Journal of Engineering Science and Technology
Special Issue on ACSAT, October (2021) 111 - 119

THE STUDY OF THE APPLICATIONS OF BIOMETRICS SYSTEMS: A LITERATURE REVIEW

NUR FATINHIEYAH AZIZAN, WAN ALIA IZZATI WAN ABDUL RAZAK, NORMI SHAM AWANG ABU BAKAR *, NORZARIYAH YAHYA, MADIHAH SHEIKH ABDUL AZIZ, LILI MARZIANA ABDULLAH

Kulliyyah of Information and Communication Technology, International Islamic University, Jalan Gombak, 53100, Selangor, Malaysia
*Corresponding Author: nsham@iium.edu.my

Abstract

Biometric systems utilize individual unique identification to verify specific characteristics of an individual to grant access to a system. The unique biometric identification makes duplication or alteration of information almost impossible. This has encouraged the acceptance of biometric technology and enabled the technology to evolve exponentially. Besides the benefits of security features promoted by the biometric system, reciprocally, biometric systems also have limitations that can cause problems. This paper reports on reviews conducted on articles with the aim to identify different types of biometric systems, the application domains, constraints, and limitations of existing biometric systems.

Keywords: Application domains, Biometric, Constraints, Technology, Security.

1. Introduction

Over the years, biometric systems have exponentially evolved and adapted to grant access to systems, devices, and data. The preference to use biometric systems is due to the high level of security the system provides compared to other authentication methods such as Personal Identification Number (PINs) and passwords. It can be seen that PINs and passwords tend to be stolen or forgotten over time. However, biometric identification is unique and specifically represents an individual characteristic with minimal chances to be changed or altered, even forgotten. Hence, biometric has become one of the important components in ensuring an individual's privacy be protected from cyber-attacks. Nevertheless, biometric is not fully safe from cyber-attacks such as Denial of Service (DoS) and identity theft; but it is a more secure authentication method because biometric belongs to an individual and cannot be stolen, forged or borrowed [1].

Biometric is a methodological study of physical or behavioural characteristics from humans that can be used to identify or verify an individual. Biometric systems can be either Identification systems or Authentication/Verification systems. Verification is a one-to-one process used to compare a user who is trying to access a system by claiming their identity against the genuine biometric details stored in the system [1]. A computer algorithm with a matching procedure will verify the user's identity, which resulted in the user either will be given the access or will be rejected from entering the system.

In our work, we are looking for a biometric system that can be used in a small smart card that contains data of the card owner. Generally, the data would include their general information, such as Name, National ID number, health related data, employment and other related data. The various types of biometric systems need to be investigated to find the best one to be used in our work. The papers under study are from the recent five years and were collected after a rigorous Systematic Literature Review (SLR) process. The objective of this paper is to present a review of articles for the purpose to ascertain different types of biometric systems, the application domains, constraints, and limitations of existing biometric systems.

2. Biometric Systems

According to Xiao [2], the word biometrics combines the Greek words *bio* and *metric*. When both words are combined, it signifies "life measurement". Biometric technology refers to the application of any technique to distinguish one person from another based on measurable behavioural and physical characteristics. The most common biometric behavioural traits include signature dynamics and keystroke rhythms, while physiological traits include fingerprints, face recognition, retina, iris and deoxyribonucleic acid (DNA).

The initial process of a generic biometric system is the enrolment procedure, where it involves having a new user to the system who is enrolled into the existing database. Information on the biometric traits of the user is fed through an algorithm that will convert it into a template stored in the database [3]. In addition, Xiao [2] states that, when the individual is required to be recognized, the system will perform a proper measurement, then interpret the information into a template by applying the same algorithm that the original template was computed with and the

system compares the new template with the database to decide whether there is a match or not. Figure 1 illustrates a generic biometric system.

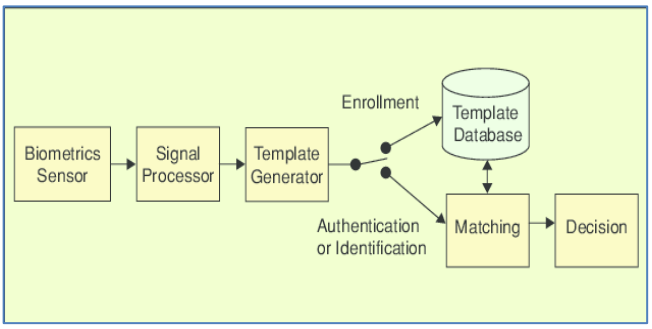

Fig. 1. Generic biometric system [4].

