Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review

Israa Majeed Alsaadi

Abstract: Reducing the growing risks of an unauthorized access to various sensitive systems is a critical issue nowadays. Examples of such sensitive systems are bank accounts, secure buildings, personal computers, mobile devices and etc. This has increased the need for deploying a reliable and powerful security technology that relies on the automated recognition of individuals. The lack of high-security systems in identifying or verifying people's identities has contributed to a growing risk of infiltration of security-related systems. This work is aimed to summarize the existing behavioral biometrics schemes and explore the key advantages and disadvantages of the most popular behavioral biometrics technologies. The study is conducted within different intervals.

Index Terms: Biometrics, Authentication Systems, Behavioral Authentication Technologies, Voice Recognition System, Gait Recognition, Keystroke Dynamics Recognition, Signature Recognition System

1. INTRODUCTION

Authenticating or identifying persons automatically based on their unique physical or behavioral traits is known as biometrics recognition. As a terminology, biometrics refer to the Greece words 'Bio' which means (life) and 'Metrics' which means (measure). Human biometrics traits are divided into two categories, physiological and behavioral. Human physiological features are face, finger print, ear, hand geometry, iris scanning, retina and DNA. These characteristics are unique for each individual and cannot be stolen, plagiarized or 100% identical even among twins. Behavioral biometrics also known as soft biometrics relay on the psychological features that are captured to create a user template. Examples of such characteristics are signature, gait, voice, lips moments and keystroke dynamics. These are the most popular behavioral biometrics techniques which have been deployed for the identification/verification purposes [1,2In general, authenticating persons can be performed based on what a person is, what he/she has, what he/she knows and what he/she does. Each human being is born with his/her unique observed characteristics such as face. Therefore, we recognize people based on who they are. Another way to identify an individual is based on what an individual has like (ID cards and PINs). When a person tries to login into his/her bank account or other online activity by using his/her username and password, this way is based on what that person knows. The last way to recognize an authorized person is based on how that person behaves. Behavioral biometrics like keystroke dynamics ,voice, gait and signature are the most dominant methods for security sector. These recognition technologies have attracted a lot of researchers due to its low cost of implementation in comparison to the physiological traits , friendly use and complexity to mimic others typing habits. Deploying such authenticating methods instead of PINs and passwords which can be easily lost or forgotten.

- *Israa Majeed Alsaadi is currently working as an assistant lecturer at the University of Baghdad, College of Sciences for Women, Iraq, E-mail: israamh_comp@csw.uobaghdad.edu.iq*

Therefore, biometrics recognition techniques can significantly provide better security level for real time identification in order to decrease any unauthorized access to many applications and services such as :

1- Desktop PCs
2- Smart phones
3- ATMs
4- Computer networks
5- Workstations
6- Smart cards

The general structure of this paper is organized as follow, section I describes a brief introduction of biometrics technologies. Section II covers the literature review of biometrics and its related terms. In Section III, a clear description of the main procedures that are done by most of biometrics authentication methods. A detailed explanation of behavioral biometrics techniques along with their advantages , disadvantages and recent applications can be found in Section IV. Finally, a conclusion and proposed future development are well described in Section V.

2. Theory of Automated Authentication Technology

Nowadays, security control and its emerging technologies in the cyber world has become a dominant research topic. Intrusions and hacking of persons' bank accounts, impersonating people in social networking sites, unauthorized access to the buildings with security nature and other security issues have impacted on the current conducted techniques and made a growing need for more accurate and reliable security systems. Passwords, PIN, ID cards are weak methods in protecting people sensitive data and information through the virtual world. However, these traditional methods of user authentication still widely used in many domains. But, the ability of hackers to break even strong and complex password became an easy task [25]. Biometrics based human identification or verification has overcome most of the requirement of other techniques with low level of security. A simple definition of biometrics theory can be derived as automated method for identifying/recognizing identities of individuals based on their unique physiological or behavioral traits [25,26].

