ISSN: 2321-7782 (Online)
Volume 3, Issue 6, June 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Biometric Authentication System: Techniques and Future

Ravi Kant Thakur
Shiva Institute of Engineering & Technology
Chandpur, Bilaspur Himachal Pradesh - India

Abstract: ***Advances in the field of Information Technology make Information Security an inseparable part of it. In order to deal with security, Authentication plays an important role i.e. verifying that the user is who he claims to be. We can authenticate an identity in three ways: by something the user knows (such as a password or personal identification number), something the user has (a security token or smart card) or something the user is (a physical characteristic, such as a fingerprint, called a biometric. Biometrics ensures that the rendered services are accessed only by a legitimate user, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity. In this paper we have outlined opinions about the usability of biometric authentication systems, different techniques, their advantages and disadvantages and its future possibilities.***

Keywords: Biometrics, authentication, security, contact biometric techniques and contactless biometric techniques, Mobile Biometric (MOBIO) Authentication, Multimodal biometric system.

I. INTRODUCTION

Authentication is the process of identifying an individual. This usually involves a username and a password. Authentication is equivalent to showing your driver's license at the ticket counter at the airport. [7] Biometrics (or biometric authentication) consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. [5] Any human physiological or behavioral characteristic could be a biometrics provided it has the following desirable properties:-

(i) Universality, which means that every person should have the characteristic,

(ii) Uniqueness, which indicates that no two persons should be the same in terms of the characteristic,

(iii) Permanence, which means that the characteristic should be invariant with time, and

(iv) Collectability, which indicates that the characteristic can be measured quantitatively. [4]

The two categories of biometric identifiers

- Physiological: Physiological characteristics are related to the shape of the body, and include fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina), and odour/scent.
- Behavioral: Behavioral characteristics are related to the behavior of a person, including handwriting identification, voice detection, typing rhythm, gait, voice, etc.[5,10]

In 1856 fingerprints were used for the first time to identity purposes. In recent years, biometric authentication has proliferated in a range of domains, servicing anti-terrorism initiatives, such as secure ID cards and Visas, as well as corporate and consumer bio-logon and bio-authentication applications. Typical implementations employ a variety of authentication means and technologies, all of which are primarily geared towards offering users a secure and convenient alternative to the use of passwords. Unlike traditional authentication techniques, e.g., PIN code or password, biometrics provides an alternative yet

natural way for personal identity authentication. Biometrics handles authentication of individuals on the basis of biological and/or behavioral characteristics (measurements of the human body). As a primary advantage, biometric features are typically unique and, therefore, cannot be misplaced and forgotten since these are always inherently associated with human beings. In general, there are two types of biometric systems: identification for identifying an unknown biometric token as belonging to one of people (registered in the system) and verification for accepting or rejecting the identity claim of a person based on an input biometric token. In this paper, the selected biometrics will be discussed in order to develop biometric authentication systems of high performance and explore other novel applications, e.g., the use of biometric information in mobile security. [8] The use of biometrics in networks as an authentication feature is gaining momentum. However the widespread use and acceptance of biometrics is, at this current time, still in its infancy. [7]

II. WHY DO WE NEED BIOMETRIC AUTHENTICATION SYSTEM?

It is easy to understand the need for biometrics if you've ever forgot or left your network password on your computer. Aside from what's known as "logical" use—using a finger scan or another type of technology to determine if a user is allowed to access information is much better. There is an increasing need to find a way to solve user identification issues and cut costs for password administration. In educational institution the students found it difficult to remember passwords, or occasionally they borrow user names and passwords belonging to other students—and misused them. [4]

III. BIOMETRIC TECHNOLOGY [4]

There are many technologies. Biometric technologies are of two types.

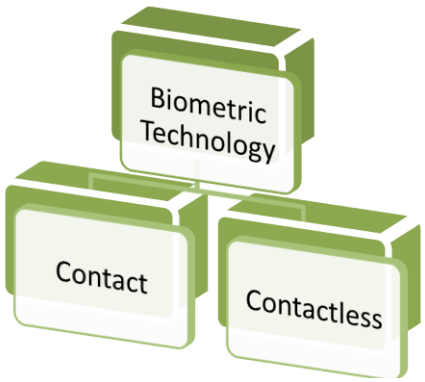

Fig 3.1 Biometric Technologies

Some of the contact biometric technologies are:

1. **Fingerprints:** Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique fingerprints [1]. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points.

Fig 3.2 Fingerprints Technology

Picture writing of a hand with ridge patterns was discovered in Nova Scotia. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals.

2. **Palm print and Footprint Authentication:** Whether it is palm prints or footprints, the evolution of the human blueprint has allowed them both to share virtually all of the same detectable characteristics as fingerprints. The major

difference is that the palm and foot are larger and can therefore yield a greater number of minutiae points to be used for comparison of the sample biometric to the stored biometric template.

3. **Dynamic Signature Verification:** Dynamic signature verification is an automated method of examining an individual's signature. It uses a stylus and surface on which a person writes. This technology examines dynamics, such as speed, direction, and pressure of writing; time that the stylus is in and out of contact with the "paper"; total time of the signature; and where the stylus is raised and lowered onto the "paper." Unfortunately, a signature is one of the least reliable methods of identification. Forgers have a myriad of ways to reproduce a signature that looks similar to the owner.

4. **Keystroke Dynamics:** Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. This technology examines such dynamics as speed and pressure, the total time of typing a particular password, and the time a user takes between hitting certain keys. This technology's algorithms are still being developed to improve robustness and distinctiveness. One potentially useful application that may emerge is computer access, where this biometric could be used to verify the computer user's identity continuously.