Biometric techniques

This section explains various biometric techniques, namely fingerprint, face recognition, retina scanning, iris scanning, DNA, signature recognition and keystrokes dynamics. These biometric techniques are widely applied in numerous domains nowadays as they provide a high level of security.

i. Fingerprint biometric: Fingerprint biometrics is one of the oldest and most common biometric techniques. Fingerprint-based authentication is greatly utilized in many applications as it has the highest reliability and provides the highest security due to the uniqueness of fingerprint for every individual. There are three characteristics of fingerprints which are distinguishable, immovable for every individual and fingerprints are also one of the unique features for identification and authentication. There are no similar fingerprints in this world even for identical twins. Fingerprint is made up of ridges and furrows where the patterns of ridges, furrows and the minutiae points on the finger are used to determine the uniqueness of a fingerprint [4]. Figure 2 illustrates the three basic categories of ridge patterns which are the loops, whorls and arches. The fingerprint matching techniques are categorized into three different types which are the minutiae-based approach, correlation-based approach and pattern based or image-based matching [4].

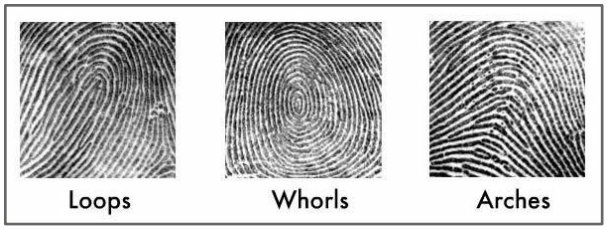

Fig. 2. Three basic categories of ridge patterns [4].

ii. Face recognition: Face recognition technique is commonly used due to its low cost, and it does not require physical contact as retina scanning and fingerprint technique. Sabhanayagam et al. [1] highlighted that face recognition is formed by the dimensions, ratio and other physiological features of the individual's face. It is

based on the proportion, position and the structure of the facial features such as the nose, lips, chin, jaw and their spatial relationships. The face recognition method is divided into three steps which are the face detection, face extraction and face recognition. Figure 3 represents the general face recognition system. The system receives input in the form of images or video and generates the output as the identification or authentication of the subject in the input received by the system. Face detection and face extraction are usually executed simultaneously. According to Srivastava and Ghoman [5], the subjects' faces that are shown in the digital images or video will be verified automatically by the face recognition system. It can perform either face authentication or face identification or even both modes.

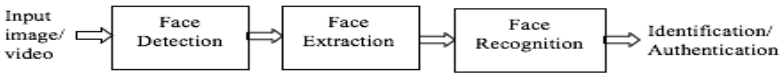

Fig. 3. General face recognition process [5].

iii. Retina biometrics: Retina scanning is one of the biometric techniques in which the patterns of the blood vessels of an individual's retina are used. The blood vessels are situated at the rear side of the eyes. According to Sabhanayagam et al. [1], every person in the world has distinct patterns of retina thus, it is impossible to imitate the retina. It decays so fast after death and it can only be accessed from a living person. By mapping a low intensity ray of visible or infrared light into the retina to illuminate the blood vessels, the computed retinal patterns are captured.

iv. Iris biometrics: Iris scan analyses the features that subsist in the elastic, thin and pigmented tissue near the pupil. Figure 4 shows the eye and iris samples. Iris is unchanged throughout life and every individual has distinct iris patterns from one to another person. The irises from the same person are also different. Eye surgery or the use of glasses or contact lenses will not change the traits of the iris. Iris recognition has the most promising accuracy as the false acceptance rate (FAR) and the false rejection rate (FRR) are low [6].

