Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review

Israa M. Alsaadi

Abstract: With the fast increasing of the electronic crimes and their related issues, deploying a reliable user authentication system became a significant task for both of access control and securing user's private data. Human biometric characteristics such as face, finger, iris scanning ,voice, signature and other features provide a dependable security level for both of the personal and the public use. Many biometric authentication systems have been approached for long time. Due to the uniqueness of human biometrics witch played a master role in degrading imposters' attacks. Such authentication models have overcome other traditional security methods like passwords and PIN. This paper aims to briefly address the psychological biometric authentication techniques. Also a brief summary to the advantages, disadvantages and future developments of each method is provided in this paper.

Index Terms: Biometrics; authentication methods; face recognition; distinguishing of human characteristics; automatic verification of identities.

1 INTRODUCTION

Automatic identification/verification of an individuals' identity based on the analysis of his/her biological (biometric) traits is broadly known as biometrics technology [1]. Naturally, people depend on the observed features of a human body such as facial traits, voice, way of walking (gait), signature and etc. These ways are ideal to recognize others because of these characteristics are unique for each person [2]. With the increased dominance and wide popularity of IT applications, especially computational systems which deal with the commercial transactions such as online banking services. Users inherently perform their daily activities using computers. For examples, bank accounts, mailboxes, daily transactions and other activities. These systems contain sensitive information of their clients that are publicly shared within the Internet environment. The frequent use of this personal information has imposed and raised the security risks of such important systems from being illegally accessed or hacked by intruders or unauthorized users. Therefore, there is a significant need to control the users access of such applications which can strongly prevent impostors from accessing the critical information and use them for personal benefits. Basically, personal biometric attributes are divided into two main categories: physiological features and behavioral features [2,3,4,5]. Physiological characteristics are related to the static traits of a human body that are not subject to change over aging. Examples of physiological traits are face recognition, hand geometry, palm print, fingerprint, iris recognition, DNA, retina and recognition of blood veins pattern. On the other hand, the behavioral approach of biometrics is limited only to the behavioral traits of a human that deal with the personal behavior of an individual such as voice recognition, signature recognition, gait and keystroke dynamics [3,4,5]. Below, Fig. 1 lists the general classification of biometric authentication schemes.

- *ISRAA ALSAADI currently works as an assistant lecturer in the Computer Science Department at the University of Kufa/College of Education in Iraq, 009647723828633.*
- *E-mail: israam.alsaadi@uokufa.edu.iq*

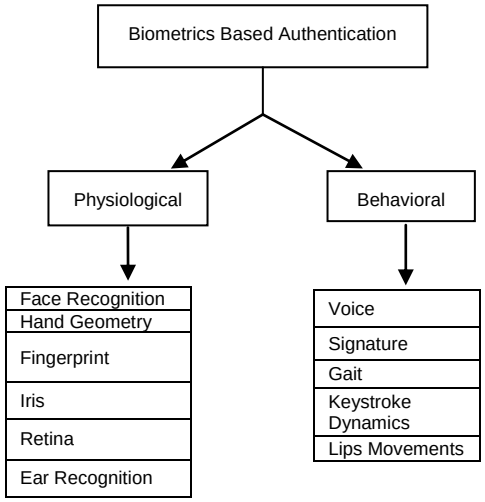

Figure 1. *General classification of Biometric schemes*

The Fig. 1 lists the current deployed biometric techniques in the computer security market. Although, biometrics authentication systems have overcome other traditional authentication schemes such as password or (pass codes) and PIN (Personal Identification Number). Till yet, there is no 100 percent guarantee about achieving highest level of performance regarding identification/verification of a person identity [3]. The purpose of this study is to provide a brief review of existing physiological biometric authentication techniques along with highlighting some of their advantages and drawbacks/obstacles. In addition, a recent literature of current developments of the reviewed authentication systems is provided in this paper. This paper has an extension of the work in [3] by including the future improvement of discussed security authentication systems. The general organization of this paper is described as follows: Section 1 is the general introduction about biometrics technology. Section 2 provides a brief historical overview of biometric authentication techniques. In Section 3, the essential mechanism of biometric security systems is introduced. Section 4 discusses the most common physiological biometric systems with more details for each method. At the end, Section 5 concludes the work of this paper and provides a future work.

