Xournals

Academic Journal of Information Security

ISSN UA | Volume 01 | Issue 01 | January-2019

Biometric devices and Security

Ranjeet Kumar Singh[1] and Mahesh Sharma[1]

Available online at: www.xournals.com

Received 7th September 2018 | Revised 3rd October 2018 | Accepted 4th December 2018

Abstract:

The major problem in our daily life is security. To deal with the information security major role is played by authentication. Biometric security is one of the widely used technology in identification and security. Biometrics is the automatic identification system of a person. The identification system of biometrics depends upon the physiological as well as behavioral characteristics of a person. In the recent system of security, biometric has depicted his work. In the prevention of unauthorized admittance of ATMs, smart cards, PCs, computer networks, etc. biometrics can be used. Many industries and companies uses biometric security for the recognition of employees. Because of liability and efficiency of biometrics, it is quite popular. This paper discusses about biometric techniques with some comparison of biometric system with other authentication method can also be discussed for the achievement of a security system with maximum advantages.

Keywords: *Biometrics, Security, Authentication, Information.*

Authors:

1. *Sherlock Institute of Forensic Science India (SIFS INDIA), New Delhi, INDIA*

INTRODUCTION

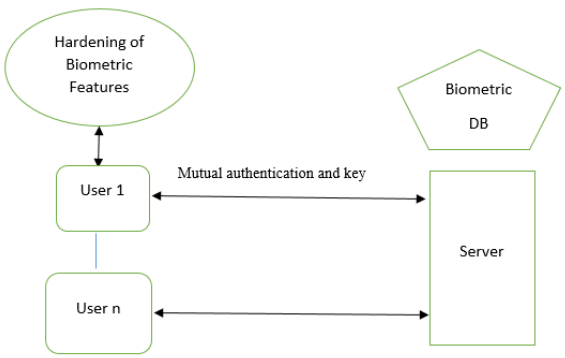
The surety of an individual's privacy, honor and availability of information in all forms is concerned under Information Security. The administration of information security is supported by many tools and techniques. But some features of information security are based on biometric.

Biometrics is derived from a Greek word 'bios' which means life and 'metrikos' which means to measure. It is a scientific technology where statistical analysis of biological characteristics takes place. In information security biometric authentication includes identification, authentication and non-repudiation. For personal identification biometric authentication is popular. The identification of person is significant in many application. The major issue concern in today's society is increasing of large number of credit card frauds and in identification of theft biometrics plays major role. A capable method for security application with many advantages over classical method is offered by biometric system.

Biometric recognition offers an auspicious approach for security, with many advantages over the classical methods, which depends upon something you have like key, id proofs, etc. or something you know password, pattern, etc. the simple stuff of biometric traits is that it is based on the data or information which you have or which you do, so there is no need to remember in anything in biometric security or neither to hold any token.

BIOMETRIC SYSTEM

To improve security of network the overall structural plan of the biometric system is shown. User's encoded bifurcation point pattern is fed and stored in the database which is preserved in the Server. Biometric feature of user should be provided to connect with the server. Since there are many techniques for biometrics and still various researches and inventions in the field of biometrics is still in curiosity. For the improvement of the authentication system numerous techniques have been combined with the biometric system. The two main problems for user authentication system are acceptance of authorized user and prevention of frauds.



Biometric is a particular portion of security system with good number of advantages over other classical Authentication methods. There are also some drawbacks which is compared with other authentication method and discussed below.

Table: Comparison of different Authentication Method

Method of Authentication	Advantages	Drawbacks
Handheld tokens (ID cards, Passports, etc.)	• If it is misplaced the new can be issued. • It is standard although moving in a different republic, facility, etc.	• Fake IDs can also be issued. • It can be shared and stolen. • With different identities people can be registered.
Knowledge Based (Passwords, pin, Patterns, etc.)	• It is simple and economical. • It can be easily replaced by your own choice.	• It can be cracked by guess. • Sometimes it is difficult to recall. • It can be shared.

		• With different identities people can be registered
Biometrics	• It cannot be lost, forgotten, stolen, shared or guessed. • If a person has sever identities it can be easily checked. • As compare to other it provides high security	• In some cases a fake one can be issued. • It can neither be replaced nor be a secret. • Difficult to substitute.

Working Principle of Biometric System

The basic working principle of all the biometric system are same, in this principle the steps include: enrollment

- Biometric data
- Presentation
- Template
- Feature extraction
- Matching

Enrollment or Registration: Initially when the biometric data of user is obtained, treated and deposited for the ongoing use in the system of template, it is known as enrollment or registration process. In further process of authentication these templates will be used.

