Programación Matemática y Software (2009)
Vol.1. Num. 2. ISSN: 2007-3283

Recibido: 06 de Octubre del 2009 /Aceptado: 10 de Noviembre del 2009
Publicado en línea: 30 de Diciembre del 2009

Advanced Tools for the estimation of basic Knowledge Level on Education and Training

José Alberto Hernández-Aguilar[1], Gennadiy Burlak[2], René Santaolaya S.[3], Alberto Ochoa[4], Messouma Atakishiyeva[1]

[1] Facultad de Contaduría, Administración e Informática, [2] Centro de Investigación en Ingeniería y Ciencias Aplicadas, Universidad Autónoma del Estado de Morelos. Ave. Universidad 1001 Col. Chamilpa CP62209
[3] Departamento de Ciencias Computacionales, Centro Nacional de Investigación y Desarrollo Tecnológico CENIDET
[4] Instituto de Ingeniería y Tecnología, Universidad Autónoma de Ciudad Juárez

jose_hernandez@uaem.mx

Resumen. Nosotros describimos el uso de nuestro sistema de evaluación en línea (Cliente-Servidor) equipado con capacidades de reconocimiento biométrico, aplicado para evaluar el conocimiento básico en una preparatoria. En este reporte discutimos la posibilidad de la identificación real de estudiantes remotos para resolver el importante problema de: ¿quién está ahí?. En nuestro experimento, seleccionamos aleatoriamente una muestra de estudiantes (n=54) y llevamos a cabo dos evaluaciones: una evaluación normal (en lápiz y papel), y una evaluación por computadora. En este último caso, nuestro sistema de evaluación en línea con herramientas biométricas puede autentificar a un estudiante por medio de la huella digital. Si un estudiante es autentificado, el sistema permite la evaluación en línea, mientras tanto el estudiante está siendo monitoreado por cámaras Web. Durante la evaluación en línea los estudiantes fueron afectados por el ambiente en línea, ellos obtuvieron bajas calificaciones en línea con respecto a los exámenes tradicionales. El reconocimiento de huella digital fue muy bien aceptado. Sin embargo, a 13% de los estudiantes evaluados les disgustó ser monitoreados con cámaras Web, y el 20% de ellos encontraron alguna forma de hacer trampa. Esta tecnología nos permite obtener estadísticas comparables de ambas evaluaciones, y discutir recomendaciones generales para la estrategia, tecnología y equipamiento de las evaluaciones en línea.

Palabras Clave. Reconocimiento de huella digital, Biometría en educación, Evaluación en línea.

Abstract. We describe the use of our online assessment system (Server-Client) equipped by biometric recognition capabilities, applied to evaluate the basic knowledge in a High School. In this Report we discuss the possibilities of real identification of remote students to solve important problem: “Who's there?” In our experiment we randomly selected a sample of students (n=54) and performed two evaluations: a normal evaluation (paper and pencil), and a computer assessment. In the latter case our online assessment system with biometric tools could authenticate a student by means of index fingerprint. If a student is authenticated, the system allows online assessment,

meanwhile such a student is being monitoring by web cams. During online assessment students were affected by the online environment, they obtained lower grades online than on traditional tests. Fingerprint recognition was very well accepted. However, 13% of students tested dislike web cam monitoring, and 20% of them noticed a way to commit cheat. This technology allows us to obtain the comparable statistics of both evaluations and discuss general recommendations for strategy, technology and equipping of online computer assessment.

1. Introduction.

Nowadays the problems of information security are of great importance, and it is not surprising that problems of "educational security" become be common also [11]. The Faculty who has not taught online often asks about cheating. Specifically, they ask how you know the person who is taking the class is the one who signed up. Unless photo IDs are checked and all course work occurs inside of a monitored classroom, faculty really does not know for sure whether the student is who they say they are in the classroom or online [10]. On online assessments in which we are not sure who is taking the test; students will be under pressure, some students perform unfairly poorly under pressure and this is a good incentive to cheat [11]. We have a wide spectrum of documented techniques to commit cheat on online assessments, for instance: modify a grade in the database (DB), to steal answers for questions, to copy from another student or cheat sheets, impostor or substitute remote students, to search for answers on the Internet or in blogs, on the messenger or cellular phone, in single words to "commit cheat" to obtain a "better grade" in an online assessment [6]. Biometrics is becoming a powerful tool to improve security on transactions and reduce frauds [7].

