ISSN 2277-3061

Security Defects in Identification Systems which depends on Biometrics and the Mechanisms of repairing

Dr. Mozamel M. Saeed, Mesfer A. Al Duhayyim
Salman Bin Abdul-Aziz University, collage of science, Dept. of computer science, KSA,
E-mail:mozamel8888@gmail.com
Salman Bin Abdul-Aziz University, collage of science, Dept. of computer science, KSA
E-mail:mesferabdu@hotmail.com

ABSTRACT

Biometrics is one of the evolving technologies widely used in different aspects of life today. The use of biometrics for identification is a system mainly established to recognize a certain person through authentication by using a set of biological characteristics. In this paper, I aim to survey the security risks and defects in identity verification systems that are based on biometrics, and try to suggest risk management solutions in order to increase the security factor whenever using such systems.

Indexing terms/Keywords

Biometrics; Biometric techniques; Identification Systems; Security Defects in Biometric; manipulation Mechanisms.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 14 . No. 2

www.ijctonline.com , editorijctonline@gmail.com

ISSN 2277-3061

1. INTRODUCTION

Biometrics technology is an automated process used for the verification of identity (living person), based on the human body physiological characteristics, including fingerprints, eye retinas and irises, facial patterns, hand measurements, signature, style of keyboard use, voice patterns and DNA to differentiate between individuals. All this data will be read and stored in a computer software. In terms of usage, the human body biometrics is considered one of the safest, easiest and most reliable processes for identity verification. It is characterized by permanency and durability that cannot be stolen (seized by others) or altered. The biometric system consists of a scanner, which saves individual bio- image (digital/ photograph), a processing/comparison system and an application interface to display the result.

Biometric application has many advantages. The most important ones are: it provides the information networks with a high degree of security, an advantage which other processes cannot provide and speeds identification. The identification of users through biometrics cannot be lost, stolen, forgotten or reproduced. It is also difficult to be transferred to other person or to be forged. Biometric identification is moreover available with the person everywhere in addition to its essential role in all civil aspects, such as issuance of identity documents, health card, bank transactions and all other daily matters that require identification or security. Likewise, we should not forget the usage of biometric application in security procedures to investigate crimes and fingerprint/footprint taken at the crime scene or in the search of criminals, terrorists and boarder intruders and to control access into restricted areas.

2. Biometric Characteristics

"Biometrics" as a term refers to human physiological characteristics to identify human being. However, the other characteristics of biometrics include:

Universal: It is a worldwide trait. Can seldom be lost as a result of an accident or disease.

Invariance of properties: They should remain unchanged over time without transformation. The trait should not consider the differences based on age, either episodic or chronic disease.

Measurability: The capability of being measured without waiting, and easy to collect the data of passive characteristic.

Singularity: The distinctive characteristics of each person should differ from the other. Regarding the height, weight, hair, and eye color. These characteristics are unique and accurate, but still not useful for more than one category.

Acceptance: The exploring should be acceptable to a large number of residents. With the exception of the persistent technology that is part of human body.

Reducibility: Data should be reduced to a file which is easy to handle.

Reliability and tamper-resistance: High reliability and reproducibility are needed, therefore the attribute should be impractical and easy to modify.

Privacy: The process should preserve the privacy of the individual and not break it.

Comparable: They should lessen the possibility of comparison with others. with less probability towards similarity and more dependence on identification.

Inimitable: Not capable of being initiated or imitated, they are matchless (Biometric technologies): fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature all satisfy the above requirements.

ISSN 2277-3061

Table 1. Strength and Weakness of Biometrics Technology

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Face	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

3. Biometric System Mechanisms

Biometric systems work in three distinct stages:

1- Entry of basic information: in case of using the biometric system for the first time, your personal information shall be registered, including your number and name, and one of your biometric features, like the image of your face or fingerprint, will be documented using the appropriate sensors.
2- Extraction of unique feature information from the biometrics and digitally store it as codes or graphs in order to create a central data base, or to be stored in smart cards dedicated for each person.
3- Subsequently, the unique information extracted by the system from your recent biometrics will be compared with the unique information previously stored therein, or with the information existing in your smart card.

Full conformity is not a requisite, but the margin should not be bigger or smaller to the extent that it rejects the correct person or accepts the wrong one.

4. Biometrics Architecture

The above mentioned work mechanism of biometrics requires three fundamental components as follows:

1- A sensor that captures the individual biometric feature, such as a camera to photograph the face, or a fingerprint scanner.
2- A PC provided with the necessary software for reading and storing information.
3- Software for the purpose of biometric features analysis from which the unique information is to be extracted, using different algorisms. The same software will conduct the subsequent comparison and give the appropriate decision.

5. Statistical Standards of Performance Assessment

There are several statistical standards set by international organizations to assess functionality of any biometric system.