2.1 Basic Categories of Human Biometrics Traits

The community of security researchers has classified biometrics characteristics into two main categories. The first one is physiological biometrics. The second category is behavioral biometrics [26]. As well known, human physiological features depend on the fact the a person is known by what he/she is observed or recognized by others. In another word, face, fingerprint, iris and hand geometry are genuine and visible traits for each living person. While the other group of biometrics traits are related to what a person acts or behaves to identify his/her identity. The popular examples of these features are voice, signature, gait and typing rhythm (keystroke dynamics). A significant distinguish among the two categories is that the first group is difficult to be changed due to the biological nature of the traits. However, each biometric system has its one limitations that may effect on the system accuracy over the time. The second group of biometrics features is related to the psychological nature of each person. Which means that there is an expected changed could be occurred on such habits. A large number of civilian applications nowadays are conducting and deploying the distinguished characteristics/features of human body for identity recognition purpose. Typically, human physiological measurements are more stable and difficult to be changed without an external influence factor. Such biological traits are fingerprint, face, iris, ear, hand geometry, retina and DNA [3]. Generally, an individual is identified or recognized by what physical characteristics he/she has. The other category of biometrics traits are behavioral features also known as soft biometrics [41]. The key feature of such human attributes is the high level of reliability and accuracy to overcome the issue of the unobserved features that are obtained by low level images which come with the physiological / hard biometrics. Therefore, soft biometrics have shown a significant performance for the surveillance purposes which make these systems more stable and robust to changes. Examples of such characteristics are gait, voice, keystroke dynamics and signature [41]. Table1 below, it illustrates some points of different biometrics technologies.

Biometrics Traits	Type	User Acceptance	Reliability	Universality
Face Recognition	Physical	M	H	H
Voice Recognition	Behavioral	H	M	M
Finger Recognition	Physical	M	H	M
Signature Recognition	Behavioral	H	M	L
Iris Scanning	Physical	M	H	H
Gait Recognition	Behavioral	H	H	M
Keystroke Dynamics	Behavioral	M	M	L
Hand Geometry	Physical	M	M	M

***Table 1** : Different biometrics methods and their features*

2.2 Related Terms

Although biometrics are used for various purposes. Biometrics has some related terms that explain the essential mechanism to deal with the biological and psychological characteristics of given persons as a way to determine their identities. Identification and verification are both the most popular terms that work on the biometric data. Identification is the process of evaluating a person's traits by making a comparison among the selected features and those which are stored in a huge biometrics database [3]. In the verification technique, also it is known as authentication technique, there is a matching process takes place between the present characteristics of the claimed person and what is already stored during the enrolment process. Thus, the result of the matching will lead to the authentication of the person's identity. In general, identification operation takes longer time than the time that is required to accomplish the verification process [3].

3. Principle Operations of Biometrics System

There are main basic processes in most of biometrics systems whether they are physical or behavioral methods. These essential operations are explained in brief below:

1. Registration: This is the initial process which is also known as enrollment process. It plays an important role in the general mechanism of the biometric system since the data collecting is performed in this stage. The created template of the user biometric traits will be stored in a database to be used at later time in the system. These data contain the required features of the user in order to create a unique template for each individual which will draw the person identity [3].
2. Preprocessing: After collecting the data in the previous stage. A preprocessing will be applied on the stored data. This operation will delete all un useful information that may cause in the degradation of the overall system performance.
3. Feature Extraction: This automatic operation is an important to be done accurately and efficiently. At this step, the best quality of features should be obtained. This means that a general filtering on the collected data will be applied as a way to generate best user pattern. The final data is converted to a computer encoding as a preparation for the next operation [3].
4. Matching: It is the most significant process in the automated recognition of individuals. Here, a matching score is detected among two of the obtained biometrics features. The first one is built at the registration process. The other one is collected at the identification or authentication step. Thus, a decision is made upon the result of this operation which leads to the announcement of the claimed identity.

