Pisco Med Publishing

Facial Authentication as A Possible Solution to the Challenges in User's Security and Privacy in Web Applications

Francisco D. Guillén-Gámez[1], Iván García-Magariño[2,3]

[1] Faculty of Education, Pontificia University of Salamanca, C/ Henry Collet, 52-70, 37007, Salamanca.

[2] Department of Computer Science and Engineering of Systems, University of Zaragoza, Teruel 44003, Spain.

[3] Instituto de Investigación Sanitaria Aragón. University of Zaragoza. Zaragoza.

Abstract: In recent years, new technologies have become the focal point of any operation or digital system. Smartphones are increasingly gaining ground as a technological tool that combines a large number of applications and online services. It is an observable reality, as operations are increasingly being carried out in electronic commerce applications, banking transactions, health applications, and distance education. However, the widespread use of these types of practices means that more risks can present themselves through the internet. Therefore, any organization must take into account changes in virtual security, having to face possible cyber attacks or identity theft. Although smartphones have become a powerful tool in daily lives of most people, it is true that it has brought a series of challenges in the security and privacy of users, where facial authentication seems to be a possible solution to this type of problems. This article reviews the most relevant current existing literature about facial authentication as a biometric system, as well as the systems available on the market, so that organizations can use them with its clients or users.

***Keywords*:** Facial Authentication; Technologies; Privacy

1. Introduction

The technological and electronic devices that have landed in the knowledge society have generated multiple challenges. In particular, the user's protection regarding their privacy and security on the internet is an important challenge to solve (Sivarajah, Irani & Weerakkody, 2015). As stated by Hu *et al*., (2017) or Miranda *et al*., (2015), every day cyber-users feel a greater attraction to the interconnection of physical objects, sensors and electronic devices, as well as human beings within the Internet of Things (IoT) who deposit all their information together in web applications. The need to correctly authenticate this user who wants to access their bank account digitally, follow a distance course or simply access their private data from their mobile phone through these applications has become an important challenge with the aim of avoiding fraudulent attacks or simply stopping another person from accessing another user's system, thus violating their privacy (Memon, 2017).

The rest of the article is organized as follows: the following section defines the concept of authentication and its existing classification; Section three shows how the functioning of a facial system works under general conditions; Section four is focused on how facial authentication is used in the most current smartphones and distance courses; Sections five and six show the most popular software that currently exists on the market for a company to use for user authentication; and, finally, Section eight shows the limitations that this biometric technology offers when having to face the possible problems that may arise.

doi: 10.18282/ics.v1i1.591

2. User authentication

The authentication of a user can be carried out through a combination of items. Siddiqui, Abdullah, Khan & Alghamdi (2018) structure authentication through things we already know (passwords, secret questions, pin); through things that the user has (security card) or through their biometric features (iris scanning, fingerprint, facial authentication). The most important feature of a facial authentication system is that the extraction of users' facial images only requires a low-cost device, such as video cameras or webcams, contrary to other recognition systems that use iris scanning or fingerprints which requires expensive sensors, as they are based on micro-cosmic characteristics that have strict requirements related to the distance between the scanners and the eyes (Zhang, Aziz, Esche & Chassapis, 2018). As shown in **Figure 1**, over time, and thanks to the technological advances of our civilization, the way in which one accesses the system has been changing; first, physically, through the identification of the user with an identification card, leading to the system of user names and passwords with the inconvenience of having to remember each password used for each application in which the user is registered; and finally, accessing the system through biomedical methods (Ometov *et al*., 2018).

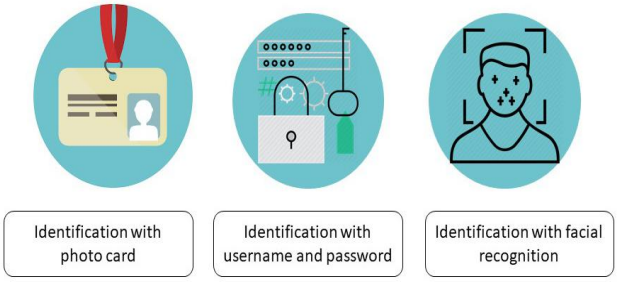

Figure 1; Conceptual example of authentication systems. Own elaboration**.**

3. Facial authentication

Facial recognition is a biometric system which uses software to verify and identify people who appear in a digital image by comparing their facial features with those previously stored in the software database. How does it work?

In general terms, when a user wants to access their personal account regardless of whether it is a mobile application or web server, the facial authentication system will request a photograph of the user through the webcam of his device. Then, this photograph is sent to the database of the biometric system, which extracts the facial features of the user and compares them with the facial features of the users contained in the software database. For this, the software identifies and verifies whether the user is the person that they claim to be, and not a fake user. Once the system verifies the correct identity of the user, it allows them to access their personal account. **Figure 2** shows the operation of a facial authentication system in general terms.

