International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 8 No. 2 Sep. 2014, pp. 743-749

http://www.ijias.issr-journals.org/

Biometrics: A Security Tool for 21st Century

Sarita Salawadgi

Department of Computer Science & Engineering,
SECAB Institute of Engineering & Technology,
Bijapur, Karnataka, India

ABSTRACT: In today's internet world the need for automated security system is critical and challenging issue. The biometric can play a major role in maintenance of information security and authentication in computing systems. The computing system requires reliable authentication and recognition of individual for confirming the identity. A biometric system recognizes an individual based on his/her physical or behavioral features which are unique. By using biometrics we can verify that the users are in fact who they claim to be. In this paper we compare and discuss various biometric traits and techniques.

KEYWORDS: authentication, biometric, features, recognition, security.

1 INTRODUCTION

In this computerized world the need for automated security system has been drastically increased. The verification of the users of these automated security systems is a crucial task. There are three methods for performing this verification. The first method is to ask the user to provide some information which is known to only the user. The second method is to ask the user to provide something only the user has access to it. The third method is to identify the user based on some trait which is unique for the user. "Biometrics" is the study of automated methods for recognizing a person based on his/her physiological or behavioral characteristic. "Biometrics" is a general term used to describe a characteristic or a process. As a characteristic: A measurable biological (anatomical and physiological) and behavioural characteristic that can be used for automated recognition. As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics. Biometric systems need to capture an individual's unique biometric features, which are converted into a digital format, called template. This template is then enrolled into a database or some other secure storage location (e.g. a smart card) and later used for comparison with new samples, to determine whether there is a match for recognition purposes.

2 A TYPICAL BIOMETRIC SYSTEM

A biometric system consists of five components: A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process uses the results from the matching component to make a system-level decision.

Many systems require reliable personal recognition schemes to either confirm or determine the identity of a person requesting their services. The purpose is to ensure that service provided is accessed only by a legitimate and authorized user. Biometric recognition refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual's identity based on "who he is", rather than by "what he possesses" (e.g., an ID card) or "what he remembers" (e.g., a password).

Corresponding Author: Sarita Salawadgi

There are different human traits that can be used by a biometric system. The following parameters are used to decide whether a human trait can be used as a biometric or not.

- Universality is how common the trait is found in each individual
- Uniqueness is how well the trait separates an individual form other
- Permanence is how the trait changes with the time
- Collectability is how easy it is to acquire the trait
- Performance indicates the accuracy, speed, and robustness of the biometric system built using the trait.
- Acceptability indicates the degree of approval of a technology by the public in everyday life.
- Circumvention is how easy it is to fill the authentication system.

The following table outlines a comparison between passwords vs. tokens vs. biometrics

Table 1. Comparison of passwords, tokens and biometrics

Method	Properties
Tokens	- Can be forged and used without the knowledge of the original holder. For example, a forger can "steal an identity" and create a fake ID document using another person's information. - Can be lost, stolen or given to someone else.
Passwords	- Can be obtained or "cracked" using a variety of techniques such as using programs/tools to crack the password. - Can be disclosed. If the password is disclosed to a person they will be able to gain access to information for which they are not authorized. - Can be forgotten which will place a further burden upon an organization's administration.
Biometrics	- Cannot be forged - Can be destroyed, and a biometric characteristic's ability to be read by a system can be reduced. An individual's fingerprints, for example, can be affected by cuts and bruises and can even be destroyed by excessive rubbing on an abrasive surface. Also, Accuracy of Biometrics depends mainly on the software that is dealing with them.

A Biometric system consists of three parts:

- Input Device: An input device such as scanner. These are used to record the inputs which are then used by the software part.
- Biometrics Software: A software processes the input and converts into digital form, extract the features, and compare the result.
- Database: A database stores the information further this information is used for comparison. Features extracted from input samples are stored in the database and storing features in the database saves the time for processing.

The two main processes involved are enrollment or registration, verification and identification.

