Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

A comprehensive survey on the biometric systems based on physiological and behavioural characteristics

Shaymaa Adnan Abdulrahman [a,*], Bilal Alhayani [b]

[a] Department of Computer Engineering Techniques, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq
[b] Department of Electronics and Communication, Yildiz Technical University, Istanbul, Turkey

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Biometrics
Physiological
Behavioral
Identification
Techniques

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 voice, finger, iris scanning, face, 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 and a brief summary to the advantages, disadvantages of each method. Main contribution it found that used EEG signals, as biometrics is the best technique compare to with five other techniques.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

1. Introduction

Biometric is can be explained as a quantifiable physiological and/or behavioral attribute that can be encapsulated and analogize to an occurrence at the lime of verification [1]. Biometric technology is defined as any method that reliably utilizes tangible physiological or behavioral characteristics for distinguishing one individual from another. The origin of biometric technology is traceable to about several thousands of years back. Biometric system can be performed using two different types of modes, including authentication and enrollment. In the latter, the individual's biometric features have been changed by the biometric system into a digital form and then store the result in another storage system [2]. However, the biometric system is designed to be used for an identification or confirmation process in authentication mode. During the confirmation procedure, the bio-metric system verifies the identity of the user by making a comparison between the recorded features with the template. This process has been illustratedFig. 1.

In biometrics, a few parts of this description have required a preparation. Usually biometrics consist of many of advantages and disadvantages including the following: All biometric identifiers have been examined to be partitioned into two major gatherings [3]. Physiological and behavior as illustrates in Fig. 2. Biometric confirmation frame-works are not 100% precise. There are two types of flounders in a common bio-metric frame-work. A bogus reject (FR) error is the termination of a confirmed individual endeavoring to get the framework. A false acknowledges (FA) blunder is the acceptance of an individual who does not know exactly who the person is. These two types of errors are conversely correlating and when all is said in done can be strained by the edge of certainty. The boundary can be extended to extend the security of the frame-work, which has been decreased FA blunders and builds FR error.

2. Biometric technologies and challenges

In this section, the major biometric traits based on human's characteristics to authenticate an individual identity along with major advantages and disadvantage of each technology are vividly discussed.

* Corresponding author.
E-mail address: Shaymaa.adnan.abdulrahman@sadiq.edu.iq (S.A. Abdulrahman).

https://doi.org/10.1016/j.matpr.2021.07.005
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

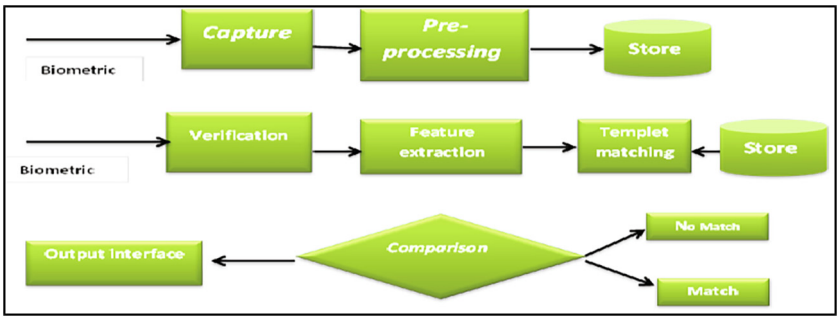

Fig. 1. Stages of the verification/registration process using biometrics.

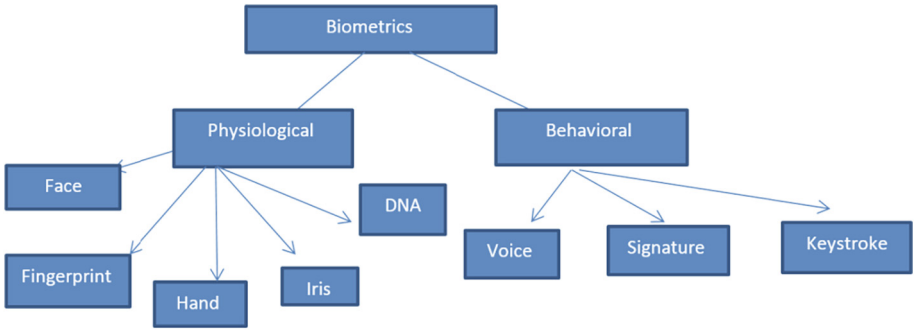

Fig. 2. Classification physiological and behavioral of biometrics.

