IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Biometrics Identity Authentication in Secure Electronic Transactions

Deepu Saini[1] and Dr. Vijay Singh Rathore[2]

[1]Research Scholar, Singhania University, Jhunjhunu, Rajasthan, India
deepu254426@yahoo.com

[2]PhD (Computer Science), Singhania University, Rajasthan, India
vijaydiamond@gmail.com

Abstract

There are so many ways by which a person can be identified, but authentication of a person by biometric methods is assumed to be more secure. There are many reasons behind this e.g. in this world each person is having different biometric features, even the twins in this world having different biometrics features. In electronic transactions, biometric method is used from very early days but now a day's it is supposed to be the best and secure method for electronic transactions. In this paper the concepts regarding biometric identity authentication are explained.

Keywords: *Biometric Authentication, Removable Biometrics, Electronic Transaction, History of Biometric.*

Introduction

In Biometric Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective. The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

requirements, we should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption.

History of Biometrics

Biometrics has been around since 29,000 BC when cavemen would sign their drawings with handprints. In 500 BC Babylonian business transactions were signed in clay tablets with fingerprints. The earliest cataloging of fingerprints dates back to 1881 when Juan Vucetich started a collection of fingerprints of criminals in Argentina.

In earlier civilizations, branding and even maiming were used to mark the criminal for what he or she was. The thief was deprived of the hand which committed the thievery. Ancient Romans employed the tattoo needle to identify and prevent desertion of mercenary soldiers. Before the mid-1800s, law enforcement officers with extraordinary visual memories, so-called "camera eyes," identified previously arrested offenders by sight. Photography lessened the burden on memory but was not the answer to the criminal identification problem. Personal appearances change. Around 1870, French anthropologist Alphonse Bertillon devised a system to measure and record the dimensions of certain bony parts of the body. These measurements were reduced to a formula which, theoretically, would apply only to one person and would not change during his/her adult life. The Bertillon System was generally accepted for thirty years. But it never recovered from the events of 1903, when a man named Will West was sentenced to the U.S. Penitentiary at Leavenworth, Kansas. It was discovered that there was already a prisoner at the penitentiary at the time, whose Bertillon measurements were nearly the same, and his name was William West.

Identification and authentication

Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that makes an assertion or claim of identity. I&A process assume that there was an initial validation of the identity, commonly called identity proofing. Various methods of identity proofing are available ranging from in person validation using government issued identification to anonymous methods that allow the claimant to remain anonymous, but known to the system if they return. The method used for identity proofing and validation should provide an assurance level commensurate with the intended use of the identity within the system. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier are that it must be unique within its security domain.

Authenticators are commonly based on at least one of the following four factors:

- Something you know, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- Something you have, such as a smart card or security token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- Something you are, such as fingerprint, voice, retina, or iris characteristics.
- Where you are, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.

Removable Biometrics

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics. It was first proposed by Ratha et al.

Several methods for generating new exclusive biometrics have been proposed. The first fingerprint based cancelable biometric system was designed and developed by Tulyakov et al. essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Some of the proposed techniques

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

operate using their own recognition engines, such as Teoh et al. and Savvides et al., whereas other methods, such as Dabbah et al., take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancelable templates more accessible for available biometric technologies.

Biometric Project by Indian Government

India is undertaking an ambitious mega project to provide a unique identification number to each of its 1.25 billion people. The Identification number will be stored in central databases, having the biometric information of the individual. If implemented, this would be the biggest implementation of the Biometrics in the world. India's Home Minister, P Chidambaram, described the process as "the biggest exercise... since humankind came into existence". The government will then use the information to issue identity cards the word which is popularly known as AADHAR CARD. Officials in India will spend one year classifying India's population according to demographics indicators. The physical count began on February 2011. See Unique Identification Authority of India for more information.

Electronic Transaction Methodology

Accountability uses such system components as audit trails (records) and logs to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations
- Re-creating security incidents

If no one is regularly reviewing your logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence.
Many systems can generate automated reports based on certain predefined criteria or thresholds, known as clipping levels. For example, a clipping level may be set to generate a report for the following:

- More than three failed logon attempts in a given period
- Any attempt to use a disabled user account

These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

Conclusion

So in electronic transactions biometric authentication is very much popular and secure. This must be encouraged and used in more and more systems. This technology is used by many countries, starting in 2005; US passports with facial (image-based) biometric data were scheduled to be produced. Privacy activists in many countries have criticized the technology's use for the potential harm to civil liberties, privacy, and the risk of identity theft. Currently, there is some apprehension in the United States (and the European Union) that the information can be "skimmed" and identify people's citizenship remotely for criminal intent, such as kidnapping. The US Department of Defense (DoD) Common Access Card, is an ID card issued to all US Service personnel and contractors on US Military sites. This card contains biometric data and digitized photographs. It also has laser-etched photographs and holograms to add security and reduce the risk of falsification. There have been over 10 million of these cards issued. According to Jim Wayman, director of the National Biometric Test Center at San Jose State University, Walt Disney World is the nation's largest single commercial application of biometrics.[47] However, the US-VISIT program will very soon surpass Walt Disney World for biometrics deployment. The United States (US) and European Union (EU) are proposing new methods for border crossing procedures utilizing biometrics. Employing biometrically enabled travel documents will increase security and expedite travel for legitimate travelers. NEXUS is a joint Canada-United States program operated by the Canada Border Services Agency and U.S. Customs and Border Protection. It is designed to expedite travel cross the US-Canada border and makes use of biometric authentication technology, specifically "iris recognition biometric technology". It permits pre-approved members of the program to use self-serve kiosks at airports,

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

reserved lanes at land crossings, or by phoning border officials when entering by water.

References

[1] A. Rattani, B. Freni, G. L. Marcialis and F. Roli,"Template update methods in adaptive biometric systems: a critical review," 3rd International Conference on Biometrics, Alghero, Italy, pp. 847-856, 2009

[2] McConnell, Mike (January 2009). "KeyNote addresses". Biometric Consortium Conference Tampa Convention Center, Tampa, Florida,. Retrieved 20 February 2010

[3] Schneier, Bruce "The Internet: Anonymous Forever". Retrieved 1 October 2011

[4] Pfleeger, Charles; Pfleeger, Shari (2007) Security in Computing (4th ed.). Boston: Pearson Education. p. 220 ISBN 978-0-13-239077-4

[5] Kent, Jonathan (31 March 2005). "Malaysia car thieves steal finger". BBC Online(Kuala Lumpur). Retrieved 11 December 2010

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, vol. 40, pp. 614–634, 2001

[7] S. Tulyakov, F. Farooq, and V. Govindaraju, "Symmetric Hash Functions for Fingerprint Minutiae," Proc. Int'l Workshop Pattern Recognition for Crime Prevention, Security, and Surveillance, pp. 30–38, 2005