Advances in Educational Technology and Psychology (2017) 1: 1-8
Clausius Scientific Press, Canada

Biometrics and education: a review about facial authentication software for the identification and verification of students who use virtual learning platform (LMS)

FRANCISCO D. GUILLÉN-GÁMEZ

Computer Science Department, Madrid Open University (UDIMA),
franciscodavid.guillen@udima.es
Carretera de La Coruña, KM.38,500, Vía de Servicio, nº 15, 28400 Collado Villalba, Madrid, Spain.

Keywords: facial authentication, biometrics, online learning, e-Learning, security education.

Abstract: In the last decade, the use of biometrics has had a lot of success applied to the security and video surveillance tools. Due to that, facial authentication has a preferred place in continuous development with the purpose of getting the identification and verification of the user. Specifically, the use of facial authentication in virtual online environments is so important in order to improve the security mechanism in e- Learning systems, mostly in the field of online exams into a virtual platform. Particularly, the authentication of an user inside a LMS is essential for the institutions or universities to make sure that the student is who he says he is (the correct user). This article focuses on analysing and comparing the different facial authentication systems to verify the students when they use e-learning platforms, detailing the costs and the features of every system listed.

1. Introduction

Nowadays, security has become a relevant topic in all those sectors where everyone looks for different ways to be protected . However, the obsession about security in some countries, due to the terrorist threats, robbery, or vandalism, has motivated the existence of a bigger interest in identifying and verifying people with the purpose of getting a good security. [1].

There are some systems in order to verify the identity of a person. However, Biometrics are considered as the safest method to determine for sure someone's identity [2]. The last advances in biometrics, combined with computing and electronics, have allowed the development of the most modern and safest solutions of personal identification. For that reason, in the last few years, biometrics has gained recognition in many fields, in which are included the university sector and specifically the online learning [3].

The long-distance education offer is more and more frequent in our society, where every year is more and more in demand for all kind of students, as it provides a more flexible way of learning in terms of location and transmission of contents through e-Learning platforms [4]. In the long-distance learning may exist the reasonable doubt of wether the student who is doing the activities is who he says he is, because in this process he cannot be observed face to face while he realizes his activities. For that, Biometrics seems to be a technology that can solve this problem [5].

The correct authentication of a student is an essential requirement for a Learning Management System (LMS), so if a third person tries to access stealing the identity of an authorized student the security of all the system can be compromised [6].

Knowing all of this, our article focus on explaining the concept of Biometrics and its different types, specifically the facial authentication. Furthermore, the different types of facial software on the market will be detailed, which allow the identification and verification of the users.

The reminder of this article is organized as follows: the next section introduces the background research related to the current work, mentioning the improvements over the existing literature; the section 3 presents the different useful authentication facial software which can be used on education, and finally the section 4 mentions the conclusions.

2. Theory frame

2.1 Approach to the biometrics concept

If we understand this concept in very broad terms, we could say biometrics has been used since the human being creation and, in fact we use it in plenty of times along the day without realizing it [7]. Example, when we pick up the phone and we'll listen the interlocutor's voice, our brain tries to check if this voice is similar to any of the samples that it has stored in its memory and has being saving during our life.

Biometrics is an automated method of personal recognition that has its base in the biological or behavioural characteristics [8]. The recognition is personal and non-transferable. To make it happens, keys, cards, passwords or any other devices are not required. It's all about a process similar to the ones that human being usually realizes recognizing and identifying other people for their physical aspect, their voice or the way they walk, etc.

In order to achieve its goal, this science is divided in Static Biometrics and Dynamic Biometrics [9]. The static Biometrics is dedicated to the study of the physiological and chemical characteristics that a person can have to be identified. In the other hand the dynamic biometrics develops its studies in the behaviour of the human being to determine what makes them unique. It can be observed the main fields that are studied by biometrics in the figure 1.

