International Journal of Computer Science and Engineering Research and Development (IJCSERD), ISSN 2248-9363 (Print), ISSN 2248-9371 (Online), Volume 2, Number 1, July-December (2012), pp. 07-14
© PRJ Publication http://www.prjpublication.com/IJCSERD.asp

A SECURITY BY BIOMETRIC AUTHENTICATION

Gurudatt Kulkarni[1], Ruchira Chandorkar[2], Nikita Chavan[3]

1, 2, 3 Lecturer in Marathwada Mitra Mandal's Polytechnic, Thergaon, Pune

ABSTRACT

This paper present a state of art about biometric hand, different techniques used. Biometric is essentially used to avoid risks of password easy to find or Stoll; with as slogan save Time and Attendance. BIOMETRICS is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics comes from two Greek words and means life measure. To provide a comprehensive survey, we not only categorize existing biometric techniques but also present detailed of representative methods within each category. Biometrics is a rapidly evolving technology which is being widely used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry devices. Although many technologies fit in the biometric space, each works a bit differently. Relatively new on the biometric scene, face recognition devices use PC-attached cameras to record facial geometry. Once the biometric data is collected, it is encrypted and stored--locally, in the case of the desktop-only products; in a central database for the network solutions. When a user tries to log on, the software compares the incoming biometric data against the stored data.

Keyword: - Retina, Authentication, Face, Speech

1. Introduction

Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics. Biometrics

refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-of identification; identification based on biometric techniques obviates the need to remember a password or carry a token.[1] With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest. Various types of biometric systems are being used for real-time identification, the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilize iris and retinal scan speech, facial thermo grams, and hand geometry. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user. An important issue in designing a practical system is to determine how an individual is identified.

2.0 History of Biometrics

Interest in biometric identification eventually moved from measuring characteristics of the hand to include characteristics of the eye. In the mid-1980‘s the first system that analyzed the unique patterns of the retina was introduced while, concurrently, work was being performed to analyze iris patterns. In the 1990‘s, research continues on developing identification systems based on a wide variety of biometric patterns, such as the traditional biometrics mentioned above (i.e. fingerprint, hand geometry, iris, and retina), along with the development of voice, signature, palm print, and face recognition systems. A few new, innovative approaches are also being examined for biometric analysis, such as ear shape, DNA, keystroke (typing rhythm), and body odor. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to moderate access to restricted systems. However, security can be easily breached in these systems when a password is revealed to an unauthorized user or an impostor steals a card. Furthermore, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user).[2]

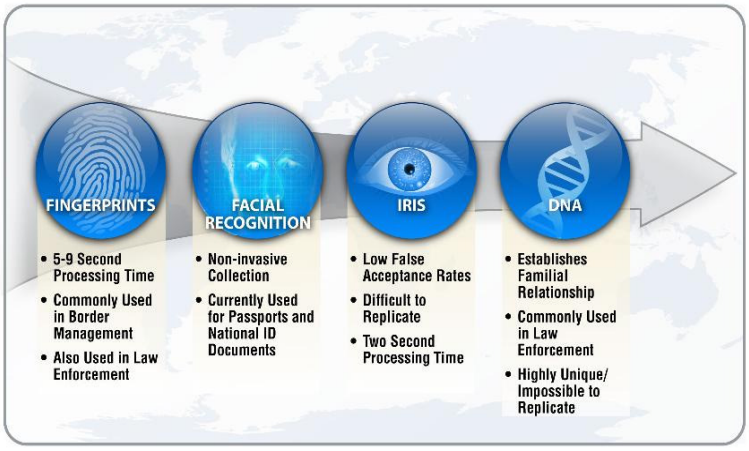

Figure 2.1 Biometric Techniques with advantages and Disadvantages [6]

3.0 TYPES OF BIOMETRICS

3.1 Face Recognition

The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image.[3] Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis. The face is the commonly used biometric characteristics for person recognition. The most popular approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features. Facial recognition templates are typically 83 to 1,000 bytes. Facial recognition technologies can encounter performance problems stemming from such factors as no cooperative behavior of the user, lighting, and other environmental variables. Facial recognition has been used in projects to identify card counters in casinos, shoplifters in stores, criminals in targeted urban areas, and terrorists overseas. [4]

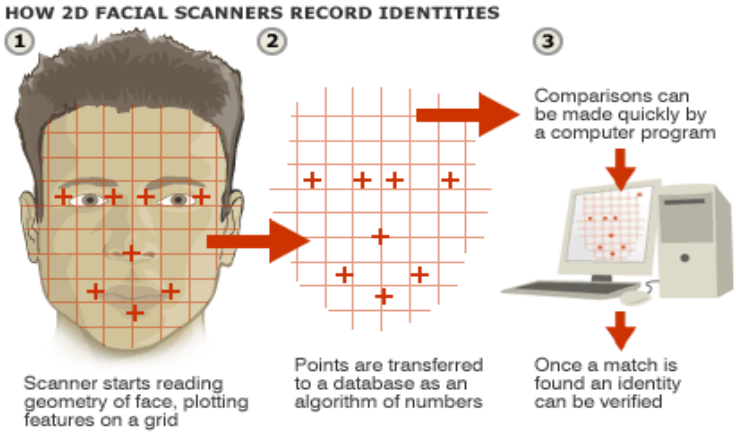

Figure 3.1 Face Recognition Systems [7]