ENROLLMENT PROCESS

It is otherwise known as registration process. In order to identify an individual, it is necessary to store the individual's characteristic features in a database, which are extracted from the reliable samples of the biometric trait either scanned or recorded using input devices like writing pads. These features are then compared with the features extracted from the traits of the individual need to be identified. In order to extract features, the input sample is preprocessed and feature extraction algorithms are applied on these preprocessed samples to form features vectors. Instead of input samples these feature vectors are stored in the database as input samples take more space on secondary memory than mathematical data and features are computed just once which saves a lot of processing time. A classifier is trained using these feature vectors which then classifies the unknown input sample. For better recognition rate multiple samples for each individual are collected during registration.

VERIFICATION PROCESS

For the verification, same set of features which have been extracted during registration process are extracted from the input samples scanned or recorded using input devices like writing pads, to form the feature vectors. Verification is 1 to 1 matching. In verification, the individual claims his/her identity which is verified by comparing these feature vectors by the feature vectors of the individual which he/she claimed to be. If the matching score crosses the threshold (determined experimentally) then the system verifies the individual as authentic user, else the system rejects the individual.

IDENTIFICATION PROCESS

For the identification also, same set of features which have been extracted during registration process are extracted from the input samples scanned or recorded using input devices like writing pads, to form the feature vectors. Identification is 1 to n matching. In identification, the feature vectors of the individual are compared with the feature vectors of every individual stored in the database. If the highest matching score crosses the threshold, then it identifies the individual as the person whose matching score is the highest.

