Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Biosecurity System in Computer Society

S. Ramesh [#1], P. Rekha [#2]
[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
Rameshmani3032@gmail.com
[2]*Asst Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*

Abstract— In biometrics recognition automated recognition of individuals is done based on a feature sets derived from their behavioral and physical characteristics computing systems require reliable and secure personal recognition and authentication scheme to either determine from or confirm the identity of an individual requesting to the services the human have used body characteristics in fingerprint and signature and stump impression very are all thinks are used by identify the person. Biometrics system function to identify individual by matching a specific personal characteristics to the previous record

Keywords— Fingerprint, voice recognition, retina scan, iris scan

1. Introduction

Biometric is purely based of physical characteristics human biometrics authentication support the face of identification authentication and non-repudiation in information security biometrics system function to identify individual by matching a specific personal characteristics the biometrics identifier with one previously recorded. Biometrics is based on two character they are

- A physiological characteristics such as a fingerprint or face.
- A behavioral characteristics such as a signature or voice

A variety of method and technique are available today retina, voice, signature , fingerprint, face, signature and voice are consider to be lower level of security than fingerprint and iris. A biometric system can be either an identification system or verification system. In this article we comprehensively converse on biometric expertise and we believe that this review will definitely provide a limelight on the past and present and future accept of this field.

2. Biometric system

A biometric system is essentially a pattern of recognition system that operates by acquiring biometric data from a human being extracting in trait set from the attain data. Depending on the application context a biometric system may function either in corroboration mode or detection mode [2]. Biometric classified by some categories: The human have used in fingerprint for personal identification. Fingerprint is an impression of the ridges and furrows located on the surface of a fingertip. The formation of fingerprint is determined during the first seven month of the fetus development. The accuracy of available fingerprint system is good enough for verification system. Since the scanning device is actually touched by the finger, it surface can become greasy and oily after using repeated which in turn could reduce the reliability, sensitivity and precision of elective scanners. This difficulty could be resolved with solid state sensor as the coated silicon chip itself is the sensor. In real-time verification system feature extraction module use the image captured by sensor to derive the feature set. The feature value usually correspond to the orientation and position of certain critical and important points known as minutiae points. Minutiae based and correlation based is two types of fingerprint matching technique minutiae technique[3].

2.2 Retina scan

Blood vessels at the rear side of the retina, have pattern which is unique for each individual form the basis of retina scan biometric technique. These patterns create an eye signature from the vascular configuration of the retina. It is most secure as retinal vasculature it not easy to change.

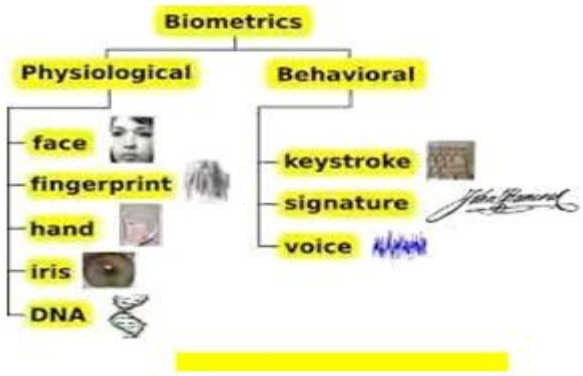

Fig 1:Biometric characteristics

Digital images of retinal pattern can be acquired by projecting a low intensity beam of visual or infrared light into the eye and capturing an picture of the retina using optics similar to a retina scope. The image acquisition involves cooperation of the identity, requires contact with the eyepiece, and a conscious effect of the user [4].

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Wireless networks contain of a number of nodes which connect with each other over a wireless frequency which have different types of networks: antenna network, ad hoc mobile network, cellular networks and dependency networks. Wireless sensor network contain of small nodes with detecting, addition and wireless communications capabilities. Data integrity confirms that the packets are traditional by the receiver in the same organization.

2.3 Iris

The colored area that surrounds the pupil is called iris. These iris pattern are unique and are obtained with the help of video based image acquisition system. The visual texture of the iris is created during fetal development and gets stabilized during the first two years. This complex texture contain very distinctive information which is used for personal recognition. The pattern can contain many distinct feature such as furrows, crypts, freckles, arching, ligaments, rings, ridges, corona and a zigzag collarets. Surgically tampering the texture of the iris is very difficult. Since the iris response change with light it can provide an important supplementary verification that the iris presented belongs to a particular user. Two identical twins also have different iris. A careful balance of focus, resolution, light and contrast is required to extract a feature set from localized image. A while the iris seems to remain the same during adulthood, it varies somewhat up to adolescence. Although the early iris based identification system required considerable user participation and were expensive, effort are underway to build more user friendly and cost effective versions[5].

2.4 Face

This is the most pervasive technology used proposition recognition it is a non-intrusive method and is suitable for covert applications. The facial recognition application range for a static, controlled "mug-shot" verification to a dynamic, uncontrolled.face identification a cluttered background. Feature set is extracted from a two dimensional image of the users face and is matched with the stored template in database.

