Journal of
INDUSTRIAL
TECHNOLOGY

Volume 27, Number 3 - July 2011 through September 2011

Student Verification System for Online Assessments: Bolstering Quality and Integrity of Distance Learning

By Dr. Suhansa Rodchua, Mr. George Yiadom-Boakye, & Dr. Ronald Woolsey

Peer-Refereed Article
Research Paper

KEYWORD SEARCH

Assessment
Distance Learning
Higher Education
Quality
Teaching Methods

Student Verification System for Online Assessments: Bolstering Quality and Integrity of Distance Learning

By Dr. Suhansa Rodchua, Mr. George Yiadom-Boakye, & Dr. Ronald Woolsey

Dr. Suhansa Rodchua is an assistant professor in the School of Technology at University of Central Missouri. She worked as an assistant project manager and a business consultant in Thailand. She received her Ph.D. from Indiana State University in the Technology Management, Quality Systems Specialization in 2005. Currently, Dr. Rodchua teaches M.S. in Industrial Management and Technology programs and holds a CQM/OE certification from ASQ. She is an active member of the ATMAE Women in Technology Division. Contact Suhansa Rodchua at rodchua@ucmo.edu

George Yiadom-Boakye graduated M.S. in Technology at University of Central Missouri in Spring 2011. He worked as a graduate assistant in the School of Technology between 2009-2010 and completed a Master's thesis. Currently, He works as an intern at Clay & Baileys, Kansas City, Missouri. Mr. Boakye received his Bachelor's degree in Biochemistry from Kwame Nkrumah University of Science and Technology, Ghana. Contact George at gboakyeyiadom@yahoo.com

Dr. Ronald Woolsey has been a university professor for twenty-five years and worked in industry for ten years in engineering and management. He received his Master's degree from Northwest Missouri State University and a Ph.D. from Iowa State University. In 1998 he accepted a position with the University of Central Missouri as Graduate Coordinator for the School of Technology. He received an award for Innovative Excellence in Teaching, Learning and Technology at the Fourteenth International Conference on College Teaching and Learning and was selected as a NAIT Outstanding University Professor in 1991 and 2003. Contact Ronald Wolsey at Woolsey@ucmo.edu

ABSTRACT

The rapid growth of online examinations using Internet-based assessment tools has continued. The inability to control a student's environment while taking exams has been a major challenge for higher education. A clear correlation exists between an increase in the number of acts of dishonesty and the failure of institutions offering courses to monitor and enforce policies on cheating. The recent article of academic dishonesty and proctor at home published by Chronicle Higher Education, the U.S. Congress is concerned about quality and integrity of distance learning and had added language into a part of legislation renewing the Higher Education Act that encourages schools to fight cheating more effectively.

The purpose of this study is to investigate the current technology and biometric systems used in remote proctoring systems to verify and monitor students taking online exams. The study also proposes the model to support the integrity and quality of online assessment; the model integrates facial recognition software, video surveillance systems, and computer restriction software into a system. In summary, online assessment and proctored testing deal with the issue of student identification and the environment in which materials are accessed effectively but it also negates much of the advantage of providing Internet based-course work. Utilization of biometric system with updated technology in video surveillance in the online examination will lead to certainty and quality assurance of student achievement and school's reputation.

INTRODUCTION AND RATIONAL

A key challenge for online-based learning in this information technology era is academic integrity. The explosive growth of online courses using the World Wide Web as the primary means of communication between instructors and students has rapidly outstripped the academic institution's ability to retain quality control measures. Continued growth in distance learning and the inability to control the student's environment is a challenge to institutions of higher education. There is strong evidence that cheating has increased in today classroom. The figures show that 84% of student say they need to cheat in order to move ahead in careers and 90% of the students say they never pay a price for cheating (Trenholm, 2007). Some examples of online exam cheating may include:

- Having someone other than the enrolled student taking an exam
- Copying and collaborating with others during an exam
- Accessing to materials that are not allowed, such as textbooks and web resources.

