Journal of Al-Azhar University Engineering Sector

Vol.16, No. 59, April 2021, 288-299

A SURVEY ON SMARTPHONE PROTECTING IDENTIFICATION AGAINST ATTACKS USING BIOMETRIC AUTHENTICATION SYSTEMS

Marwa Said[1]*, Khalil Mohamed[1], Ayman Elshenawy[1,3], AND Mohamed Ezz[2,1]

[1] Systems and Computers Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt.

[2] College of computer and information sciences, Jouf University, Saudi Arabia.

[3] Software Engineering and Information Technology Department, Faculty of Engineering and Technology, Egyptian Chinees University, Cairo, Egypt.

*Corresponding Author's E-mail: marwa_abdelsalam@azhar.edu.eg

ABSTRACT

Recently, a lot of Biometric Authentication Systems (BAS) techniques for the purpose of security in both industrial and academic organizations because it improves the authentication system's usability by overcoming the existing difficulties of using passwords. Although of the rapid spread of BAS's systems especially in smartphones, it still has defects and are subjected to attacks, and suffers from the intrusion of user privacy, because some biometric features have not been deeply studied and investigated. In this survey, the existing BAS techniques are explored and classified focusing on the security issues that they are used for and the corresponding solutions provided in this domain. The advantages and disadvantages of each BAS technique are also reviewed, the threats of each BAS technique are listed, summarized, and discussed. The relevant research studies are also presented and several open problems, research direction are also presented.

Keywords: **Biometric authentication; Spoofing attacks; Biometrics; Attack detection.**

دراسة عن حماية الهوية في الهواتف الذكية من الهجمات باستخدام أنظمة المصادقة البيومترية

مروة سعيد[١] *, خليل محمد[١], أيمن الشناوي[٣,١], محمد عز[٢,١]

[١]قسم النظم والحاسبات، كلية الهندسة، جامعة الأزهر، القاهرة، مصر

[٢]كلية علوم الحاسب والمعلومات, جامعة الجوف, المملكة العربية السعودية

[٣]قسم هندسة البرمجيات وتكنولوجيا المعلومات, الجامعة المصرية الصينية, مصر.

*البريد اللإلكتروني للباحث الرئيسي: marwa_abdelsalam@azhar.edu.eg

الملخص

للتغلب على صعوبة إدارة كلمات المرور وتحسين إمكانية استخدام أنظمة المصادقة ، تمت دراسة المصادقة البيومترية على نطاق واسع واجتذبت اهتمامًا خاصًا في الأوساط الأكاديمية والصناعية. حيث تم بحث وتطوير العديد من أنظمة المصادقة البيومترية، خاصة للأجهزة المحمولة. ومع ذلك، قد تكون الأنظمة الحالية عرضة للهجمات، مما يجعلها تعاني من اختراق خصوصية المستخدم، مما يعيق بشكل كبير قبولها من قبل المستخدمين. لا تزال الأعمال السابقه تفتقر إلى مراجعة شاملة للتطورات الأخيرة في المصادقة البيومترية لغرض تحديد الهوية الآمن والمحافظة على الخصوصية.

في هذه الدراسه ، نقوم بتصنيف ومراجعه بدقة أنظمة المصادقة البيومترية الحالية من خلال التركيز على حلول الأمان والخصوصية. نقوم أيضا بتحليل تهديدات المصادقة البيومترية فيما يتعلق بالمصادقة الآمنة والمحافظة على الخصوصية. نراجع كذلك الأعمال الحالية للمصادقة البيومترية من خلال تحليل الاختلافات بينها وتلخيص مزايا وعيوب كل منها بناءً على المعايير المقترحة. على وجه الخصوص ، نناقش مشاكل الكشف عن النشاط وحماية الخصوصية في المصادقة البيومترية. استنادًا إلى المراجعه الذي أجريناها ، اكتشفنا عددًا من مشكلات البحث المفتوحة ونحدد كذلك عددًا من اتجاهات البحث المهمة التي تستحق جهودًا خاصة في البحث المستقبلي.

1. INTRODUCTION

Authentication systems have been widely used for accessing Internet services and accessing mobile devices. They can be used to protect user devices, accounts, and contents especially for users who own several accounts on different applications with high levels of security. this type of user requires the use of password management applications which is considered a hard process in practice. Due to their special characteristics, BAS's have been presented as a solution for these problems. Person identity can be checked using biometric features that differ from one person to another instead of using the traditional password (Mastali, 2010).