Most of e-learning tools providing online assessment uses only basic and standard security measures and normally do not provide advanced security mechanisms, for instance the Blackboard system [2] that use an username and password to verify the student identity, and profiles in database (DB) to avoid unauthorized access.

An advanced security measure can be implemented by means of modern biometric technologies. Much of the hot discussion about biometrics has come about the level of research and interest was drawn to large-scale implementations of the technology by Governments [4]. They may provide added robustness in access and control to high security facilities within higher education. Since the unit price for biometric devices continues to fall it is possible to employ them to replace the normal systems used for workstation and network access [13].

1.1 The problem at hands.

The main problem on online assessments is how to know "who's there?" . In this paper,

we propose the use of biometrics, particularly the use of fingerprint recognition on real time to authenticate students into the assessment system, and web cam monitoring during online assessments to deal with the well-known problem of: who is taking the exam? The contribution of this paper is the use of biometrics on online assessments as a new approach for remote identification on real time, we realized several proposals considers this problem, however none documented implementations of such technologies has been tested with flesh and bone students. Some of these proposals reflect separated point of views of IT, educational professionals with different perspectives. However in general such a problem can be solved by efforts of multidisciplinary team works jointed with mathematical professors, psychologists, statistics professionals and IT consultants.

2. Methodology.

Sample. For our experiment, we selected a random sample of students (n=54) from the José María Morelos y Pavón High School, located in Temixco, Morelos, México. A school located in urban area located near capital city of Cuernavaca, Morelos. Total population of school is 642 students. The students profile was: 15 to 17 years old, socio-economic level C-, D (low middle class-, upper low class) 89% owns a computer, 65% of their parents complete elementary school studies only, and just 56% of those are married.

Tests design. Professors of this school designed the tests (from August 5th and 6th 2007); one of such a test was implemented for the discussed online assessment with the use of our authoring tools. The tests consisted of 30 questions with similar complexity level; we evaluated the mathematics basic knowledge, specifically: arithmetic, algebra, geometry, statistics, probability and trigonometry.

Type of task. Typical task is to select one of six answers to proposed question.

i.e. which value of X makes true the next equation 7X-9 = 3X+1?

a) 12 b) 8 c) 2.5 d) 5 e) 3.2 f) -5

We carried out two evaluations, a normal evaluation (paper and pencil), and a computer assessment with our online system equipped with biometric recognition.

Setting up. Computers were prepared with our online client software installed; biometric devices and network connectivity was attached.

The traditional test. The paper-and-pencil test was conducted on August 14th. 2007.

Enrollment. Students were enrolled into the system by taking their left-hand index fingerprint on August 15th 2007. We verified that the students were identified clearly by the recognition system after their enrollment.

Online assessment with biometric recognition test. Was conducted on the Computers Network Laboratory located at the High School facilities from August 16th to August 17th 2007, each computer used in the experiment had attached a Microsoft Fingerprint Reader, a web cam, a broad band connection to our server as well as our proprietary client system. Students were instructed in how to use the system, we explained them that a web cam was monitoring their activities, later students authenticated by means of their fingerprint into our Server. After that the computerized assessment started. The use of calculator and cellular phones was avoided.

Statistical Analysis. After termination of assessment, obtained data were processed using standard statistical tools with the use of Ccount gnu free software.