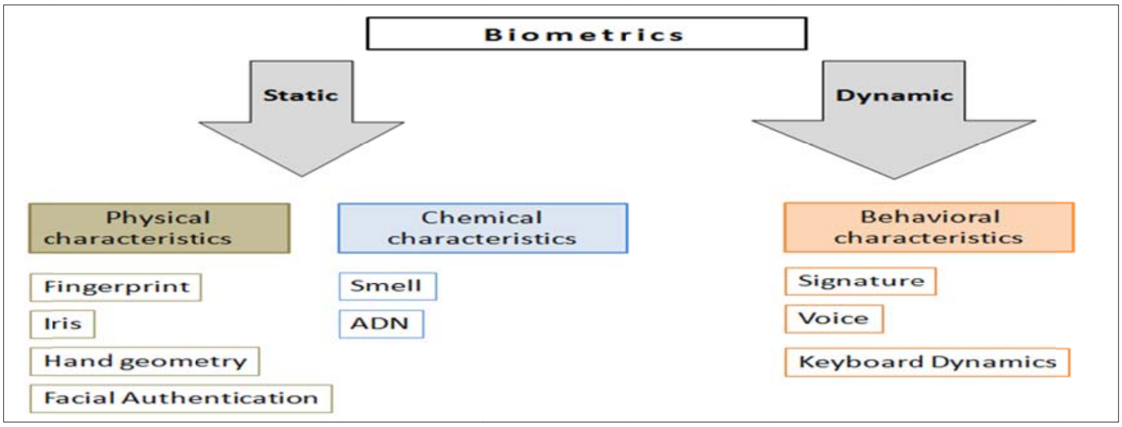

Figure 1 Types of biometrics. (García-Hernández & Paredes, 2005).

While some methods require any voluntary action from the user, the facial recognition can be used in a passive way. This can be an advantage to make more useful its utilization and become, for example, in a video surveillance system. Following the thesis realised by Valvert (2006), the facial authentication presents less weaknesses and more strengths than the rest of the methods [10]. Some of its advantages are:

In which concerns the data acquisition, is much easier to obtain images of a good facial quality than good fingerprints (cuts in fingers, bandaged fingers, callosities, dry or wet skin...). Iris

Scanners can provide a high effectiveness for the recognition of the users, however, due to the little size of the iris, a high-resolution camera is needed to capture it. In the other hand, signature is used to legalize documents, but usually people vary their sign significantly due to: (1) they don't remember their previous signature, (2) they can move while signing changing its shape; or (3) because they are using a different pen; all of this reduce the reliability of the signing identification systems.

For that, the facial recognition is presented as a possible alternative to the user identification with better possible results, because it is a non-intrusive method, which means that data can be acquired without any kind of additional action from the user, in which a webcam is all you need to capture the facial images.

2.2 Approaching to the facial authentication concept

A facial authentication system is a software directed by a computer to identify automatically a person person in a digital image using the comparison of certain facial characteristics [11].

Regardless of the technique used for the solution, the facial authentication requires three stages: (1) the detection of the face in a photograph, (2) the extraction of the facial characteristics and (3) the identification and/or verification of the face by means of the classification of the characteristics. In the identification, the system provides the identity of the person, while the verification confirms o rejects it. In the figure 2, it can be observed how this system works.

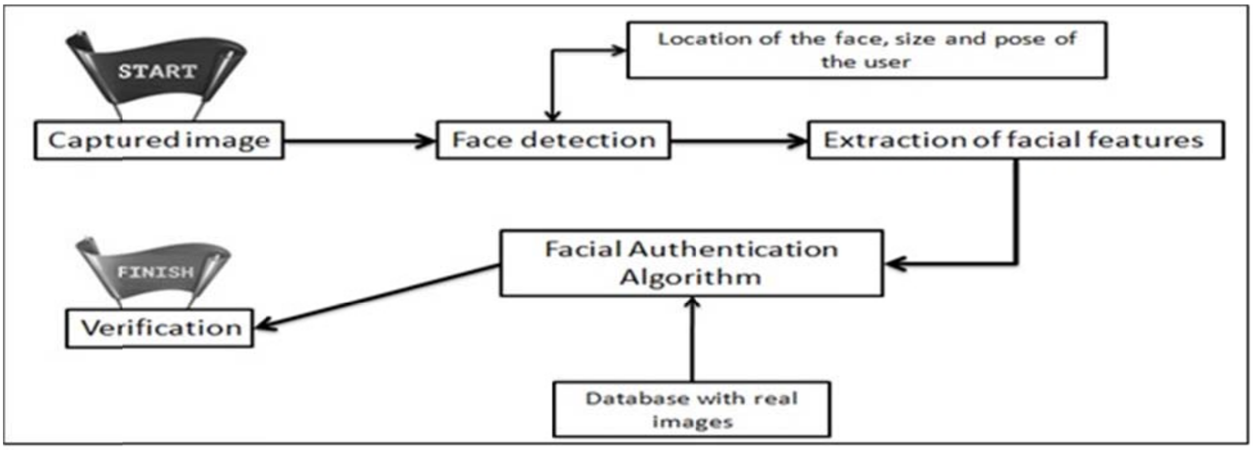
START
Captured image
Location of the face, size and pose of the user
Face detection
Extraction of facial features
Facial Authentication Algorithm
FINISH
Verification
Database with real images

Figure 2 Stages of facial authentication method.