4. Existing Behavioral Biometrics Systems

Although physical biometrics like fingerprint and face recognition are still among the mostly used technologies for the authentication purposes. However, newer security systems are growing up rapidly. These authentication technologies have received a significant amount of attention due to their low cost of deployment and the non-intrusive environment in comparison to other physical biometrics systems. Below are the most used behavioral biometric systems:

1- Voice recognition
2- Gait recognition
3- Signature recognition
4- Keystroke dynamics

There are several behavioral biometric characteristics have been used for multiple security purposes. These systems vary from each other in the nature of the biometric traits themselves , the environment of the use and their advantages and disadvantages. Most of them have not met a 100% of the expectations by the applications [4,20]. Behavioral biometrics have reached an interesting level of usability and deployment due to various advantages. The very low efforts that are required by the users for data collection. Also, there is no particular hardware apart from a traditional keyboard for the authentication process by the system. Therefore, behavioral biometrics technologies are inexpensive systems in terms of cost of implementation. Several numbers of proposed behavioral biometrics systems have shown sufficient level of accuracy for identities verification [5].The operational developments in both of the applications and the biometric traits still on work in order to reach an optimal authentication method that can effectively overcome most of security applications challenges. In the below section, a brief description of the most dominant biometrics methods is provided along with their advantages, obstacles and recent applications.

1-Voice recognition:

- General Scenario: Speech recognition as a technology was firstly launched by Texas Instruments in 1960 [6].By the time, this identification method has received a significant amount of attention by the researchers society due to the rich information that can be obtained by the analysis of different voice synthesis [7]. like other human biometrics traits, voice is a unique identifier for each person. As known, each human has several vocal organs where the voice is achieved by various proportions of both mouth and throat as discussed in[8]. The system starts when sets of sound waves are obtained by a user speaking raw through an Analog-to-Digital converter (ADC) [38]. After that, a measurement process takes place by the system on the collected sound waves to extract frequencies by making a wave segmentation in different intervals. A matching process is made by the system between the extracted waves and those which are stored in the system to get a unique voice pattern that leads to an individual's identity. A simple implementation of a typical speech recognition system is shown in Fig.1[10].

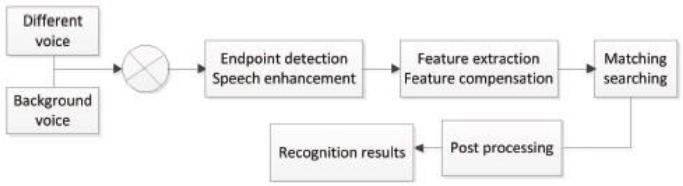

***Figure 1**. Block diagram of voice recognition system*

- Advantages: Nowadays, voice recognition has been mostly used as one of the robust and reliable login methods. Several technology sectors have deployed voice recognition such as , online banking (over the phone), gaming systems, phones, televisions and computer systems , etc [38]. Moreover, voice identification/ authentication has been conducted in many security sectors, forensic field and surveillance, etc [39].
- Disadvantages: Similar to other human biometrics traits, reliability and accuracy of voice recognition system can be effected by a number of factors. For example, illness or the throats infection, under the control of emotions and the issue of ageing [39].
- Recent applications: Recently, lots of smart systems have employed voice recognition in the development of many domains. For example, in the medical field, a recent application has conducted voice recordings in order to recognize Parkinson's disease [9]. Apart from security purpose, Voice interaction has been used in the education process based on mobile environment [10]. Other researchers have proposed a smart system which can detect victims who are buried under rubble of building when a large scale-disasters such as earthquakes [11].

In addition, a new system was proposed to deploying voice recognition based intelligent wheelchair and GPS system for those who are physically handicapped for the purpose of driving the wheelchair by giving voice commands [12]. A smart voice- controlled robot that works and acts on some predefined tasks by given commands [30]. The researchers in [31] they employed a voice user interface model to propose a real-time, robust and universal speaker recognition system. Another group of researchers have worked on introducing a smart vision stick that can powerfully assists visually impaired people to interact via voice recognition commands [32]. However, voice recognition system has a enormous growth which makes a smart interaction with other technologies like Internet of Things (IOT). Such work is deeply discussed in [33] where the authors showed a significant impact on the proposed system in detecting ultrasonic – based inaudible voice attacks to smart homes systems.