3. The Online Testing System with Biometric Recognition.

Virtual proctoring involves using biometric technology to monitor students at remote locations. For virtual proctoring, is recommended using a layered approach depending on critical maturity of the test. With high stakes tests, video monitoring and a biometric measure such as iris scanning may be used. For medium stakes tests, a single biometrics measure may be acceptable [3]. Despite most of online assessments are located in the middle of both definitions; we consider the fact of high levels of cheating in remote assessments. In one hand, fingerprint recognition is a single biometric measure, the cheapest, fastest, most convenient and most reliable way to identify someone. And the tendency, due to scale, easiness and the existing foundation, is that the use of fingerprint will only increase [8]. Cars, cell phones, PDAs, personal computers and dozens of products and devices are using fingerprint recognition more and more [5].

One current trend is to incorporate fingerprint scanners into personal computers, laptops, and mice. In addition, computer networks and large databases can be secured using fingerprint technology. This is a hot topic of discussion since the phenomenon of the Internet and the development of Intranets has spawned new

digital technologies such as E-commerce and on-line services [7]. Besides, users are more willing to use fingerprint recognition than iris recognition [1], they believe is more secure for health. Unfortunately, fingerprint recognition is used just to authenticate into systems, but then what? The student is free

to use any media to commit cheat, to avoid that situation we considered the possibility to use web cams. Web cams are inexpensive and most of students are used to deal with them, they form part of their common tools to work and chat. Is for sure that some students will reject the possibility to be monitored, percentages vary from country to country, but is our intention to measure this figure as a part of our research. Based on above exposed, we propose the use the mix of video monitoring, by means of web cams, and fingerprint recognition to provide a secure online assessment environment.

3.1 Technical requirements.

3.1.1. The Server Side. Keep information of biometrics measures (fingerprints) and associated student information in database; Scanning of fingerprints (enrollment of students); Provide a recognition tool to determine validity of fingerprint and grant authorization to online assessment; Monitor remote students by means of web cams located in remote locations. Support the online assessments process; Provide security mechanisms to ensure confidentiality and validity of data: Encryption of data transmitted and received, and generation of log files.

3.1.2. The Client Side. Scanning of fingerprints; Enrollment of students (optional);

Avoid the unauthorized access to online assessment; Show the diagnosis of security.

Provide capacity of students' monitoring using web cams during assessment process; Provide mechanisms for client setup, students' authentication (using fingerprint), and evaluation preferences; Support the evaluation process and show final results of evaluation.

3.2 Performance Schema.

We separated the application in two main modules: the first one is on charge of the online assessment conduction, and the second one on charge of the fingerprint recognition and web cam monitoring on real time. Server must be in listening mode waiting for Clients that requires a service. In order to use fingerprint recognition, the first step is to enroll students –top, right side in Figure 1-, the students fingerprint is saved and indexed in the Features Database, we

highly recommend to separate this from the Assessment System Database, using even separated servers, to improve system overall performance. In the features database is assigned the Student Personnel ID that is used to link the students' personnel information with fingerprint image.

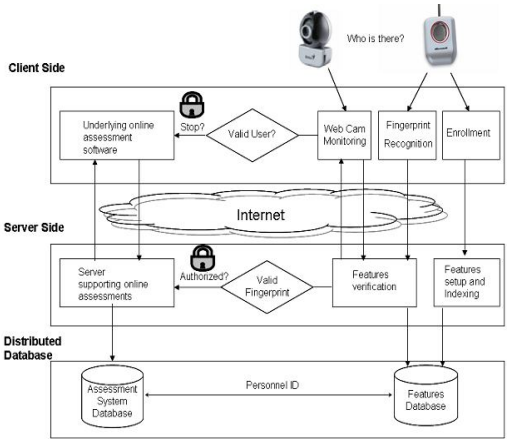


Fig. 1. Fingerprint recognition on real time.

If the Sever is on listening mode and the student has been enrolled, the assessment process can start. The student enters to the online assessment application, and when system requires the user and password, his or her uses the Mouse Id –superior right side of Figure 1- to scan his/her fingerprint.