Recently some researchers have been presented a survey about using neural networks in BAS to recognize biometric features of a person like a face (Boulgouris et al., 2020), iris (Singh et al., 2020), voice (Patel et al., 2018), signature and fingerprint (Yang et al., 2018), etc. (Kumar, 2016) has been studied the limitations of unimodal BAS and presented a mmultimodal BAS such as the combination of the face with fingerprint traits for a more secure authentication system.

Other researchers have been concentrated on the applications of BAS in different environments. (Kortli et al.) presented a survey on face recognition approaches based on hybrid, holistic and local features. They provide a list of advantages of using these approaches, challenges, drawbacks, and some improvements in this field. (Carmel, 2020) provided a survey on existing BAS deployed in the cloud environment to overcome the problem of theft detection. Besides, Padma and Srinivasan (Srinivasan, 2016) presented a review about cloud-based BAS and classify these techniques into two main categories: behavioral-based biometric traits and physical-based biometric traits. (Mahfouz et al., 2017) reviewed many active authentication mechanisms used in smartphones and presented in more detail the behavioral biometric traits used in active authentication. (Meng et al., 2015) reviewed about eleven BAS used in smartphones.

Although of the rapid development in the field of BAS, there are still some drawbacks in using it such as spoofing attacks, which make the systems are highly subjected to hacking, threaten user's data and privacy. (Meng et al., 2015) presented several types of potential biometric authentication attacks such as spoofing attacks, and privacy detection of the biometric data itself.

In this paper, a survey of existing BAS related to security and liveness detection is presented, analyzed, compared. Open research issues related to this subject are also presented.

The organization of the paper is as follows: Section 2 explains the structure of biometric authentication systems and discusses the potential threats in it. In Section 3, the biometric authentication techniques are reviewed, their accuracy, advantages, and disadvantages as a way to comment on their performance. Finally, a summarization of the whole paper besides open research points is presented in the last section.

2. BIOMETRIC AUTHENTICATION SYSTEMS

1.2 STRUCTURE OF BIOMETRIC AUTHENTICATION SYSTEMS

BAS, in general, consists of three main modules: User Agent (UA), Identity Provider (IdP) and Relying Party (RP) (Mosenia, 2017), (Teh, 2013) as shown in Fig.1. In the UA module, the user is asked to be authenticated and authorized to the devices or the internet service. In the IdP module, the user who wants to be authenticated is identified through the obtained data from the UA module for that user. The RP module allows access control for the verified user.

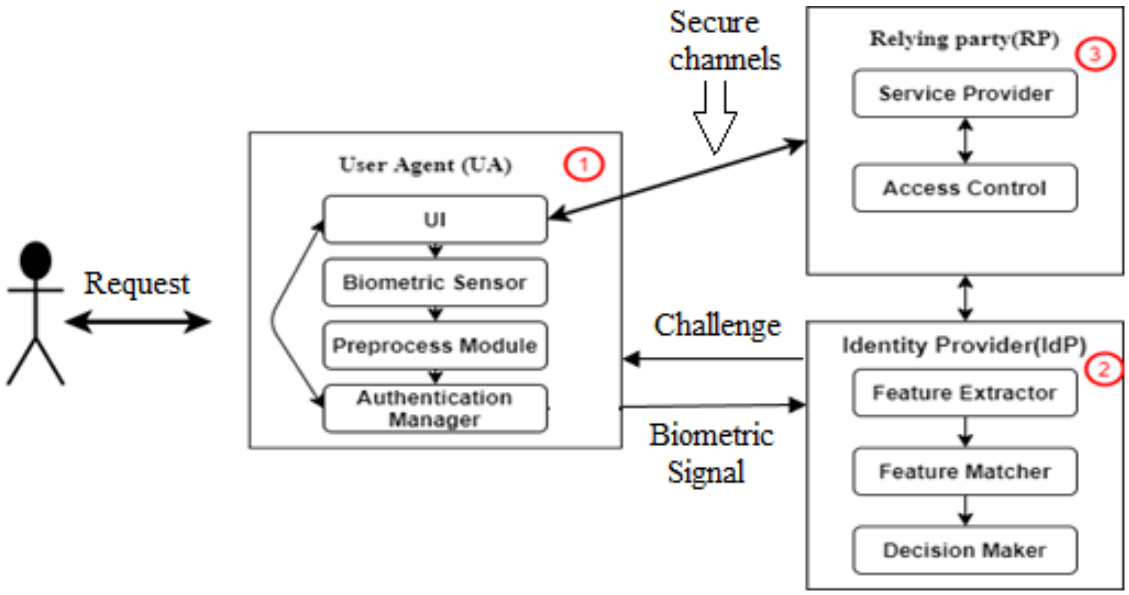

Fig. 1. An example of the structure of a Biometric authentication system (Mosenia, 2017)