2-Gait recognition

- General Scenario: Human gesture/gait has been used as a modern method to identify/authenticate individuals identities[13]. Due to the increased demand of employing an efficient technology that provides high level of security, gait recognition received a significant attention by various security researchers communities. It is an emerging technology that showed an acceptable performance in video surveillance. The Fig.2, shows the basic mechanism of gait recognition system.

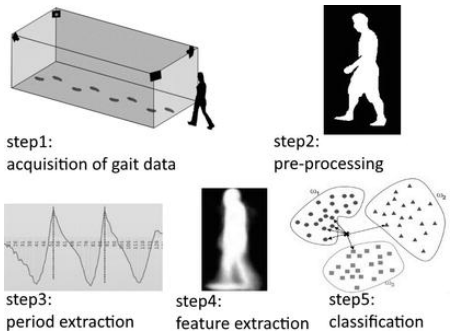

***Figure 2**. Block diagram of gait recognition system*

Identifying/recognizing a person based on his/her style of walking is one of the behavioral biometrics techniques since it depends on the analysis of body structures or body movements. As a general idea, the limbs movements in any

living organism refers to the ability of walking which is also known among human being as human locomotion [34]. In order to provide a unique identity, an extraction of a body movements can be obtained from a repeated style of walking (gait cycle) that comes from a balanced cooperation among a human legs, body and arms. There are two main categories of Gait recognition, model-free and model-based. A detailed explanation can be collected from [34,36].

- Advantages: Gait recognition technology has become more preferable authentication method specially in crowded areas that require reliable access control system to the sensitive buildings. Due to special features in comparison to other biometrics traits like face, finger and voice. For example, the effectiveness of individuals recognition from long distances and the less cooperation between the technology itself and the observed object or even no need to have a persons' permission. Therefore, gait recognition is marked as non intrusive authentication technology [13,14,15]. Another advantage of this biometrics mechanism, it doesn't require any deployment of a particular sensor or hardware device. Traditional CCTV may work perfectly. Moreover, the most attractive feature of this type of identity recognition technologies is the ability to recognize a person even with less resolution of the captured images from the selected videos [14].
- Disadvantages: Although gait recognition has the ability to overcome some difficulties of other biometrics traits, there are factors that affect the overall system performance. One of these factors is an injured leg affects gait recognition performance [16]. In addition, when a person carries an object, wearing different types of clothes and views change.

Recent Applications: A recent identification system was proposed by [27] where the researchers applied gait recognition in detecting human motions by using Dynamic Vision Sensor (DVS) to capture body features. A new article has introduced a modern application in detecting people. The system is implemented by using single Laser Imaging Detection and Ranging (LIDAR) sensor[28]. Moreover, smart phones have the contribution on the deployment of using gait pattern for individuals characterization. The work in [29] has developed a new model to capture a person walking habit from smart phone sensor.

3-Signature recognition

- General Scenario: As a general definition of signature recognition technology, it is a behavioral biometric method to recognize individuals by the process of analyzing their written signatures either online or offline [16,17]. This technology was used in the earliest decades as a way to distinguish between persons [18,19]. It can be acquired either online or offline[16]. In another word, a signature can be sketched on a paper based using traditional way that is made by usual inc. The other way of providing a person handwritten signature could be done using electronic devices such as mobiles, iPads and stylus [16,20]. Below in Fig. 3, main processes of signature recognition system are explained.

