Journal of Pattern Intelligence
ISSN: 2230-9330 & E-ISSN: 2230-9349, Volume 2, Issue 1, 2012, pp.-22-25.
Available online at http://www.bioinfo.in/contents.php?id=49

FINGERPRINT RECOGNITION SYSTEM FOR INTRUSION DETECTION

MUDHOLKAR S.S.*, SHENDE P.M., KHARAT V.P. AND KHODWE S.S.

Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India.
*Corresponding Author: Email- smi.mudholkar@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- There are the different biometric systems that are used for authentication. This paper represents various issues in face recognition systems, soft biometrics recognition system, keystroke recognition system, and DNA recognition system. This paper also gives brief description about fingerprint recognition system, types of fingerprints and how this system is better than other biometric system. Practical Biometric system should meet specified recognition requirements such accuracy, speed, and resources. Fingerprint recognition is harmless to the users hence it is accepted by the intended population.
Keywords- biometrics, sof biometrics, fingerprints recognition, Face Recognition.

Citation: Mudholkar S.S., et al. (2012) Fingerprint recognition system for intrusion detection. Journal of Pattern Intelligence, ISSN: 2230-9330 & E-ISSN: 2230-9349, Volume 2, Issue 1, pp.-22-25.

Introduction

The password based system is not so long secure system so now days the security problems are increases more and more and biometrics is one secure technique which is used for security purpose. Biometric is a science of using digital technology to identify individuals based on individual's unique physical or biological qualities. But there are many different types of biometric system like face recognition, voice recognition, keystroke recognition, soft biometric system, DNA recognition system etc. But the fingerprint recognition system is more secure than the other biometric system. And there are many different types of fingerprint scanners are available in market and this system not more costly so its use is also increases. Few year before biometric systems are so expensive so people avoid using this system due to this region. This are used in military, banks, hospital etc. There are two types of classification of biometrics (1) physical biometrics which measure the physiological characteristics of a person, such as fingerprint, iris scan, face recognition, and (2) behavioral biometrics which measure the behavior of a person, such as keystroke dynamics and mouse dynamics. Fig.1-

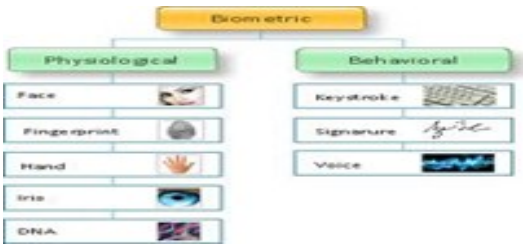

Fig. 1- Categories of biometrics

The difficulty of biometrics system is depends on three main part i.e. accuracy, usability, and size of database. The challenge is to design a system that would operate on the extremes of all these three axes. If size of database and usability increases then time period for the accurate matching for input pattern in database and input gives to the system should be increases and thus accuracy of the system for the gives the accurate result is decreases. Figure 2 show the Biometric system characterization [1].

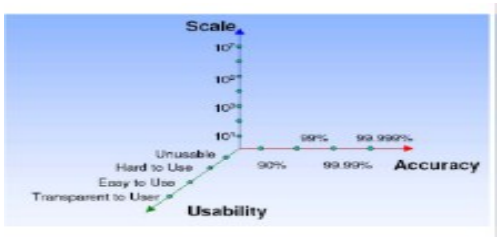

Fig. 2- Biometric system characterization. Accuracy axis represents the intrinsic 1:1 accuracy of the matcher.

Difficuties faced by other biometic system

Face Recognition system-

In face recognition system main challenges occurs due to change in position, different light effects, different facial expression, and change in hairstyle and age problems etc. Due to change in pose, an appearance based face recognition system will not be able to match these 3 images successfully, even though they belong to the same individual. (Figure 3) [1].