The fingerprint is verified in the Features Database, and if it is recognized as a valid, then the Server authorizes access to the online assessment application, else an error message is sent to the Client to try again. In other hand, if the student's fingerprint is valid, the user is authenticated into system, the evaluation process starts and web cam transmission is initialized at Client Side to conduct real time monitoring by means of multitasking. If someone else tries to get the control of the computer during the online assessment, the evaluation process is finished prematurely, and results are sent to server side to be processed as they are. To the contrary, the evaluation process is finished successfully, the assessment is processed at Server Side, and the final results of evaluation and security status are shown at Client Side.

To measure the security level provided by the fingerprint recognition system at the stage of authorization we used two ratios:

- **False Acceptance Rate (FAR)**. is defined as the ratio of impostors that were falsely accepted (IFA) over the total number of impostors tested (TNIT) described as a percentage. This indicates the likelihood that an impostor may be falsely accepted and

must be minimized in high-security applications.

$$FAR = IFA / TNIT \quad (1)$$

- **False Reject Rate (FRR)**. is defined as the ratio of clients that are falsely rejected (CFR) to the total number of clients tested (TNCT) described as a percentage. This indicates the probability that a valid user may be rejected by the system.

$$FFRR = CFR / TNCT \quad (2)$$

On fingerprint recognition the speed and storage requirements acquired relevancy, specifically the time required to enroll, verify or identify a person is of critical importance to the acceptance and applicability of the system [13]. Below we listed the specifications of the selected hardware and software.

3.3 Implementation.

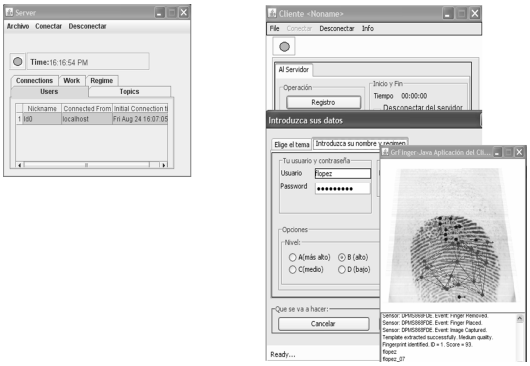
We separated the application in two main modules: the first one is on charge of the online assessment conduction

3.3.1. Hardware.

- **Client System Requirements (minimal).** Pentium class (i386) processor (200 MHz or above) with 128Mb or higher, 100Mb disk space.
- **Fingerprint mouse.** 250 DPI (Digits per Inch) or higher, 500 DPI is recommended.
- Broadband Internet. Minimum 128 Kbps, recommended 256 Kbps.

3.3.2. Software.

- **Biometrics SDK.** Griaule GrFinger SDK 4.2 [5] allows you to integrate biometrics in a wide variety of applications. Provides Support for dozens of programming languages – including Java- and integration with several Database Management Systems. Besides, provides multiple fingerprint reader support, and even after application development or deployment, makes you able to change the fingerprint reader you're using, without modifying your code.
- **Fingerprint template size.** 900 bytes average.
- **Programming language.** Java. due the online assessment software tool was developed using this technology.
- **JMF Java Media Framework.** To allow transmission of video and/or photographs over the Internet.
- **Web Server. Apache 2.0.** Database Management System. MySQL.
- **Operating System.** Windows 98, and Windows NT. Windows 2000, Windows XP and 2003.



(a) (b)

Fig. 2. The Server Application (a) supporting fingerprint recognition in Client-side (b) to authenticate students in online assessments.

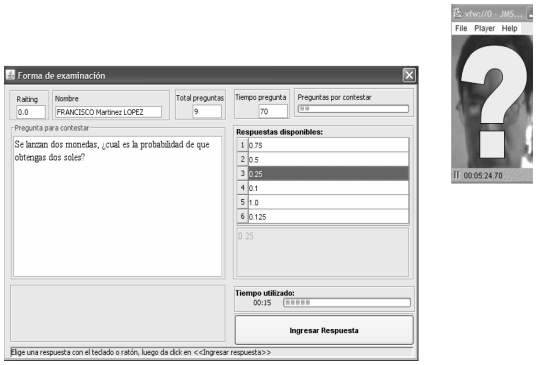


Fig. 3. Web cam monitoring while online assessment is in progress.