Some of the Contactless Technologies are:

1. **Facial Recognition:** Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. Noncooperative behavior by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies. Facial recognition has been used in projects designed to identify card counters in casinos, shoplifters in stores, criminals in targeted urban areas, and terrorists overseas.

2. **Facial Thermography:** Facial thermography employs the use of an infrared camera to capture the emission of heat patterns that are generated by the vascular system of the face. Heat that passes through facial tissue of a human being produces a unique and repeatable pattern (aura). The captured aura is converted into data and then compared to stored auras of authorized individuals, at which point possible matches are generate along with probability percentages.

3. **Voice Recognition:** Voice recognition is an automated method of using vocal characteristics to identify individuals using a pass-phrase. The technology itself is not well-developed, partly because background noise affects its performance.

4. **Retinal Scan:** Retinal scans measure the blood vessel patterns in the back of the eye. The device involves a light source shined into the eye of a user who must stand very still within inches of the device. Because the retina can change with certain medical conditions, such as pregnancy, high blood pressure, and AIDS, this biometric has the potential to reveal more about individuals than only their identity.

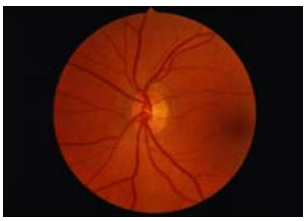

Fig 3.3 Retina Scan

5. **Iris Scan:** Working on completely different principles from retinal scanning, iris recognition is far more user friendly and offers very high accuracy. Furthermore, iris scanning has been adopted under license by certain high profile electronics companies who are able to develop good quality, interesting products and have existing marketing options for their distribution.

MULTIMODAL BIOMETRIC TECHNOLOGY

Multimodal systems are those which combine more than one biometric identifier. For example, it is currently planned to use face and fingerprints in European Union border control systems. Research initiatives have been launched on the application of multimodal biometrics in mobile communications (e.g. mobile telephones and other devices).

MOBILE BIOMETRIC (MOBIO)

MOBIO concept is to develop new mobile services secured by biometric authentication means. As mobile phone use involves transfer of personal data through the Internet, financial transactions etc, the technology selected should be stringent on false accept rate, which means that chances of permitting access to an imposter will be the least, even at the cost of denying access to an authentic user. At times our mobile phones become our bank cards. They are used as retail card, for ticketing. [11]

IV. Benefits of Biometric Authentication System

- Highly reliable, unobtrusive, fun and easy to use
- Truly compelling and captivating user experience that encourages users to rely on biometrics in a broad range of applications
- Based on a dynamic, intrinsic signal that inherently ensures "proof of life" and cannot be spoofed
- One-of-a-kind, single-chip "all in one" biometric solution
- Simple, low-cost integration and fast time-to-market
- Uniquely compact form factor and ultra-low power consumption
- Highly durable – suitable for use in any environment [9]

V. Applications of Biometric System

Most biometric applications fall into one of nine general categories:

- Financial services (e.g., ATMs and kiosks).
- Immigration and border control (e.g., points of entry, precleared frequent travelers, passport and visa issuance, and asylum cases).
- Social services (e.g., fraud prevention in entitlement programs).
- Health care (e.g., security measure for privacy of medical records).
- Physical access control (e.g., institutional, government, and residential).
- Time and attendance (e.g., replacement of time punch card).
- Computer security (e.g., personal computer access, network access, Internet use, e-commerce, e-mail, encryption).
- Telecommunications (e.g., mobile phones, call center technology, phone cards, televised shopping).
- Law enforcement (e.g., criminal investigation, national ID, driver's license, correctional institutions/prisons, home confinement, smart gun). [4]

VI. Feature use and Conclusion

Biometric system is actually a pattern recognition system that utilizes various patterns like iris pattern, retina pattern, and biological traits like fingerprints, facial geometry, voice recognition, etc. Biometric authentication is really attractive because of the fact that the PIN codes and the passwords can be interchanged but the physiological trait can't be. [9] The discussion above shows that biometric authentication is an interesting topic that a lot of research is going on in this area and that it can be used for secure systems despite all disadvantages. [2] There are various pros and cons of biometric authentication. The main advantage is basically the high levels of security as compared to conventional methods .Problems associated with passwords can be avoided

and a biometric characteristic can't be stolen as opposed to passwords etc. The various disadvantages are low acceptance rate, high cost associated with biometric authentication due to the integration into the current network and the acquisition associated with the hardware and the software, the danger of the individuals biometric data can be exploited. So all these disadvantages have to be worked upon to incorporate this brilliant technology in all security systems to ensure safer transactions and restricted access to them to prevent any kind of breach of security. [9]

References

1. "Biometric Authentication Systems", Faculty of Informatics Masaryk University, November 2000.
2. Birgit Kaschte: "Biometric Authentication systems today and in future", University of Auckland, October 2005.
3. "Introduction to Biometrics" by Anil Jain, Michigan State University, East Lansing, MI and Ruud Bolle and Sharath Pankanti, IBM T. J. Watson Research Center, Yorktown Heights, NY
4. http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies
5. http://en.wikipedia.org/wiki/Biometrics
6. http://httpd.apache.org/docs/1.3/howto/auth.html
7. http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/now.html
8. http://www.findaphd.com/search/ProjectDetails.aspx?PJID=21165
9. http://www.idesiabiometrics.com/in_the_news/..%5CIDesia%20Biometric%20Authentication%20Brochure.pdf
10. http://www.youtube.com/watch?v=B14ZiNdcOx8
11. http://www.youtube.com/watch?v=vpw9KcqgVvE
12. www.idesiabiometrics.com/applications/index.html