2.1. Finger print

Fingerprints have been the best quality level for individual ID inside the legal network for multiple hundred years. Fingerprints and fingerprints combine to give the most dominant methods for individual distinct evidence accessible to police and courts. The basic examples of finger-prints are circles, loops and curves that can be set up in finger-prints [4]. So finger print acknowledgment is broadly used due to its reliability. Finger print is broadly utilized in legal and business applications, for example, criminal examination, internet business also novel ID cards as shown in Fig. 3.

Fingerprints consist of some usually, confronted accordingly named designs. There are mainly more five examples such as: arch, tented arch, right loop, left loop and whorl [4]. Finger knuckle print can be very helpful for individual character. Finger knuckle as another biometric approach which providing immense extension for specialists in few of years. Out about this finger impression will be extra standard biometric method and need been utilized to particular ID number more than 100 a longtime. Those unquestionable quality might be because of those methodologies that fingerprints never show signs for change also no two fingerprints would identical [5]. The Finger print scanner is public security boundary which can be found in a wide range of top of the line gadgets that are as of now available everywhere. Its quick and simple to utilize, it is utilized as an option or a supplement for the difficult recalled passwords, it has been also utilized by the requirement of law to discover the doubtful; yet it has been utilized to recognize the good person also.

2.2. Face recognition

Amid the entire history of mankind, individuals utilized face to recognize individuals from each other [4]. Facial acknowledgment is a PC tool that naturally recognizes or confirms an individual accompanied by the assistance of an advanced picture or video out-line from a source of the video One of the strategies to do the concerned procedure is to contrast the specified precedent and the precedents in the database as shown Fig. 4.

Face recognition can be considered as a standout amidst the most fruitful biometric discernible verification methods included in a few kinds of biometric distinguishing proof [4]. Face admission

Fig. 3. Finger print definition [4].

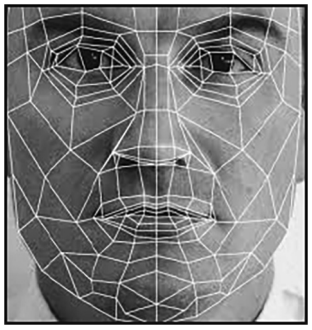

Fig. 4. Example of face scanning [4].

has been used as a validation operation in different domains and especially in PC security associated exercises, for example the security of country, criminal ID, building access, a client distinguishable verification in cell phones and etc. Face acknowledgment likewise assumes a noteworthy job in the exploration field of biometric and PC vision [6]. The objective of a face acknowledgment framework is to have an immaterial misclassification. The face recognition is a PC framework that distinguishes the static picture or on the other hand the face picture in powerful video matches with the put away face database in PC and afterward performs single or numerous face distinguishing proof Face acknowledgment innovation is a sort of physiological component acknowledgment in the field of acknowledgment. Many features lead to the variance of a single face images that contribute to the recognition problem complication, if they cannot be prevented by careful pattern of the capture state. Inadequate limitation or handling of such variance definitely leads to recognition failures [7].

2.3. Iris recognition

The iris can be defined as a fluffy rounded diaphragm which locates between the lens and cornea and of the human eye [8]. The iris is cribriform near to its core by a rounded hole which is known as the pupil. The capacity of the iris is to observe the measure of light which has been entered through the pupil, and this is finished by the sphincter muscle and the dilator muscles which adapt the area of the pupil. Show Fig. 5. They are even distinct for the congruous twins. Iris can be applied for different authenticity and security execution that involve ID cards and passports, prison protection, data-base access and computer log-in, boundary control and government schedule [9].

Iris biometric is more dependable and precise when it compared to other bio-metric features such as finger-print. Iris tissue is firm all over life and is very high secured. Iris is less susceptible to attacks. The eye Iris has various models for right and left eye.