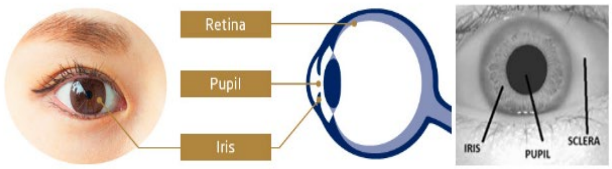

Fig. 4. Eye and iris sample [6, 7].

v. DNA biometrics: DNA is the genetic material present in each living organism and in the cell's nucleus. DNA remains constant throughout a person's lifetime and even after their death. DNA is also a genetic code thus, it is unique to everyone and only identical twins have the same DNA. Identical twins share their DNA code with each other because they were formed from the exact same egg and sperm of their parents. Commonly, DNA recognition is applied for identification rather than verification or authentication. DNA sequencing or genetic profiling is the process of creating a DNA profile. The similarity between these DNA profiles is matched

with the captured and stored DNA samples in the existing database [7]. These days, DNA recognition biometric is used by forensics to identify criminals and has been used in the court of law to prove one's innocence or guilt. It is applied to identify missing people or dead body and it also can verify paternity.

vi. Signature recognition biometrics: It has been highlighted in [1] that signature biometrics is one of the behavioural biometrics and it uses signature patterns to identify a person. According to Tomer and Sarao [8], users place their signature on a tablet or paper that is positioned over a sensor tablet. Generally, signature biometrics work in two ways which are the Static and Dynamic signature recognition.

(a) Static signature recognition- signature is placed on a paper and it can be computed through a camera or an optical scanner.

(b) Dynamic signature recognition- signature is obtained through digitized tablets in real time, capturing the behavioural attributes like speed, pressure, direction of stroke, size of signature and time duration [9].

vii. Keystroke dynamics biometrics*:* Keystroke is a behavioural biometric technique. Mohd. Isa et al. [9] emphasized that it provides sufficient discriminatory information when a person types on a keyboard in a characteristic way. This biometric technique analyses an individual's typing pattern, rhythms and the speed of typing on a keyboard. Studies have disclosed that keystroke biometrics can give a very high accuracy identification of the person who is typing by the two factors (shown in Fig. 5)- dwell time which is the duration of time for which a key is pressed and another factor is the flight time, the elapsed time between releasing a key and pressing the following key or inter-character timing [9].

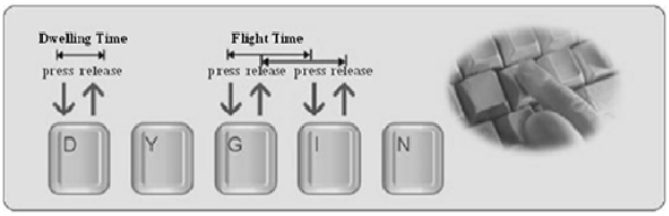

Fig. 5. Dwell time and flight time of keystroke biometrics [9].

3. Application Domains

For its security purposes, biometrics can help ease an individual's life by making activities or transactions safer and more practical. Therefore, biometric has been widely used in various sectors such as government, legal and commercial.

3.1. Government

The use of biometric systems in the government sector is not a new thing. Many countries have utilized this technology in many different services including healthcare, border service and identification documents [10].

i. Healthcare services: In the healthcare system, the issue of security is often a concern in the matter of confidentiality of medical information. Access to the system that contains patients' medical records should only be granted to the authorized person such as medical professionals because if unauthorized people can access the

system as well, they could easily change the information. This will lead to incomplete or misunderstood healthcare records which can result in giving the wrong medication, and in the worst-case scenario, this may cause the death of the patient [10]. Thus, the use of biometrics such as fingerprints for identification in healthcare services can help to sustain information privacy and security of the system. Azeta et al. [10] also emphasized that biometrics identification can be used to obtain a patient's medical record in emergency cases. For example, medical professionals can retrieve the unconscious patient's medical records from the centralized health database with privacy policies by scanning their fingerprint to give them immediate treatment.

ii. Border control: Tourism has experienced continuous growth over the years, and it has become one of the fastest growing sectors in the world. Consequently, it resulted in border guards having less time to make decisions due to the increase in passenger traffic. Therefore, the introduction of the Automated Border Control (ABC) with biometric technologies which is also known as e-Gate can give a positive impact in verifying the identity and authorization of the travellers before crossing the border. This e-Gate can check whether the traveller is permitted to cross the border by comparing the biometrics data stored in their documents such as passports, visas and Identification documents (IDs) to the live captured samples in the biometrics verification process. If this process is successful, the gate will automatically open to allow the traveller to cross the border. According to Labati et al. [11], there are multiple biometric techniques that can be used in e-Gates such as fingerprint, iris and face scan. The implementation of biometrics authentication can maintain the security and integrity of border control.

iii. Identification document (ID): ID is a document that can be used to uniquely identify or prove an individual's identity and citizenship. Passport and identity card (IC) are the most common types of ID where they contain personal information such as photo, name, address and date of birth. ICs are regularly presented as smart cards with microchips that can store features like fingerprint and facial information for recognition purposes [12]. Since an ID contains private and sensitive personal information, it needs to be protected from security threats, for instance, identity theft, clone documents and fraud. The implementation of integrating biometrics in IDs provides a stronger authentication and verification identity of ID holders [3]. This will help in making sure the privacy of the individual can be securely protected.