2 Historical Overview of Biometric Systems

For the last few decades, security systems based biometrics have obtained a wide popularity and considerable amount of attention. However, the utility of biometric traits of human body started in the early past [2]. Biometrics as a terminology refers to the combination of the Greece words (Bio) and (Metrics) which means ''life measurements''[7]. Biometrics as a technology indicates the use of human physiological and behavioral characteristics for several security purposes such as identification/verification of one's' identity, access control, users authorization, data protection and security management [9]. There are numerous biometric authentication technologies were adopted by many committees in their security applications for long time. In contrast to the traditional security systems such as login passwords and PIN, biometric security techniques have shown an enhanced level of security [9,10]. However, these techniques have their own advantages and disadvantages as well. Below, is a brief overview of biometric authentication systems and some exposes to future developments of each method.

3 General Mechanism of Biometrics Authentication Systems

In general, most of biometrics based authentication systems have a common scenario of the practical implementation of each method. This general mechanism is divided into two main processes: the enrolment process and release process [2,6,7]. In the enrolment stage, a collection of data of user biometric attributes is included. The gathered information of system participants is manipulated in order to capture as much as biometric features of each individual. Then, these captured attributes are mathematically analyzed via specific algorithms and later on an unique template will be created for each user and stored in a database which will be used in the second stage [3,6]. In the release process, a comparison is made between sample of data of a subject and the template that is already stored in the database from the first process. The obtained result from the comparison process leads to the decision of either identifying or verifying a person identity. However, there is a potential difference between identification and verification of biometric authentication systems. The same scenario is conducted in most of biometric based authentication techniques to perform the security checking [2,3,7,8]. The general mechanism of biometrics technologies is well described in the blog diagram in Fig. 2 below.

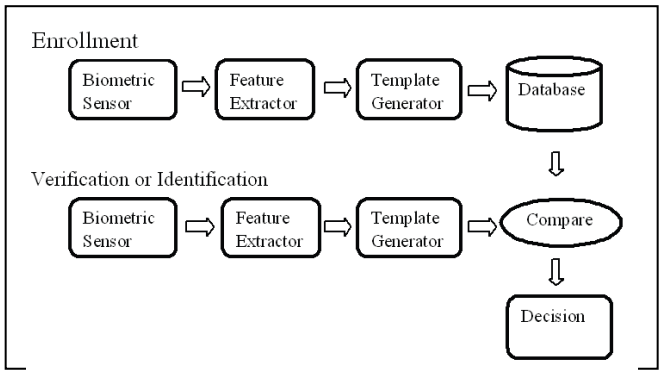

Figure 2. *Block diagram of biometric methods*

4 Physiological Biometric Authentication Systems

The subsections below introduce a brief overview of mostly used physiological characteristics for the automatic recognition of individuals.

4.1 Fingerprint Recognition

Fingerprint based biometric authentication systems became one of the most conducted, popular and successful authentication techniques among other biometrics security methods for both of identification and verification processes of one's' identity [2,3,8]. This biometric authentication method was developed based on the natural truth which indicates that each an individual has unique fingerprints of his/her hand that distinguish him/her from others. Moreover, each person has a different print on each finger. Even though when two identical twins have an observed similarity in their visible features but still they have totally different prints on each ones fingers [3]. This method was firstly studied by Francis Galton in 1892 when he firstly classified fingerprints into three main classes [11]. Figure 2. shows sample of a human fingerprint.

Figure 3. *Sample of human Fingerprint*

General scenario of the method: Biologically, the pattern of a fingerprint surface is basically classified into three main patterns are loop, arch and whorl [8]. As a biometric authentication system the automatic distinguish between two individuals is based on capturing the two main fingerprint characteristics are the valleys and ridges on the finger surface. These two patterns have specific followings in their direction and locations on the fingerprint. The process of collecting the fingerprint formation is done by scanning the finger surface using a specific device is called sensor [2,3,8]. Fig. 3 shows a sample of optical sensor.

