Realistic Measurement of Student Attendance in LMS Using Biometrics

Elisardo GONZÁLEZ-AGULLA, Jose L. ALBA-CASTRO, Enrique ARGONES-RÚA
Signal Processing and Communications Department
{eli, jalba, eargones}@gts.tsc.vigo.es
University of Vigo, Spain.

and

Luis ANIDO-RIFÓN
Telematics Engineering Department.
lanido@det.uvigo.es
University of Vigo, Spain.

ABSTRACT

In this paper we propose a solution to obtain useful and reliable student session logs in a Learning Management System (LMS) combining current logs with biometrics-based logs that show the student behaviour during the whole learning session. The aims of our solution are to guarantee that the online student is who he/she claims to be, and also to know exactly how much time he/she spends in front of the computer reading each LMS content. Even when the proposed solution does not completely avoid cheating, the use of biometric data during authentication and face tracking provides additional help to validate student performance during learning sessions. In this way it is possible to improve security for specific contents, to gain feedback of the student effort and to check the actual time spent in learning.

Keywords: biometrics and student tracking.

1. INTRODUCTION

Currently, online learning is widely spread. Thousands of courses are available using e-learning environments worldwide. Nevertheless, some limitations of current LMSs do not allow to properly provide virtual educational environments with the whole set of functionality available in conventional systems.

One drawback in current LMSs is the lack of proper mechanisms to record the actual learning time a trainee spends in a given course. Of course, the time a particular student uses a given learning object can be recorded, simply by checking his/her entering and exiting time. Nevertheless, this is not always the actual figure. Let us give one example: a student enters a lesson describing a complex mathematical algorithm. He follows the explanation for a while but then decides to have a coffee with his roommate that has just arrived to their shared apartment without checking out from the course. If no time out expires at the LMS the recorded learning time would be longer than the actual time.

The above described situation is particularly important in those courses where the actual time spent by the student is of special relevance (e.g. professional certifications, some life-long-learning courses, European ECTS, feedback for course creator, etc.)

Moreover, current tracking in LMSs is based on actions performed by students in any of the computer input devices (e.g. keyboard or mouse), but there is no way to check who actually performed that action.

In our approach we apply biometric verification to improve LMS's security access control, using an internet-based platform for biometric authentication developed by our research group and opened to the research community as an open-source project, BioWebAuth (BWA) [1] [2], which provides Central Authentication Service compatible with LMS like ILIAS, Moodle, or Claroline [3]. In this work we also apply continuous student face tracking and automatic face verification along the LMS session to guarantee the student presence. With this approach the LMS goes a step forward to interpret the student behaviour more accurately.

The output of our approach for each student session is a set of different categorized time-intervals related with presence, verification and pose [4]. From these time-intervals the LMS can extract important and useful information particularized for one student, such as the actual time that one student spent in one specific resource, or for a subset of them, such as the mean time that students spent in a given LMS content. Summarizing, our solution offers the LMS reliable information about the actual student behaviour during each LMS session.

Session logs of current LMSs store information about when a user gets a resource. However, there is not any mechanism to obtain precise and reliable information about how much time the student spends in each content. For this reason with current LMS session logs, it is difficult to detect, for example, when the student changes the web browser in order to perform any Internet search related to the current LMS content, when the student switch the browser to other PC application such as a dictionary, etc. To solve this, we propose an improvement to the LMS log system giving to each LMS resource the capability of knowing when it is in foreground and when it is in background mode and storing this information. This approach can be implemented detecting browser focus events, when a web resource gains and loses the focus, and reporting to the LMS using AJAX. From improved LMS logs, the system has a detailed trace of the interaction between the student and the browser during the whole LMS session. This log is useful to know what resources were watched in each session, and to know the maximum time the student spent on each of them. Combining this log data with the biometric log, the LMS can know exactly how much time the student spends for each LMS content.

Nowadays biometric face tracking is not a perfect solution; there are some problems to deal with, such as bad light conditions in the student room, that may lower the performance of the biometric module.

2. RELATED WORK

As far as we know, there are no similar applications applied to e-learning environments that combine biometric web authentication and biometrics-based tracking. Nevertheless, it is possible to find some related applications in other domains:

NEC NeoFace [5] time clock system uses webcams for employee surveillance, replacing the classic punch-card reader with facial recognition software, so that old canard of getting someone else to clock in for you is useless.

Auernheimer et al [6] discuss design considerations and a prototype for a biometrics (fingerprint) based identification and authentication system to support web-based course examinations, this system is similar to BioWebAuth.

Milton Chen discusses the utility of video tracking as real-time teacher feed-back during online classes [7]. In [8] he proposes gesture detection to manage the video flow in videoconference systems in order to minimize the use of the bandwidth.