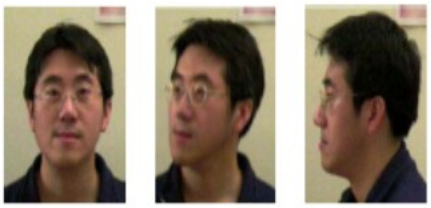

Fig. 3- due to change in pos position face recognition system not offer a correct design

The same person imaged with the same camera and seen with almost the same facial expression and pose may come out considerably different with changes in the lighting situation. The two leftmost images were taken inside the door and the two rightmost were taken out-of-doors. All four images were taken with a standard EOS 1D digital camera. Before each getting the subject was asked to make an unbiased facial expression and to look directly into the lens. It has been observed that the variations between the images of the same face due to lighting and viewing direction are almost always larger than image variations due to change in face identity.

As is clear in Figures 4s the same person, with the same facial expression, can appear noticeably different when light source direction and viewpoint vary. These variations are made even greater by additional factors such as facial expression, hair styles, makeup, and even changes due to age [2].

Fig. 4- due to different light effect system will not match the input gives to the face recognition system and input in database

Fig. 5- due to change in hairstyle and facial expression and age problems face recognition system will not match the input gives to the face recognition system and input in database.

Soft Biometric Recognition system

Soft biometric characters are those characteristics that offer some information about the individual, but be deficient in the uniqueness and permanence to sufficiently differentiate any two individuals. The soft biometric character can either be continuous or disconnected. Characters such as gender, eye color, ethnicity, etc. are discrete in nature. On the other hand, character like height and weight are continuous variables. A system that is completely based on soft biometric character cannot offer the required accuracy in the recognition of individuals [5].

Fig. 6- Soft Biometric recognition system

Keystroke Recognition system

The functionality of this biometric is to measure the dwell time (the length of time a key is held down) and flight time (the time to move from one key to another) for keyboard actions. Keystroke biometrics work on the basis of multiple feature extraction being used to create a profile of an individual. This profile is used to identify or authenticate the user. Keystroke analysis is concerned with the frequency, accuracy, the pause between strokes and the length of time a key is depressed. The performance of the keystroke is affected by various circumstances of the human users, such as a hand injury or fatigue of the legitimate user. Limited accuracy. The systems developed for this biometric method are costly since they use neurological methods and dedicated terminals [7].

Fig. 7- Keystroke Recognition System

Voice Recognition System

Voice recognition system are uses a speech signal that is analyzed to determine characteristics in voice. Many difficulties affect its accuracy. These include poor-quality voice samples; the variability in a speaker's voice due to illness, mood, changes over time;

background noise as the caller interacts with the system; and changes in the call's technology [3].

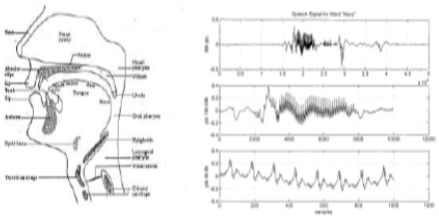

Fig. 8- Voice Recognition system

DNA Recognition system

DNA recognition system is also use in biometrics. The department of defense (DOD) system implements to get betters the U.S government ability to track and identify national security. The system contain mandatory collation of ten rolled fingerprint, minimum five mug short from various angle and oral swap to collect DNA.DNA recognition system is more expensive and that's why this system is not used more.

What is fingerprint recognition system

Fingerprint recognition describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint.. Among all biometric techniques, fingerprint recognition is the most popular method due to the following advantages:

1) Universality—the size of the population with readable fingerprints exceeds the size of the population with passports.
2) High individuality—even identical twins who share the same DNA have different fingerprints.
3) High presentation—At the age of seven months, a fetus's fingerprints are fully developed, and fingerprint characteristics do not change in the absence of injury or skin disease. However, after a small injury to a fingertip, the pattern will grow back as the fingertip heals. Fingerprints are classified into six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e)whorl, and (f) twin loop (fig:9) [8].

