Volume 2, No. 11, November 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

BIOMETRICS BASED IDENTIFICATION TECHNIQUES (BIT)

Akash Srivastva[*1], Vedpal Singh[2]
CSE Dept. Dev Bhoomi Institute of Technology (DBIT), Dehradun, INDIA [1, 2]
akash.10may@gmail.com*[1], vedpalsiet101@gmail.com[2]

Abstract: - A large number of systems require the reliable and efficient personal recognition methods to either confirm/determine (authenticate) the identity of an individual that requesting their services. Purpose of such type of methods is to ensure that rendered services are accessed only by a authenticate user and no one else. In biometric recognition, biometrics refers automatic recognition/authentication of individual totally based on their physiological and behavioral properties. By using biometrics, it's possible that to confirm/establish an individual's identity based on "who he is," rather than by "what he possesses" (e.g. ID card) "what he remembers" (e.g. password). In this paper, we give a brief overview of the field of biometrics and summarize some biometric identification techniques with their strengths, limitations, and related privacy concerns and comparisons with each other.

Keywords: - biometrics, Identification, Authentication, security and privacy.

INTRODUCTION

Now a day's all systems that has been used are going to be automated in all different domain like access buildings, computer systems, laptops, cellular phones, ATMs etc. But these all systems need to be secured as these all accessed by general public. It just indicate that these systems need a great security as if it could not be accessed by anyone from whom that system has threat to be used. Currently we have a lot of techniques which can be applied to systems and could be secured but on the counterpart there are lot of threats and attacks also have been developed which easily let the unauthorized entity to access these all above systems defined. So this insecurity inspired us to develop such a system that uniquely identified the persons on the basis of their feature. This system is termed as Biometric System.

Biometric literally means biological measurements of human features. This system has been used for securing the system to allow the person access on the basis of their individual human body parts which is unique for any particular individual. Those human parts could be iris, retina, and fingerprint and hand respectively. These all parts are really rare parts of any human it could not be resemble any of other individual ever. It means that part must be recognized at the time of accessing system, it's another issue that to which human body part that biometric system is dedicated among them. Hence, we can define biometric system as the system which is essentially a pattern recognition system used to secure the system acquiring the individual human body parts data by extracting a feature set from the acquired data and then matching these data set against the predefined feature set stored in the database.

Now depending on this methodology biometric system working can be segregated into two modes:

a. Verification Mode.
b. Identification Mode.

These terms has been explaining as follows:

Verification Mode*:* In this mode, biometric system already has a database in which it stores the authorised individual feature set as a template. This database strictly only has legitimate details regarding the human parts. Then the system validate the person's by matching their extracted feature set against to those feature set that has been stored as a template in a database. In such a case, an individual who willing to recognize himself as an claimed identity usually via PIN (Personal Identification Number), smart card, user name etc and the system then performs one to one matching to determine whether the claim is true or not. This mode is typically used for positive recognition just to prevent the other people from using the same identity.

Identification Mode: In this mode, the system already assumes to check if the claimed identity would be false. For this purpose, it check all the stored templates in their database by matching the individual feature set one to one, provided it doesn't matter whether to test claiming identity. This mode works on negative recognition nature where it checks whether the individual is who to which they denies to be. It simply signifies that the biometric has been extracted it would be further tested by matching the entire template stored in database that those biometrics are legitimate or not.

As through whole introduction we can generalize the term recognition which is the combination of Identification and Verification. It does simply match the pattern extracted involving the human features. On the basis of this recognition the person or individual would be proven to access the system as being a claimed identity.

Biometric system involves some issue to be concerning while developing this system to be used practically. These issues are:

Performance*:* It refers to resources required to achieve accuracy and speed of recognition of human features and the factors that could affect these aspects.

Acceptability*:* It refers to the extent up to which how much people would accept use of a particular biometric identifier in their general routine.

Circumvention: It refers that in how many ways the system can be easily get fooled by fraudulent methods.

BIOMETRIC IDENTIFICATION / RECOGNITION TECHNIQUES

Fingerprint Recognition:

Fingerprinting is the biometric technique that is most widely used in securing system. Fingerprinting was not a new concept as it was earlier born in 14th century in China. Chinese merchants used this technique in stamping's their children palm prints along with the footprints for identify them differently. After these from last three decades, this technique had brought revolution in security field either it is regarding to computer system or any of the automated system where security is a major concern. In Fingerprinting an image of finger has been taken and stored in the database as a template.