Advantages: Deploying fingerprint recognition for the security purposes has been increasing in thousands of institutions for several reasons. First, the ease of use of this method by the users in comparison to the old method which was using physical inking of an individual fingertip in which a difficulty of removing the ink later on. Second reason is the low cost of implementation where the optical sensor is a cheap device [2,4,11,12]. Moreover, fingerprint-based authentication system does not require so much power [4]. Also, this method is implemented in mobile environment especially smart phones (e.g. iPhones) which makes it more desirable authentication technique [4].

Disadvantages: Although fingerprint recognition system has various its advantages ,this system has some drawbacks. This biometric system has some complexity in obtaining high-quality images of images of finger patterns. Due to the issues of dirty, cuts, tear and wear that can easily effect the ridges

and minutiae of fingertip [4,8].

Future Development: A new and challenging approach in biometric based individuals authentication has been recently introduced. Finger nail plate is an emerging authentication technology in the biometric study. This technique is based on the discriminate features on the surface of the finger nail plat. More details can be found in paper work of [13].

4.2 Face Recognition

The facial features (eyes, nose , lips and chin) of human have played a significant role in the recognition of individuals for long time. Depending on the unique shaping of each person's face, it has been a popular method in biometric recognition area [2,3,8]. Computers have contributed in the automatic recognition of individuals using the obvious facial characteristics which led to wide popularity of the Face Recognition System (FRS). There are many commercial software that are programmed to do the real identification of human facial features.

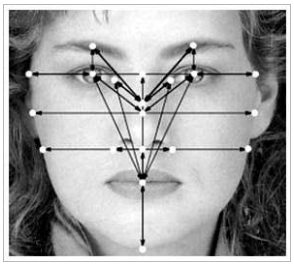

Figure 4. *Automatic face recognition system*

General scenario of the method: This method mainly conducts two ways for the facial authentication of individuals. First is static recognition of person's facial features depending on collecting a set of images by using photo-camera. Second is real time identification of persons based on video-camera. The captured images are used for creating a template for each sample (individual) and then a matching process is taken for the recognition purposes [2].

Advantages: Ease of use and the low cost of system implementation.

Disadvantages: Number of factors affect the overall performance of biometric based face recognition system. For examples, quality or resolution of collected photos for each individual, light conditions , angles of face rotation, etc. Also, different facial expressions impose some challenges on the automatic recognition of people identities such as sad expression, happy, angry and others [2,3,8].

Future Development: A lot of work has been done on the development of face recognition system. One of these recommendations on the improvement of this biometric authentication method is using 3-dimensional camera for data collection. In addition, some new trends of increasing the face recognition accuracy is using more accurate sensors to capture images of face skin. This method looks for the distinctive features in a user's face skin such as visual spots, lines and other unique patterns [3].

4.3 Iris Recognition

Iris is that colored circular part that is located in centre of the eye. The distinctiveness of iris pattern provides an effective recognition scheme of individuals. Based on the biological composition of the iris, it has a specific network of tissues that are visibly recognized. However, an individual's iris forms over the first year of the life when the iris characteristics cannot be genetically changed [2,8].

Figure 5. *Iris recognition system*

General scenario of the method: Similar to retina recognition, the general process of identifying/verifying a person is accomplished by capturing images of his/her iris. Then pass the iris images to the data analysis for extracting the discriminating features for each sample as preparing for the authentication process. This process is done by using a special camera that does the iris scanning.

Advantages: It is an optimal method for the automatic authentication of individuals due to the widespread of iris scanners in different security sectors. Also, the ease of use and flexible operating of scanning devices that make this technique in an increased demand [2,15]. Furthermore, this technique achieved a proper level of reliability in acquiring as much distinguished features as possible.

Disadvantages: A number of researchers have addressed different issues/factors that contribute in decreasing the accuracy of iris recognition. Some of these factors are wearing glasses, eye lenses and etc. Another difficulty of deploying iris-based biometric is the high cost of implementation of such authentication technique [8].

Future Development: Various papers have proposed more developments on the accuracy of iris scanning for the authentication mode in which three-dimensional camera is essentially preferred for this purpose.

