



SECURABLE AUTHENTICATION IN COMPUTER TECHNOLOGY: BIOMETRIC RECOGNITION

***DR. M. RAMYA**, Assistant Professor, PG & Research Department of Commerce,
Hindusthan College of Arts and Science, Coimbatore. TN INDIA
****MRS. K. RENUGADEVI**, Assistant Professor, PG and Research Department of
Commerce, Hindusthan College of Arts and Science, Coimbatore. TN INDIA

Abstract

Computer is a term expanded as "Common Operating Machine Particularly Used for Trade Educational and Research". It is a machine used to perform various operations in Trade and educational field. As Trade and Educational sectors have grown, similarly technical use of computers also has grown in these sectors. Earlier way (i.e, manual) of performing business is not efficient so operations changed from manual to computer. An assortment of Computer Technology have grown like Accounting Software, Business Intelligence, Business management, Customer management, Resource management, Communications Software etc to facilitate the process efficiently. Accessing and securing the data are necessary for software to maintain its confidentiality.

1. Introduction

Computer Security is vital term refers to a "software system", guarantees the data stored in a computer cannot be read or concession by any individuals without authorization. Computer Security involves data encryption and passwords, data encryption is the conversion of data into a ambiguous form and password is a word which allows the user to access the application. A new password mechanism used in Computer Technology is "Biometric" recognition. 'Biometrics' is the study of computable physical quality of an individual. Biometrics is a computerized technique for a person identity based on a physical characteristic. Various biometrics used for identification like face recognition, fingerprint marks, hand geometry, eye recognition (iris, retinal, vein) and voice recognition. Biometric data are disparate from password, Biometric cannot be reverse-engineered to recreate authentic information and they cannot be stolen also.

2. Biometric Systems

a. Finger Print recognition

Fingerprints are often used Biometric technique to differentiate individuals and their identity. Fingerprints are differs for every individual, even it differs for identical twins. The figure 1 shows a various fingerprints, each print is different from other, similarly every individual has their own finger prints and identify their individuality. Fingerprints are used systematically for criminal investigation in 1900, by Sir Edward Henry of the Metropolitan Police in London, England; they were compared slowly and laboriously by hand.



Figure 1: Fingerprints

Fingerprint recognition is a automated system uses finger prints for authentication by matching human finger prints. A Fingerprint recognition system scans the finger print from individual as shown in Figure 2. The systems are consist of a scanner for scanning a fingerprint and processor to differentiate the individual, fingerprint database to store the fingerprint and software to compares with appropriate data in database. Fingerprint in database is mapped with a individual reference number and that will attach to a Individual account.



Figure 2: Finger Recognition System

The fingerprint of individual is differentiate based on their Minutiae points like ridge ending, dot, lake, bridge, bifurcation, island, hook as shown in figure 3. Each fingerprint is unique, based on its characteristics, can match and get an accurate comparison.

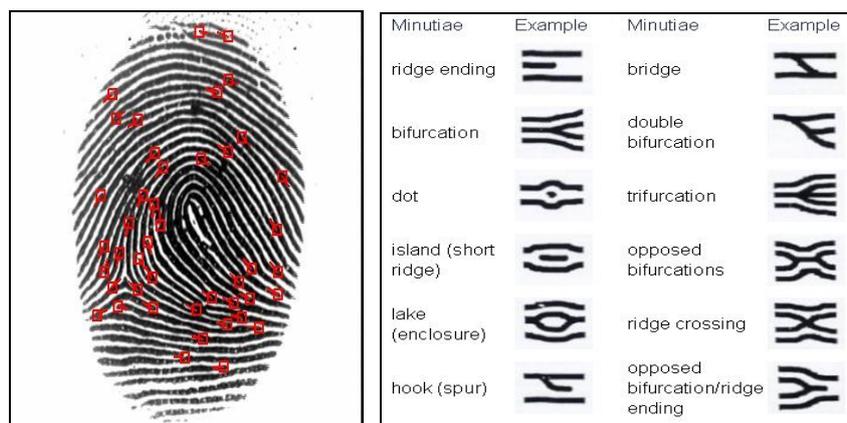


Figure 3: Minutiae points

b) Face Recognition

Face recognition is a security system identifies a person through face. How a human mind is excel to remember a person by viewing various features of face like eyes, nose, ears and mouth, similarly face recognised system also works in same fashion. Face recognition system is proficient system to identify or verify a person through digital image. The system operates by comparing certain face characteristics of the image with various geometrical relations as shown in figure 4 and identifies the distances between significant points in a face and uses recognition algorithm to match these distances with eigenfaces, and Euclidian or Mahalanobis distance and stores in face database.

