with time.

4.4 Collectability

This means that the characteristics must be measured quantitatively and obtaining the characteristics should be easy.

4.5 Performance

This refers to the achievable identification/verification accuracy and the resources and working or environmental conditions needed to achieve an acceptable accuracy.

4.6 Acceptability

It will choose fields in which biometric technologies are acceptable.

4.7 Circumvention

It will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process.

5. Biometric Applications

Biometrics are an effective personal identifier because the characteristics measured are distinct to each person. Unlike other identification methods that use something a person has, such as an identification card to gain access to a building, or something a person knows, like a password or PIN to log on to a computer system, the bio-metric characteristics are integral to something a person is, since biometrics are tightly bound to an individual, they are more reliable, cannot be forgotten, and are less likely to be lost, stolen, or otherwise compromised.[10]

5.1 Fingerprints

Fingerprint biometrics have four main application areas:

- Large-scale Automated Fingerprint Imaging Systems (AFIS) that are generally used by law enforcement.
- For fraud prevention in entitlement programs.
- Physical access control (doors).
- "Logical" access to computer systems.

More recent application includes use of fingerprints for administering drugs and controlled substances to patients.

5.2 Hand Geometry

Hand geometry can be suitable for one-to-one applications where there are larger user databases and/or where users may access the system infrequently and, therefore, be less disciplined in their approach to the system. It is mostly used in

- Access control
- Time and attendance applications

5.3 Iris

Some applications of iris include

- Airline passenger screening
- Inmate identification in correctional facilities.
- Border security, facility access control, computer login, ATMs and grocery stores.

The United Arab Emirates has used an iris recognition biometric screening system for over two years to screen all arriving visa holders at their points of entry to detect previously deported persons.

5.4 Face

Unlike other biometric technologies, implementing a facial recognition system has its own set of challenges that other technologies may not experience.

Application environments for facial recognition systems can be categorized as "controlled- In a controlled environment, there is not much variation in the background conditions or

lighting" and "random- In a random environment, however, there is more variation." It can be used in areas like

- Identify card counters in casinos.
- It is applied as a tool for screening individuals to see if they are already known to the system.
- It is used for fraud prevention when individuals apply for visas or driver's licenses.

5.5 DNA

Deoxyribonucleic Acid (DNA) is the one-dimensional ultimate unique code for a person's identity with the exception of identical sibling sets (twins/triplets), which have identical DNA patterns. DNA is currently used mostly in forensics applications for identifying people.

5.6 Keystroke

One potentially useful application is computer access, where this biometric could be used to verify the computer user's identity continuously. Dynamic or ongoing monitoring of the interaction of users while accessing highly restricted documents or executing tasks in environments where the user must be "alert" at all times (for example, air traffic control) is an ideal scenario for the application of a keystroke authentication system.

- Key-stroke dynamics may be used to detect uncharacteristic typing rhythms such as those brought on by drowsiness, fatigue, etc., and alarm a third party.

5.7 Signature

Despite its user friendliness, long history, and lack of invasiveness, signature verification has not become a market leader like other biometric technologies. Some documented applications include

- Chase Manhattan Bank, the first known bank to adopt signature verification technology.
- IRS for verification purposes in tax returns that have been filed online.
- Charles Schwab & Company for new client applications.
- Most likely, the biggest market application for signature verification will be in document verification and authorization.

5.8 Voice

Although speaker verification technology has not been as widely adopted and utilized as other biometric technologies, there are indications that speaker verification could be adopted on a larger scale in the future. The voice recognition biometric systems are used in

- For access control.
- Banking.
- Government offices, Entertainment applications.
- Smart cards, PIN and other Security purposes.

6. Conclusion

The biometric systems overcomes the drawbacks of the traditional computer based security systems. The biometric recognition systems have been proved to be accurate and very effective in various applications. The biometric features can be easily acquired and measured for the processing only in the presence of a person. Many business applications such as fingerprint-based systems have been proven to be very effective in protecting information and resources in public sector units and offices. The use of biometrics raises several privacy questions such as in case of face recognition technology privacy will be wiped out. In spite of all these, it is quite sure that in future biometric based recognition will have a great influence on our daily routine and business.

References

[1] Joseph Lewis, University of Maryland, Bowie State University, "Biometrics for secure Identity Verification: Trends and Developments" January 2002. (journal style)
[2] Lia Ma, Yunhong Wang, Tieniu Tan, "Iris Recognition Based on Multichannel Gabor Filtering", ACCV2002: The 5th Asian Conference on Computer Vision, 23-25 January 2002, Melbourne, Australia. (journal style)
[3] Muhammad Khurram Khan, Jiashu Zhang and Shi-Jinn Horng, "An Effective Iris Recognition System for Identification of Humans", IEEE 2004. (journal style)
[4] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42. (journal style)
[5] K P Tripathi, International Journal of Computer Applications (0975 –8887) Volume 14–No.5, January 2011. (journal style)
[6] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, August 2002, pp. 744-747. (journal style)
[7] J. Daugman, "How Iris Recognition Works", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 21-30, January 2004. (journal style)
[8] Steve Lawrence C. Lee Giles Ah Chung Tsoi, Andrew D. Back, "Face Recognition: A Convolutional Neural Network Approach", IEEE Transactions on Neural Networks, Special Issue on Neural Networks and Pattern Recognition. (journal style)
[9] Schuckers, 2001] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001. (journal style)
[10] Biometric technology application manual, volume : (I), Biometric Basics compiled by: National Biometric Security Project Updated Summer 2008.(e-book chapter style)

Author Profile

Shilpa Shrivastava Student of M.Tech (Information Security) from Disha Institute of Management and Technology. She has received the Bachelors of engineering degree in (Information Technology) from Shri Shankara Charya Institute of Professional Management and Technology in2013.