Towards a Framework of Biometric Exam Authentication in E-Learning Environments

Michelle M. Ramim, Nova Southeastern University, USA, 3301 College Avenue, Fort Lauderdale, FL 33314, USA; E-mail: ramim@nova.edu
Yair Levy, Nova Southeastern University, USA, 3301 College Avenue, Fort Lauderdale, FL 33314, USA; E-mail: levyy@nova.edu

ABSTRACT

In the past fifteen years the use of Internet technologies has been substantially growing for delivery of educational content. E-learning environments have been incorporated in many universities for the delivery of e-learning courses. However, opponents of e-learning claim that a central disadvantage of such teaching medium is the growing unethical conduct in such environments. In particular, opponents of e-learning argue that the inability to authenticate exam takers is a major challenge of e-learning environments. As a result, some institutions proposed to take extreme measures including asking students to take exams in proctor centers or even abandon completely the offering of e-learning courses in their institutions. This paper attempts to address this important problem by proposing a theoretical framework that incorporates available fingerprint biometric authentication technologies in conjunction with e-learning environments to curb unethical conduct during e-learning exam taking. The proposed framework suggests practical solution that can incorporate a random fingerprint biometric user authentication during exam taking in e-learning courses. Doing so is hypothesized to curb exam cheating in e-learning environments. Discussions on future research and possible implications of the proposed theoretical framework for practice are provided.

Keywords: E-learning Environments, Biometric Systems, Unethical Conduct, Academic Misconduct, Online Exam Security, Secured Exam Submission.

1. INTRODUCTION

This paper proposed a theoretical framework for fingerprint biometrics authentication of exam takers in e-learning environments. The following section provides literature review on the increase use of e-learning environments in higher educational institutions. Additionally, the subsequent section provides a review of literature on issues related to unethical conduct in educational settings and in e-learning environments. The subsequent section provides a review of literature related to security issues in e-learning environments, biometric solutions and fingerprints biometric solutions. Subsequent section suggests the theoretical framework combining existing technologies into electronic exams (e-exams). The final section addresses the conclusions with expected contribution of the proposed framework, review of some observed limitations of the proposed theoretical framework, and proposed future research.

2. THEORETICAL BACKGROUND

2.1 E-Learning and E-Learning Environments

Teaching via the Internet has become a popular choice for academic institutions as well as business organizations (Hiltz & Turoff, 2005). Advances in information systems have enabled educational institutions to implement electronic learning (e-learning) systems as a teaching environment (Alavi & Leidner, 2001). Furthermore, e-learning has become a powerful medium for academic institutions and corporate training due to the incorporation of cutting edge technologies. Hiltz and Turoff (2005) have commented that e-learning is "the latest of social technologies that ... has improved distance learning" (p. 59).

The spectacular growth in e-learning in the past decade has been documented in numerous studies. The U.S. National Center for Education Statistics (NCES) reported that "56 percent of all 2-year and 4-year degree-granting institutions offered distance education courses…during 2000–2001 academic year" (US NCES, 2005, p. 3). The dramatic growth in distance and e-learning is evident in the number of institutions that offer e-learning. US NCES reported that "undergraduate level online courses were offered at 48 percent of all institutions while graduate level online courses were at 22 percent of all institutions" (p. 3). Among these institutions, e-learning courses and video technology were the most common kinds of instruction delivery systems. NCES reported that 90% of institutions employed e-learning courses using asynchronous communication systems. While, only 43% of institutions employed synchronous communication systems for the delivery of e-learning courses (US NCES, 2005).