3.2 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

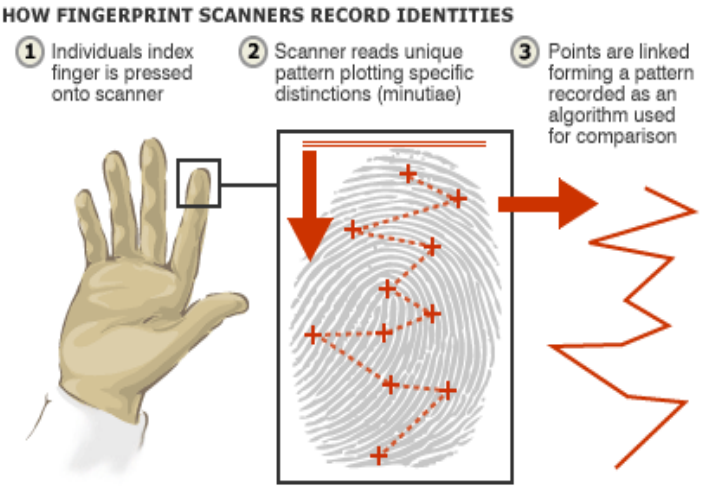

Figure 3.2 Fingerprint Identification [7]

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.[5] 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.

3.3 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. 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.[5] 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. Figure 3.3 shows Iris recognition system points that is to be considered.

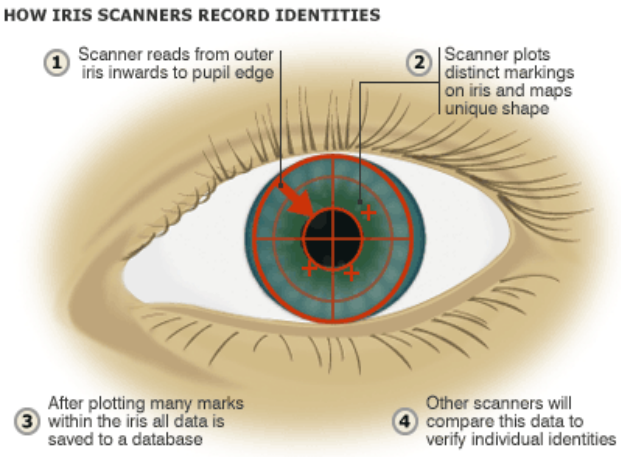

Figure 3.3 How Iris Scanners Record Identities [6]

3.4 Voice Recognition

Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. Voice recognition can be affected by such environmental factors as background noise. Additionally it is unclear whether the technologies actually recognize the voice or just the pronunciation of the pass-phrase (password) used. This technology has been the focus of considerable efforts on the part of the telecommunications industry and NSA, which continue to work on improving reliability. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology. Voice authentication is a fairly simple process. To register, a user records sample(s) of their voice which are stored in the authenticating system and become known as their _voiceprint‘. Then, to access this resource subsequently, they supply a sample of their voice to the system, and it decides if it matches their voiceprint before allowing them access. Voice authentication is best used for identifying persons over the phone or in an environment that can control background noise; however, today‘s solutions are better equipped to handle background noise than they were a few years ago. Mobile phone conversations are less of an issue, and the migration to voice over IP (VoIP) will help with the integration. The technology, however, has taken a back seat to other initiatives such as enhanced voice identification and routing systems. Figure 3.4 shows voice based authentication system.

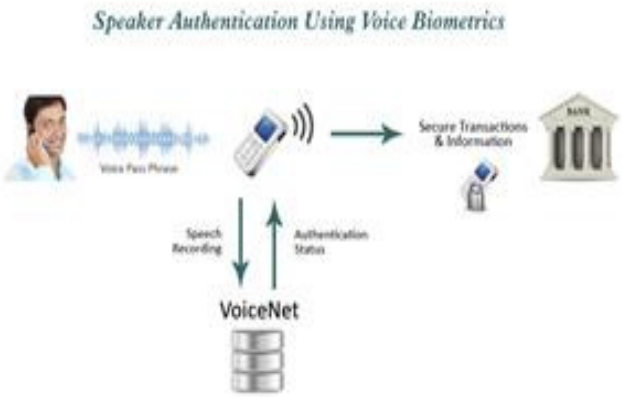

Figure 3.4 Speech Recognition System

4.0 ISSUES OF BIOMETRICS [2]

While biometric systems can offer greater levels of security, various attacks exist to gain unauthorized access to a system that is protected by biometric authentication. The various issues of the biometric system are dealt here.