To deal with these issues, popular stop gap measures like proctored testing centers, access passwords, time restricted tests, database pools of test questions randomly selected for an exam are tools that have been developed to reduce the temptation to be dishonest. Each of these tools deals with symptoms of the real issue, loss of control of a traditional classroom environment. They come with drawbacks of their own. According to the Chronicle Higher Education, the U.S. Congress is

concerned about quality and integrity of distance learning and had added language into a part of legislation renewing the Higher Education Act that encourages schools to fight cheating more effectively (Lardinois, 2008). In addition, education industry analysts expect the demand for online examination methods proctoring using student identification products will skyrocket in 2010. The U.S. Department of Education starting to require schools to make sure that persons taking an exam are actually the students enrolled in the course (Webwire, 2009).

SIGNIFICANCE, PURPOSE, AND LIMITATIONS OF THE STUDY

Technology has progressed to the point that biometric systems, such as facial recognition, fingerprint, and eye scanning, have been implemented successfully in many organizations and processes. Authentication system using server technology with biometric systems and video surveillance system, has gained popularity in monitoring activities in small businesses, big corporations, government, households, municipalities and educational institutions.

The purpose of this study is to investigate the current technology used as remote proctoring systems to verify and monitor student's identification while taking online examinations. The authors conducted a historical-based research on different systems on remote proctoring and types of biometric devices. In addition a proposed model to support the integrity and quality of online assessment will be presented. This model discusses the integration of facial recognition software, video surveillance systems, and computer restriction software. The major contents in this paper are a discussion of different systems being developed for remote proctoring of examinations, various types of biometric identification, and finally a proposed model for verifying and student monitoring.

This study is limited to information gathered from the review of literature and personal interviews; and the proposed model was designed based only on functions in the Blackboard delivery software from Blackboard Inc.

DIFFERENT SYSTEMS ON REMOTE PROCTORING EXAMINATION

Proctored examination is one of the major concerns for online course delivery. A growing number of students choose online courses either as an alternative to a traditional college experience or as a supplement. Colleges and universities have started to worry about how to prevent these students from cheating on remotely administered examinations. What is a proctored examination? There are diverse definitions of proctored examination. The University of West Florida's Online Campus defined: a proctored exam as one that is overseen by an impartial individual (called a proctor) who monitors or supervises a

Table 1. Today's Remote Proctor Systems with Characteristics

Systems	**Description (identification and proctoring)**	**Technical specification**	**Costs**
Secureexam Remote Proctor (SRP) http://www.remoteproctor.com	fingerprint for student identification video surveillance system /audio recording with SRP device	- SRP equipment - Computer - High speed Internet	$125 for SRP equipment and $30 annual fee
ProctorU http://www.proctoru.com (virtual online proctoring)	username - password, and ID photo for student identification human proctor in real-time and video surveillance system /audio recording	- Webcam 640x480 - Computer - High speed Internet - headphones or working speakers - microphone - live proctor from ProctorU	$17.50 per 2 hours exam
ProctorCam http://www.proctorcam.com (virtual online proctoring)	username - password, and ID photo for student identification human proctor in real-time and video surveillance system /audio recording	- Webcam 640x480 - Computer - High speed Internet	Average $20 per 1 hour exam, discount on the group of students
Webassesor™	Facial recognition software and patterns of keystroke rhythms Secure Browser Control video surveillance system	- Webcam with audio - Computer with Webassesor application - High speed Internet	Webcam $50-$80 plus costs of application

student while he or she is taking an examination (University of West Florida, 2009). Another definition published by the University of Colorado Denver is "Test proctoring is testing overseen by an authorized, neutral, proctor, who ensures the identity of the test taker and the integrity of the test taking environment" (University of Colorado Denver Online Help Desk, n.d., para 2). In summary, the proctoring process helps to prevent dishonest students from cheating on examinations and ensures the security and integrity of the process. According to a USA Today's article, college students taking courses online has surged and created a tough dilemma for educators. Should instructors trust students to take an exam on their own computers, even though it may be easy to sneak a peek at the textbook? Or should institutions force students to trek to a proctored testing center, which detracts from the convenience that drew students to online classes in the first place? (Pope, 2007). Utilizing the existing technologies in online exam proctoring is becoming the focal point of many institutions efforts.