The authentication process starts when a user asks for authentication through a User Interface (UI) exist in the UA module. The authentication manager sends this request to the IdP through a secured channel and the IdP module replies by a challenge to the UA module. The UA module collects the biometric signals throw the biometric sensor and perform some process on it such as coding and noise reduction. The results of this processing are sent back through a secured channel as a reply to the authentication challenge to the IdP module and other modules. The IdP module extracts the main features of the biometric signals and compares it with a record stored in the database for that user. The matching results help the IdP to decide whether the user is legal or not. As a consequence, the access control policy of the current user is allowed or not based on the decision made by IdP. The position of the IdP and RP module varies from one structure to another. In some BAS structures the IdP and RP exist in local terminals, and the authentication process is completely performed in the terminal. In other BAS structures, the IdP and RP modules are located on the cloud as part of the server, and the authentication process requires that the terminal communicate with the server via the network.

BAS has three mode of operations as the following:

- **Enrollment mode**: the first time an individual uses a BAS, the biometric information about the user is captured using a sensor or an image acquisition system that acquire all the necessary data, and then the captured data is stored on a database or a card or both. The basic operations of BAS are presented in Fig. 2 (Marcel et al., 2014). First, an image acquisition system (sensor) is used to acquire all the necessary data. Second, the acquired data is processed and enhanced, background noise is removed, etc. Third, the essential features are extracted, a template of relevant characteristics is created and stored, and the unimportant biometric data that are not used in the authentication process are ignored to reduce the file size. The matcher compares the created template with other existing templates to calculate the difference between them. Then the matching program will compare the template with the input.

- **Verification Mode:** in this mode, the biometric information of the user is detected and compared with the information stored at the time of enrollment. BAS verifies a person in

three steps: first, a reference model is generated for all users and stored in the model database. Second, some samples are with the stored models to generate scores and calculate the threshold. Third, the testing step is performed, where a username, smart card, or ID number can be used to determine which template should be used for the comparison.

- **Identification mode**: in this mode, the BAS system makes several comparisons against a biometric database. the system can successfully identify individuals if the comparison result with the stored template falls under a specified threshold.

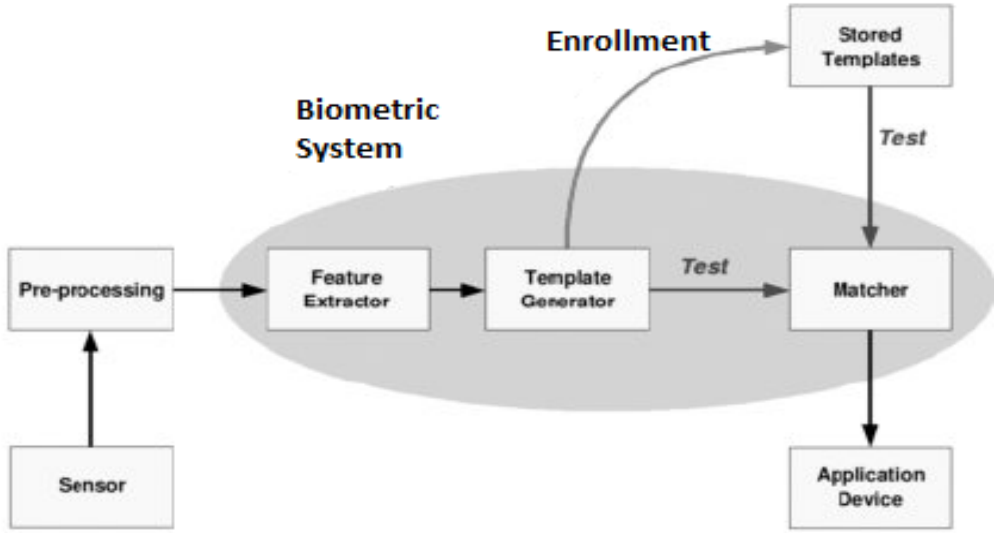

Fig 2: Biometric Authentication block diagram (Marcel et al., 2014)

1.3 POSSIBLE ATTACKS IN BAS

In this section, several potential attacks will be identified. These attack points may attack systems from different points such as UI, RP, IDP (Meng et al., 2015).