3.2. Commercial

The commercial sector typically includes non-manufacturing businesses such as utilities, mining, services and banking. Some of the services that implement biometric systems are discussed below.

i. Entrance system: The integration design of fingerprint biometric into a smart card which can be used as an identification at the entrance system is very practical as well as increasing the security level of the place. Smart card is easy to carry as an intelligent device because it can manipulate and store the card holder's data. The study in [13] presented an implementation of fingerprint biometric on smart cards for the Military Police camp which is the PULAPOT Main Entrance. Users need to enrol their fingerprint template along with other personal information such as name, IC number, rank and address into the system and smart card. Then, for the authentication process, users have to insert their cards in the card reader device, and they would be asked to momentarily put their fingerprint on the fingerprint

scanner [13]. If the template stored matched the presented fingerprint, the user is successfully identified and allowed to enter the camp.

ii. Financial transactions: Biometric technologies help make financial transactions such as banking and purchasing become safer and convenient. This is because people might have different PINs if they own multiple bank accounts which later will lead to misremembrance. Moreover, biometric technology is a more efficient and secure method compared to PINs in countering forgery and identity theft [2]. In addition, the uniqueness of biometrics helps to verify the user before obtaining sensitive financial data and prevent unauthorized people from illegally accessing the user's bank account.

3.3. Legal

Legal industry is bound to involve criminal, civil litigation and other legal proceedings that need to use concrete evidence. Therefore, the use of biometrics in legal industry like forensics can help to bring justice and penalize the right people.

Forensics: Due to the large range of criminal activities, the accuracy and efficiency to identify an individual's identity has become a crucial requirement for forensic application. Saini and Kapoor assert that biometrics has turned into a strong alternative for crime detection as it provides a reliable way to identify an individual based on his or her physical and behavioural characteristics [14], for example, fingerprint, face, iris, signature, voice and odor. Usually, finger marks and other biological traces are the priority while searching for any traces in a crime scene because these biometric traits are more distinct and unique. Therefore, biometric technology used in forensic identification has become a major contribution to crime detection by linking the traces found with suspects' data stored in databases [14].

4. Biometric Limitations

Biometric technologies are undeniably convenient in identifying and verifying individuals with high performance security. However, there are a few limitations in biometric systems such as fingerprint, iris and signature biometrics.

4.1. Fingerprint

In their work, Drahanský and Kanich reported that, for fingerprint biometric, there are three major factors that could influence the fingerprint acquisition which are finger condition, sensor condition and the environment [15]. The physical damage of the finger like cuts and scars can cause problems during the recognition process. Dry or moist fingers are also one of the most typical cases that lead to the increase of failure to acquire (FTA) rate. Other than that, dirt on the surface of the finger or scanner can create a common error for every user and there is a risk that these users will not be able to be identified even after cleaning up the device [15]. Lastly, for the environment factor, movement such as large vibration will result in blur fingerprint or break down of internal components in the device.

4.2. Iris

According to Sabhanayagam et al. [1], one of the limitations of iris biometric is that it is relatively costlier in comparison with fingerprint biometric. It is also less convenient in usage because users need to stay still throughout the scanning

process. Moreover, iris biometric is less effective when there is a vast distance between the user and scanner because of inadequate image quality. This type of biometric system is also reported to be obscured by eyelashes, lenses and reflections which can cause inconvenience to some people [4]. In addition, iris scanning for identification or verification is not suitable for people who are affected with alteration in their iris caused by serious disease such as diabetes. Hence, the application of iris biometric can only be used in certain conditions.

4.3. Signatures

The constraint for the signature recognition system is that the verification must be done in the similar environmental background as during the enrolment time [8]. Furthermore, the signatures can be forged by experts to deceive the recognition system. A same person can also have inconsistent signatures and an individual tends to change their signature over time.