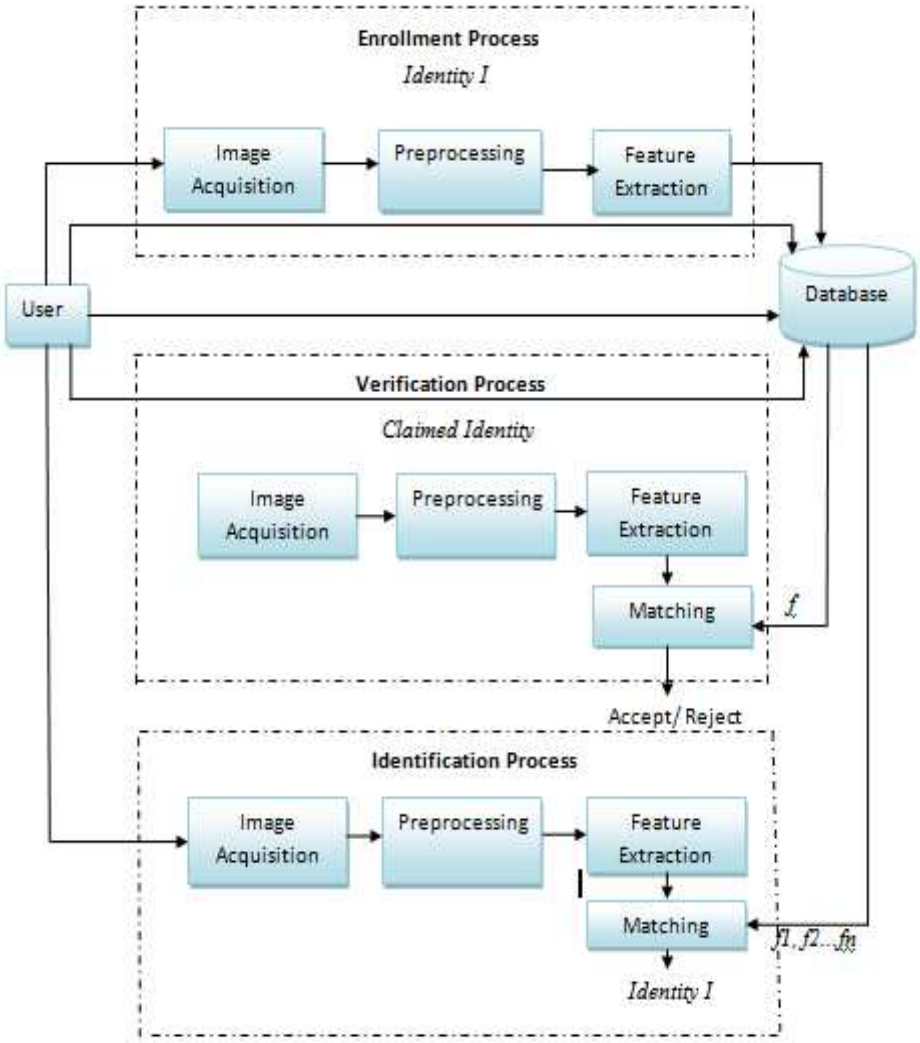

Fig. 1. Biometric System Architecture

3 BIOMETRIC TRAITS

Biometric systems use different physiological and/or behavioral traits of an individual for verification/identification. Different biometric traits have different characteristics and potential applications. There are two types of biometric methodologies: physiological and behavioral. Figure 1.1 shows some of the most used biometric characteristics and the category into which they fall. Physiological methods try to identify the user by some sort of physical trait that is typical to the user. Examples include fingerprint, face, iris, retina etc. On the other hand, behavioral try to identify a user based on some sort of behavior that is typical for a user like the way they walk, or the way they hold the pen while writing or the way they press the keys while entering the PIN etc.

Given below are some of the biometric technologies:

3.1 FINGERPRINT

Fingerprint identification has drawn considerable attention over the last 25 years. Fingerprint is used for the identification and considered one of the most reliable and unique characteristic for identification. It is being used from the time when people did not know how to write. Biometric systems based on fingerprint authentication are very popular, reliable and accurate. Fingerprint technology can be used for both verification (1:1) matching as well as for Identification (1: n) matching. The most popular methods of fingerprint authentication are based on minutia features and general fingerprints patterns. The problem with these systems is the difficulty to collect samples as contact with sensor is required to take the fingerprints which can be unhygienic. Also, some people do not have clear fingerprints because of their physical work or problematic skin. Also as the fingerprints are used for legal procedures people hesitate to give their fingerprints.

3.2 PALMPRINT RECOGNITION

The palmprint of a person can be also taken as a biometric as different persons have different palmprints. A palmprint scanner is used to scan the palm and store in a database. A digital camera can also be taken as an image acquisition device for collecting samples of palmprints from a person in different ways. Line features and Texture analyses are used for feature extraction for palmprint verification or identification.

3.3 FACE RECOGNITION

Face recognition is a Biometric technology that uses an image or series of images either from a camera or photograph to recognize a person. It does not require a person's cooperation. Face recognition is completely oblivious to differences in appearance as a result of race or gender differences and is a highly robust Biometrics. However, the face changes considerably with age, and even due to make-up and expression changes. Face recognition systems can be divided into two main categories. Systems used to verify the identity of a person in a known environment at a fairly constant distance and systems that try to identify a person from a group of people in a dynamic environment and at a random distance.

3.4 RETINA SCANNING

The retina is the layer of blood vessels at the back of the eye. The biometric technology based on retinal scanning is known for low FAR (False Acceptance Ratio) and have therefore been used for years in very high security facilities. But it requires considerable cooperation from the subject as it is inconvenient as intrusive. The retinal scanner requires that the subject should stand still during the scanning process.

3.5 IRIS RECOGNITION

The iris at first seems to be a bad choice for a biometric. But if observed closely, it has considerable texture detail that makes it a good biometric trait. Iris recognition is considered to be the most accurate biometric technology and is being used very effectively all over the world. Iris recognition technology is safe, accurate and works with high speed without sacrificing accuracy.

3.6 EAR RECOGNITION

Ear is a relatively new class of biometrics. It has been suggested by the researchers that the shape and features of ear are unique for each person and invariant with age, which has made ear a biometric trait. Several approaches such as two-stage scale and rotation invariant geometric approach which is based on the concept of max-line, the longest line that has both its end points on the edges of the ear, have been proposed for ear recognition.