- Faking biometric data (attack point 1). Is considered as the most critical one that affects the UA module. In this type of attack the real biometric features can be replaced with a reproduced one, such as a fake photos, finger, a voice record, etc.

- Attacks (attack points 2 and 3): it affects the IdP and RP modules, it makes easy for attackers to gain access via several common attacks, such as power lifting, hijacking, SQL injection, etc. After that, attackers can get users biometric data that only legal users can know or access.

In practice, the attacks related to different types of biological characteristics can be summarized as the following:

- Face recognition attacks (Frahm et al., 2016): this can be easily done by obtaining user face images and videos from the Internet, particularly from social networks. And using use those photos or videos to cheat a face recognition system.

- Iris recognition attacks (Arora, 2020): iris recognition system can be attached using fake iris image.

- Fingerprint attacks (Chakraborty et al., 2019): fake finger can be designed using different types of materials, such as latex, Silica gel, gelatin, etc. Or collected from surfaces touched by the users.

- Voice recognition attacks (Abdullah, 2019), attackers can record a user's voice and reuse it during user authentication.

3. Biometric Authentication Solutions

A. FACE RECOGNITION

Face recognition methods can be used to distinguish users by comparing their faces. Faces are nearly similar in shape and structure and small differentiate between individuals. So, the face characteristics are not accurate enough to recognize human beings. Face observation angle, expression, user age, and lighting conditions are all challenging factors to face recognition systems.
Face recognition systems identify persons by capturing image or video frame and compare them with face images stored in the database to decide if the person is authorized or not. This technique is (Ali et al., 2019) technique is very important for surveillance and security systems. Also, it can be used in many organizations such as universities, airport, other areas need a fast, and effective way for authentication.
Many researchers have studied face authentication systems. (Yang et al., 2016) introduced a WIDER FACE dataset that contains rich annotations about faces. It was divided according to the image size into three types small, medium, and large. The used techniques achieve an accuracy of 90 % for large and medium images and less than 30% for small images.
(Ashish et al., 2019) introduce a face recognition system for marking student attendance at school. Viola-Jones is used for face detection, features are selected using principal component analysis (PCA), and classification is performed using a Support vector machine (SVM). (Ali et al., 2019) presented a face detection method based on Haar cascaded classifiers. The used database contains 500 color images with 96% accuracy. The system is effective in face detection and has high accuracy, but the dataset used is too not sufficient besides the way to secure user information is not provided.
(Singh et al., 2018) (Erdogmus, 2014) found that most face recognition systems can be spoofed easily using the printed image of faces, and generated faces using plastic surgery. Many researchers try to solve the spoofing problem, but the provided solutions are very limited (Zhao et al., 2003). The provided solution must differentiate between the live image of the user and the spoofing photos obtained from a person's facial images or even videos or downloaded from social networks or capturing it by a camera.
Recently, (Proov, 2018) has used machine learning to enhance the accuracy of face recognition systems.
Many anti-spoofing techniques for BAS have been developed, especially for face recognition systems by making face authentication systems more dynamic to solve the spoofing problem. Such as using contextual information mechanism by analyze the area surrounding the face (Komulainen et al., 2013), face liveness detection that checks the face movement and eye blink (Rogmann et al., 2015), texture analysis technique that analysis the texture of the faces image (Maatta et al., 2011), face flashing that apply the challenge-response protocol (Tang et al., 2018), and user interaction that challenge the user to perform an action (Saad, 2015). All the above research is mainly used to detect the real image of the user from the spoofed image.

B. FINGERPRINT-BASED AUTHENTICATION

The fingerprint is a kind of biometric feature that differs from one individual to another and is commonly owned by human beings, it can be used by authentication systems to identify persons. Authentication systems based on a fingerprint is are widely used in several organizations and are

highly acceptable by users. Many researchers have presented the fingerprint authentication systems as BAS. Such as (Abellanas et al., 1999), (Khanban et al., 2003) and (Yang et al., 2018). To increase the security level of fingerprint authentication systems, (Pavešić et al., 2007) introduce a multimodal BAS based on the surface of the palm. (Pishva, 2007) proposed a spectroscopic approach to prevent spoofing attacks.