4.4 Retina Recognition

In each person's eye, the retina is that layer which is made of a complicated network of neural cells at the back of the eye. This part has a unique features for each retina due to the complicated capillaries that is responsible for providing the retina with the blood [8]. Many studies have concluded that the blood vessel pattern is distinctive pattern for each single retina of the same person. This complication pattern of the retina has contributed in the development of new automatic authentication system for the fast distinguish among individuals [3]. In addition, any identical twins do not have the same patterns of their retina.

General scenario of the method: The technology of retinal scan-based authentication system uses a specific sensor for the data acquisition. In this process, a person is required to peep where the sensor directs on a particular spot in the visual

field in which the capturing of characteristics of blood vessel pattern is performed [3].

Advantages: This biometric authentication technique has obtained a large amount of attention because of the high level of accuracy of samples that can be obtained from the recognition of individuals.

Disadvantages: It causes kind of user's discomfort due to the hard efforts by the contributors while capturing their retina vessels. However, retina-scan based biometrics has some medical factors that can affect the accuracy of its authentication process such as high blood pressure[8]. Also, different papers have addressed other conditions that can decrease the performance of retina scanning like wearing glasses, lenses and etc [14].

Future Development: A few studies is conducted on the improvements of the blood vessel pattern of the retina for the automatic recognition of the individuals. Such as using a high resolution sensor for capturing more accurate images of blood vessel sample. Also, a new trend in retina recognition tries to provide an efficient implementation of this biometric method in mobile phones [4].

4.5 Hand Geometry Recognition

Many security systems and applications depend on the recognition of hand geometry as an automated technique for the identification/verification of their legitimate users. This biometric authentication method started taking a wide popularity in various security sectors. It was early installed and used as a biometric method since the late of 60s [2,3,15,16].

Figure 6. *Scanning of hand/palm geometry*

General scenario of the method: The measurements of the hand-geometry is obtained by scanning the hand area using a specific scanner for this purpose. A three-dimensional scanning takes different angles of the hand for better feature extraction in order to composite an accurate sample [2].

Advantages: This method has its positive points among other biometric authentication techniques. For example, ease of use and the wide acceptance by participants which make this method more friendly authentication system than other biometric systems.

Disadvantages: It requires a special hardware device for scanning the hand geometry. Such scanner needs to be a three-dimensional in order to acquire full information of the palm. In contrast with other devices which take only a few fingers information. Therefore, this method is considered as an expensive biometric authentication system [2]. Furthermore, there are some constraints which may impact the extraction of palm information such as the wearing some jewelries and etc. Another drawback of hand scanning is the large space which is required for storing the scanned information of palm geometry [8].

Future Development: One of the current improvement of hand recognition is working on simplifying the sensor device in order to reduce the overall cost of features extraction of an individual's hand geometry [8].

4.6 Ear Recognition

Another biometric authentication technique is conducted based on the recognition of the unique shape and appearance of human being ear. Naturally, a person is born with a visual shape of his/her ears. However, human ear is not subject to change while a person's growth and even aging [3,14]. It has a dependable stability which increases its level of security as a proposed method for the security identification/verification of individuals.

Figure 7. *Ear based biometric authentication system*

General scenario of the method: Ear recognition has the same scenario of face recognition in terms of ear features extraction and also matching processes. The actual recognition scenario of this approach is using specific measurements of outlook of the ear in which a mathematical model is created for providing a unique template.

Advantages: It is more comfortable/friendly method in terms of user contribution than iris and retina recognition.

Disadvantages: As like other biometric recognition schemes, ear-based biometric authentication has its own drawbacks. This method has not achieved a remarkable level of security yet. One of the disadvantages of ear recognition is the simple distinguished features of the ear that cannot provide a strong establishment of an individual's identity [3].

Future Development: Current efforts of pattern recognition researchers work on the development of ear recognition.