The iris scanner does not require any specific lighting circumstances or any specific light type (dissimilar to the infrared light which required for the scanning of retina). There are two techniques for using the eyes features for authenticity. First one can be based on the recognition of retina [10]. The person has to gaze in a device that operates a laser based scanning of his/her retina. The specific device anatomized the vessels of blood arrangement of the desired retinal image. Incidentally, it validates the person. This arrangement of blood vessels is distinct for each eye. The device is not genial because the user has to confirm a point when laser is analyzing the eye. It looks alike hard to cheat on the authentication system. The second method is iris based recognition. The scanner has to work by using a camera [11]. Dissimilar to the retinal procedure, the user does not need to be near the device to be verified. The provided picture is analyzed by using the device, and it contains 266 various spots. It is known that it is the most authentic biometric verification method. Moreover, iris is still the same through the entire life.

Fig. 5. Example of Iris scanning [4].

2.4. Signature

The signature which has been done by handwriting checks and ID has been roughly partitioned into two classifications: online and offline. These techniques differs in sort of data they utilize, in offline technique, the signature which has to be confirmed is saved as an image and processed as pixel models or textures, in online technique the signature can be captured by a special pen which works electronically through production in addition to static attribute is also captures the dynamic features such as pen location, physical force, angle, elapsed time to sign in [12].

The dynamic signature is a biometric quality broadly utilized and acknowledged for checking an individual's personality, Current automatic signature-based biometric approach regularly require five, ten, or significantly more examples of an individual's user to learn intrapersonal fluctuation adequate to give a precise check of the person's personality. On-line signature verification systems are depending on two techniques feature- or time functions-based systems (global and local systems) [13]. Signature is a biometric property made by a mind boggling process starting in the underwriter's mind as an engine control "program", executed through the neuromuscular system and left on the composition surface by a handwriting device. The mainly aim of signature based biometric authentication with forensic application is the protection of crime [14–16].

2.5. EEG signals

Electroencephalogram (EEG) is an observing technique for cerebrum movement that records it electro-physiologically. EEG signal is recorded from a subject by setting electrodes on the scalp [17]. EEG estimates voltage changes of the cerebrum. These changes are made by the ionic current inside the neurons. Biometric application on electroencephalography (EEG) distinguishes people by utilizing individual qualities in human brainwaves. Bio-metric Based on EEG system have been generated by different studies. Some studies utilized the data-set of BCI contest using multiple traits, involving AR co-efficient, linear complication, energy spectral intensity, and phase synchronicity [18]. Brain Computer Interface (BCI) technique, which supplies an electronic interface directly and can transport commands and messages instantly from the human brain to a computer [19].

EEG is one of the most active capturing techniques that can be utilized in bio-metrics because of its hardware devices evolution. It is a very unique, secure and cannot be replicated method. Besides that, EEG signals are biodynamic and possess a proof of aliveness for a particular individual [20,21]. Thus, it cannot be duplicated like most of the other static physical biometric techniques. For security sector, three kinds of authentication are used, including your information, such as your password, PIN code, or piece of personal information (such as your pet's name); your possession such as your smart card, or token; and/or a biometric. The obsession protocol is usually classified into three various classes. Through these signals, various work such as the applications of medical field like (brain dis-order, motion sick-ness, smoking, alcoholism, detection and diagnosis, sleep dis-order, brain tend. In addition, the execution of an EEG based biometric system relies on the main design of the protocol [22–27].

3. Result and discussion

This section presents the results and explanation of our analysis in this study. Biometrics evident points of interest over secret phrase and security based on token. The best application of biometric innovations is the programmed fingerprint recognition for

Table 1
Explains the advantage and dis advantages of each type of biometric.