All these works provided high-performance fingerprint authentication and solved many problems in usability and aliveness detection but the way they solved these problems is more complicated that they require extra data such as hand thermal, etc. which by default requires additional sensors to process this information. Besides, these systems did not mention how to make sensitive user information secure and that makes these systems exposed to spoofing risks. For this problem, (Li et al., 2013) proposed a fingerprint authentication based on data hiding by combining two different fingerprints of the user into a new identity. At the registration level, the system captures two fingerprints of the user for different fingers and extracts the features from them such as the specific position of one fingerprint, the orientation from another fingerprint, and reference points for both fingerprints. Based on these features combined features of two fingerprints are embedded and stored in the database. By doing that, the complete features of a single fingerprint cannot be attacked when the database is hacked. Their experimental results showed that the system has a high level of privacy with an EER of 0.4%. But they did not mention how efficient it was.

C. VOICE RECOGNITION

Another kind of biometric feature that can be used in distinguishing a person in a simple and easy way is the voice. Because it can be easily acquired and collected by a microphone that is was available in almost all computers and smartphones. Many users have been used voice in BAS. (Jayamaha et al., 2008) have applied Hidden Markov Model (HMM) for a voice authentication system to recognize the user speech for a period of by extracting features from the voice waveform. To increase the security level, (Galka, 2014) proposed implemented HMM and Gaussian Mixture Model (HMM-GMM) as an embedded solution for voice authentication.

D. IRIS RECOGNITION

For each person, the iris pattern is an identical and unique biological feature, making it a valuable and effective human identification tool. But this criterion faces some problems like resolution issues and brightness which distorts the iris recognition process, so it requires a high-quality hardware device which makes it not widely used in mobile devices.
(Pillai et al., 2011) proposed a framework based on scattered representations and random projections. User information cannot be obtained by attackers through simple reverse engineering methods. So, the sensitive user's biological information can be safe to some extent.
(Singh et al., 2020) use machine learning in iris recognition. (Bodade et al., 2009) introduces a technique for detecting the inner iris border based on differences in eye pupil size, where the eye pupil size can change according to the light conditions. That change can be used for detecting the aliveness of the iris. They used 384 iris images to experiment with the system with 99.48% accuracy. Although this method proved its high accuracy, the way of protecting iris information is not provided.
Although the anti-spoofing techniques have already led to the solution of many spoofing issues of BAS as shown in table 1, there are still some unresolved problems and defects of existing anti-spoofing techniques.

E. EYE BLINKING

Eye blinking is the action of closing and opening an eye quickly. Eye blinking tracking provides a promising solution to system security and usability. But before we start talking about eye blinking authentication, we will talk about another usage of eye-tracking and detection used techniques.

Eye blinking and gaze tracking are very important topics and solved different issues in different fields such as face emotion analysis and computer vision.

Many researchers proposed to use eye-blinking for eye status detection. Eye blinking is very useful for several applications such as detecting driver drowsiness. (Galab, 2014) proposed a webcam-based approach for eye tracking. The states of the eyes can be classified as open or closed for each video frame. The System was tested on users wearing glasses and without glasses, it performed well in both conditions.

(Batista, 2007) proposed a monitoring system to monitor the drowsiness and attention of a person based on the eye blink technique. A camera is installed on a car, the head movement and eye blink sequence are detected to detect whether the driver is alive or not.

(Amna et al., 2015) proposed an eye blink monitoring method to detect driver drowsiness, then an alarm is opened if the driver is drowsy. They used a webcam by capturing each video frame, detect the face, crop the eye region, and by using eye features points and the time assumed to blinks, the system can detect if the eye is closed or not.

Besides these works, eye blinking detection can be used for disabled people who cannot use their hands. (Mohammed, 2014) proposed a real-time eye-blink detection method for disabled people to enable them to interact and use mobile phones.

Researchers try to discover the availability of the other behavioral or physiological characteristics for biometric authentication purposes like using eye blinking. (Chu et al., 2018) proposed an eye blinking detection, which finds face using Haar feature and Kth-Nearest Neighbor (KNN) to compare the feature points. For face recognition, they used Eigenface and Fisherface methods. After detecting the face, the eye position is located on the face image based on the structure of the human face. They detected the eyeball's movements and the number of blinkers to enhance facial recognition for mobile devices to unlock the screen.