The image can be taken in two ways, one is the simplest one through ink and other is digital scanned. In the first method the popularity of ink could be an issue so later one has been preferred i.e. digital scanning. Digital scanner scans the pattern of fingerprint when user presses finger on the optical reader surface where the fingerprint pattern is taken and stored in the memory which is actually the database of that system. From that database the image of finger pattern that has been stored as a template then further used for the recognition by verification and identification comparison of claim's identity. Fingerprint has many advantages over other techniques, primary advantage is that no one has to remember their login Credentials (Username & Password), flexibility , interoperability and also the user can be unlimited. The main challenge of this technique is to maintain and clean the optical surface of scanner so that it would easily scan and match the pattern of any individual. As none of the technique is ideal so it could be possible that somehow someone could tricks the fake fingerprint in place of claim's identity pattern. Recently fingerprinting introduced through memory stick fingerprint scanner widely used in corporate sector. But there could be lot of works that has to be done regarding fingerprinting.

Fingerprinting examples are given as Casio computer and Alps Electric have developed a small fingerprint scanner built into a short, thin cylinder for use in cellular phones and other portable devices. Also, HP (Hewlett-Packard) became the first manufacturer to add biometric identity checking to electronic portable device, when its built small fingerprint scanner into its HP PDA. [1, 2, 3]

IRIS RECOGNITION

As we have many biometrics techniques, fingerprinting, hand shape and many more. These all are really very efficient techniques to secure any of the system by the use of human parts. The usage of these techniques involves the physical involvement of human parts like in fingerprinting one has to press finger on the optical scanner. Likewise, in other techniques also operator is required to make a physical contact with a sensing device or otherwise take some special action. Apart from this challenge, also a bit difficult stuff is to evaluate this scanned data from the scanner. One of the solutions of this difficulty could be automated face recognition, which is also an inherent subject for research. But if we would come more specific then iris recognition could be the most preferable biometric technique which doesn't involves any physical contact. Just as face iris is also the overt body part which is another alternative for the non-invasive human verification and identification. Let's have a detail of iris so that we have a clear picture that why it is preferable over other biometrics parts.

There are several layers which comprises iris actually, its posterior surface consists of heavily pigmented epithelial cells that make it light tight. Anterior to this layer are two cooperative muscles for controlling pupil. The other layer is Stromal Layer, consisting of collage nous connective tissue in arch-like processes. The most anterior layer of iris is the anterior border layer, which is densely packed somewhat differ from stromal especially with the pigment cells called chromataphores. The visual appearance of iris has itself given its multilayer vision. So this all about the detail of iris structure which is important to be known for moving into the technical issues for developing the system that can match its pattern uniquely for any individual. [4, 5]

Now there are three technical issues could be drawn to work with iris recognition. The primary issue is the IMAGE ACQUISITION. The second issue is to localize the iris pattern from the captured image. Final issue is as usual just to match the recognized pattern of iris with the candidate entry of their iris pattern. In this way Iris recognition system could be designed and implemented. There is lot of stuffs comes across the above defined technical issues which would be sorted out while the system actually going to be implemented and developed. [6, 7]

RETINAL RECOGNITION

Retinal Recognition is considered as the most reliable and effective biometric technique in the contrast of others like face recognition, fingerprint, hand geometry, keystroke dynamics and many more. But as we know along with these techniques we have to make physical contact on the optical scanner so that it could capture the image of human feature being used and thereby match the pattern. So to remove this dependency iris and retinal recognition has been preferable. Between the Iris and retina, it is little bit confusing as they both are too closed term. So, to clear this doubt let's have a look at below diagram

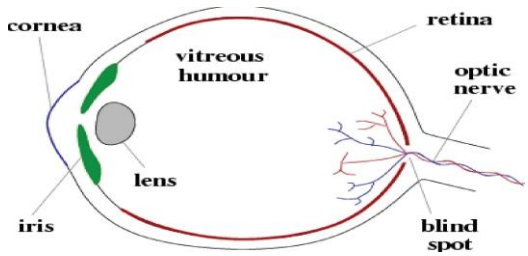

Figure 1: position of Iris and Retina in Eye

This diagram clearly shows us the iris and retina view in eye. The retina consists of multiple layers of sensory tissue and millions of photoreceptors which converts the transform light rays to electrical impulses. These impulses are travel through the optic nerve to brain, where they are converted into images. Retina consists of two distinct types of

photoreceptors: Rods and Cones. Rods facilitate clear night and peripheral vision and cones helps to watch out different colour around. It is the blood vessel pattern in retina which makes it fit for retinal recognition system used in the field of science and technology.