3. BIOMETRICS-BASED STUDENT ACCESS CONTROL MODULE

To address the problem of "access control" using biometrics we made use of the Biometrics for Web Authentication project at SourceForge, known as BioWebAuth project. BWA is an open source Java framework intended to provide single sign-on web authentication based on BioAPI-compliant biometric software or devices. It uses the JA-SIG Central Authentication Service architecture [9]. BWA only provides biometric-based access control service [10] [11], but it does not offer the continuous user tracking that we need for our purposes. Using BWA as the access control mechanism, which provides biometric verification with multiple biometric traits (face, fingerprint, etc.), the LMS has the guaranty that the student accessing LMS contents is actually sat in front of the computer, avoiding the case of unauthorized access without student collaboration (such as stolen passwords). But a biometric access control does not guarantee that once the student has logged in the system, other person doesn't supplant him the rest of the session. Due to this reason we have developed a face tracker module that is able to track the people who appears in the webcam video flow and verifies whether any of them is the student or not.

4. BIOMETRICS-BASED STUDENT ATTENDANCE MODULE

We implemented a continuous student monitoring system that stores the student behaviour during the whole learning session. This attendance module is mainly composed by a FACE tracker and a FACE verifier. So we combine a frontal face detector with a skin and eyes tracker for each new face appearing in the field of view of the webcam, and we use a BioAPI-compliant verification module for matching each of them with the student biometric template. In this way we monitor the student and his context. The tracker was developed using C++ programming language and the image processing library OpenCV. The biometric verifier module was developed using also C++ programming language and it is BioAPI-compliant. The output of this module is a biometric log that provides precise information about the time that the student was in front of the computer, and, specifically, when the student was looking at the screen. This biometric log is combined with the LMS session log to tie, as much as possible, the link between intellectual activity and actual attendance.

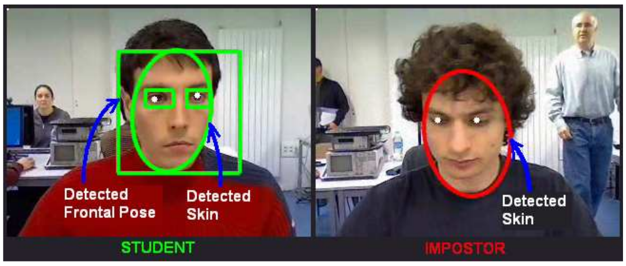

Figure 1. Real-time visual output of biometrics-based tracking module. At left side, verified student in frontal pose. At right side, impostor in not frontal pose.

Figure 1 shows an example of student tracking where the square identify the face and eyes location and tracking; and the ellipse identify the face-skin location. The colour of the squares and ellipse determine whether the student was verified successfully (green), unsuccessfully (red), or whether the student identity was not yet verified (orange).

5. EVALUATION

We carried out a real test to evaluate the utility and design of the biometric-based student attendance module.

Methodology: The goal of this study is to check the accuracy of the measurements obtained by our attendance module. In this study, sixteen students of the Image Processing subject, of Telecommunications Engineering School at Vigo University, were tracked while they were using the LMS Moodle to solve a quiz test about subject contents. The test scenario was the actual classroom of the Image Processing subject, and there was a computer with web cam per student.

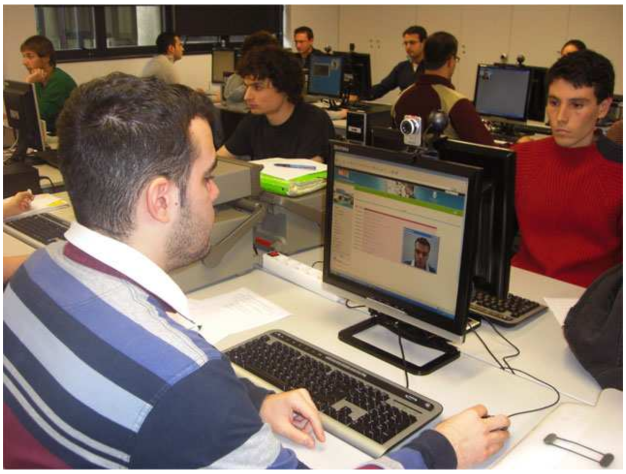

Figure 2. Students checking that their faces were correctly framed by the web cam located on top of the computer.

The designed test contained three parts: student fills a quiz, student fills another quiz as an impostor, student consults his/her score. Next, we explain with more detail the test protocol:

1. Student checks out that the web cam is located on top of the computer screen and that he is visible in the webcam video flow (see Figure 2).

2. The student face template used by the verification module is created (20 seconds at maximum) analysing the video flow.
3. Student performs a short quiz of 7 questions using Moodle; student is in the role of client (8 min).
4. Student moves to the computer at his/her left to take the role of impostor for the student previously using that computer.
5. Student performs other short quiz of 7 questions using Moodle again at that new computer; student is now in the role of impostor (8 min).
6. Student comes back to his/her own computer.
7. Student checks out the obtained scores obtained in the two quizzes using Moodle; student is again in client role.
8. End of the test.