A variety of 'free' and 'for a fee' organizations are used as proctoring services. For example, research centers, public libraries, campus testing and assessment centers or Sylan Learning Centers that charge $50 for each exam (University of Colorado Denver Online Help Desk, n.d.). Today technology allows an online proctoring system to utilize the software, hardware, fingerprint scanners, video monitoring personnel and so on to identify the online students and monitor them while taking examinations without commuting to a proctored location. Some commercially available examples of providers of remote proctoring methods discussed in this section are: Secureexam Remote Proctor, ProctorU, ProctorCam, and Webassesor™. Table 1 presents descriptions, technical specifications, and services costs for these 4 companies. Data on costs on ProctorU and ProctorCam were gathered from email contacts and personal interviews with the companies' representatives.

Securexam Remote Proctor (SRP)

Troy University, Alabama, and some other colleges and universities currently adopted the Securexam Remote Proctor (SRP) System from Software Secure, Inc. of Cambridge, MA.

The Securexam Remote Proctor addresses areas of exam security by:

- Authenticating the student with a fingerprint scanner prior to providing access to the exam
- Restricting the computer's functions with Securexam solution
- Monitor video and audio during exam, capturing all suspicious changes in sound and motion, just as a proctor would in a traditional exam environment.

Figure 1 shows the image of SRP, which is a small stand-alone device that connects to the test taker's computer via USB. www.remoteproctor.com/SERP/Description.aspx

According to the Office of University Relations Media, SRP equipment will cost students about $125. The authentication is done through a server with a fingerprint scanner; the system verifies each test taker against the fingerprints provided at registration. This system also records the test-taker's voice and image through a camera that records 360-degree real-time video and audio of the environment during the entire exam. All suspicious sound, activity and motion are catalogued during the recording, limiting the need for constant monitoring. Professors do not need to watch students taking the exam live; they can view the streaming audio or video at any time (Troy University, n.d.).

ProctorU

Next commercial software is called ProctorU. It is developed by Andrew Jackson University and spun off into a separate company. Jarrod Morgan, co-developer of Proctor stated "We have improved the system by adding live certified proctors, real time audio/video using TokBox, technical assistance, practice exams, identify authentication and the ability to assist exam-takers by remotely controlling their computers during an exam" (Webwire, 2009, para 2). The system has proctored 1,500 exams so far and attracted more and more interested colleges and universities each week (2009).

ProctorCam

ProctorCam is a name of business and system that provides a virtual online proctoring service. The test takers and organization that require proctor tests can use this service with their own equipment at their convenience and at their chosen location. The company has developed a software-enabled online exam proctoring service for online course publishers. Remote proctors, average US$20 per hour, hired under contract by the fledgling company, monitor students and answer their questions via webcams (Moore, 2010). To use ProctorCam, the system integrates desktop sharing software, a web cam, a microphone and a reliable internet connection.

WebassesorTM

Kryterion Inc. is an organization that specializes in secure test development and delivery (Case & Cabalka, 2009; Kryterion, 2009). They provide live proctoring for many distance learning and businesses (2009). The technology is called Webassesor™ and has the capability of secure online testing for proctoring students wherever they live, learn and work (Case & Cabalka, 2009). According to Kryterion this technology works with the various

test engines and learning management systems. The Webassesor™ is capable of online proctoring employing web-cams with audio features to monitor test takers. Test takers purchase the camera for between $50 to $80, which allows proctors to view student's face, keyboard and workspace (Foster, Matton & Walker, 2009). The technological features built into the Webassesor include: Photo Matching Authentication (Sentinel™ security technology), Secure Browser Control (System Lockdown), video surveillance system, and Data Forensics. Some of the institutions that have used this technology include the Pennsylvania State University and Western Governor's University (Kryterion, 2009; Foster et al, 2009).