The overall working of retinal recognition has three parts, first is Image signal acquisition and processing for capturing the image of retina and changes it into the digital format. Then match that format with the user pattern. Finally represent the unique feature of retina of any individual as and template. As this process is same as other biometrics techniques but in retinal recognition the image acquisition and processing is somewhat a difficult task. Its simplicity is completely depends on the user stability towards the scanner as user has to fix their position very close to lens. Once user has a look in scanner it actually sees a green light in white background and immediately the scanner gets activated and thereby green light moves in a complete 360 degree circle. During this process the blood vessel pattern of retina has been captured. Then in the data extraction stage the reliability of retinal recognition have been realized as it is able to given 400 data points in contrast to other biometric techniques like fingerprint it has only 30-40 data. Hence on the basis of extracted data converted into template will be used for the matching pattern.

HAND GEOMETRY

There are so many biometrics techniques which have been used for the security system. But some techniques like fingerprinting have some inconvenience of using two different sensors. This inconvenience avoided in the hand geometry and palm geometry as well. The thing is how it could be avoided in this biometrics as these techniques also using the human feature. So the answer is the features including the hand geometry have been using same image captured from the digital camera at the same time. Every grey level image are aligned and used to extract hand geometry features. Then finally these are the features, which would be used for matching the pattern of individual. [8]

Hand geometry doesn't use any kind of special illumination technique for acquiring the feature; its working is really very simple which wouldn't lead any difficulty to user and system for the identification and verification process. For every process of identification many of the human features have been suggested like face, finger, iris, retina and fingerprint. But the problem with this entire feature is that it is much time variant means it could be varied time to time. Like if let's say iris recognition totally depends on person mood if one is upset or depressed then never would be fix their pose towards the scanner. In the same way, fingerprinting also has limitation if the person belongs to manual labours or there is an issue of minor detail. So having so many limitations we could prefer hand geometry.

Hand geometry includes the size of hand, area of palm, length and width of fingers. These all are the measurements that are responsible for the hand geometry. The current research involves the system in which user doesn't have to go through multiple sensors, also it includes palm geometry means integrates the palm print feature as well. They both would be acquired by getting single hand image. This all have been achieved by the image that had been taken from digital camera would be undergone for thresholding. Then the binary image which is a resultant binary image is used to determine the actual orientation of image. Then hand has to align in the preferred direction. The rotated binary image is then finally used for acquiring the hand geometry. To avoid any of the fraud with the hand geometry the palm print have been included with this method as in the verification process it will give the much more detail of geometry features of hand. [9]

KEYSTROKE DYNAMICS

Since internet or online systems are widely used in the current scenario. Really they are amazing and highly effective way of accessing the resources over network. But along with this truth it is also a fact that there are lots of security threat to this systems and sometimes it would hard to determine what type of attack could harmful for the system? For these shortcomings biometric systems are deployed for identification and verification of claim's identity. Biometric techniques generally basis on the human feature and after capturing these features it will match them with the predefined template and verified. It includes the static or non-static means behavioural aspects influence these systems. Therefore it indicates that biometric should be robust in nature and adaptive to change. Hand, face, iris & retina are the features that are widely used for the biometric technique. There are many devices available commercially based on these techniques. But among these techniques some would be easy to fool and rest of the technique like iris or retina pattern recognition are highly expansive and invasive. To overcome these limitations a foolproof method which can be deployed is keystroke dynamics. Keystroke dynamics is not to determine what user typing on the keyboard rather than to analyse how the keys had been typed on the keyboard device. Pattern recognition involves Representation, Extraction and Classification.

Representation used for represents the input data that measures characteristics of pattern or object to be recognized. Extraction actually involves only the relevant characteristics that should be extracted from the input data. Classification finally indicates the extracted data have been belonging to which class. Keystrokes dynamics have been analysed by monitoring the keystrokes typed on keyboard thousands of times per second. Keyboard typing rhythm is unique sign for any individual. It includes that how a person speedily type a word on keyboard, how hard one would type keys on keyboard etc. According to these monitoring an individual would have been authenticated. It involves static and continuous ways for monitoring. Static verification only does on the specific times while the continuous verification of keystroke dynamics does throughout the interaction. [10]

SIGNATURE RECOGNITION

We are familiar to the term digital signature, signature in the image form or could be captured as an image and used for verification. But signature recognition is not such a simple process. Signature recognition has been evolved just for the unique way of finding the signature in this process. It includes data that have been captured like dynamically captured direction, stroke, pressure and individual signature

shape. These all could help in making the individual hand writing much unique and make one's identity legitimate. Signature recognition actually goes through the close and rare analysis of an individual handwriting on the basis of not only a single but multiple characteristics. However, it varies vendor to vendor and all are using different sensitive technologies for analysing all these characteristics. These technologies include PDA & digitizing tablets. It doesn't use any of the static or general characteristics rather than it uses dynamic characteristics although some of the vendor has also includes static characteristics. This multiple characteristics include velocity, acceleration, timing, pressure and direction of strokes generated after signature. These are determined in all the directions X, Y & Z. Among these directions X & Y are used to analyse the velocity and Z direction used to analyse the changes in the pressure in the respect of time. Some of the algorithms have been implemented in the signature recognition that could be helped in also determining the changes in the natural drift or changes that have been occurred in the human signature time to time. The characteristics that have been involves in the signature recognition could not be forged so easily and hence it is really be much difficult task to copied the same signature used for any illegal offense. [11, 12]