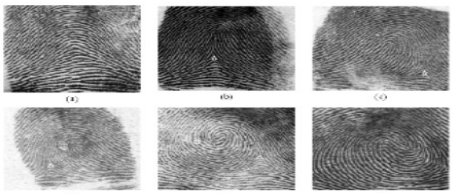

Fig. 9- classification of fingerprint

Fingerprint matching algorithm can be found into two categories: minutiae-based and correlation based. In this method we, first get minutiae points and then map their comparative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points exactly when the fingerprint is of poor quality. Also this algorithm does not take into account the global pattern of ridges and furrows. Fingerprint Verification System is a system that determines the correspondence of an input fingerprint with a input fingerprint stored in data base. A typical block diagram of biometric matching systems is shown in Fig 10 [8].

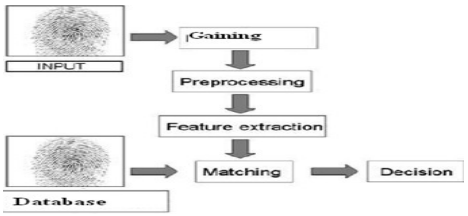

Fig. 10- Flow of fingerprint matching

In this following process user give his fingerprint sample to the fingerprint recognition system. First system creates the database for user and when user enter his fingerprint for authentication then system matches the input patter give by the user and template stored in database if both are matches with each them user get the access of the system and if both fingerprint are not match then user not get access of the system [3].

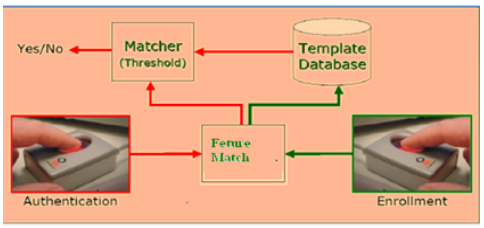

Fig. 11- Process of Fingerprint recognition system

There are different electronic devices highly available in market for various security purposes in various areas. Following figure shows the different fingerprint scanners which are available or used of security purpose [4].

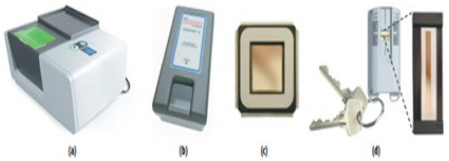

Fig. 12- Fingerprint scanner:(a) 10-print (b)single print scanner (c) touch (d)sweep sensor embedded in privaris pluseID devices

Example of fingerprint recognition system which used in mobail phone

By attaching a fingerprint scanner to the mobile phone, this biometric could also be utilized for phone associated security in a similar manner. A classic example can be seen from a research that utilizes a fingerprint sensor for gaining of fingerprint images and implements an algorithm on internal hardware to perform corroboration of users This implementation has a relatively high-quality performance. The prototype of this mobile phone based fingerprint system could be seen in Fig.13 [6].

Fig. 13- A representation for fingerprint mobile phone

Fig. 14- Snapshots of fingerprint security.

One major problem with mobile phone based fingerprint biometric is that it requires an external attachment as a scanner of fingerprint images. Recently, iPhone launched an application named Fingerprint Security by using such features together [6].

Conclusion

There are a number of attacks that try to bargain a computer system using a variety of methods such as unauthorized access. These attacks could be reduced if an identification tool is used to complement already deployed intrusion detection system. The most trustworthy identification systems are based on biometrics. Therefore, several biometrics technologies start to convoy host-based Intrusion detection systems. Until Now, behavioral biometric was the only techniques that have been used so far, since they do not require any special devices. In contrast, some researchers proved that these techniques are not very proficient which was the motivation to design an identification system based on fingerprint technique.

Reference

[1] Jain A.K., Pankanti S., Prabhakar S., Hong L. and Arun *Biometrics-A Grand Challenge*.
[2] Belhumeur P.N. (2003) *Ongoing Challenges in Face Recognition*.
[3] Biometrics *http://scgwww.epfl.ch/courses.*
[4] Jaina A.K., Dassb S.C. and Karthik Nandakumara *Can soft biometric traits assist user recognition.*
[5] Shuo Wang and Jing Liu, *Biometrics on Mobile Phone*.
[6] Tom Olzak (2006) *Keystroke Dynamics: Low Impact Biometric Verification*.
[7] Chander Kant and Rajender Nath *Reducing Process-Time for Fingerprint Identification System.*