Results: After processing the reports generated by the biometrics-based tracking module we have obtained the next average and std figures:

1) *TotalSessionTime* (TST): 0:26:23 is the average time necessary to perform the test with a std of 0:02:49.
2) *DetectedAnyPresenceTime* (DAPT): 0:22:33 (86% of TST) is the time that our biometrics-based tracker has detected people presence, with a std of 0:03:09.
3) *DetectedStudentPresenceTime* (DSPT): 0:12:10 (54% of DAPT) is the time that our biometrics-based tracker is sure that the student with granted permissions was detected, with a std of 0:03:54.
4) *StudentFrontalPoseTime* (SFPT): 0:03:54 (29% of DSPT) is the time that our biometrics-based tracker has detected the student in a frontal pose, with a std of 0:03:33.

Validation: Analysing previous results we checkout that they reflect quite well the defined protocol in the experiment. It can be observed that figures related directly to the defined protocol (time of quiz tests) are more accurate, while figures measuring person-dependent behaviour have a standard deviation comparable to the mean.

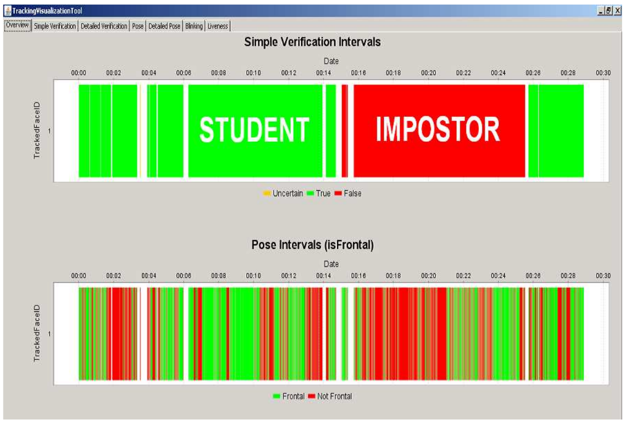

Figure 3. Biometrics-based traces log viewer. First row shows the student verification intervals during the whole session. Second row shows frontal pose intervals (green) during the whole session.

Figure 3 visually shows, for one of the students, the behaviour that our tracking module has recorded. We can see there that the verification intervals are coherent with the specified protocol in the test.

6. CONCLUSIONS

Summarizing, our contribution is a way to generate a more useful and reliable student session logs that current LMS logs, which provides us with the chance to obtain important statistics about the users' activities.

As we have said before, the proposed solution does not completely avoid cheating. Nevertheless, the use of biometric data during authentication and tracking provides additional help to validate student performance during learning sessions. Therefore it is possible to improve the security in the online learning process whenever it was required, such as in those courses where the actual time spent by students need to be validated.

7. ACKNOWLEDGMENTS

This work has been partially supported by Spanish Ministry of Science and Innovation through project TEC2008-05894

8. REFERENCES

[1] E. Otero, E. González, J. L. Alba**,** C. García and O.W. Márquez. "An Open Framework For Distributed Biometric Authentication In A Web Environment", **Annals of Telecommunications**. Special issue on multimodal biometrics, Vol. 62 (1/2), pag.177-192, 2007.

[2] Biometrics for Web Authentication (BioWebAuth): http://sourceforge.net/projects/biowebauth/

[3] E. González, E. Otero, J.L. Alba, C. García. "An open source Java framework for biometric web authentication based on BioAPI". 11th **International Conference on Knowledge-Based and Intelligent Information & Engineering Systems** (KES2007), Vietri sul Mare (Italia), Sept. 2007.

[4] E. González, L.E. Anido, J.L. Alba, C. García. "Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments" Proceedings of Eighth IEEE **International Conference on Advanced Learning Technologies** (ICALT '08), pp. 551-553, July 2008.

[5] NeC NeoFace Time Clock
http://www.techeblog.com/index.php/tech-gadget/face-recognition-time-clock

[6] Auernheimer, B., Tsai, Max. J., "Biometric Authentication for Web-Based Couse Examinations" in **HICSS**, 2005.

[7] Chen, M., "Visualizing the Pulse of a Classroom", in **Proceedings of the eleventh ACM international conference on Multimedia**. 2003, pp. 555 – 561.

[8] Chen, M., "Achieving Effective Floor Control with a Low-Bandwidth Gesture-Sensitive Videoconferencing System" in **Proceedings of the tenth ACM international conference on Multimedia**. 2002, pp. 476 – 483.

[9] Central Authentication Service project
http://www.jasig.org/cas

[10] Elisardo González-Agulla, Enrique Otero-Muras, Carmen García-Mateo**,** José L. Alba-Castro. "A Multiplatform Java Wrapper For The Bioapi Framework", **Computer Standards & Interface.** Vol. 31, N. 1, pp. 186-191, jan. 2009, ISSN: 09205489.

[11] Enrique Otero-Muras, Elisardo González-Agulla, José L. Alba-Castro, Carmen García-Mateo and Oscar W. Márquez-Flórez. "An Open Framework For Distributed Biometric Authentication In A Web Environment", **Annals of Telecommunications. Special issue on multimodal biometrics.** Vol. 62, N. 1/2, pp. 177-192, 2007, ISSN: 0003-4347.