Gunasekaran, McNeil, and Shaul (2002) described the growth in e-learning as the "new dynamic learning models…and is leading the [academic] market to a significant paradigm and cultural change" (p. 45). Courses and entire degree programs are delivered via the Web anywhere at anytime. In addition, e-learning courses are offered by private, public as well as corporate universities. As a result, new resources such as e-books, books on CD-ROMs and e-exams have been adapted to e-learning courses. Students' enrollment in e-learning courses has proliferated reaching more than three million students in the U.S. in 2005 (US NCES, 2005). About 82% of those online students were enrolled in undergraduate level courses during the year 2000-2001 (US NCES, 2005). As a result numerous academic institutions are planning to increase the number of e-learning courses to meet the growth in this demand. However, security issues related to e-learning systems have been raised by several scholars (Ramim & Levy, 2006). Moreover, opponents of e-learning argue that the inability to authenticate exams takers is one of the major challenges of e-learning medium. Although there is a major growth in e-learning programs, some institutions proposed to take extreme measures including asking e-learning students to take exams in proctor centers (Gunasekaran et al., 2002). However, this requirement may not be feasible for e-learning programs with students in remote locations or under various circumstances such as students who are in military service in remote or combat areas, students with severe disabilities, and working professionals. In order to protect the integrity of exams in e-learning environments, solutions for such a significant problem are warranted.

2.2 Unethical Conduct in E-Learning

Given the development of technologies and the demonstrated growth of e-learning usage in academia, students' unethical conduct in e-learning has become a major concern (Kennedy Nowak, Raghuraman, Thomas, & Dacis, 2000). Pillsbury (2004) argues that students' unethical conduct has intensified as a result of the use of technology and the Internet. Most administrators and instructors focus on one type of unethical conduct, namely plagiarism (Naude & Hörne, 2006). However, students' unethical conduct encompasses a wide array of behaviors including technology enabled behaviors such as cheating during an exam by using technology devices (i.e. PDA, calculator, and cellular phone), engaging in online collaboration when it's forbidden (i.e. groupware like Instant Messenger services, chats, forums, and newsgroups), and deceiving (i.e. logging with another student's username/password). These unethical technology enabled conducts are often undetected by instructors in e-learning courses. Moreover, numerous researchers admit that most e-learning programs adopt policies and practices from traditional learning programs and ignore the technology related issues (Kennedy et al., 2000;

McCabe, 2003; Gunasekaran et al., 2002). Pillsbury (2004) noted a number of Web enabled detection mechanisms such as turnitin.com™ that are available to curb plagiarism. Though, extensive body of knowledge is available on plagiarism detections (Decoo, 2002; Hamilton, 2003; Hannabuss, 2001; McLafferty & Foust, 2004), very little attention has been given to providing solutions to other students' unethical conduct such as cheating on exams in e-learning courses. Pillsbury (2004) noted that detection mechanisms for unethical conduct are necessary not only in the initial portal access. Moreover, additional mechanisms are necessary to authenticate users' access in various e-learning course activities (Newton, 2003). For example, instructors attempt to verify that e-exam submission is truly performed by a given student rather than another one.

According to the Center for Academic Integrity (2005), cheating on exams has been reported at an alarming range of 74%. McCabe and Trevino (1996) reported that 70% of students in their study confessed to cheating on multiple exams. A study by Pincus and Schmelkin (2003) compared faculty members' perceptions on various students' unethical conducts seriousness. They concluded that students' unethical conduct related to exam taking perceived by faculty to be one of the most serious unethical behaviors (Pincus & Schmelkin, 2003). Similarly, Dick et al. (2002) also noted that 24% their study participants believed that "advances on technology have lead … to increase cheating" (p. 173). The perceived seriousness of cheating on exams has led numerous academic institutions to reduce their e-learning course offering and in other instances, cease e-learning altogether. In fact, Gunasekaran et al. (2002) admitted that the inadequate technology has led some academic institutions to cease offering e-learning courses due to concerns over the quality of students' assessment and standards. Thus, the central aim of this paper is to propose a conceptual level security solution for this out-braking phenomenon by suggesting a theoretical framework of biometrics authentication to secure e-exams.