In Fig. 2, the left section (a) shows the Server Side and the users connected, specifying remote IP address, date and connection time. The right section (b) the client-side, here the user enters to the client application, setup the client and establish connection with server on a specific port and host, once the server and the client have established connection, the student authenticates into server by means of fingerprint using the fingerprint reader, the student can see graphically displayed her/his fingerprint, if the fingerprint is found at server side, the interface automatically fills the user and password fields and allows the student to continue with subject selection to be assessed, and later with the assessment process.

In Fig. 3, the online assessment interface is shown, the questions and respective answers are randomly sorted, questions have a limited time to be answered, if a question can not be answered on assigned time, test will continue with the next question automatically. Student must select an answer by giving double click or by selecting one of the available answers and then giving a click on the enter button. As soon as the assessment starts, web cam monitoring sends information to server side to know who is in control of the computer. The biometric information is verified at server side and if an identity error occurs the test is interrupted and the assessment is processed as it is. Else assessment continues normally operation. At the end of the assessment, the grade, the protocol of the assessment and the security report is shown at client side.

3.3.3. Accumulation and analysis of information. The biometric information and the responses of students were stored in a MySQL Database Version 5.0. We selected this software, because is a powerful free software that can be downloaded from the internet for academic purposes, and is strong enough to support hundreds of online transactions –in our case online assessments- simultaneously, besides provides security mechanisms that makes applications work secure. We recommend obtaining a commercial license of this software, if is required managing thousands of simultaneous transactions, or for commercial applications.

Quality of analysis depends on how well structured was the database, for this purpose, we identify the whole relevant entities: Students, Students' Perception, Results of evaluation, history log, Careers, Subjects,

Topics, Students perception, Subject environment and Professor, and we implemented these on a MySQL database Schema.

4. Results and Discussion.

Considering the number of students enrolled (n=54) on this test with obtain a FAR of 99.99% and a FRR of 97.09%, only one student could not be recognized despite several trials, although we try to enroll her using different fingers of her left hand we could not, she has tiny long fingers and the enrollment results were always the same. Her fingerprint template is unintelligible to the fingerprint recognition system, her fingerprints seems like stains. Something related has been documented in [9], Asiatic persons has similar problems to be identified by fingerprint readers. We faced this problem by providing to this student an user and a strong (mix of capital letters, lower letters and numbers) password.

Our results showed that students were affected by the online environment, they obtained lower grades online versus grades on traditional tests. The average grade in paper and pencil test was 3.8 meanwhile the online grade was 3.5, this difference is explained due an small percentage of students must improve their computer skills, we noticed that video games and chat could

improve skills of students as well as general performance in online assessments. Students

perceived our system as faster, easy to use; fingerprint recognition played an important role in this perception. However, they disliked time limited questions, and 13% disliked web cam monitoring. When we asked them

directly if they disliked being monitoring, 33% answered this fact bothers them. They said

feeling under pressure, getting nervous and disliked being monitored or watched.

A 20% of the students tested, noticed a way to commit cheat using a system like ours, the identified ways were: turn the camera to some else, use a photo, use a cheating list, and just one person thinks to dirt the fingerprint reader. We made in-depth analysis and discovered that students with poor performance (low grades) are willing to commit cheat. 78 % of the students would like the system being implemented at their high school. We consider that the online assessment system with biometric recognition was very well accepted, but must be adapted to be more user friendly, to improve perception of students, process to enroll users must be improved too. We believe that our results are quite interesting and hot, despite in [14] is discussed the application of fingerprint readers and the use of cameras in online assessments, there are not figures to analyze; as we explained, we tested our system with flesh and bone students which is an improvement regarding this previous work. State of the art systems like Blackboard [2] provide some basic biometric recognition facilities (i.e. photo ids), but they require that a human proctor verify the identity of students, the purpose of our

system is to perform this task automatically online.

5. Future work.

We intend to improve the human-computer interface and assessment methodology with the use of students' comments and feedback. We want to test the tool within different groups at different high schools and Universities. Regarding of the biometric recognition, we intend to improve strongly the quality of recognition.

6. Conclusions.

Biometric recognition is a promising technology to solve the problem of who is there? As it is shown in this report, this technology already is well accepted in online assessments, but it still should be subject to improvement.

References.

[1] AIDC. Automated Identification and Data Capture Web Site, http://et.wcu.edu/aidc/

[2] Blackboard. Security, http://www.blackboard.com/us/index.aspx

[3] BSU. Ball State University. Technology assessment reports on: The use of

Biometrics in education. http://web.bsu.edu/dpmuller/biometrics/

[4] Clarke, N. and Furnell, S. "Biometrics: The promise versus the practice". Computer Fraud & Security 2005, Issue 9, September 12-16.

[5] Griaule. Biometrics FAQ, http://www.griaule.com/page/en-us/faq_biometrics

[6] Hernández-Aguilar J.A., Ochoa, A., Muñoz, J., and Burlak, G. "Detecting cheats in online student assessments using Data Mining". Dmin06, Las Vegas Nevada, USA 2006. June 26-29, pp. 204-210.

[7] ITEDU. Biometrics, http://et.wcu.edu/aidc/

[8] Maltoni, D., Maio, D., Jain, A., and Prabhakar, S. "Handbook of Fingerprint Recognition", Springer 2003.

[9] Michigan Org, http://www.reachoutmichigan.org/funexperiments/agesubject/lessons/prints_ext.html

[10] MSU Michigan State University, "Quizzes and Exams: Cheating on exams and Quizzes". http://teachvu.vu.msu.edu/public/pedagogy/assessment/index.php?page_num=3.

[11] Neil, R. "Cheating in Online Student Assessment: Beyond Plagiarism". Online Journal of Distance Learning Administration, Volume VII, Number II, Summer 2004 State University of West Georgia, Distance Education Center.

[12] Savvas, A. "Online assessments and biometrics used in new immigration system". Computer Weekly Section IT Management Politics and Law. 3/14/2006, pp .10-10, 1/7p.

[13] Wasniowski, R. "Using Data Fusion for biometric verification". Transactions on Engineering, Computing and Technology APRIL 2005. pp. 72-74.

[14] Wisher, R. Curnow, C. and Belanich J. "Verifying the Learner in distance learning". 18 Annual Conference on Distance Teaching and Learning 2005.

José Alberto Hernández Aguilar. Obtained his Doctorate degree on Engineering and Applied Sciences in November 2008 at Universidad Autonoma del Estado de Morelos (UAEM). Since November 2008, he is working as full time professor at UAEM. He is candidate to SNI. Areas of interest: Databases, Artificial Intelligence, On-line Assessment Systems, Marketing Research and e-commerce.

Gennadiy Burlak. Worked in the Physics faculty at the National University of Kiev where he occupied several faculty positions- His last position was full-time professor at the Physics Faculty. Dr. G. Burlak entered to UAEM since 1998. He delivers several courses in the Physics and Computers areas. Nowadays he is full time professor at CIICAp-UAEM and SNI 2.

Messouma Atakishiyeva. She is full time professor at Sciences Faculty at UAEM. She is working at the Department of Mathematics. She is member of SNI.

René Santaolaya. Is a researcher in the National Center for Research and Technological Development (CENIDET), Cuernavaca, Morelos, México. His research interest includes software process models, software architectures, software reuse, legacy software re-engineering, service oriented architectures and web services. René Santaolaya received a PhD in Computer Science (Software Engineering) from National Polytechnic Institute, Computing Research Center. He teaches in the Advanced Msc. Program in the Software Engineering Area. He is a senior member of the IEEE.

Alberto Ochoa. Bs'94–Eng.Master'00–PhD'04-Postdoctoral Researcher'06 & Industrial Postdoctoral Research'09). He has 1 book, and 7 chapters in books related with AI. He is SNI 1. His research interests include evolutionary computation, natural processing language, applications of Artificial Intelligence in Optics and social data mining.