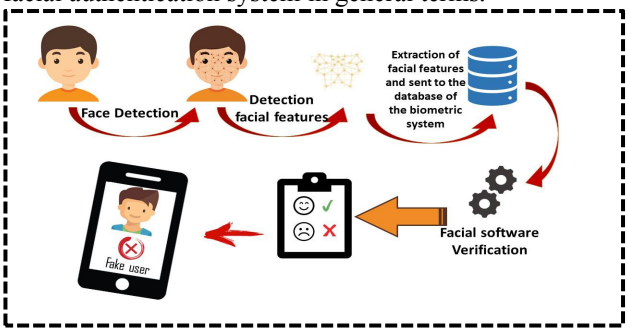

Figure 2; Steps in the operation of a facial authentication system. Own elaboration**.**

4. Authentication in smartphones

According to the data recorded by Jiang & Meng (2017), more than 334.9 million smartphones were sold worldwide in the first quarter of 2016, demonstrating the strength that these devices have acquired in people's lives. Due to this great popularity, users have begun to store more sensitive and private information, whose most current terminals have sensors for biometric applications. In general terms, the most current smartphones have enabled the screen to become unlocked within microseconds by the user taking their device and looking at it, without the need to carry out any further action to unlock it. This is thanks to the biometric sensors implanted in some mobile devices, such as the iPhone X or the Samsung Galaxy S8. Both devices already have robust protocols for user authentication, both fingerprint and facial systems (Galdi, Nappi, Dugelay & Yu (2018).

For example, Apple (2018), ensures that its facial system, Face ID, is much more reliable than the previous security method, Touch ID (fingerprint). Apple claims

that its Face ID software uses 30,000 facial measurement points working just as well even when parts of the face are covered or even if the person ages 10 years. On the other hand, Samsung (2018) goes one step further in its biometric methods, incorporating an authentication system through the iris, which is one of the safest ways to keep the user's personal account blocked and protected.

5. Authentication in online courses

Due to the exponential growth of distance education, different facial software is revolutionizing the market with the aim of verifying the identity of students trying to access online courses (Traoré *et al*., 2017; Karim & Shukur, 2015; Guillen-Gamez, Garcia-Magarino, Bravo & Plaza, 2015). This type of system seems to be the key to guaranteeing security in e-Learning systems, since it is only necessary for students to acquire a common webcam next to their laptop, thus making authentication secure and continuous throughout the entire evaluation session.

Authors, such as Zhang, Aziz, Esche & Chassapis (2018), Shah, Shah, Shah, Shinde Gharat (2017) and Fenu, Marras & Boratto (2017), are some of the most current researchers who have published their results on the authentication of users in distance courses. Most of them combine different biometric methods (face, voice, touch, mouse, and keystroke) in order to ensure the correct identification of students with greater reliability.

6. Software available for user authentication

There is currently a wide variety of facial methods that an organisation can integrate into its virtual platforms. For example, Labayen, Vea, Florez, Guillen-Gamez & García-Magariño (2014) propose software that allows the student's identity to be re-authenticated multiple times during the evaluation session. Its main feature is that the company offers the software in the form of a plug-in which can be inserted in any LMS, such as Moodle, allowing the identity of students to be monitored when carrying out, for example, an activity in a forum, a lesson, a control type test or other types of tasks.

As opposed to Smowl, OpenFace free software offers a source code so that any user with programming knowledge can integrate it into their platform as an identification access point. Since its source code is the great advantage that it offers, it is true that the software is not as visually and dynamically developed as Smowl, which offers its monitoring services at a specific price. For example, Guillen-Gamez, García-Magariño, Bravo-Agapito, Lacuesta & Lloret (2018) propose the use of OpenFace as an access alternative for health applications in which it is necessary to identify patients who access their medical records through smartphone applications. For this purpose, they checked the reliability of the software through a database of facial images of patients, determining levels of accuracy of 78.87.

7. Limitations of facial authentication in virtual environments

The need to protect sensitive data and remote access to virtual services of users has become a fundamental task to develop algorithms to protect users' privacy. Facial authentication is one of the new technologies which could improve the security of navigation systems; however, it still presents certain risks that are important to highlight.

As facial algorithms work in real time, they are not yet able to detect a face if the user is not in front of a webcam (Kawamata, Ishii, Fujimori & Akakura, 2016). In addition, facial occlusion often occurs in facial systems because users wear accessories on their faces, such as sunglasses, scarves or have their hands on their faces, among other objects (Li, Xu, Yan, Li & Deng, 2014).