4.1 System Design Issues

Biometrics is invariably associated with security; hence the biometric system itself should be reasonably secure and trustworthy. Some of the biometric security issues are

- ✓ Rogue sensors and unauthorized acquisition of biometric samples
- ✓ Communications security between sensors, matchers and biometric databases
- ✓ Accuracy
- ✓ Speed
- ✓ Scalability
- ✓ Resilience
- ✓ Cost
- ✓ Privacy

4.2 Authentication or Identification

The various key issues to be considered during the examination of biometrics for authentication systems are discussed here. First we need to identify whether the system is meant for identifying users, or simply authenticating users. Identification of a user is a much more difficult task. In contrast, identification does not involve a claim of identity at all. Instead, the system is presented with a set of (ideally complete) credentials, and asked to compare this set of credentials against the users it knows of, returning a result, which identifies the user, in question. This is known as a one to many tests, and it should be evident that this type of test is both more labour intensive for the system, and more reliant on having a wide range of attributes to compare users with.

4.3 Failure Rates

Failure rates are a critical consideration in the configuration and day to day running of a biometrics system. Two types of failure rates must be considered; false acceptance rates, and

false rejection rates. These failure rates are a function of how precisely the system attempts to verify each user against the characteristics registered for them. Thus, a system, which is configured, to be very precise and have very low false acceptance rates will almost invariably be performing a higher number of false rejection rates, relative to a balanced system. Similarly a system, which involves lower value access, will likely be granted to be less precise to ensure that the positive customer experience is delivered.

4.4 Liveness

A number of attacks on biometrics systems have been proposed over the years, and a number have been quite successful. Fingerprinting systems were originally entirely reliant on fingerprints for authentications, meaning that moulded synthetic fingers with imprints of fingerprints could be used to authenticate users. Similarly, hand geometry systems were entirely reliant on superficial physical attributes. Since these attacks have been proposed, a new area of biometrics has arisen which focuses entirely on determining whether the authenticating attributes being measured are in fact the attributes of a living being, as opposed to a recording or a synthetic imitation. The mechanisms are varied, relying on things such as prompted user actions to smile for facial recognition. In the area of fingerprinting systems have been developed to measure both perspiration and the pulse of the authenticating user. Hence, liveness testing is becoming a vital part of biometrics systems.

4.5 Circumvention

It is the key that when rolling out a biometrics system, the view of a system as a chain is maintained, along with the understanding that a system is only as secure as the weakest part of that chain. Biometrics offer a strong means to authenticate users for systems, however attackers will tend to attack systems at their weakest point, not their strongest. It is vital that biometrics serve a supporting role in well designed, properly secured systems. Installing biometrics into a fundamentally weak system is a waste of both resources and time.

4.5 Scalability

There are general concerns related to the scalability of biometrics systems - it is key that any solutions vendor be pressed to prove that the solution offered is going to be appropriately scalable.

CONCLUSION

Biometrics is a promising and exciting area, where different disciplines meet and provide an opportunity for a more secure and responsible world. There are a number of popular biometrics mechanisms currently deployed, some with strong histories, and some relatively new mechanisms. Each mechanism has its own strengths and weaknesses. When properly applied, biometrics can be used to combat fraud, and ensure that timekeeping systems are honest and accurate. Using one biometric feature can lead to good results, but there is no reliable way to verify the classification. To achieve robust identification and verification two different biometric features can be combined. A multimodal biometrics can provide a more balanced solution to the security and convenience requirements of many applications 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. "A Survey of Biometrics Security System",Mohammed Nasir Uddin, Selina Sharmin, Abu Hasnat Shohel Ahmed and Emrul Hasan,Shahadot Hossain5 and Muniruzzaman, IJCSNS International Journal of Computer Science and Network 16 Security, VOL.11 No.10, October 2011.
2. "Biometrics: An Overview of the Technology, Issues and Applications", S. Asha, C. Chellappan, Department of Computer Science & Engineering Anna University, Chennai , International Journal of Computer Applications (0975 – 8887) Volume 39– No.10, February 2012
3. "Analysis of various Biometric Techniques", Mr. Sanjay Kumar, Dr. Ekta Walia, Department of Computer Science & Engineering, Maharishi Markandeshwar University, International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1595-1597
4. "BIOMETRIC: CASE STUDY" Sushma Jaiswal Lecturer, S.O.S. in Computer Science, Dr. Sarita Singh Bhadauria Professor & Head, Department of Electronics Engineering Journal of Global Research in Computer Science Volume 2, No. 10, October 2011
5. " BIOMETRICS BASED IDENTIFICATION TECHNIQUES (BIT)", Akash Srivastva, Vedpal Singh, CSE Dept. Dev Bhoomi Institute of Technology (DBIT), Journal of Global Research in Computer Science, Volume 2, No. 11, November 2011
6. http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/index.html
7. http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn2page1.stm