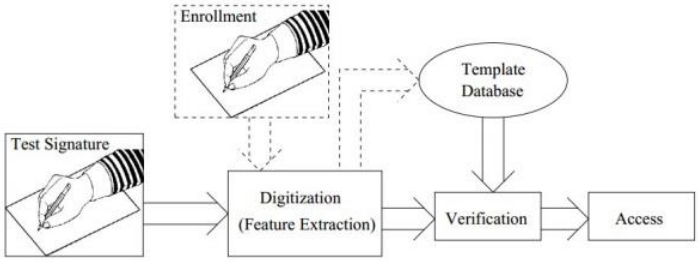

***Figure 3**. Block diagram of signature recognition system*

- Advantages: for long time, handwritten signature has been considered as the most popular way of verifying a personal identity [20]. Also, it has a special characteristic among other soft biometrics methodologies in which very low measurements requirements while analyzing a person signature. In addition, the widespread use of this technology has made it the most familiar and close to everyone's daily life [19,20]. An attractive feature of signature recognition is the difficulty of taking a person hand writing signature when he/she is unconscious. Unlike other biometrics technologies such as finger print methodology in which the print of the person can be easily collected even when the person is unconscious. The genuine nature of an individual handwritten signature also is an important factor to study this type of biometrics attributes.
- Disadvantages: Although signature recognition has shown a number of competitive features, it has some points of obstacles or shortcomings. A person may change his/her sketch of the signature over the time. Also, sickness condition can effect an individual way to provide his/her signature.
- Recent Applications: Implementing signature recognition has raised in many domains. Recently, an intelligent database management system is proposed by [21] for controlling examination process using handwritten verification method. Another deployment of signature recognition was implemented by [22] on Microsoft Azure cloud environment.

4-Keystroke Dynamics

- General Scenario: Keystroke Dynamics (KD) is an interesting authentication method where a user is recognized based on his/her typing rhythm [21]. However, KD can be categorized into two modes, first is Static Keystroke Dynamics (SKD) where the user is asked to provide a predefined password by him/her at the beginning of the session. The other mode is Continuous Keystroke Dynamics (CKD) in this type the change in a user behavior is being monitored throughout the validity of the authentication session. Basic explanation of keystroke dynamics operations is illustrated in Fig. 4.

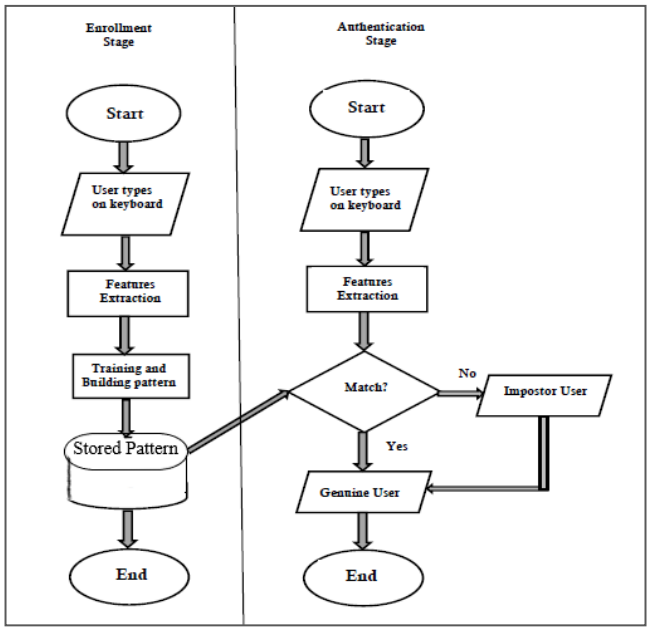

Figure4. *Block diagram of Keystroke dynamics [40]*

- Advantages: one of the most attractive pros of keystroke dynamics is that no need for external hardware components to be connected to the system. The only sensor or the device to be used for data collection is a traditional keyboard [22]. This technology has provided an effective extension to the current old password verification mechanism. Furthermore, recognizing persons based on their typing rhythm is an embedded security technique which makes it difficult to be observed by outsiders[22]. Also, the analysis of keystroke dynamics doesn't produce huge computing process.
- Disadvantages: Although the keystroke dynamics has some drawbacks that result on the degradation of its performance. This method of verification since it deals with keyboards typing tasks, therefore it requires a good typing skills in order to acquire a good feature for each individual [22,23].
- Recent Applications: A new authentication system is proposed by [24] based on Android mobile environment to provide better security mechanism, rather than the simple username and password method for access control to mobile applications. The researchers in [24] deployed CKD for continuous recognition of systems users. The researchers in [25] delivered an improvement on the accuracy of personal authentication using free text keystroke dynamics. They applied one of the data mining techniques by clustering users to provide Keystroke Cluster Map(KCM) to be used as a classifier.