TYPES OF BIOMETRIC IDENTIFICATION

Biometrics has become a vital method of ensuring security against threats such as theft and malicious intents in this era of globalization. It involves the identification of an individual based on one or more unique physical attributes. Biometric identification can be physiological such as fingerprint, retina, DNA or behavioral such as handwriting, gait, speech pattern etc. A biometric method is evaluated based on specific qualities including its universality, uniqueness, permanence, collectability, performance, acceptability and circumvention (Wikipedia, 2010).

The biometric devices are considered better than password protection or card scanners because the actual person must be present for the computer, doorway, or other device to become enabled for usage. Different parameters have been used to judge performance or accuracy of a biometric system. The extensively used parameters are:

- Force Acceptance Rate (FAR); the probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database
- Force Reject rate (FRR); the probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database (Laha, 2008).

Other performance parameters include Receiver (or relative) operating characteristic (ROC), Equal error rate (EER), Failure to enroll rate (FTE or FER), Failure to capture rate (FTC), and Template capacity (2008). Table 2 presents widely used biometric technologies including their advantages and disadvantages.

Table 2 Advantages and Disadvantages of Different Biometric Systems

Type of Biometrics	Advantages	Disadvantages
Fingerprint	Has a higher reliability and stability compared to iris, voice and face recognition methods. Equipments are less expensive compared to other biometric systems.	Dirt and twist can lead to noise and distortion problems. Some people feel offended when asked to put their fingers at where many other people have continuously touched.
Retina	It is a highly accurate method with an error rate of 1 in 10,000,000. There is no known way to replicate retina; varies from person to person (Wikia Technology, n.d).	It is an expensive and intrusive process. Comparison of template records can take a long time depending on the size of the database. Retinal pattern can be affected by disease like glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome.
Facial recognition	Images can be acquired without posing; it is therefore non-intrusive and contact free process. Capable of integrating with existing surveillance systems. Capable of simultaneous multiple face processing. Capable of live face detection. Multiple samples of the same face can be acquired easily. Tolerant to face posture and capable of fast face matching.	Needs a well-controlled light source in automated face recognition system. Technical challenges are associated with face authentication. Disguise can be used to circumvent an authentication process.

To establish an effective remote proctoring system, biometric is one of vital tools that has increased in use for online exams and it need to be investigated before implementation, for example, some concerns with biometric systems and forgery of the authorized user. In general, the literature shows that fingerprint scanners are the most widespread usage of biometrics. They are easily obtained and less expensive. The retina scanner is newer technology and still high cost, but it is generating

popularity due to high accuracy rate. The facial recognition has many variables involved in the system, but it has the most potential to develop into many different users in the future. According to Biometric Institute (2011), no system is invulnerable to attack. Each device has to be evaluated based upon the typical method of attack for that system. Incorporated into the system design is a given level of assurance of how many attacks will probably succeed. The above analysis on advantages and disadvantages of these biometric tools assists in the design of a proposed model of this study.

PROPOSED MODEL ON ONLINE VERIFICATION AND MONITOR SYSTEM

Even though some academic programs have systems in place to discourage dishonesty, some students have developed methods to cheat on examinations and to outsmart current systems included in such course delivery software as Blackboard from Blackboard Inc. The Master's degree program in Industrial Management in the School of Technology has offered 100% online delivery of coursework since 2002. The program is very successful with continued increases in number of enrollment and consistently high ratings of student satisfaction for the past nine years. Continuous improvement is part of the program's philosophy and establishing the Academic Integrity Program (AIP) to identify students through facial recognition systems and proctoring students with video surveillance while restricting computer software, is a proposed solution.