Table 1: Comparison of Biometric Authentication Systems

Biometric Authentication	Method and Techniques	Results and Metrics	Pros	Cons
Face recognition	WIDER FACE dataset (Yang et al., 2016)	Accuracy = 90 %	perform better than the other methods	Not sufficient for small images
	PCA and SVM (Ashish et al., 2019)	Not provided	detecting students face effectively	The efficiency and privacy are not provided
	Haar cascaded files combination (Ali et al., 2019)	Accuracy = 96%	face detection with a high accuracy	The dataset used is too small
	Face flashing technique (Tang et al., 2018)	Accuracy 97.3%	Face liveness detection	requires negligible time for processing
	Texture analysis (Hadid et al., 2011)	EER 2.9 %	defeat the spoofing problem related to the face authentication system	Requires additional infrared devices
	User interaction (Saad, 2015)	FAR 67.5%	Strengthen the security	requires face images to be upright for face detection
Fingerprint	Delaunay Triangle-Based framework (Khanaban, 2003)	Not provided	achieved good results	some defects in this structure still exist
	Delaunay quadrangles-Based framework (Yang, 2014)	Not provided	template data more secured	the experimental results are not available
	Multimodal biometric using hand features (Pavešić, 2007)	EER=0.0020%	increased the system reliability against aliveness attacks	requires an external hardware device

	data hiding technique (Li, 2013)	EER=0.4%	increased privacy	efficiency it not mentioned
Voice Recognition	HMM (Jayamaha, 2008)	Accuracy=86%	Increased security level	The accuracy is not high
	HMM-GMM (Galka, 2014)	EER = 3.4%	More secure	Privacy and performance not mentioned
	Challenge response (Zhao, 2016)	Accuracy=80.6%	More secure	The accuracy of the system is not high
	SURF, HoG, Haar feature extractor and HMM (M. Ezz, 2020)	Performance=96.2%	increased the system reliability against aliveness and replay attacks	The dataset is small and needs to be in different domains
Iris recognition	machine learning schema (Khuzani, 2020)	Accuracy=99.64%	Improved accuracy	The efficiency and privacy are not mentioned
	detecting the inner iris border (Bodade, 2009)	Accuracy=99.48%	Increased the system security	The efficiency and privacy are not mentioned
Eye blinking	Haar feature and Kth-Nearest Neighbor (KNN) (Chu, 2018)	Accuracy=95.88%	Improved face recognition security	average execution time for authentication is to slow
	Android Open CV (Arutselvan, 2018)	Recall=93.3%	A new way for authentication via mobile phones	Dataset is small and not sufficient

(Arutselvan et al., 2018) proposed a method for face recognition with eye blink count detection that was used for authenticating the mobile user. They used Android OpenCV for the face detecting and recognizing process. Although the proposed method is easy to use for authentication with a recall of 93.3%, it was tested for a single person so testing data is not sufficient and the system is proposed for the user who did not wear spectacles.
(M. Saied et al., 2020) have proposed a two-level BAS, in the first level the face is detected and the second level the system asks the user to perform a challenge-response based on a sequence of eye blinking, then the proposed system lock or unlock the service based on the matching process with the previously stored data of the user. The proposed system has achieved accuracy up to 98.4%.

4. CONCLUSION AND FUTURE WORK

In this paper, a review of existing biometric authentication systems was presented, and the potential attacks and security issues in existing BAS were discussed. Some of these systems are exposed to be hacked and user information is not protected. Based on our review BAS require an additive research to enhance the current system performance and accuracy and to overcome the drawbacks of the current systems. Also, the implementation of multi-level BAS is considered as a future research point that requires more studies and investigations.

REFERENCES

[1] Boulgouris, N. V., Plataniotis, K. N., & Micheli-Tzanakou, E. (2020). A Comparative Survey on Biometric Identity Authentication Techniques Based on Neural Networks. In Biometrics: Theory, Methods, and Applications (pp. 47-79). IEEE.

[2] Kunal Kumar, M. F. (2016). A Review Of Multimodal Biometric Authentication Systems. International Journal of Scientific & Technology Research, 5(12).

[3] Mastali, N. (2010). Authentication of subjects and devices using biometrics and identity management systems for perdevices using biometrics and identity management systems for persuasive mobile computing: A survey paper. Proceedings of the 5th International Conference on Broadband and Biomedical Communications, 1-6.

[4] Patel, N., & Kale, A. (2018). Optimize Approach to Voice Recognition Using IoT. In Proceedings of the 2018 International Conference on Advances in Communication and Computing Technology (ICACCT), 251–256.

[5] Singh, G., Singh, R. K., Saha, R., & Agarwal, N. (2020). IWT Based Iris Recognition for Image Authentication. Procedia Computer Science, 171, 1868 - 1876.

[6] Kortli, Y., Jridi, M., Falou, & Atri, M. (n.d.). Face Recognition Systems: A Survey. Sensors, 20, 1-34.