2.3 Security in E-Learning

Given the importance of e-learning environments for academic institutions, security related challenges of such environments are capturing the attention of program administrators. Ramim and Levy (2006) discussed a case study of an academic institution that faced a tragic cyber attach to their e-learning environment by an insider intruder. Other scholars have documented related security problems in academic institutions. Yu and Tsao (2003) discussed security challenges of e-learning environments. However, their exploration focused on shielding the technology infrastructure against unauthorized users. Current security practices in e-learning systems relay principally on the utilization of passwords authentication mechanisms. Similarly, Huang, Yen, Lin, and Huang (2004) discussed aspects of security in e-learning systems and suggested attention to two layers when securing e-learning systems. The first layer addresses security of the technology infrastructure used to facilitate e-learning (i.e. hardware, networks, etc.) and the second layer addresses the various applications employed in enabling e-learning (i.e. learning management systems, rich media communication tools, etc.). Huang et al. (2004) criticized existing proprietary e-learning systems for not paying enough attention to the issue of properly authenticating students, in particular during quizzes and exams. Hugl (2005) noted numerous security related technologies that are not currently employed in e-learning. One such solution can include biometric technologies that may potentially become an integral part of e-learning systems.

2.4 Biometric Solutions

According to Tabitha, Pirim, Boswell, Reithel, and Barkhi (2006) *biometric* is defined as "the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans" (p. 3). Such unique biological characteristics relies on individual humane identities such as DNA, voice, retinal and iris, fingerprints, facial images, hand prints, or other unique biological characteristics. Tabitha et al. (2006) note that *biometric* is "a method of identification that has been growing in popularity" (p. 2). Moreover, Pons (2006) notes that *biometric devices* are technological devices that utilize an individual's unique physical or behavioral characteristic to identify and authenticate the individual precisely. Essentially, biometric technologies operate by scanning a biological characteristic and matching it with the stored data. Jain, Hong, and Pankanti (2000) note that a biometric system is "essentially a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user" (p. 92).

Coventry, De Angeli, and Johnson (2003) discussed the usability aspect of authentication systems and noted that it is a "tradeoff between usability, memorability and security." (p. 153). Additionally, they note that in order to increase security, traditional PINs and password authentication methods are regularly "increasing their length, ensuring they do not form words and ensuring all are different, makes them more difficult to remember and error-prone" (Coventry et al., 2003, p. 153). Similarly to other scholars such as Jain et al. (2000), Pons (2006) and Tabitha et al. (2006), Coventry et al. (2003) maintained that most biometric systems include a digital identifier, a template and a recognition algorithm and they follow similar matching processes. However, they maintained that biometric systems can be separated into physiological biometric (i.e. finger, iris) as well as behavioral biometric (i.e. voice, key board typing behavior). Biometric systems performance can be assessed by employing statistical methods in which accuracy is calculated. Although biometric systems are relatively reliable, Coventry et al. (2003) asserted that system malfunction stems from users' lack of establishing the biometric during the initial stage as well as potential interruptions during transmission of the biometric image in the validation process. Subsequently, they concluded that although the trade off between security and usability aspects remains, biometric systems can facilitate automatic verification for public environments.

Pons (2006) maintained that fingerprints biometric scans are the most commonly used biometric solution as they are less expansive compared with other biometric solutions. According to Jain et al. (2000), a fingerprint is a unique "pattern of ridges and furrows on the surface of a fingertip, the formation of which is determined during the fetal period" (p. 95). Fingerprints are unique for each individual, where even identical twins have different fingerprints (Jain et al., 2000). Several scholars documented the increase popularity of fingerprint biometric-based systems and their decline in costs (Jain et al., 2006; James et al., 2006; Pons, 2006). For example, fingerprints systems are currently used in the Disney® parks and appear to be useful for its high volume traffic and low price authentication. Full hand fingerprint is also used by the U.S. immigration services. Similarly, fingerprints can be used for authenticating students' submissions of exams via the use of biometric devices. Furthermore, Williams (2002) pointed out that fingerprints have been universally acceptable in the legal system worldwide. Fingerprints are a permanent attribute unique to an individual. Fingerprints can be scanned, transmitted and matched with the aid of a simple device. McGinity (2005) pointed out that biometric have been commonly employed in replacing conventional password systems. She cited examples of ISPs that provide fingerprints based biometric for a small monthly fee (i.e. AOL charges $2 per month). Biometric devices enable portable scanning and rapid identification. Thus, finger biometric can be a suitable solution for rapid authentication of users. Using a portable device, users can scan their fingerprints and send a print image via the Internet to the University's network. The network will consist of an authentication server that will house a database of students' fingerprints images. The server will than process the matching of the transmitted print image with a stored copy of the fingerprint (called "template"). Following that, the server will generate a matching result. Thus, McGinity predicted that fingerprints based biometric would become a household activity in the near future.