5. Conclusion and Future Development

Various security and business procedures rely on the automatic recognition of individuals nowadays. Biometrics recognition is the process of identifying/verifying a personal based on the analysis of his/her unique physiological or behavioral traits. As a general speech, there is no 100% accurate and reliable biometric system to be deployed in the security sectors. Each method has its own advantages and disadvantages. A comprehensive study has been conducted in this work to introduce the most used biometrics technologies for the recognition of individuals identities. As a future work on this discipline, a comprehensive investigation is planned on the analysis of multiple techniques along with their mostly used algorithms. Furthermore, a comparative study is also required to provide a better analysis of such systems for the security researchers.

REFERENCES

[1] J. V. Monaco, J. C. Stewart, S.-H. Cha, and C. C. Tappert, “Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works,” 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Sep. 2013. doi:10.1109/btas.2013.6712743

[2] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, “Authentication and Biometrics,” Guide to Biometrics, pp. 17–30, 2004. doi:10.1007/978-1-4757-4036-3_2

[3] K. P Tripathi, “A Comparative Study of Biometric Technologies with Reference to Human Interface,” International Journal of Computer Applications, vol. 14, no. 5, pp. 10–15, Jan. 2011. doi:10.5120/1842-2493

[4] Jain AK, Ross A, Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2004 Jan;14(1):4–20. Available from: http://dx.doi.org/10.1109/tcsvt.2003.818349

[5] Yampolskiy RV, Govindaraju V. Behavioural biometrics: a survey and classification. International Journal of Biometrics [Internet]. Inderscience Publishers; 2008;1(1):81. Available from: http://dx.doi.org/10.1504/ijbm.2008.018665

[6] Hanzo L, Somerville FCA, Woodward JP. Voice Compression and Communications. IEEE; 2001; Available from: http://dx.doi.org/10.1109/9780470546871

[7] Rashid RA, Mahalin NH, Sarijari MA, Abdul Aziz AA. Security system using biometric technology: Design and implementation of Voice Recognition System (VRS). 2008 International Conference on Computer and Communication Engineering [Internet]. IEEE; 2008 May; Available from: http://dx.doi.org/10.1109/iccce.2008.4580735

[8] Chovancova E, Dudlakova Z, Fortotira O, Radusovsky J. Multicore processor focused on voice biometrics. 2014 IEEE 12th IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA) [Internet]. IEEE; 2014 Dec; Available from: http://dx.doi.org/10.1109/iceta.2014.7107551

[9] Haq AU, Li JP, Memon MH, khan J, Malik A, Ahmad T, et al. Feature Selection Based on L1-Norm Support Vector Machine and Effective Recognition System for Parkinson’s Disease Using Voice Recordings. IEEE Access [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2019;7:37718–34. Available from: http://dx.doi.org/10.1109/access.2019.2906350

[10] Tao Y. An Intelligent Voice Interaction Model Based on Mobile Teaching Environment. 2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS) [Internet]. IEEE; 2019 Jan; Available from: http://dx.doi.org/10.1109/icitbs.2019.00099

[11] Yamazaki Y, Tamaki M, Premachandra C, Perera CJ, Sumathipala S, Sudantha BH. Victim Detection Using UAV

with On-board Voice Recognition System. 2019 Third IEEE International Conference on Robotic Computing (IRC) [Internet]. IEEE; 2019 Feb; Available from: http://dx.doi.org/10.1109/irc.2019.00114

[12] Aktar N, Jaharr I, Lala B. Voice Recognition based intelligent Wheelchair and GPS Tracking System. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) [Internet]. IEEE; 2019 Feb; Available from: http://dx.doi.org/10.1109/ecace.2019.8679163

[13] Babaee M, Li L, Rigoll G. Gait Recognition from Incomplete Gait Cycle. 2018 25th IEEE International Conference on Image Processing (ICIP) [Internet]. IEEE; 2018 Oct; Available from: http://dx.doi.org/10.1109/icip.2018.8451785