2.5 Hand geometry

It is based on the fact that various dimensional of human hand, including its shape, location of joints, size of palm and length and width of the finger can be used biometric characteristic. These characteristics do not change after certain age. Hand geometry based biometric system have been installed at hundreds of locations around the globe. The technique is very easy, simple and comparatively less expensive. External factors like dry skin does not have an impact on the identification accuracy. It is generally used as a verification technique using in identification mode is not desirable. Limitation of this is low discriminative capability. Hand geometry information could not be invariant over the life time of an individual specifically during childhood[6].

2.6 Gait

The technology is not consider to be very distinctive but could be used for low level security application. Gait based system are input intensive and computationally expensive as the video sequence footage of a walking person is used to measure various different movement of each articulate joint. It is a manner which one walks and involves complex spatia-temporal biometric technology.

3. Advantage and Disadvantages

The main advantages of biometric is more accurate and it is more securable. Let us now examine of biometrics in two group of applications the commercial positive recognize application that may work either in verification or the identification mode and the government and forensic negative recognition application that require identification. It is one of the most expensive one. Such password are easily to crack by guessing are by a simple brute force dictionary attack to keep different password different application and change them frequently.
The hacker may then try to use the same login name and password to the attack the user. Longer are more secure but harder to remember which promotes some user to write them down in accessible location [8].

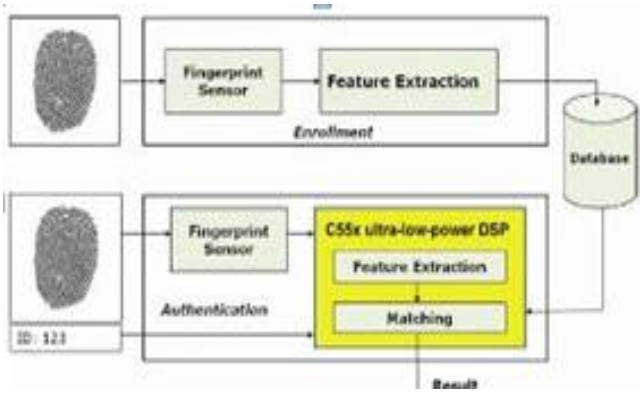

Fig 2. Block diagram of biometric system

4. Methodology of biometrics

Fingerprint classification large volumes of fingerprint was collected and stored every day in a wide range of applications including forensics access control driving license registration. A routine detection of inhabitants

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

based on fingerprints require that the input of fingerprint be matched with a large number of fingerprint in a database(FBI database contain approximately 70 million of fingerprint) to reduce the hunt time and computational complication it is enviable to classify this fingerprints in accurate and consistent manner so that input fingerprint is required to the matched only with a subset of the fingerprints in the database. In fingerprint image enhancement a critical step in automatic fingerprint matching is to automatically and reliably extract trivia from the input fingerprint pictures. Though, the performance of a minutiae extraction algorithm relies heavily on quality of the input fingerprint images.

In order to insure that the performance of an automatic fingerprint detection scheme will be vigorous with reverence to the quality of the fingerprints images. We have evaluated the performance of image enhancement algorithm using the goodness of index of the extracted minutiae and accuracy of an online fingerprint verification system. Experimental results show that incorporating in enhancement algorithm improve both the goodness index and the verification accuracy[9,10].

5. Conclusion

Biometric authentication and security is highly reliable since forging the physical human characteristics are much more difficult password, security code and hardware keys. The use of biometric raises several privacy questions. Biometrics are highly secure they are not a perfect solution. How biometrics can be embedded in day to day use and in application still need to be more research but still it is true that biometric will have a profound influence on our life in day to come.

6. Future work

In my biometric future work are fingerprint scanning timing can be reduced by the fraction of second and the increasing the accurate performance of fingerprint.

References

[1] A.K. Jain, R. Bolle, and S. Pankanti, eds., "Biometrics: Personal Identification in a Networked Society", Kluwer Academic Publishers, Vol-3, 1999, pp.90.
[2] Best Practices in Testing and Reporting Biometric Device , Version 2.0, Tech. Report, United Kingdom Biometric Working Group, 2002; www.cesg.gov.uk/technology/biometrics.
[3] D. Maltoni et al., "Handbook of Fingerprint Recognition", Springer, Vol.2,2003, pp.45.
[4] Password Clues, "The Central nic Password Survey Report", Central Nic, 13 July 2001; www.centralnic.com/page.php?pid=73.
[5] A. Jules and M. Sudan, "A Fuzzy Vault Scheme," Proc.IEEE Int'l Symp. Information Theory IEEE Press, 2002,p. 408
[6] J.D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?" Proc. IEEE, vol. 85, no. 9, Sept. 1997, pp.1480–1492.
[7] Millee Panigrahi, Rina Mahakud, Minu Samantaray and Sushil Kumar Mohapatra, "Comparative analysis of different Edge detection techniques for biomedical images using MATLAB", Engineering and Scientific International Journal, Volume 1, Issue 1, October - December 2014, PP.23-28.

S.Ramesh is holding a Under Graduation Degree inB.Sc (CS) from J.H.A. Agarsen College of Arts and Science and pursuing PG in master of computer applications from S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar