Online teaching: Do you know who is taking the final exam?

Qinghai Gao

Department of Criminal Justice & Security Systems, Farmingdale State College

Abstract: In recent years Distance Learning has been steadily gaining popularity. More and more courses are being taught online. However, one question remains for those who teach online courses: who is doing the real course work? In this paper we will briefly survey the commonly used methods to prevent students from e-cheating, attempt to answer the question whether present technology has made it possible to completely eliminate student dishonesty in Distance Learning. In particular we look at how biometrics as identification tools can be applied to achieve this goal. The main purpose of the paper is to ask college educators and policy makers to rethink the credibility and quality of modern college education which could be endangered by issuing college degrees to the students who never really took the required courses.

Introduction

As the Internet usage becomes an indispensable part of our daily routine and everything goes online, Distance Learning has been steadily gaining popularity. A significant portion of the students take online courses. To meet this needs and to attract remote students many colleges and universities now offer online courses as replacements or as supplements to the traditional classroom based face-to-face courses. However, one question remains for those who teach online courses: who is doing the real course work? Especially when it comes to e-exams, online teaching makes it extremely difficult to deal with one serious problem: student dishonesty [1].

To solve the problem many scholars [2][3][4] have proposed different methods, such as:

- Design open-book exams
- Use discussions, essay, and other written projects; reduce the percentage of exams
- Use a large pool of questions to randomly generate exams for each student
- Require students to take exams on site

In order to reduce the possibility of e-cheating in our college, which uses ***Angel*** as the online teaching tools, we utilize the following measures to minimize the chance of e-cheating:

- Divide a typical course into a number of modules. Inside each module we set up a discussion forum to require every student to submit his or her opinion for an issue and respond to a minimum of three submissions from others.
- Set up quizzes and exams consisting of a set of randomly selected questions from a large question pool so each student will have a different exam/test. For the multiple choice questions

the answer choices of a question are randomized also for different students. The questions are also given one at a time.

●Set up the time restriction. Once an exam/test is started it has to be finished within the specified time frame. And students are given only one chance to attempt it.

●Compare the IP addresses to see if two students are in the vicinity of each other. Make use of plagiarism detection tool ***Turnitin*** and search engine to check some questions for possible dishonesty.

To date the majority of colleges and universities use these methods. However, these measures are not enough to prevent e-cheating since the traditional password-based system is inadequate to successfully authenticate students remotely. For example, a student can give his or her account information to a person and let that person take the exam for him/her. One proposed solution to the problem is to use biometrics. We believe that the recent developments of biometrics have made it a viable technology to prevent e-cheating. With this paper we will look at the state of the arts of the solution.

The rest of the paper is organized as the following. Section 2 will first introduce how biometrics system works and then describe a few commonly used biometrics. Section 3 briefly surveys the literature proposals on using biometrics to authenticate students for e-exams. Section 4 introduces three commercially available products designed for proctoring e-exams. Lastly, section 5 will summarize the paper and propose future research direction.

Biometrics recognition

Biometrics is defined as the identification of an individual based on physiological and *behavioral* characteristics. Commonly used physiological characteristics include face (2D/3D facial images, facial IR thermogram), hand (fingerprint, hand geometry, palmprint, hand IR thermogram), eye (iris and retina), ear, skin, odor, dental, and DNA. Commonly used behavioral characteristics include voice, gait, keystroke, signature, mouse movement, and pulse. And two or more of the aforementioned biometrics can be combined in a system to improve the recognition accuracy. In addition, some soft biometric traits like gender, age, height, weight, ethnicity, and eye color can also be used to assist in identification.

Generally a biometric system is designed to solve a matching problem through the live measurements of human body features. It operates with two stages. First, a person must register a biometric in a system where biometric templates will be stored. Second, the person must provide the same biometric for new measurements. The output of the new measurements will be processed with the same algorithms as those used at registration and then compared to the stored template. If the similarity is greater than a system-defined threshold, the verification is successful; otherwise it will be considered unsuccessful. Due to the fuzzy measurements of

biometrics error-correction coding is needed. Table 1 lists a few biometrics and their features for identification and/or authentication.

Table 1 Biometric features for identification/authentication

Biometrics	**Identifying Features**	**Error Correcting**	**Ref.**
Keystroke	Duration, latency: a computer user's typing patterns consist of durations for each letter typed and latencies between keystrokes	Discretization	[5]
Voice	Text-dependent or text-independent speaker utterance units	Discretization	[6]
Signature	Dynamic signature features, such as pen-down time, max forward *Vx* (Velocity in x direction), max backward *Vy* (velocity in y direction), time when the last peak of *Vx* or *Vy* occurs, pressure, height-to-width ratio, and so on.	Averaging	[7]
Face	Facial features: positions, sizes, Angles, etc	RS code	[8]
Iris	Digital representation of iris image processed with Gabor wavelet	RS code Hadamard	[9]
Fingerprint	Minutiae points: ridge ending and ridge bifurcation	Quantization	[10]
Palmprint	Unique and stable features such as principal lines, wrinkles, minutiae, delta points, area/size of palm	RS code	[11]

.

Literature review

A few scholars have proposed to use biometrics for E-learning. Rabuzin et al. [12] and Asha et al. [13] proposed to combine several different biometric traits in the field of e-learning. Levy and Ramin [14] proposed approach that can incorporate a random fingerprint biometrics user authentication during exam taking in e-learning courses. Flior et al. [15] presents a method for providing continuous biometric user authentication in online examinations via keystroke dynamics. Penteado and Marana [16] proposed to use face images captured on-line by a webcam in Internet environment to confirm the presence of users throughout the course attendance in an educational distance course. Alotaibi [17] also proposed using fingerprints for E-exams.
In all these proposals a webcam is required to monitoring student activity while taking the exam. Another default requirement is a high-speed internet connection.

We believe that it is necessary to ask students to provide two or more live biometrics for a few times during the exam, though it may cause inconvenience. Keystroke and mouse clicking biometrics do provide continued authentication. However, false recognition rate can be very high for behavior biometrics.

Commercial products for proctoring E-exams

At least three products have been adopted by some colleges and universities for their online courses. The first one is named *Secureexam*, a remote proctor made by *Software Secure*; The second one is named *Webassessor*, made by *Kryterion*; and the third one is named *ProctorU*, made by *Axicom*. A brief description of each product is followed.

●**Securexam Remote Proctor**, *Software Secure Inc*. [18][19]

Securexam Remote Proctor, a small device which features a fingerprint scanner, microphone, and a video camera with a 360 degree view. To start an exam, students need to provide their fingerprints for identification. During the exam, the microphone and video look out for anything suspicious like an unknown voice or movement on the camera.
College example: Troy University, New York University
Price: $150 per student

●**Webassessor,** *Kryterion Inc*. [18][20]

Kryterion's Webassessor uses face image captured by webcams, and keystroke biometrics (typing styles) captured by software to authenticate the test taker and alerts the proctors if there is a change when somebody else has taken over
College example: Penn State University
Cost: $50 ~ $80 per student

●***ProctorU***, *Axicom Corp*. [18][21]

The system gathers some personal data from a variety of databases, including criminal files and property records, and uses the data to ask students a few questions, such as address, employers, etc. Students need to answer the questions correctly before they can start the exams. In order to use ProctorU, each student also needs to reserve a time slot for an exam and has a webcam ready that can monitor the exam environment. With a webcam a human proctor would remotely guide a student in the process of starting an exam.
College example: National American University
Cost: $10 per student

In summary, these products provide us with technological solution to prevent dishonesty. However, it seems that they have yet to take full measures to protect the security and privacy of students' home environments and their biometrics information, which could affect their acceptance and wide adoption.

Conclusion

In this paper we summarized the commonly used methods to prevent students taking online exams from e-cheating and attempted to answer the question whether they have helped to achieve the goal of eliminating student dishonesty in distance learning. In particular we looked at how biometrics can provide an effective solution to the problem and briefly surveyed the existing proposals of using biometrics to authenticate remote students. We survey three commercially available products that have been tested by some universities and can be used to proctor e-exams.

The main purpose of the paper is to ask educators to rethink the credibility and quality of modern college education which could be endangered by issuing college degree to the students who never really took the required courses.

References

[1] Camille F. Rogers (2006). Faculty perceptions about e-cheating during online testing. *Journal of Computing Sciences in Colleges*, 22(2): 206-212.

[2] Barbara Christe (2003). Designing online courses to discourage dishonesty. *Educause Quarterly*, 4:54-58.

[3] Neil C. Rowe. *Online Journal of Distance Learning Administration* (2004). Available at: http://www.educause.edu/Resources/CheatinginOnlineStudentAssessm/153159.

[4] Kikelomo Maria Apampa, Gary Wills, David Argles. Towards Security Goals in Summative E-Assessment Security. *International Conference for Internet Technology and Secured Transactions*, pp.1-5 (London, 9-12 Nov. 2009).

[5] F. Monrose, M. Reiter, and S. Wetzel (1999). Password Hardening Based on Keystroke Dynamics. *Proc. of the ACM Conference in Computer and Communications Security*, pp: 73– 82.

[6] F. Monrose, M. Reiter, Q. Li, and S. Wetzel (2001). Cryptographic key generation from voice. *Proc. of the IEEE Symposium on Security and Privacy*.

[7] F. Hao, and C. Chan (2002). Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 10(2): 159–164.

[8] B. Chen, and V. Chandran (2007). Biometric Based Cryptographic Key Generation from Faces**.** *Proc. of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Application*, pp: 394 – 401.

[9] F. Hao, R. Anderson, and J. Daugman (2005). Combining cryptography with biometrics effectively. *Technical Reports*, University of Cambridge, Computer Laboratory.

[10] U. Uludag, S. Pankanti, and A. Jain (2005). Fuzzy Vault for Fingerprints. *Proc. of Audio and Video-based Biometric Person Authentication*, pp: 310-319.

[11] A. Kumar, and A. Kumar, A. (2008). A palmprint-based cryptosystem using double encryption. *Proc. of SPIE*, 6944:1-9.

[12] K. Rabuzin, M. Baca, and M. Sajko(2006). E-learning: Biometrics as a Security Factor. *International Multi-Conference on Computing in the Global Information Technology* (ICCGI'06), pp. 64.

[13] S. Asha and C. Chellappan. Authentication of e-learners using multimodal biometric technology. *International Symposium on Biometrics and Security Technologies*, pp. 1-6, Islamabad (23-24 April, 2008).

[14] Yair Levy and Michelle M. Ramin. A Theoretical Approach for Biometrics Authentication of e-Exams. Available at: http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf

[15] Eric Flior, and Kazimierz Kowalski. Continuous Biometric User Authentication in Online Examinations, pp.488-492. *Seventh International Conference on Information Technology* (2010).

[16] Bruno E. Penteado and Aparecido N. Marana (2009). A Video-Based Biometric Authentication for e-Learning Web Applications. *Enterprise Information Systems. Lecture Notes in Business Information Processing*, 24(IV): 770-779.

[17] S. Alotaibi. Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. *The 4th Saudi International Conference*, The University of Manchester, UK (July 2010).

[18] Frederic Lardinois. The Proctor at Home: Using Technology to Keep Online Students from Cheating (July 25, 2008). Available at:

http://www.readwriteweb.com/archives/online_students_cheating_fraud_technology.php
[19] Refer to: http://www.softwaresecure.com/
[20] Refer to: http://www.kryteriononline.com/
[21] Refer to: http://www.proctoru.com/