[14] Bhargavas WG, Harshavardhan K, Mohan GC, Sharma AN, Prathap C. Human identification using gait recognition. 2017 International Conference on Communication and Signal Processing (ICCSP) [Internet]. IEEE; 2017 Apr; Available from: http://dx.doi.org/10.1109/iccsp.2017.8286638

[15] Singh JP, Jain S, Arora S, Singh UP. Vision-Based Gait Recognition: A Survey. IEEE Access [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2018;6:70497–527. Available from: http://dx.doi.org/10.1109/access.2018.2879896

[16] Gandhe ST, Jawale TK. Human identilication using fusion of iris, signature and gait recognition. 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC) [Internet]. IEEE; 2016 Dec; Available from: http://dx.doi.org/10.1109/icgtspicc.2016.7955312

[17] Popplewell K, Roy K, Ahmad F, Shelton J. Multispectral iris recognition utilizing hough transform and modified LBP. 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC) [Internet]. IEEE; 2014 Oct; Available from: http://dx.doi.org/10.1109/smc.2014.6974110

[18] Morocho D, Hernandez-Ortega J, Morales A, Fierrez J, Ortega-Garcia J. On the evaluation of human ratings for signature recognition. 2016 IEEE International Carnahan Conference on Security Technology (ICCST) [Internet]. IEEE; 2016 Oct; Available from: http://dx.doi.org/10.1109/ccst.2016.7815681

[19] Galbally J, Gomez-Barrero M, Ross A. Accuracy evaluation of handwritten signature verification: Rethinking the random-skilled forgeries dichotomy. 2017 IEEE International Joint Conference on Biometrics (IJCB) [Internet]. IEEE; 2017 Oct; Available from: http://dx.doi.org/10.1109/btas.2017.8272711

[20] Impedovo D, Pirlo G. Automatic Signature Verification: The State of the Art. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2008 Sep;38(5):609–35. Available from: http://dx.doi.org/10.1109/tsmcc.2008.923866

[21] Bours P, Komanpally V. Performance of keystroke dynamics when allowing typing corrections. 2nd International Workshop on Biometrics and Forensics [Internet]. IEEE; 2014 Mar; Available from: http://dx.doi.org/10.1109/iwbf.2014.6914257

[22] Meszaros A, Banko Z, Czuni L. Strengthening Passwords by Keystroke Dynamics. 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications [Internet]. IEEE; 2007 Sep; Available from: http://dx.doi.org/10.1109/idaacs.2007.4488486

[23] Monrose F, Rubin AD. Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems [Internet]. Elsevier BV; 2000 Feb;16(4):351–9. Available from: http://dx.doi.org/10.1016/s0167-739x(99)00059-x

[24] Ali ABA, Ponnusamy V, Sangodiah A. Correction to: User Behaviour-Based Mobile Authentication System. Advances in Computer Communication and Computational Sciences [Internet]. Springer Singapore; 2019;C1–C1. Available from: http://dx.doi.org/10.1007/978-981-13-6861-5_64

[25] Sultana M, Paul PP, Gavrilova M. A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends. 2014 International Conference on Cyberworlds [Internet]. IEEE; 2014 Oct; Available from: http://dx.doi.org/10.1109/cw.2014.44

[26] Maghsoudi J, Tappert CC. A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones. 2016 European Intelligence and Security Informatics Conference (EISIC) [Internet]. IEEE; 2016 Aug; Available from: http://dx.doi.org/10.1109/eisic.2016.047

[27] Sokolova A, Konushin A. Human identification by gait from event-based camera. 2019 16th International Conference on Machine Vision Applications (MVA) [Internet]. IEEE; 2019 May; Available from: http://dx.doi.org/10.23919/mva.2019.8758019

[28] Alvarez-Aparicio C, Guerrero-Higueras AM, Rodriguez-Lera FJ, Calvo Olivera MC, Matellan Olivera V, Gines Clavero J, et al. LIDAR-based people detection and tracking for @home Competitions. 2019 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC) [Internet]. IEEE; 2019 Apr; Available from: http://dx.doi.org/10.1109/icarsc.2019.8733624 Kala N, Bhatia T, Aggarwal N. Person Identification and Characterization from Gait Using Smartphone. 2019 11th International Conference on Communication Systems & Networks (COMSNETS) [Internet]. IEEE; 2019 Jan; Available from: http://dx.doi.org/10.1109/comsnets.2019.8711131