- False acceptance rate (FAR): it is the acceptance rate for individuals who are not identical.
- False acceptance rate (FRR): it is a non- acceptance rate for individuals, despite the correctness of the identities they claim.
- Failure to enroll rate (FER): it is a rate of failure to enroll the basic information.
- Failure to capture rate (FCR): it is a rate of failure of some sensors to capture biometric features.
- Central data base optical capacity: it stores the individual biometric information.

By applying the above mentioned statistical standards the extent of the system ability and efficiency can be measured.

6. Security Gaps in Biometric-based Identification Systems

Although such systems are highly secure, they have some security problems that expose them to risks. These problems can be summarized as follows:

1. Provision of false or counterfeit entry to the sensor, such as a mask or false finger, hand or signature (signature copy).
2. Sending of stored signals from earliest message, such as early voice or fingerprint registration.
3. Retrieval of distinctive features by viruses that produce features and traits specified by the assaulter.
4. Replacing of the distinctive features by the assaulter who enters into the channel that links the feature to the data base for the purpose of comparison.
5. Changing of the comparison so that the assaulter can attack the stored features in order to produce results similar to the results already entered.
6. Changing of the stored templates to enable the assaulter attack the database and change it, particularly if the data base is distributed among more than one server.
7. Attacking of the channel between the data base and the sender, then altering the transmitted template.
8. Falsification of the final result: this kind of assault is not usually possible; however, if that happens the system will be useless.

7. Mechanism for enhancing the security level in the biometric- based identification systems

To enhance the security level in such systems, the following factors should be observed:

1. Use of many types, such as taking of fingerprint and iris together or index and pollex fingers together, or ask the user to make entry more than once.
2. Use of multiple methods, such as use of a password with one type of the individual features.
3. Liveliness Check: use of methods and styles to make sure that the user is alive, such as measuring the body physical features, or checking of vital sing, like blood pressure, brain waves and heart signs.
4. Response: the system may require the user to make gesture like moving his head or blink his eyes, etc…This method is related to the previous one.
5. Maintenance of data: some systems, for instance, omit the images after comparing them. However, this complicates the process more and more for the assailants.
6. Encryption: it shall be made through the encryption of the stored data bases, or that the biometrics will be used as a key for the data encryption.

8. Conclusion

Bearing in mind the crucial role that the biometric systems play in the field of identification, this paper has indicated the risks which the biometric system may encounter and recommended the necessary protection approaches. However, they are not considered as the only optimal approaches for the information security, because there is no as yet full protection for this system (biometrics) and for all other systems in general. As the matter of fact, the enhancement of security aspect in these systems requires application of certain preventive processes/ procedures to prevent errors as well as to support the systems with state- of- the- art technologies in this field.

REFERENCES

[1] A. K. Jain, A. Ross, K. Nandakumar, "Introduction to Biometrics",Springer, 2011.

[2] A. K. Jain and A. Ross, “Multi biometric Systems,” Communications of the ACM 47(1), 34-40 ,2004.

[3] Anil K. Jain, Arun Ross, and Salil Prabhakar, “An Introduction to Biometric Recognition”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.

[4] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman,” Biometrics: A Grand Challenge”, Proceedings of International Conference on Pattern Recognition, Cambridge, UK, Aug. 2004.

[5] Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.

[6] C.C. Han, H. L. Cheng, C. L. Lin, and K. C. Fan, “Personal authentication using palm print features,” pattern Recognition 36,2003, 371-381.

[7] CHARACTERISTICS OF BIOMETRIC SYSTEMS

http://www.ccert.edu.cn/education/cissp/hism/039-041.html

[8] Ffingerprintrec(2006) ,http://www.biometrics.gov/documents/fingerprintrec.pdf.

[9] M. Indovina, U. Uludag, R. Snelick, A. Mink, A. K. Jain , “Combining COTS Finger and Face Biometrics for Identity Verification,” in Proceedings of Workshop on MultiModal User Authentication, , (2003), pp. 99-106.

[10] Papers to appear in biometrics

http://www.biometrics.tibs.org/FPpaperstoappear.htm , 2011 vol. 67, no. 3.

[11] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, Guide to Biometrics. Springer, 2003.

[12] R. Snelick, M. Indovina, J. Yen, and A. Mink , “Multimodal Biometrics: Issues in Design and Testing,” in Proceedings of Fifth International Conference on Multimodal Interfaces, , 2003, pp. 68–72.

[13] Renu Bhatia, “Biometrics and Face Recognition Techniques”, IJARCSSE, Volume 3, Issue May 2013.

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

[15] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92, No. 6, June 2004.

[16] X. Yang, J. Feng, J. Zhou, "Localized Dictionaries Based Orientation Field Estimation for Latent Fingerprints", PAMI 2014.

[17] Zdene˘k R íhaVáclav Matyáš “Biometric Authentication Systems,” FI MU Report Series, November 2000.

Author’ biography with Photo

Dr. Mozamel M. Saeed is the head department of Computer Science at Faculty of Science, Salman Bin Abdul Aziz University. I've published some papers internationally.

Mesfer A. Al Duhayyim is a lecturer department of Computer Science at Faculty of Science, Salman Bin Abdul Aziz University.