Yang and Verbauwhede (2003) proposed a secured technique for matching fingerprints in a biometric system. Similarly to McGinity (2005), they argued that biometric systems enhance security far more than the current systems. Biometric systems are more accurate as well as simpler to operate compared with passwords systems. Yang and Verbauwhede (2003) described a fingerprint based biometric system in which the fingerprint template is kept in a server during initiation. Upon scanning the finger, an input device scans a biometric signal and transmits it to a server where it is processed for matching. In an effort to shield the system against security compromises, they recommended processing the matching of fingerprints images in an embedded device rather than the server and only transmitting the results to the servers. Furthermore, they suggested encrypting the fingerprint template prior to storing it on the server. Fingerprints templates can be decrypted whenever a matching process occurs. Yang and Verbauwhede (2003) provided additional solutions useful for building up multiple layers of security in fingerprint based biometric systems.

2.4.1 Fingerprint Biometric Solutions

In the past decade the price of biometric authentication devices has been falling (Pons, 2006). Currently there are low cost solutions for biometrics authentication via fingerprint recognition. For example, Figure 1 provides an image of a biometrics mouse by JayPeetek Inc. called Scan.U.Match™. This devise is part of a package of fingerprint authentication mechanism. The mouse is about the same

Figure 1. JayPeetek Inc.'s Scan.U.Match™ Fingerprint Biometric Authentication Mouse[1]

Figure 2. JayPeetek Inc.'s Biometric Authentication Server, the Authenteon™ Server[2]

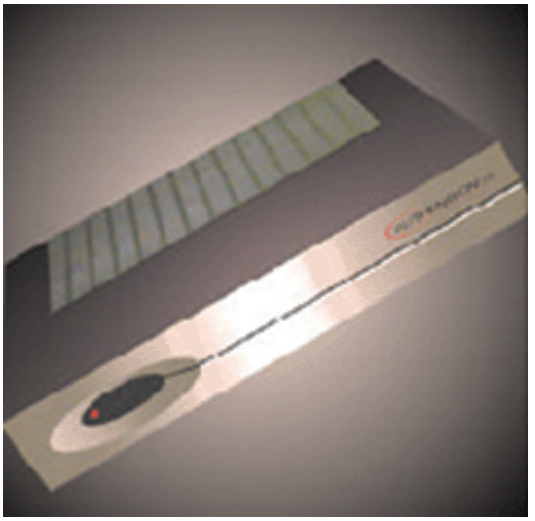


Figure 3. SecuGen®'s Keyboard III™ with fingerprint pad scanners[3]

Figure 4. onClick®'s PCMCIA FingerPrint™ Reader[4]

Figure 5. Sony®'s Puppy® Fingerprint Identity Token by Corp[5]

size as standard mouse, however, it also has an integrated fingerprint scanner that is managed by client side software and controlled by server side software centralized on an authentication server. Figure 2 provides an image of Authenteon™, a biometrics authentication server. JayPeetek Inc. claims that their patented Scan.U.Match™ biometrics mouse solution is unique as it "does not capture the finger image and scrambles the algorithm at the point of scan", rather it "creates a 500 byte secure template that cannot be replicated into a user fingerprint" (JayPeetek Inc.). As such, the Scan.U.Match™ is claimed to be highly reliable with "false rejection rate" that is only 0.01%, or 1 out of 100,000 cases.