8. Considerations

For most of the world, the use of facial authentication could be a solution to keep the privacy of our data and maintain security in our social networks, applications and network servers. However, what is the future that will keep this biometric technology in our lives? Due to advances in the field of facial authentication, privacy issues are even more frequent. Although there is a fascination with the science behind our biometric data, society cannot be directed towards a

future in which any step of our lives will be monitored by this technology. So, we should ask ourselves in this way, are we improving the privacy of our data, or, to the contrary, are we encouraging the interaction of private information through biometric servers? Society should ask itself what is biometric authentication intended to achieve, in order to prevent it from becoming a means of invasion of privacy by multinational companies who register our biometric data.

References

1. Sivarajah, U., Irani, Z., & Weerakkody, V. (2015). Evaluating the use and impact of Web 2.0 technologies in local government. Government Information Quarterly, 32(4), 473-487. DOI: https://doi.org/10.1016/j.giq.2015.06.004
2. Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2017). Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. IEEE Internet of Things Journal, 4(5), 1143-1155. DOI: 10.1109/JIOT.2017.2659783
3. Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., & Murillo, J. M. (2015). From the Internet of Things to the Internet of People. IEEE Internet Computing, 19(2), 40-47. DOI: 10.1109/MIC.2015.24
4. Memon, N. (2017). How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight]. IEEE Signal Processing Magazine, 34(4), 196-194. DOI: 10.1109/MSP.2017.2697179
5. Siddiqui, Z., Abdullah, A. H., Khan, M. K., & Alghamdi, A. S. (2014). Smart environment as a service: three factor cloud based user authentication for telecare medical information system. Journal of medical systems, 38(1), 9997. DOI: https://doi.org/10.1007/s10916-013-9997-5
6. Zhang, Z., Aziz, E. S., Esche, S., & Chassapis, C. (2018). A Virtual Proctor with Biometric Authentication for Facilitating Distance Education. In Online Engineering & Internet of Things(pp. 110-124). Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-64352-6_11
7. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. Cryptography, 2(1), 1-31. DOI: 10.3390/cryptography2010001
8. Jiang, L., & Meng, W. (2017). Smartphone user authentication using touch dynamics in the big data era: Challenges and opportunities. In Biometric Security and Privacy (pp. 163-178). Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-47301-7_7
9. Galdi, C., Nappi, M., Dugelay, J. L., & Yu, Y. (2018). Exploring New Authentication Protocols for Sensitive Data Protection on Smartphones. IEEE Communications Magazine, 56(1), 136-142.
10. Apple (2018). https://www.apple.com/es/iphone-x/ Website of Apple. Last visit: March 05, 2018.
11. Samsung (2018). http://www.samsung.com/es/smartphones/galaxy-s8/ Website of Samsung. Last visit: March 05, 2018.
12. Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J. D., & de Faria Quinan, P. M. (2017). Ensuring Online Exam Integrity Through Continuous Biometric Authentication. In Information Security Practices (pp. 73-81). Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-48947-6_6
13. Karim, N. A., & Shukur, Z. (2015). Review of user authentication methods in online examination. Asian Journal of Information Technology, 14(5), 166-175. DOI: 10.3923/ajit.2015.166-175
14. Guillén-Gamez, F. D., García-Magariño, I., Bravo, J., & Plaza, I. (2015). Exploring the influence of facial verification software on student academic performance in online learning environments. Int. J. Eng. Edu., 31(6A), 1622-1628.
15. Shah, K., Shah, S., Shah, T., Shinde, R., & Gharat, S. (2017). Secure Examination System using Biometric and QR Code Technology. International Journal of Engineering Science, 10365.
16. Fenu, G., Marras, M., & Boratto, L. (2017). A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognition Letters. DOI: https://doi.org/10.1016/j.patrec.2017.03.027
17. Labayen, M., Vea, R., Flórez, J., Guillén-Gámez, F. D., & García-Magariño, I. (2014). Smowl: a tool for continuous student validation based on face recognition for online learning. In Edulearn14 Proceedings (pp. 5354-5359). IATED.
18. Guillén-Gámez, F. D., García-Magariño, I., Bravo-Agapito, J., Lacuesta, R., & Lloret, J. (2017). A proposal to improve the authentication process in m-health environments. IEEE Access, 5, 22530-22544. DOI: 10.1109/ACCESS.2017.2752176
19. Kawamata, T., Ishii, T., Fujimori, S., & Akakura, T. (2016, November). Student authentication by updated facial information with weighting coefficient in e-Learning. In Region 10 Conference (TENCON), 2016 IEEE (pp. 551-555). IEEE. DOI: 10.1109/TENCON.2016.7848061
20. Li, Y., Xu, K., Yan, Q., Li, Y., & Deng, R. H. (2014, June). Understanding OSN-based facial disclosure against face authentication systems. In Proceedings of the 9th ACM symposium on Information, computer and communications security (pp. 413-424). ACM. DOI: 10.1145/2590296.2590315