[7] V.Vanitha Carmel, D. (2020). A SURVEY ON BIOMETRIC AUTHENTICATION SYSTEMS IN CLOUD TO COMBAT IDENTITY THEFT. Journal of critical reviews, 7(3), 1-8.

[8] Srinivasan, P. P. (2016). A survey on biometric based authentication in cloud computing. in Proc. Int. Conf. Inventive Comput. Technol. (ICICT), 1, 1-5.

[9] Mahfouz, A., M. Mahmoud, T., & Sharaf Eldin, A. (2017). A survey on behavioral biometric authentication on smartphones. Journal of Information Security and Applications, 37, 28-37.

[10] Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. IEEE Community Surveys Tuts, 17(3), 1268–1293.

[11] Zabidi, N. S., Norowi, N. M., & Rahmat, R. W. (2018). A Survey of User Preferences on Biometric Authentication for Smartphones. International Journal of Engineering & Technology, 7, 491-495.

[12] Chakraborty, A., Pathan, S., Kabir, M., & Thakur, K. (2019). Fingerprint Authentication Security: An Improved 2-Step Authentication Method with Flexibility. International Journal of Scientific and Engineering Research, 10, 438-442.

[13] Xu, Y., Price, T., Frahm, J.-M., & Monrose, F. (2016). Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos. USENIX, 497-512.

[14] Jain, R., & Kant, C. (2015). Attacks on Biometric Systems: An Overview. International Journal of Advances in Scientific Research , 1(7), 283.

[15] Arora, S. B. (2020). Presentation attack detection for iris recognition using deep learning. International Journal of System Assurance Engineering and Management , 11, 232–238.

[16] Hadi Abdullah, W. G. (2019). Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. Network and Distributed Systems Security (NDSS), 24-27.

[17] Arsalan Mosenia, S. S.-K. (2017). CABA: Continuous Authentication Based on BioAura. IEEE Transactions on Computers, 66(5), 759-772.

[18] Pin Shen Teh, A. B. (2013). A Survey of Keystroke Dynamics Biometrics. The Scientific World Journal, 24.

[19] Singh, S., & S.V.A.V.Prasad. (2018). Techniques and Challenges of Face Recognition: A Critical Review. Procedia Computer Science, 143, 536-543.

[20] N. Erdogmus, S. M. (2014). Spoofing face recognition with 3D masks. IEEE Trans. Inf. Forensics Secur, 9(7), 1084–1097.

[21] Zhao, W., R. C., J. P., & A. R. (2003, December). Face Recognition: A Literature Survey. ACM Computing Surveys, 35(4), 399-458.

[22] Komulainen, J., Hadid, A., & Pietikainen, M. (2013, September). Context based Face Anti-Spoofing. IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, 1-8. doi:10.1109/BTAS.2013.6712690

[23] Rogmann, N., & M. K. (2015). Liveness Detection in Biometrics. International Conference of the Biometrics Special Interest Group (BIOSIG), 1-14.

[24] Maatta, J., Hadid, A., & Pietiktiinen, M. (2011). Face Spoofing Detection From Single Images Using Micro-Texture Analysis. International Joint Conference on Biometrics (IJCB), 1-7. doi:10.1109/ijcb.2011.6117510

[25] Tang, D., Zhou, Z., Zhang, Y., & Zhang, K. (2018, Aug 22). Face Flashing: a Secure Liveness Detection Protocol based on Light Reflections. Network and Distributed Systems Security (NDSS) symposium 2018.

[26] Saad, A. M. (2015). Anti-Spoofing Using Challenge-Response User Interaction. AMERICAN UNIVERSITY IN CAIRO SCHOOL OF SCIENCES AND ENGINEERING, 1-72.

[27] Alom, M., M. Taha, T., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M., . . . Vijayan K. Asari. (2019, March 5). A State-of-the-Art Survey on Deep Learning Theory and Architectures. Electronics, 8(3), 1-66. doi:10.3390

[28] Wencheng Yang, J. H. (2014). A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 9(7).

[29] Pavešić, N., Savic, T., Ribaric, S., & Fratric, I. (2007). A multimodal hand-based verification system with an aliveness-detection module. Annals of Telecommunications, 62(1), 1655-1680.

[30] Khanban, A., & Edalat, A. (2003). Computing Delaunay Triangulation with Imprecise Input Data. CCCG, 94-97.

[31] Li, S., & Kot, A. C. (2013). Fingerprint Combination for Privacy Protection. IEEE Transactions on Information Forensics and Security, 8(2), 350-360.