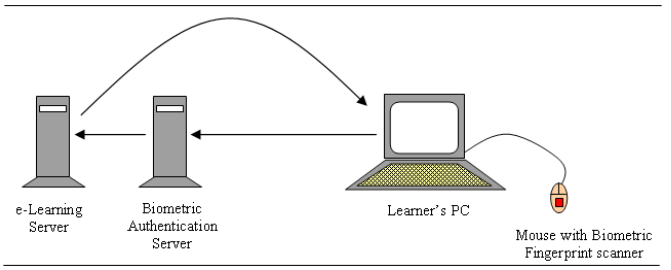
There are numerous other vendors that offer similar solutions in attractive prices. Examples of some of the other vendors include SecuGen® Biometrics Solutions (2005) with their OptiMouse III™, onClick® Corp. (2005) with their VIA™ solution, to name a few.

Aside from the biometrics fingerprint mouse solutions, there are other biometrics fingerprint solutions including keyboard with fingerprint pad scanner (See Figure 3), PCMCIA fingerprint scanner (See Figure 4), and USB fingerprint token scanners (See Figure 5).

3. PROPOSED METHODOLOGY AND DATA COLLECTION

The proposed theoretical framework that this work focuses on is to incorporate biometric fingerprint solutions for user authentication during e-exams. Figure 6 demonstrate the proposed conceptual solution. In standard e-exam, the learner's access is authenticated once by the e-learning server at login for the entire duration of the activity session, while the repeated authentication performed is based on the password cashed in the browser. As such, students are able to login to the e-learning server and have someone else take the e-exam on their behalf. The proposed solution will enhance the current authentication process by adding the fingerprint biometrics solution. For example, in WebCT, during e-exam a random fingerprint authentication can occur to validate the e-exam taker. Although not a foolproof approach, requiring the fingerprint authentication of the learner randomly during

Figure 6. Proposed fingerprint biometric solution for e-exam user's authentication



e-exam with required very short fingerprint scanning response time should provide additional added security. It may discourage learners from having someone else take the e-exam for them. Therefore, the central claim of this proposed approach is that the incorporation of fingerprint biometrics solution in conjunction with e-learning environments will enable a reduction in exam cheating.

5. CONCLUSION AND RECOMMENDATIONS FOR FUTURE RESEARCH

Unethical conduct, in particular cheating in e-exams was documented in literature as a growing concern by many higher educational institutions. The proposed theoretical framework suggested above is unique as it proposed a biometric solution for exam taking in e-learning environments. This theoretical framework may add to the general knowledge of e-learning environments by addressing a major issue of e-exam cheating. Future work in this line of research should incorporate this theoretical approach and conduct a study on the incorporation of biometric solutions in e-exams. One example of a study may include comparison of the same instructor teaching two e-learning sections of the same course, where one section will use regular e-exams and the other section will use the fingerprint biometric approach proposed. The study can propose that:

Proposition 1: Students taking e-exams using the fingerprints biometric solution will have lower grades on the e-exam than their counterparts.

Proposition 2: Students taking e-exams using the fingerprints biometric solution will take longer time to complete their e-exam than their counterparts.

Results of such study can provide initial investigation in an attempt to address the outgrowing phenomena of unethical conduct in e-learning exam taking. If results of this propose study will show that the group of learners who took the exams using the fingerprints biometric solution will have lower grades and take longer time to complete their exam, thus, have a lower cheating rate. Having such results will allow suggesting the proposed framework for higher educational institutions to incorporate it in order to reduce cheating in online exam taking.

Future investigation should be performed by implementing the proposed framework and conducting the experiment proposed above. Additional research can be conducted on the incorporation of biometric solutions to address other academic misconduct behaviors in e-learning environments. However, researchers must be aware of the limitations associated with the theoretical framework proposed here. The first observed limitation deals with the fact that in a remote setting, students may ask to have a subject matter expert seat next to them while they take the exam. The current proposed framework is overlooking this possibility and additional work to address such unethical behavior is warranted. The second observed limitation of the proposed framework is the funding the costs associated with implementing such study in an experimental basis, let alone in a large scale e-learning program. Additional work is needed in exploring the costs and funding sources needed to provide the technological and implementation aspect of this framework. A third observed limitation is related to individual perceptions on the use of biometric systems. For example, Alterman (2003) note several perceived ethical issue with biometric systems, while Tabitha et al. (2006) document a study on the acceptance of such system by individuals. Future research is warranted to further explore issues related to the ethical and acceptance of biometric systems in the context of e-learning.