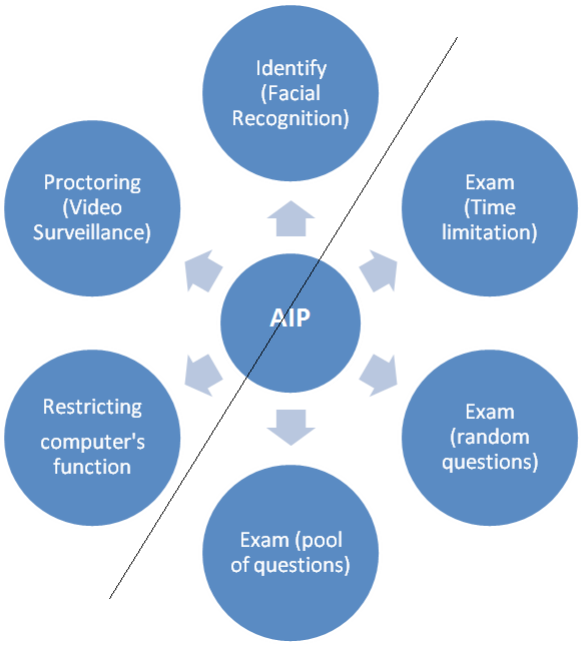
Facial recognition is a biometric system that utilizes the characteristics of the face to identify an individual. Facial recognition has several important advantages over other types of biometric data. Facial recognition data can be captured at a distance, can be done without physical contact, and it can often be leveraged against existing surveillance systems including surveillance cameras and closed circuit television (Woodward, Horn, Gutane & Aryn, 2003). This proposed model on student verification and examination proctoring shows a line cutting the graphic below in half, as presented in Figure 2. This represents actions taken to ensure the integrity of the programs since 2002 (on the right) and the ways the AIP will modify that program in the future (on the left).

Currently, the Blackboard, course delivery courseware, offers useful functions in the test/exam section. Instructors are able to set up the exam with a large pool of questions, random questions, and limit the time for taking exam. However, there are still some questions on student cheating remained, for example, having someone other than student taking the exam, copying and collaborating with others during the exam, and using materials that are not allowed in the examination. AIP proposed to solve these problems with three additional functions; using facial recognition to identify students, video surveillance in the exam proctoring, and software in restriction of computer's function. Figure 3 describes the process flowchart of the system beginning when student log-in and ending of exam and surveillance. This proposed model includes the following steps:

- Step 1: access to the online exam using 'username' and 'password
- Step 2: read an instructions set for the exam and verification process
- Step 3: capture a student's image via the webcam, then submit for verification
- Step 4: verify 'image capture' with the database. If match, student will go on to take exam (to Step 5). If not match, student will be able to retry. After retry 3 times and still unsuccessful, student will be asked to contact a course instructor.
- Step 5: while taking an exam, student is monitored and recorded by the video surveillance. The Internet restriction software will activate; and students will have no access to any other websites and applications, except only the exam.
- Step 6: If the system was interrupted (e.g. lost of Internet connection) while taking exam, the system will ask student to verify his/her image again. After passing verification process, then the student will continue on the exam and be monitored by the video surveillance and the Internet restriction software.
- Step 7: after completing the exam, student will click "Submit", end of the exam and surveillance.

Figure 2. Major task components of AIP

The program proposed to establish remotely identify and proctor students while taking exam.



The program is currently set up large randomized pool of questions with a limited time for completion.

This proposed model has preliminary been tested with a group of on-line students. After the study, some limitations that were identified included:

- The webcam proctors raised questions of privacy;
- Facial recognition software was still not 100% accurate due to some variations on pose and illumination; and
- No discussion on students who may need special assistance under the guidance of the Americans with Disabilities Act (ADA).