3.7 HAND GEOMETRY

Hand Geometry is also one of the most famous biometric. There are two types of hand geometry based systems. One type uses the entire hand for recognition and another type uses only two fingers. It is based on the fact that for every person hand is shaped differently and it does not change significantly with time. The shape and length of the fingers and knuckles are used. Hand recognition systems are especially useful in outdoor environments and it also has the advantage that the templates are very small in size as small as 9 bytes.

3.8 DNA MATCHING

DNA stands for Deoxyribo Nucleic Acid and is found in every cell of an individual. It is completely unique for every person and is most reliable when a positive identification is required. But as it requires extensive testing, it is not the most cost efficient biometric trait.

3.9 VOICE RECOGNITION

Voice recognition systems work by analyzing the waveforms and air pressure patterns produced while a person talks. These systems may use the characteristics of an individual voice or some pre-arranged words. Voice is one of the most convenient biometric but is not reliable due to bad accuracy. Voice can be mimicked and also a person with a cold or throat problems may face problems using the voice recognition system as it may be rejected.

3.10 SIGNATURE VERIFICATION

The handwritten signature is a behavioral biometric. Signatures have been used to verify transactions for centuries and are therefore a well-established method. Automatic signature verification systems do not only examine the appearance of the signature, they also examine the dynamics of the writing. How hard is the pencil pressed against the surface during different phases of the signature?

How fast are the different letters written? How long time does it take to write the whole signature? How and when is the letter \t" crossed? There are also several more behavioral biometrics that can be used to verify a user identity using signatures.

3.11 KEYSTROKE DYNAMICS

Keystroke dynamics is a very new technology and can be said as an extension to passwords and PINs. It is a behavioral biometric. It works by analyzing the way one types the keys, the factors like, the time taken by the user to find the keys, the speed of typing. But the method is sensitive to the mood of the user. And the typing dynamics all change as the user is used to typing.

3.12 GAIT RECOGNITION

Biometric gait recognition (i.e. recognizing people from the way they walk) is one of the recent attractive topics in biometric research. There are five factors that may influence gait recognition. These factors include change in viewing angle, in shoe type, in walking surface, carrying or not carrying briefcase, and the elapsed time between samples being compared. Some of the external factors may have various effects on different gait recognition approaches. For example, while carrying an object may influence the dynamics of gait .When carrying backpack the gait recognition may not be accurate.

The table 2. Shows comparison of different biometric traits.

Table 2. Comparison of various biometric traits

Biometric Trait	Accuracy	Permanence	Universality	Collectability	Acceptability	Uniqueness	Ease of Use
Fingerprint Recognition	M	M	M	M	H	H	H
Palmprint Recognition	H	H	M	M	M	H	H
Face Recognition	L	L	H	H	H	M	M
Retina Scanning	H	H	H	L	L	H	L
Iris Recognition	H	H	H	M	L	H	M
Ear Recognition	L	M	M	M	H	M	H
Hand Geometry	M	M	M	H	M	M	H
DNA Matching	H	H	H	L	L	H	L
Voice Recognition	M	L	M	M	H	M	H
Signature Verification	M	L	L	H	H	L	H
Keystroke Dynamics	L	L	L	M	M	L	M
Gait recognition	L	L	M	H	H	L	M

4 PERFORMANCE

The following are used as performance metrics for biometric systems:

a) **False accept rate or false match rate (FAR or FMR):** The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

b) **False reject rate or false non-match rate (FRR or FNMR):** The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

c) **Receiver operating characteristic or relative operating characteristic (ROC):** The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

d) **Equal error rate or crossover error rate (EER or CER):** The rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

e) **Failure to enroll rate (FTE or FER):** The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

f) **Failure to capture rate (FTC):** Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

g) **Template capacity:** The maximum number of sets of data which can be stored in the system.