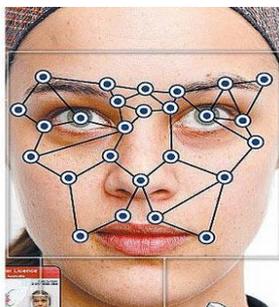


Figure 4: Face Characteristics

A Face recognition system uses camera to capture a face and needs a face to be turned in proper degrees toward the camera to register. Once face is captured, the system aligns the head position, size, pose and various geometrical indications as shown in figure 5. The system converts the aligned face into unique code as per geometrical template. The template is compared with stored face data in database and authenticates the user.



Figure 5: Face Recognition System

3. Process flow of Biometric system

The figure 6 shows the process flow of Biometric system, with two phases, first phase is Registration phase and second is authentication phase. The registration phase captures the physical characteristics of a individual and extracts the appropriate characteristics and store in Database, while registration the system captures Biometric for three times. The Second phase is a authentication, captures the Biometric and extract the data, compares it with database and authenticate the user with successful or unsuccessful.

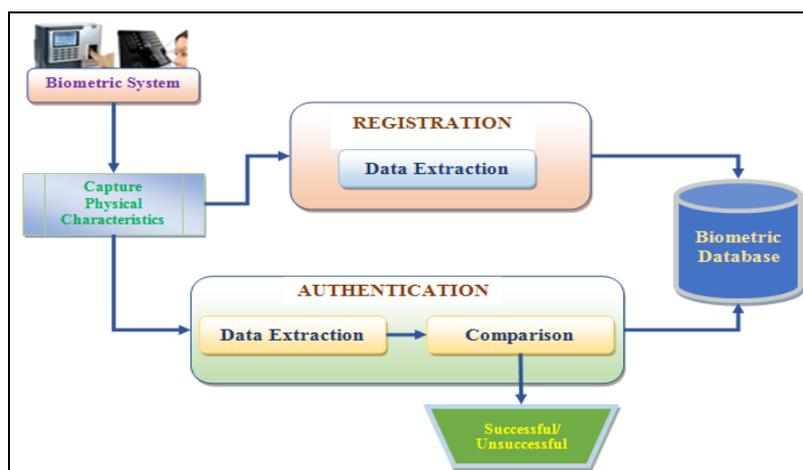


Figure 6: Process Flow of Biometric System

4. Benefits of using Biometric Systems

a) Accuracy

As a traditional password system, anyone can able to access the system if they knows the password but in Biometric system authorized person only able to access the system by using biological characteristics like fingerprint recognition, so Biometric offers unique and accurate identification. Biometric technology gives accurate results with minimal invasiveness by a simple scan.

b) Saves time



Time is essential in every business so use of technology offers more beneficial; a Biometric identification operates in a fraction of time and reduces time by checking and arguing with imposters.

c) Easy and Safe for Use

Installation of Biometric hardware and software can done easily and using of system also easier without need of any excessive training.

d) Adaptability

The most benefit of Biometric system is adaptability, can apply the Biometric system to any applications in concerns like Employee attendance, entering into a confidential section, exiting, doorways, and Biometric systems decide who can access certain systems and networks.

e) Convenient

People forget passwords or loss of ID in traditional security makes a person in trouble to access a application. Biometric system is considered as a convenient security solution because not necessary to remember password or carry ID cards.

5. Conclusion

As Computer technology has is grown in various areas, so need of appropriate securable technology. Biometric uses physical characteristics of human as securable feature which provides is higher level authentication security system and offers a variety of benefits to various application like payroll system, doorway access and used in Financial application with efficient response and provides higher advantages over traditional security systems.

6. References

1. <http://www.explainthatstuff.com/fingerprints scanners.html>
2. <http://sites.psu.edu/jlipton/2014/06/03/fingerprints-unique-to-us-all/>
3. <http://www.engineersgarage.com/articles/face-recognition>
4. <http://eagleeyett.com/biometric-systems.php>
5. Cyber Laws and IT Protection, Harish Chander, Prentice Hall India Learning Private Ltd. (2012)