CONCLUSIONS AND RECOMMENDATIONS

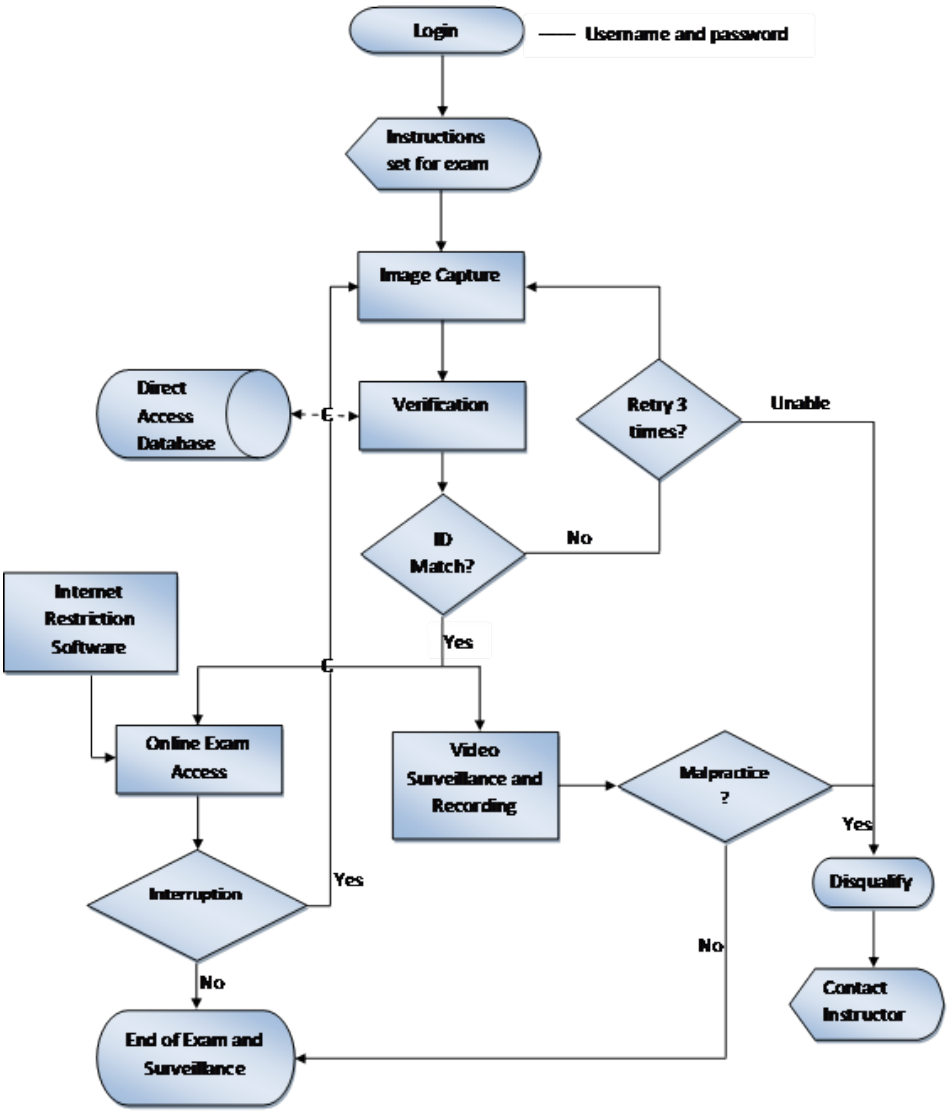
Harnessed technology, biometrics, software programming, and optics in a symphonic correlation expanding the reach of academic institutions to students without regard to geographic separation or intellectual compromise is this study's promise. Academic merit is the yardstick by which every university measures the progress of every student but without physical contact. How does the instructor know whose work is being measured? This paper is not about developing new technology, but applying technology in a new way to solve what is perhaps to greatest obstacle to any university's ability to offer academic programs online, dishonesty. The value of every degree is the reputation of the institution and the students produced. Without academic rigor, without confidence in the processes by which it is measured, are their values in the program?

Utilization of biometric system, either fingerprint or facial recognition, with updated technology in video surveillance in the online examination will lead to certainty and quality assurance of student achievement and learning effectiveness. This paper gathered the available technology currently used in proctored testing and proposed the model of online verification and monitor system that mainly promote the quality and integrity of distance learning.