2.3 Advances in the use of the facial authentication in the educational field

Kalikova, Koukol & Krcal [12] developed a biometric system called Biotest with the purpose of identifying the students during the exams and tests in random intervals. Using this software, the teacher can see if the identification of a student was positive. If the identification of a student is not verified positively on three occasions, the system sends a notification to the teacher.

In the same line of this work, Fayyoumi & Zarrad [13] developed a facial authentication software for the identification of the students when they had to do their exams on line. The researchers not only configured the software in the login process of the online exam, but they also did a continuous monitoring (in short time intervals) during the exams period, in order to assure that the student that has started the exam is the same that stayed there until the end and avoid the possibility of committing fraud.

Finally, the authors Owayjan, Dergham, Haber et al., [14] propose a facial recognition security system which can detect the intruders and deny them the access to security areas where only the real user can access. The system they present is divided in two parts, in first place a webcam for the detection of the face of the user, and in second place, the facial authentication software for the identification and verification of the user. The software works as follows: when the user accesses to the area in question, the user's webcam starts working capturing different pictures and sends them to de database of the software for its later comparison and analysis with a real photograph of the student. If the user is not who says he is, an alert is sent.

3. Precision of the different facial authentication systems

Due to the growth that long-distance education has acquired in the last decade and to the inability to control the student's environment in his exams and online activities, is a challenge for the long-distance universities to improve this critical aspect. As Trenholm [15] assures, there are better techniques for cheating in the classroom. As the author said, an 84% of the students say that they need to cheat to go on their academic careers. Some examples of the academic frauds that they are able to do are: (1) a fake user doing the exam; (2) the collaboration of some other students during the exam; y (3) the use of materials and resources not allowed in the exams.

In this context and due to the importance of security and verification of the students that are studying in long distance education, it is important to find a way for these institutions to use any mechanism for helping to solve this problem.

The technology has advanced to remark that biometric systems like facial authentication, fingerprints or iris, have been successfully applied in the different organizations for the identification and verification of the users, being nowadays, facial authentication, the most demanded system. The utilization of biometric systems and technologies for the verification and surveillance of the students while they do their online activities and exams will help to improve the security of the academic institutions and the performance of the students [16].

The purpose of this paragraph is to know the existing technologies such as facial authentication systems to check the identity of the students that use virtual learning platforms in their education with the purpose of being able to rent the services provided by some of those technology companies. In this research, it has been analysed and compared the features that every biometric system offered.

3.1 Securexam Remote Proctor

As Gao [17] assures, Securexam Proctor[1] is a device made by the company Software Secure Inc; that has a fingerprint scanner, a microphone and a webcam with 360 degrees view in order to obtain a complete sight of the scenario where the user is. The software includes a safe browser to block and restrict key functions during the exams (for example, copy and paste, access to files and folders, opening applications, the access to the browsers, etcetera). As said by the author, different universities have used the system, such as "Troy University" or "New York University". Renting this biometric system has a price. The hardware costs 100 dollars, it costs 20 dollars and the technical support costs 10 dollars a year. In general, the total price per student is 150 dollars a year.

3.2 ProctorU

The research of Xiao & Ji [18] includes the system ProctorU[2] supported by the company Axicom, it is a real-time service that verifies the identity of the student when he does his online exams. The system includes some personal information of the user from a variety of databases,

[1] http://ww. softwaresecure.com/

[2] www.http://www.proctoru.com/

using them to ask the user a series of questions about his privacy, for example, his address or his job. The students must answer them correctly to start the exam. In addition, the user has to save some time to do it, having a webcam to monitor him or her during the online exam. Through this webcam, a person from the software company will guide and monitor the student in the examination process. As said by the author, the "National American University" has used this system in the exams of their students. Regarding the price, using this service costs 25 dollars for two hours of exam. That means a price about 75 dollars a year approximately.