Biometric	Advantages	Disadvantages
Fingerprint	1- Very secure method. 2- They have been used to lock or unlock gadgets and applications without waiting to remember passwords. 3- Very simple method, cheap and faster to set-up. 4- It is also a stand-out among the most generated bio-metrics. 5- Mall storage size desired for the bio-metric format that lessens the extension of the data-base desired memory.	1- Portable fingerprint can be considered as a very easy to steal method. 2- Inexpensive components in the structure can cause an authorized person to be denied by accessing due to a little sweat on the finger or an improperly cut. 3- Damage, whether short or permanent, can interfere with the control operation. 4- It is feasible to create copies with the fingerprint to imitate the person.
Face Recognition	1- No connect required.2-Available sensors.3- Easy to use.	1-May be influenced by hats, glasses, hair.2- Face change during age.3- Influenced by lighting or expression.
IrisRecognition	1- Stable over life time. 2- More dependable and precise when it compared to other bio-metric features such as finger-print. 3- No connect required. 4- Very high secured.	1- May be fooled by pictures. 2- When acquisition iris image it requires more training than most Biometrics. 3- Complicated when to capture for some individuals.
Signature	1-classifications online and offline2- Captured by a special pen	1- Narrow range of applications2- Difficult to control sensor
EEG	1-Stable over time2- subject must be alive3- available sensors like electrodes4- Difficult to Forgery and Theft	1- Lengthy registration process.2- High processing

volatiles security from an examination of the systems' necessities: security, roughness, estimation, the factor of usability structure, protection and functional temperature extend It is developing and very much demonstrated center. This innovation has a high exactness. It is the most researched and standardized technology of biometric. It desires more accumulation for the format of bio-metric. It is exceedingly steady, and unchangeable with age which is the opposite of facial and voice acknowledgment. It is a cheap equipment with low power consumption. In addition, it has a high responsibility, implies it can monitor client's movement like who, what and when. Also it gives advantageous and extra security to the framework. All the previous points represent the advantages of biometric systems. While the disadvantage that can be in these systems are: Execution is falling apart by oil, dust, water on the finger surface. It can't be utilized in synthetic industrial and medical clinics since utilization of synthetic compounds can change the unique mark design in hands. Also**,** It Is highly connected to forensic and causes a loss in protection and security. In addition, problem of forgery by artificial, spoofed, gummy or fake fingers. Bigger data-base required for the recognition of fingerprint and signature. Picture Capturing division feature normalization extraction comparison result. While Table 1 illustrates represent advantage and dis advantages of each type of biometric.

4. Conclusion

Biometric technology is very adopted and accepted everywhere to identification or authenticate an individual's identity. The focus towards, the biometric systems has been increased. In the last years due to its, different applications in various domains. For this reason it was used biometric system to facilitate the task of identifying the human. Seven techniques were compared in this study in terms of the advantages and disadvantages each one of them. The study contains comparative analysis for previously used technique. Summarized advantages and disadvantages of biometrics systems. Comparison each of techniques according to performance and accuracy as indicated. Through our study, it found that used EEG signals as biometrics is the best technique compare to with seven other techniques. Because they are stable over time and subject must be alive. In addition Difficulty in imitating it are among the most important advantages of using EEG signals. Because they represent the reflection of the individual's mental tasks. Finally, some type's techniques can be used as Multimodal biometric systems to increase accuracy and performance. Multimodal biometric systems combine multiple sources of biometric, features. As well as some feature extraction has been superficially, explored but require future study, to be completely understood.