5 Conclusion and Future Work

Securing critical and sensitive systems from being illegally accessed by imposters has been a potential research field. Biometric based security authentication obtained considerable attention for its accuracy, reliability, universality and permanence etc. This paper overviewed the most conducted physiological biometric authentication techniques. The focus of this work is to briefly present various physiological biometric security methods. General scenario or mechanism of each technique is introduced. Also, some exposes to their key advantages, disadvantages and future improvements for each security system. A combination of several biometric security systems is highly recommended for best level of reliability and

accuracy. For example, face recognition can be easily combined with finger print system for achieving a better performance. Iris scanning is compatible with retina recognition were a high differentiating in person iris/retina features is perfectly obtained. Moreover, transforming such security authentication techniques from traditional practical environment into more flexible one such as mobile phones it can potentially upgrade the integration of the overall system.

ACKNOWLEDGMENT

THE AUTHOR OF THIS WORK WOULD LIKE TO THANK ALL ANONYMOUS REVIEWERS FOR THEIR MOTIVATION, SUPPORT AND COMMENTS DURING THE COMPLETION OF THIS RESEARCH.

REFERENCES

[1] Yanushkevich, S.N., "Synthetic Biometrics: A Survey," in Neural Networks, 2006. IJCNN '06. International Joint Conference on , vol., no., pp.676-683, 0-0 0

[2] Eng, A.; Wahsheh, L.A., "Look into My Eyes: A Survey of Biometric Security," in Information Technology: New Generations (ITNG), 2013 Tenth International Conference on , vol., no., pp.422-427, 15-17 April 2013

[3] Kataria, A.N.; Adhyaru, D.M.; Sharma, A.K.; Zaveri, T.H., "A survey of automated biometric authentication techniques," in Engineering (NUiCONE), 2013 Nirma University International Conference on , vol., no., pp.1-6, 28-30 Nov. 2013

[4] Weizhi Meng; Wong, D.S.; Furnell, S.; Jianying Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," in Communications Surveys & Tutorials, IEEE , vol.17, no.3, pp.1268-1293, thirdquarter 2015

[5] Pahuja, G.; Nagabhushan, T.N., "Biometric authentication & identification through behavioral biometrics: A survey," in Cognitive Computing and Information Processing (CCIP), 2015 International Conference on , vol., no., pp.1-7, 3-4 March 2015

[6] Lifeng Lai; Siu-Wai Ho; Poor, H.V., "Privacy-security tradeoffs in biometric security systems," in Communication, Control, and Computing, 2008 46th Annual Allerton Conference on , vol., no., pp.268-273, 23-26 Sept. 2008

[7] Xiao, Q. (2007). Technology review-biometrics-technology, application, challenge, and computational intelligence solutions. Computational Intelligence Magazine, IEEE, 2(2), 5-25.

[8] Dharavath, K.; Talukdar, F.A.; Laskar, R.H., "Study on biometric authentication systems, challenges and future trends: A review," in Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1-7, 26-28 Dec. 2013

[9] Ye Wang; Rane, S.; Draper, S.C.; Ishwar, P., "A Theoretical Analysis of Authentication, Privacy, and Reusability Across Secure Biometric Systems," in Information Forensics and Security, IEEE Transactions on , vol.7, no.6, pp.1825-1840, Dec. 2012

[10] Deutschmann, I., Nordstrom, P., & Nilsson, L. (2013). Continuous authentication using behavioral biometrics. IT Professional, 15(4), 12-15

[11] Zaeri, N. (2011). Minutiae-based fingerprint extraction and recognition. INTECH Open Access Publisher.

[12] Faundez-Zanuy, M., "Biometric security technology," in Aerospace and Electronic Systems Magazine, IEEE , vol.21, no.6, pp.15-26, June 2006

[13] Narhar, U.K.; Joshi, R.B., "Highly Secure Authentication Scheme," in Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on , vol., no., pp.270-274, 26-27 Feb. 2015

[14] Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," in Circuits and Systems for Video Technology, IEEE Transactions on , vol.14, no.1, pp.4-20, Jan. 2004

[15] Liu, Simon; Silverman, M., "A practical guide to biometric security technology," in IT Professional , vol.3, no.1, pp.27-32, Jan/Feb 2001

[16] Delac, K.; Grgic, M., "A survey of biometric recognition methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium , vol., no., pp.184-193, 18-18 June 2004