[32] Zargari Khuzani, A., Mashhadi, N., Heidari, M., & Khaledyan, D. (2020). An approach to human iris recognition using quantitative analysis of image features and machine learning. ArXiv, 1-6.

[33] Bodade, R., & Talbar, S. (2009). Dynamic iris localisation: A novel approach suitable for fake iris detection. International Conference on Ultra Modern Telecommunications & Workshops, 1-5.

[34] Ali, A. A., El-Hafeez, T. A., & Mohany, Y. K. (2019). An Accurate System for Face Detection and Recognition. Journal of Advances in Mathematics and Computer Science, 1-19.

[35] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2018). A fingerprint and finger-vein based cancelable multibiometric system. Pattern Recognition, 78, 242–251.

[36] Yang, S., Luo, P., Loy, C. C., & Tang, X. (2016). Wider face: A face detection benchmark. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

[37] Neela Ashish, K., P, S., Prudhvi, C., Jai Krishna, N., & Kailasa Sandeep, K. (2019). Smart Attendance Marking System using Facial Recognition. Research Journal of Science and Technology, 11(2), 101-108.

[38] Ali, A. A., El-Hafeez, T. A., & Mohany, Y. K. (2019). A Robust and Efficient System to Detect Human Faces Based on Facial Features. Asian Journal of Research in Computer Science, 1-12.

[39] Chu, C.-H., & Feng, Y.-K. (2018). Study of Eye Blinking to Improve Face Recognition for Screen Unlock on Mobile Devices. J Electr Eng Technol, 13(2), 953-960.

[40] K. Arutselvan, Sridhathan. C, & M. Senthil Kumar. (2018, Number 24). Unlocking Mobile Devices using Improved Face Recognition and Eye Blinking Technique. International Journal of Applied Engineering Research, 13(24), 16907-16909.

[41] R. G. M. M. Jayamaha, M. R. (2008). VoizLock - Human Voice Authentication System using Hidden Markov Model. 2008 4th International Conference on Information and Automation for Sustainability, 330-335.

[42] J. Galka, M. M. (2014). Voice authentication embedded solution for secured access control. IEEE Transactions on Consumer Electronics, 60(4), 653–661.

[43] Zhao, Z. Y. (2016). A usable authentication system based on personal voice challenge. Advanced Cloud and Big Data (CBD), 194–199.

[44] Meng, W., Wong, D., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surveys Tuts., 1268–1293.

[45] Bhatt, H. S., Bharadwaj, S., Singh, R., & Vatsa, M. (2013). Recognizing surgically altered face images using multiobjective evolutionary algorithm. IEEE Trans. Inf. Forensics Security, 89–100.

[46] Proov, A. (2018). Facing the future: The impact of Apple FaceID. Biometric Technol. Today, 5–7.

[47] Abellanas, M., Hurtado, F., & Ramos, P. (1999). Structural tolerance and delaunay triangulation. Inf. Process. Lett., 221–227.

[48] Pishva, D. (2007). Spectroscopic approach for aliveness detection in biometrics authentication. 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol., 133–137.

[49] Jayamaha, R., Senadheera, M., Gamage, T., & Weerasekara, K. (2008). Voizlock—Human voice authentication system using hidden Markov model. 4th Int. Conf. Inf. Automat. Sustainability, 330–335.

[50] Pillai, J., Patel, V., Chellappa, R., & Ratha, N. (2011). Secure and robust iris recognition using random projections and sparse representations. IEEE Trans. Pattern Anal. Mach. Intell., 1877–1893.

[51] Galab, M. K. (2014). Adaptive real time eye-blink detection system. Int. J. Comput. Appl, 29–36.

[52] Batista, J. (2007). A drowsiness and point of attention monitoring system for driver vigilance. Intelligent Transportation Syst. Conference(ITSC).

[53] Amna , R., Mehreen, S., & Khan, A. (2015). Real Time Drowsiness Detection using Eye Blink. National Software Engineering Conference.

[54] Mohammed, A. A. (2014). Efficient eye blink detection method for disabled helping domain. Int. Adv. Comput. Sci. Appl, 5, 202–206.

[55] S. Marcel, M. S. Nixon and S. Z. Li, Handbook of Biometric Anti-Spoofing, London: Springer London, 2014.

[56] Saied, M., Elshenawy, A. & Ezz, M.M. A Novel Approach for Improving Dynamic Biometric Authentication and Verification of Human Using Eye Blinking Movement. Wireless Pers Commun 115, 859–876 (2020). https://doi.org/10.1007/s11277-020-07601-x