Declaration of Competing Interest

The authors declare that they have no known competing financial interest or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A.K. Jain, K. Nandakumar, A. Ross, 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognit. Lett. 79 (2016) 80–105.
[2] V. Agarwal, A. Sahai, A. Gupta, N. Jain, Human identification and verification based on signature, fingerprint and iris integration, in: 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2017, pp. 456–461.
[3] A.K. Sharma, A. Raghuwanshi, V.K. Sharma, Biometric system-a review, Int. J. Comput. Sci. Inf. Technol. 6 (5) (2015) 4616–4619.
[4] S.A. Abdulrahman, W. Khalifa, M. Roushdy, A.-B.-M. Salem, Comparative study for 8 computational intelligence algorithms for human identification, Comput. Sci. Rev. 36 (2020) 100237.
[5] C. Champod, C.J. Lennard, P. Margot, M. Stoilovic, Fingerprints and Other Ridge Skin Impressions, CRC Press, 2004.
[6] G. Guo and N. Zhang, "What is the challenge for deep learning in unconstrained face recognition?," in: 2018 13th IEEE International Conference on Automatic Face \& Gesture Recognition (FG 2018), 2018, pp. 436–442.
[7] I.M. Alsaadi, Physiological biometric authentication systems, advantages, disadvantages and future development: a review, Int. J. Sci. Technol. Res. 4 (12) (2015) 285–289.
[8] A. Bapat, V. Kanhangad, Segmentation of hand from cluttered backgrounds for hand geometry biometrics, in: 2017 IEEE Region 10 Symposium (TENSYMP), 2017, pp. 1–4.
[9] S. A. Abdulrahman, W. Khalifa, M. Roushdy, and A.-B. M. Salem, "A survey of biometrics using electroencephalogram EEG," Int. Journal" Inf. Content Process., 6(1), 2019.
[10] S. Angadi, S. Hatture, Hand geometry based user identification using minimal edge connected hand image graph, IET Comput. Vis. 12 (5) (2018) 744–752.
[11] S.A. Abdulrahman, M. Roushdy, A.-B. Salem, Human Identification based on electroencephalography Signals using Sample Entropy and Horizontal Visibility Graphs, WSEAS Trans. Signal Process. 15 (2019) 2224–3488.
[12] C. Wu et al., Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array, Mater. Today 21 (3) (2018) 216–222.
[13] L.G. Hafemann, R. Sabourin, L.S. Oliveira, Offline handwritten signature verification literature review, in: 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), 2017, pp. 1–8.

[14] B.A. Khalaf, S.A. Mostafa, A. Mustapha, M.A. Mohammed, W.M. Abduallah, Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods, IEEE Access 7 (2019) 51691–51713.
[15] H.J. Mohammed, I.A.M. Al-Jubori, M.M. Kasim, Evaluating project management criteria using fuzzy analytic hierarchy Process, AIP Conf. Proc. 2138 (1) (2019).
[16] S. Hashemi, A. Marzuki, H.J. Mohammed, S. Kiumarsi, The effects of perceived conference quality on attendees' behavioural intentions, Anatolia 31 (3) (2020) 360–375.
[17] S. Abdulrahman, M. Roushdy, A.-B.-M. Salem, Support vector machine approach for human identification based on EEG signals, J. Mech. Contin. Math. Sci. 15 (2) (2020) 270–280.
[18] S. A. Abdulrahman, M. Roushdy, and A.-B. Salem, "Overview of Acquisition techniques brain signals in disease diagnosis: Applications and challenges," TEST Eng. Manag. Mag. J., pp. 10564–10575, 2020.
[19] W. Yahya et al., Study the influence of using guide vanes blades on the performance of cross-flow wind turbine, Appl. Nanosci. (2021) 1–10.
[20] A.S. Kwekha-Rashid, H.N. Abduljabbar, B. Alhayani, Coronavirus disease (COVID-19) cases analysis using machine-learning applications, Appl. Nanosci. (2021).
[21] S. Hasan, A. Abdallah, I. Khan, H. Alosman, A. Kolemen, B. Alhayani, Novel unilateral dental expander appliance (udex): a compound innovative materials, Comput. Mater. Contin. 68 (3) (2021) 3499–3511.
[22] H.J. Mohammed, H.A. Daham, Analytic hierarchy process for evaluating flipped classroom learning, Comput. Mater. Contin. 66 (3) (2021) 2229–2239.
[23] H.J. Mohammed, The optimal project selection in portfolio management using fuzzy multi-criteria decision-making methodology, J. Sustain. Financ. Invest. (2021).
[24] B. Alhayani, H.J. Mohammed, I.Z. Chaloob, J.S. Ahmed, Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry, Mater. Today Proc. (2021).
[25] B. Alhayani, S.T. Abbas, D.Z. Khutar, H.J. Mohammed, Best ways computation intelligent of face cyber attacks, Mater. Today Proc. (2021).
[26] J.S. Ahmed, H.J. Mohammed, I.Z. Chaloob, Application of a fuzzy multi-objective defuzzification method to solve a transportation problem, Mater. Today Proc. (2021).
[27] H.A. Daham, H.J. Mohammed, An evolutionary algorithm approach for vehicle routing problems with backhauls, Mater. Today Proc. (2021).