5 LIMITATIONS

There are few limitations of Biometrics due to some factors:

a) Because these technologies apply to human beings, they are affected and are limited by many situations that may affect the individual. For example, fingerprint technology may not be effective if the subject has dirty, deformed, or cut hands; iris technology may not be effective if the subject has a bad eye; and voice technology may be affected by infections. Also background noise can interfere with voice recognition systems.

b) Because biometric technologies are new technologies, they tend to be rather expensive without widespread use. For example, facial and voice recognition and iris technologies are still not yet affordable.

c) While an increasing number of available technologies are “plug and play”, they still require some user education. Users need to know how to position their finger, face, and eyes etc., to be clearly read.
d) We cannot replace a biometric that has been lost or misappropriated.
e) Once a biometric has been compromised, it cannot be made right again.
f) Biometrics evolves and degrade over time and require constant updates of the reference biometric.

6 CONCLUSION

The forging of physical human characteristics or personal traits is difficult than passwords and security codes. Biometric authentication and security is highly reliable. There are lots of applications and solutions in biometrics technology. They are used in security systems, surveillance, attendance system etc. They are used by various organizations such as forensic department. Biometric can be easy to use and make life more secure and comfortable. Though biometric are highly secure, they are not a perfect solution. A robust security system will require the blend of both biometric and non-biometric components to provide reliable personal authentication and recognition. How to adopt biometrics in day to day use and in applications still need to be more researched. The biometric will have a huge influence on our life in days to come.

REFERENCES

[1] James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer.
[2] Anil K Jain, Biometrics Personal Identification in Networked Society, Spinger.
[3] Lakhmi C. Jain, Intelligent Biometric Techniques in Fingerprint and Face recognition.
[4] John Chirillo, Scott Blaul, Implementing Biometric Security, Wiley Red Books.
[5] John Woodward, Nicholas M. Orlans, Peter T. Higgins, Biometrics, Tata McGraw Hill.
[6] K P Tripathi, *International Journal of Computer Applications* (0975 – 8887) vol. 14, no.5, January 2011.
[7] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, Guide to Biometrics*, Springer*, 2003.
[8] Martti Juhola, Youming Zhang, Jyrki Rasku, “Biometric verification of a subject through eye movements”, *Computers in Biology and Medicine*, vol. 43, no. 1, pp. 42-50, January 2013.
[9] A. K. Jain, S. C. Dass and K. Nandakumar, "Soft Biometric Traits for Personal Recognition Systems", *Proceedings of International Conference on Biometric Authentication*, Hong Kong, July 2004.
[10] A. K. Jain and A. Ross, "Multibiometric Systems", *Communications of the ACM*, *Special Issue on Multimodal Interfaces*, vol. 47, no. 1, pp. 34-40, January 2004.
[11] Yooyoung Lee, James J. Filliben, Ross J. Micheals, P. Jonathon Phillips, “Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs”, *Computer Vision and Image Understanding*, vol. 117, no. 5, pp. 532-550, May 2013.
[12] Peiyang Shen, Yingfeng Zheng, Xiaohu Ding, Bin Liu, Nathan Congdon, Ian Morgan, Mingguang He,” Biometric measurements in highly myopic eyes”, *Journal of Cataract & Refractive Surgery*, Volume 39, Issue 2, February 2013, Pages 180-187.
[13] James B. Hayfron-Acquah, Mark S. Nixon, John N. Carter,” Automatic gait recognition by symmetry analysis”, Pattern *Recognition Letters*, vol. 24, no.13, pp. 2175 – 2183, September 2003.
[14] Xiang-qian Wua, David Zhang, Kuanquan Wanga, Bo Huanga, “Palmprint classication using principal lines”, *Pattern Recognition* ,vol. 37,pp. 1987-1998,2004.
[15] J. A. Unar, Woo Chaw Seng, Almas Abbasi, “A review of biometric technology along with trends and prospects”, *Pattern Recognition*, vol. 47, no. 8, pp. 2673-2688, August 2014.