After considering all types of biometric technologies, we decided to choose the fingerprint biometric because it is more portable and has leaner implementation which is more suitable for usage on a small smartcard.

5. Conclusion

Biometric is an advanced technology that has been applied extensively in numerous domains. As discussed in this paper, there are various biometric techniques available such as fingerprint, iris recognition, retina recognition, keystroke dynamics and signature recognition biometrics that can be applied to distinguish one individual from another based on the measurable behavioural and physical characteristics. Biometric has become one of the most crucial components in protecting an individual's privacy from cyber-attacks and it plays a significant role in many applications such as healthcare service, border control, financial transactions and forensics. Though there are several vulnerabilities that can disrupt the efficiency of the biometric system, it undoubtedly gives great influence and convenience in everyone's lives.

Acknowledgement

This research is fully funded by Appscard (M) Sdn Bhd, Grant ID: SPP21-046-0046.

References

1. Sabhanayagam, T.; Venkatesan, V.P.; and Senthamaraikannan, K. (2018). A Comprehensive survey on various biometric systems. *International Journal of Applied Engineering Research*, 13(5), 2276-2297.
2. Xiao, Q. (2007). Technology review - biometrics-technology, application, challenge, and computational intelligence solutions. *IEEE Computational Intelligence Magazine*, 2(2), 5-25.
3. Singh, P.K.; Kumar, N.; and Gupta, B.K. (2019). Smart cards with biometric influences: an enhanced id authentication. *International Conference on Cutting-edge Technologies in Engineering (ICon-CuTE)*, 33-39.
4. Guan, H.; Lee, P.; Dienstfrey, A.; Theofanos, M.; Lamp, C.; Stanton, B.; and Schwarz, M.T., (2017). Analysis, comparison, and assessment of latent

fingerprint image preprocessing. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 126-133.

5. Srivastava, A.K.; and Ghoman, N.K. (2013). A review on various popular feature extraction and classification methods and their effectiveness in face recognition technology. *Proceeding of International Conference on Computing Sciences (ICCS)*, 393-401.
6. Dua, M.; Gupta, R.; Khari, M.; and Crespo, R.G. (2019). Biometric iris recognition using radial basis function neural network. *Soft Computing*, 23(22), 11801-11815.
7. NEC (2018). Iris recognition: biometric authentication. Retrieved May 12, 2021, from, https://www.nec.com/en/global/solutions/biometrics/iris/index.html.
8. Tomer, V; and Sarao, P. (2015). Comparative Analysis of Various Biometric Techniques. *Protagonist International Journal of Management and Technology*, 2(3), 1-8.
9. Isa, M.R.M.; Yahaya, Y.H.; Halip, M.H.M.; Khairuddin, M.A.; and Maskat, K. (2010). The design of fingerprint biometric authentication on smart card for PULAPOT main entrance system. *2010 International Symposium on Information Technology (ITSim)*, 1-4.
10. Azeta, A.A.; Iboroma, D.A.; Azeta, V.I.; Igbekele, E.O.; Fatinikun, D.O.; and Ekpunobi, E. (2017). Implementing a medical record system with biometrics authentication in e-health. *IEEE AFRICON proceedings*, 979-983.
11. Labati, R.D.; Genovese, A.; Muñoz, E.; Piuri, V; Scotti, F.; and Sforza, G. (2016). Biometric recognition in automated border control: A survey. *ACM Computing Surveys*, 49(2), 1-39.
12. Páez, R.P; Pérez, M.; Ramírez, G.; Montes, J.; and Bouvarel, L. (2020). An architecture for biometric electronic identification document system based on blockchain †. *Future Internet*, 12(10), 1-20
13. Li, Y.; Zhang, B.; Cao, Y.; Zhao, S.; Gao, Y.; and Liu, J. (2011). Study on the beihang keystroke dynamics database. *2011 International Joint Conference on Biometrics (IJCB),* 1-5
14. Saini, M.; and Kapoor, A.K. (2016). Biometrics in forensic identification: application and challenges. *Journal of Forensic Medicine*, 1(2), 1-7.
15. Alaswad, A.O.; Montaser, A.H.; and Mohamad, F.E(2014). Vulnerabilities of biometric authentication "threats and countermeasures". *International Journal of Information and Computation Technology*,4(10), 947-958.