3.3 Kryterion Webassessor

Frank [19] defined Kryterion website[3] as one of the best solutions for the online identification of the users in comparison with other methods. The tool uses the image of the user captured through his webcam and of his keystrokes. A person of the company supervises the online exams of the students who have got locked different applications of their computers while they do their exams to prevent them from committing academic fraud. As said by the author, "Penn State University" has used this system in the exams of their students. Regarding the cost, Rose [20] assures that it is around 50-80 dollars for the webcam and 20.000 dollars to adapt their software to the university's support.

3.4 Smowl

Labayen, Vea, Flórez et al., [5] assure that Smowl is directed to companies that require high security levels, such as financial companies, but also to other sectors such as online training, in which checking the identity of the user is essential to avoid frauds in the obtaining of academic titles. It comes up to give a solution to this requirement of a continuous authentication of the online student. Using an appropriate procedure, it is possible to verify not only the user's identity while he logs in his virtual learning platform, but during the entire online interaction which is the most important [6].

As said in the Smowl website4, the company that created the software is currently working (March 2016) with 31 clients in 9 countries, with more than 6 million of analyzed pictures. As said by Staubiz, Teusner, Renz et al., [6], the ANECA5 has approved the use of the facial authentication system Smowl in two online Masters of Rey Juan Carlos University (URJC).

However, all those systems present a common characteristic: The kind of company. All those software have been created by private companies, therefore, each of them has a price for being used. As a solution for this cost which universities have to face, they are currently developing another kind of software that doesn't require a payment for the use, included in the category of free software. Openface[6] is a software that is acquiring great popularity, which we will detail it below.

3.4 OpenFace: Free and open source face recognition

Amos, Ludwiczuk & Saryanaranayan[22] have been the creators of OpenFace in the Carnegie Mellon University of Pennsylvania under the license Apache 2.0. Since OpenFace is an open-source

[3] http://www.kryteriononline.com

[4] http://www.smowl.net/

[5] (National Quality Evaluation and Accreditation of Spain which is dedicated to contribute to the improvement of the quality of the Superior Education system)

[6] https://cmusatyalab.github.io/openface/

project based in a research project of google, its creators have uploaded the source code to their website so everyone who is interested in the project can download it and consult it for free.

To use it is necessary to previously introduce the information of every subject (name and a minimum of 10 pictures of this person) so OpenFace can learn how to differentiate every person using his features. This way, once the information of some subjects has been introduced, the system can find out who is who in real-time. It implements state-of-the-art facial behaviour analysis algorithms including: facial landmark detection, head pose tracking, eye gaze tracking, eye gaze and facial Action Unit estimation [23].

The table 1 presents the descriptions, technical specifications and paid services of these software from the research of Rodchua, Yiadom-Boakye& Woolsey [21], and the ones of the author of the article.

Table 1 Features of the different biometric systems.

Biometric System	Description	Price
Secureexam Remote Proctor	- Utilization of fingerprints for the user's identification. - Requires a video surveillance system.	150 dollars a year.
ProctorU	- Requires the username, password and a picture to identify the student. - The identification of the user in real-time done by a person of the company.	It is around 20-30 dollars for a two hours' exam.
Webassessor	- A facial recognition software and keystrokes rhythm patterns are required. - Video surveillance system using a webcam.	50-80 dollars for the webcam plus the costs for using the application.
Smowl	- Webcam of the student's terminal to capture images and sounds. - App that can be downloaded from Smowltech server and can be executed in the user's browser without any kind of installation process.	4,99€ per hour.
Openface	- The code is available on GitHub at cmusatyalab/openface.	Opensourse (free of charges)

4. Conclusions

Currently a lot of companies and organisms have started to experience the possibilities of using security systems based in biometrics. It offers a new way to identify a person using something that is part of his body, his identity, in which is a very difficult possibility to steal a biometric characteristic and, in all the cases, there are ways to detect if that characteristic has been stolen.

Consequently, is necessary that the universities that use virtual learning platforms, do a self-study, evaluate themselves and start using and checking the results obtained from the utilization of facial authentication software in the learning and teaching process that the student does in this kind of platforms, with the purpose of verifying and identifying his identity and avoiding or minimizing the academic fraud.

References

[1] Ngo, D. C. L., Teoh, A. B. J., &Hu, J. (Eds.). (2015). *Biometric Security*. Cambridge Scholars Publishing.

[2] Evans, N., Marcel, S., Ross, A., & Teoh, A. B. J. (2015). Biometrics Security and Privacy Protection [From the Guest Editors]. *IEEE Signal Processing Magazine*, *32*(5), 17-18.