[29] Andrews N, Jacob S, Thomas SM, Sukumar S, Cherian RK. Low-Cost Robotic Arm for differently abled using Voice Recognition. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) [Internet]. IEEE; 2019 Apr; Available from: http://dx.doi.org/10.1109/icoei.2019.8862757

[30] Xie Y, Shi C, Li Z, Liu J, Chen Y, Yuan B. Real-Time, Universal, and Robust Adversarial Attacks Against Speaker Recognition Systems. ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) [Internet]. IEEE; 2020 May; Available from: http://dx.doi.org/10.1109/icassp40776.2020.9053747

[32] Bastaki MM, Sobuh AA, Suhaiban NF, Almajali ER. Design and implementation of a Vision Stick with Outdoor/Indoor Guiding Systems and Smart Detection and Emergency Features. 2020 Advances in Science and Engineering Technology International Conferences (ASET) [Internet]. IEEE; 2020 Feb; Available from:

http://dx.doi.org/10.1109/aset48392.2020.9118187
[33] Mao J, Zhu S, Dai X, Lin Q, Liu J. Watchdog: Detecting Ultrasonic-Based Inaudible Voice Attacks to Smart Home Systems. IEEE Internet of Things Journal [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2020 Sep;7(9):8025–35. Available from: http://dx.doi.org/10.1109/jiot.2020.2997779
[34] Limcharoen P, Khamsemanan N, Nattee C. Gait Recognition using Double-Window and CNN Classification on Freestyle Walks. 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS) [Internet]. IEEE; 2018 Dec; Available from: http://dx.doi.org/10.1109/scis-isis.2018.00194
[35] Wang Y, Sun J, Li J, Zhao D. Gait recognition based on 3D skeleton joints captured by kinect. 2016 IEEE International Conference on Image Processing (ICIP) [Internet]. IEEE; 2016 Sep; Available from: http://dx.doi.org/10.1109/icip.2016.7532940
[36] Zou W, Kamata S. Frontal Gait Recognition from Incomplete RGB-D Streams Using Gait Cycle Analysis. 2018 Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2018 2nd International Conference on Imaging, Vision & Pattern Recognition (icIVPR) [Internet]. IEEE; 2018 Jun; Available from: http://dx.doi.org/10.1109/iciev.2018.8640960
[37] Luo C, Xu W, Zhu C. Robust gait recognition based on partitioning and canonical correlation analysis. 2015 IEEE International Conference on Imaging Systems and Techniques (IST) [Internet]. IEEE; 2015 Sep; Available from: http://dx.doi.org/10.1109/ist.2015.7294548
[38] Mitchell C, Shing C-C. Discussing Alternative Login Methods and Their Advantages and Disadvantages. 2018 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD) [Internet]. IEEE; 2018 Jul; Available from: http://dx.doi.org/10.1109/fskd.2018.8687163
[39] Tandel NH, Prajapati HB, Dabhi VK. Voice Recognition and Voice Comparison using Machine Learning Techniques: A Survey. 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) [Internet]. IEEE; 2020 Mar; Available from: http://dx.doi.org/10.1109/icaccs48705.2020.9074184
[40] Darabseh A, Pal D. Performance Analysis of Keystroke Dynamics Using Classification Algorithms. 2020 3rd International Conference on Information and Computer Technologies (ICICT) [Internet]. IEEE; 2020 Mar; Available from: http://dx.doi.org/10.1109/icict50521.2020.00027
[41] Martinho-Corbishley D, Nixon MS, Carter JN. Analysing comparative soft biometrics from crowdsourced annotations. IET Biometrics [Internet]. Institution of Engineering and Technology (IET); 2016 Dec 1;5(4):276–83. Available from: http://dx.doi.org/10.1049/iet-bmt.2015.0118