Biometric Data: During registration the information provided by the user is known as unprocessed image data, which is also mentioned as raw data or biometric sample. The biometric performance is generated by the help of feature extraction process biometric templates is used to generate to perform biometric matches because the raw biometric data cannot be used.

Presentation: It is a process in which user's biometric data is presented to the devices, the hardware collects and store the data in the device. For example finger should be placed on finger reader device.

Template: After using a number of feature extraction, algorithms mathematical depiction of raw biometric data is obtained which is known as template. The size of templates can differ in size from few to several thousand bytes. At the time of registration the template is created is known as stored template and at the time of verification it is called as live template.

Feature Extraction: To generate a template, locating and programming distinctive features from biometric data is processed which is known as feature extraction. Feature extraction is conducted during enrollment and verification, any time a template is shaped.

Matching: At the time of authentication the templates which are stored template is matched with live and a score is obtained, on the basis of this score a conclusion is drawn whether a user is authenticate human or not.

TECHNIQUES AND TECHNLOGIES OF BIOMETRICS

Finger Prints

For personal identification fingerprints have been used from a very long time. It is an imprint of grooves and ridges of a finger. Fingerprints are unique even identical twins have different fingerprints, that is why fingerprints are considered as an identity of a person. Scanning of fingerprint of a person is easy and affordable. This traditional method ink is used to get fingerprints but now live fingerprint scanners are used which are based on the principles of optical, thermal, silicon or ultrasonic technologies. This fingerprint recognition system is becoming reasonable in various applications like in Adhar card, banking, Passport etc.

Face recognition technology

Here, identification or verification of a person is done with the help of digital image or from a video source. It is one of the most usual means of biometric identification. On the basis of shape of facial characteristics such as nose, eyes, lips, eyebrows, chin and the relationships of these features, face recognition are done. This technology has recently developed into two categories which are facial metric and Eigen faces.

Iris technology

The iris is part of a human eye. It is unique and persists over a person lifetime. Iris is a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings. Even the iris of identical twins are also different. The information of iris can be collected by iris image or by video based image acquisition system. It gives a promising accuracy for recognition. The recognition system of iris is cost effective. It is more accurate

Hand Geometry

Hand geometry technology is based on the fact that the shape of every individual's hand is different and it does not change after attaining a certain age. On the basis of the measurement like shape, size of palm, length and width of the fingers the hand geometry recognition works. This method is very simple and easy to use. This method is also accurate to near as environmental condition has significantly no effect on the geometry of hands.

Speaker Recognition Technique

In various sectors and applications voice recognition systems are used. Person voice are based on the features like vocal tracts, mouth, nasal activities and lips movement that are used synthesis of sound. Over time due to age, medical conditions, and emotional state the behavioral part of the person's speech changes. Speaker recognition system consists of three styles of speech inputs viz.

(a) Text dependent (b) Text prompted (c) Text independent

Conclusion

The systems in which the physical characteristics like finger print, hand geometry, face, voice and iris are used for the purpose of security and identification of a person is done. In various application biometric security system have been proved to be accurate and very effective. On the risk to privacy and threat to identify the influence of biometric on society is very facilitation through regulation. The drawbacks of traditional computer based security system which are used at the places like ATM, Passport, Payroll, driver's licenses, government offices and network security was overcome by biometric security. Biometric authentication offer high level security but still improvement is needed in various aspects.

References:

Bhattacharyya, Debnath, et al. "Biometric Authentication: A Review." *International Journal of u- and e-Service, Science and Technology*, vol. 2, no. 3, Sept. 2009, pp. 13–27.

Gomathi, P M, and G M Nsira. "A Survey on Biometrics Based Key Authentication Using Neural Network." *Global Journal of Computer Science*, vol. 1, no. 11, July 2011.

Kodituwakku, S R. "Biometric Authentication: A Review." *International Journal of Trend in Research and Development*, vol. 2, no. 4, Aug. 2015, pp. 113–123.

Shradha Tiwari, et al. "A Review of Advancements in Biometric Systems." *International Journal of Innovative Research in Advanced Engineering*, vol. 2, no. 1, Jan. 2015, pp. 187–204.

Srivastava, Himanshu. "A Comparison Based Study on Biometrics for Human Recognition." *IOSR Journal of Computer Engineering*, vol. 15, no. 1, 2013, pp. 22–29.

Subban, Ravi, and Dattatreya P. Mankame. "*A Study of Biometric Approach Using Fingerprint Recognition." Lecture Notes on Software Engineering*, 2013, pp. 209–213.

Uddin, Mohammed Nasir, et al. "A Survey of Biometrics Security System." *IJCSNS International Journal of Computer Science and Network Security*, vol. 11, no. 10, Oct. 2011, pp. 17–23.

Zanuy, Marcos Faundez. "Biometric Security Technology." *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, June 2006, pp. 15–26.