[3]Valera, J., Valera, J., &Gelogo, Y. (2015, November). A Review on Facial Recognition for Online Learning Authentication. In *2015 8th International Conference on Bio-Science and Bio-Technology (BSBT)* (pp. 16-19). IEEE.

[4] Venkataraman, S., & Sivakumar, S. (2015). Engaging students in Group based Learning through e-learning techniques in Higher Education System.*International Journal of Emerging Trends in Science and Technology*, *2*(01).

[5] 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. *Edulearn14 Proceedings*, 5354-5359.

[6] Staubitz, t., Teusner, R., Renz, J., &Meinel, C. (2016). An experiment in automated proctoring. *Proceedings of the European stakeholder summit on experiences and best practices in and around Moocs (Emoocs 2016)*, 41-54.

[7] Faundez-Zanuy, M., Hussain, A., Mekyska, J., Sesa-Nogueras, E., Monte-Moreno, E., Esposito, A., ... & Lopez-de-Ipiña, K. (2013). Biometric applications related to human beings: there is life beyond security. *Cognitive Computation*, *5*(1), 136-151.

[8] Duarte, T., Pimentão, J. P., Sousa, P., &Onofre, S. (2016, November). Biometric access control systems: A review on technologies to improve their efficiency. In *Power Electronics and Motion Control Conference (PEMC), 2016 IEEE International* (pp. 795-800). IEEE.

[9] García-Hernández, J., & Paredes, R. (2005). Biometric identification using palm print local features. *Biometrics on the Internet Fundamentals, Advances and Applications, 11-14.*

[10] Valvert, J. R. (2006). Métodos y técnicas de reconocimiento de rostros en imágenes digitales bidimensionales. (Final project, Universidad de San Carlos de Guatemala).

[11] Jain, A. K., Flynn, P. J. y Ross, A. A. (eds.) [2008]: *Handbook of biometrics*, Springer.

[12]Kalikova, J., Koukol, M., &Krcal, J. (2015). User authentication system for testing students in computer sciences subjects. In *The 4th International Symposium on Next-Generation Electronics (ISNE 2015)*, (pp. 1-4). IEEE.

[13] Fayyoumi, A., &Zarrad, A. (2014). Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. *Advances in Internet of Things*, 4 (2), 5-12.

[14] Owayjan, M., Dergham, A., Haber, G., Fakih, N., Hamoush, A., & Abdo, E. (2015). Face Recognition Security System. In *New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering* (pp. 343-348). Springer International Publishing.

[15] Trenholm, S. (2007). A review of cheating in fully asynchronous online courses: A math or fact-based course perspective. *Journal of Educational Technology Systems*, *35*(3), 281-300.

[16] Rodchua, S., Yiadom-Boakye, G., & Woolsey, R. (2011). Student Verification System for Online Assessments: Bolstering Quality and Integrity of Distance Learning. *Journal of Industrial Technology*, *27*(3), 1-8.

[17] Gao, Q. (2012). Online teaching: Do you know who is taking the final exam?*Fall 2010 Mid-Atlantic ASEE Conference, Villanova University.* http://www.asee.org. Last visit: January 22, 2016.

[18] Xiao, H., & Ji, W. (2011). Authentication of Students and Students' Work in E-Learning: Report for the Development Bid of Academic Year 2010/11.

[19] Frank, A. J. (2010, July). Dependable distributed testing: Can the online proctor be reliably computerized? In *e-Business (ICE-B), Proceedings of the 2010 International Conference on* (pp. 1-10). IEEE.

[20] Rose, C. (2011). Virtual proctoring in distance education: An open-source solution. *American Journal of Business Education (AJBE)*, *2*(2).

[21] Rodchua, S., Yiadom-Boakye, G., & Woolsey, R. (2011). Student Verification System for Online Assessments: Bolstering Quality and Integrity of Distance Learning. *Journal of Industrial Technology*, *27*(3), 1-8.

[22] Amos, B., Ludwiczuk, B., &Satyanarayanan, M. (2016). *OpenFace: A general-purpose face recognition library with mobile applications*. Technical report, CMU-CS-16-118, CMU School of Computer Science.

[23] Baltru, T., Robinson, P., &Morency, L. P. (2016, March). OpenFace: an open source facial behavior analysis toolkit. In *2016 IEEE Winter Conference on Applications of Computer Vision (WACV)* (pp. 1-10). IEEE.