It is likely that the information derived from this study will lead to a better understanding of the utilization of remote proctoring assessment in an Internet-based distance environment. The following items are recommendations for further study.

- The facial recognition software may not work as advertised; different software vendors should be considered.
- The proposed Academic Integrity Program (AIP) model may not work on all broadband platforms. Extra effort should be made to insure that the software architecture works with most applications and broadband platforms.
- Using one biometric device does not seem to be the best way to ensure the best possible outcome for accurate identification. Creating multifaceted layers of devices can be an appropriate approach for the implementation.
- Students may perform poorly in this online integrity assessment due to a lack of understanding of the system. A training program and providing proper webcam for students will help to resolve this mistake.

Figure 3. Flowchart of online verification and monitor system



ACKNOWLEDGMENTS

Thank you to William Ford and Ravi Kanuri for their contribution to this study.

REFERENCES

Biometrics Institute. (2011). Biometrics Institute Biometric Vulnerability Assessments. Retrieved February 20, 2011, from Biometrics Institute: http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=48

Case, R, & Cabalka, P. (2009). Remote Proctoring: Results of a Pilot Program at Western Governors University. Retrieved on June 10, 2010 from http://www.uwex.edu/disted/conference/Resource_library/proceedings/09_19933.pdf

Foster, D., Matton, N. & Walker, P. (2009). Using Multiple Online Security Measures to Deliver Secure Course Exams to Distance Education Students. Retrieved on June 10, 2010 from http://www.ou.nl/Docs/Campagnes/ICDE2009/Papers/Final_Paper_101Walker.pdf

Kryterion. (2009). *Online Secure Testing*. Retrieved on May 16, 2010 from http://www.kryteriononline.com/

Lardinois, F. (2008). *The Proctor at home: using technology to keep online students from cheating*. Retrieved from http:/www.readwriteweb.com/archives/online_student_cheating

Laha, J. (2008). *Biometric Techniques - Enhancing Security Standards In High Performance Enterprise*. Retrieved on May 16, 2010, from, http://ezinearticles.com/?Biometric-

Moore, G. (May, 2010) ProctorCam betting on e-learning upswing. Retrieved on June 10, 2010 from http://www.masshightech.com/stories/2010/05/10/daily29-ProctorCam-betting-on-e-learning-upswing.html

Pope , J. (2007). *Web cam watches students taking tests online*. Retrieved May 17, 2010 from http://www.msnbc.msn.com/id/19315329/ns/technology_and_sc

Trenholm, S. (2007). A Review of Cheating in Fully Asynchronous Online Courses: A math or Fact-Based Course Perspective. *J. Educational Technology Systems*, 35(3), 281-300.

Troy University (n.d.). Securexam Remote Proctor System. Office of University Relations. Retrieved May 17, 2010 from http://www.troy.edu/news/mediakits/remote_proctor.pdf

University of West Florida. (2009). *Online campus*. Retrieved on April 15, 2010 from http://onlinecampus.uwf/class/proc_exams.cfm

University of Colorado Denver Online Help Desk. (n.d). *Exam proctoring for online course q&a*. Retrieved on May 18, 2010 from http:// www.cuonline.edu

Webwire (July, 2009). Fifteen hundred college exams proctored live online. Retrieved on May 18, 2010 from http://www.webwire.com/ViewPressRel.asp?aId=99265

Wikipedia (2010). *Biometrics*. Retrieved on May 15, 2010 from http://en.wikipedia.org/wiki/Biometrics

Wikia Technology (n.d.). *Retina Recognition*. Retrieved on May 17, 2010 from http://itlaw.wikia.com/wiki/Retina_recognition

Woodward, J. D., Horn, C., Gatune, J., & Thomas, A. (2003). *Biometrics: A Look at Facial Recognition.* Prepared for the Virginia State Crime Commission. Arlington: RAND Public Safety and Justice.