SPEECH RECOGNITION

Speech recognition is not an unfamiliar term as it had been in used from long time in different forms. Speech recognition is now widely used as a security purpose. In earlier time's sound recorders was an inspiration to deploy the security system including speech recognition. Speech recognition actually traces the pattern of voice. We can elaborate this by saying that the vibrations one has been produced in the environment has been captured in by the speech recognizer machine and hence that vibration transform into the pattern and would be save as a template in the database. Then this pattern would be further used for the verification and identification of the claim's identity.

COMPARISONS OF BIOMETRIC TECHNIQUES

Table: 1

Techniques / Aspects	Fingerprint Recognition	Iris Recognition	Retinal Recognition	Hand Geometry	Keystrokes Dynamics	Signature Recognition	Voice Recognition
Security	m	H	H	m	H	h	h
Flexibility	h	M	M	h	H	h	h
Reliability	m	H	H	m	M	m	m
Distinguish ness	m	H	H	h	H	m	m
Effectiveness	m	H	H	h	M	m	m
Cost	h	H	H	m	M	h	h
Scope	m	H	H	h	H	m	m

Where, High = h, Medium = m & Low = L

CONCLUSION

Reliable personal recognition is crucial for multiple business applications. Biometrics refers, automatic recognition of the individual based on his/her behavior and physiological properties. Biometrics, means of verifying the personal identity by measuring and analyzing physical and behavioral properties like fingerprints or voice patterns. Biometric payment system in which no body have to take with dozens of cards for shopping, traveling, pass in office, university or bank as door lock. Conclusion of this whole paper is that, paper gives the brief description of the all biometric based identification techniques with their comparisons.

REFERENCES

[1]. Anil K. Jain, Arun Ross and Salil Prabhakar "An Introduction to Biometric Recognition" Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[2]. RICHARD P. WILDES, MEMBER, IEEE "Iris Recognition: An Emerging Biometric Technology" Manuscript received October 31, 1996; revised February 15, 1997.

[3]. Ravi Das " Keesing Journal of Documents & Identity, issue 22, 2007"

[4]. Fabian Monrose, Aviel D. Rubin "Keystroke Dynamics as a Biometric for Authentication" 2009, page no. 1-15.

[5]. Ajay Kumar1, David C. M. Wong1, Helen C. Shen1, Anil K. Jain "Personal Verification using Palmprint and Hand Geometry Biometric" 2010.

[6]. B.H. Juang# & Lawrence R. Rabiner "Automatic Speech Recognition – A Brief History of the Technology Development" 2011.

[7]. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and PrivacyConcerns", IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

[8]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, NY, 2003.

[9]. A. K. Jain, R. Bolle, and S. Pankanti (editors), Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.

[10]. CNN World News, "Schiphol Backs Eye Scan Security", March 27 2002. Available at http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security.

[11]. Y. A. Zuev and S. Ivanon, "The Voting as a Way to Increase the Decision Reliability. Foundations of Information/Decision Fusion with Applications to Engineering Problems, pp. 206-210, Washington D.C., USA, August 1996.

[12]. R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 12, No. 10, pp. 955-966, Oct 1995.

Short Bio Data for the Authors

Er. Akash Shrivastava received the B.Tech (Information Technology) degree from United College of Engg.& Research, Allahabad, Uttar Pradesh Technical University (UPTU), Lucknow (U.P.), INDIA, in 2010. Pursuing M.Tech (Information Technology) from Graphic Era University, Dehradun, INDIA. Currently, working as an Assistant Professor in Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), INDIA. My research areas are Web Mining and Web Security, Biometrics Identification and Authentication Techniques.

Er. Vedpal Singh received the B.Tech (Computer Science and Engineering) degree from Shobhit Institute of Engineering and Technology, Saharanpur, Uttar Pradesh Technical University (UPTU), Lucknow (U.P.), INDIA, in 2009. Completed M.Tech (Computer Engineering) from University Institute of Engineering and Technology (Kurukshetra University Kuruukshetra), Haryana, INDIA in 2011. Currently, working as an Assistant Professor in Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), INDIA. My research areas are Smart Card Security Techniques, Biometrics Identification and Authentication Techniques and Cryptography and Aerospace Security.