REFERENCES

Alavi, M., & Leidner, D. (2001). Research commentary: Technology mediated learning-a call for greater depth and breadth of research. *Information Systems Research, 12*(1), 1-10.

Alterman, A. (2003). ''A piece of yourself'': Ethical issues in biometric identification. *Ethics and Information Technology, 5*(3), 139-150.

Center for Academic Integrity (2005). Retrieved September 12, 2006, from http://www.academicintegrity.org/cai_research.asp

Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability of large scale public systems: Usability and biometric verification at the ATM interface. *Proceedings of the Conference on Human Factors in Computing Systems.* Florida, USA, 153-160.

Decoo, W. (2002). *Crisis on campus: confronting academic misconduct*. Cambridge, MA: MIT Press.

Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T., & Laxer, C. (2002). Reports from ITiCSE on innovation and technology in computer science education. *ACM SIGCSE bulletin working group, 35*(2), 172-184.

Gunasekaran, A., McNeil, R. D., & Shaul, D. (2002). E-learning: Research and applications. *Industrial and Commercial Training, 34*(2), 44-54.

Hamilton, D. (2003). Plagiarism: Librarians help provide new solutions to an old problem. *Searcher, 11*(4), 26-29.

Hannabuss, S. (2001). Issues of plagiarism. *Library Management, 22*(6/7), 311-319.

Hiltz, S. R., & Turoff, M. (2005). Education goes digital: The evolution of online learning and the revolution in higher education. *Communication of ACM, 48*(10), 59-64.

Huang, W., Yen, D. C., Lin, Z. X., & Huang, J. H. (2004). How to compete in a global education market effectively: A conceptual framework for designing a next generation eEducation system. *Journal of Global Information Management, 12*(2), 84-107.

Hugl, U. (2005). Tech-developments and possible influences on learning processes and functioning in the future. *Journal of American Academy of Business, 6*(2), 250-256.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 91–98.

JayPeetek Inc. (2005). *Scan.U.Match Biometric Authentication System embedded in a mouse*. Retrieved September 12, 2006, from http://www.jaypeetex.com/products/Biometrics/Fingerprints/Scanumatch.htm

Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Dacis, S. (2000). Academic dishonesty and distance learning: student and faculty views. *College Student Journal, 34*(2), 309-315.

McCabe, D. L. (2003, Sep 10). Caught copying: electronic plagiarism is a new addition to the IT lexicon. *Businessline*, 1-3.

McCabe, D. L., & Trevino, L. K. (1996). What we know about cheating in college. *Change, 28*(1), 28-34.

McLafferty, C. L., & Foust, K. M. (2004). Electronic plagiarism as a college instructor's nightmare-prevention and detection: Cyber dimensions. *Journal of Education for Business, 79*(3), 186-190.

McGinity, M. (2005). Staying connected: Let your fingers do the talking. *Communications of the ACM, 48*(1), 21-23.

Naude, E., & Hörne, T. (2006). Cheating or collaborative work: Does it pay? *Issues in Informing Science and Information Technology, 3*, 459-466.

Newton, R. (2003). Staff attitudes to the development and delivery of e-learning. *New Library World, 104*(10), 412-426.

onClick® Corp. (2005). Retrieved September 12, 2006, from http://www.onclickbiometrics.com/

Pillsbury, C. (2004). Reflections on academic misconduct: An investigating officer's experiences and ethics supplements. *Journal of American Academy of Business, 5*(1/2), 446-454.

Pincus, H. S., & Schmelkin, L. P. (2003). Faculty perceptions of academic dishonesty: A multidimensional scaling analysis. *Journal of Higher Education, 74*, 196-209.

Pons, A. P. (2006). Biometric marketing :targeting the online consumer. *Communications of the ACM, 49*(8), 60-65.

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

SecuGen® Biometric Solutions (2005). Retrieved September 12, 2006, from http://www.secugen.com/

Tabitha J., Pirim, T., Boswell, K., Reithel, B, & Barkhi, R. (2006). Determining the intention to use biometric devices: an application and extension of the technology acceptance model. *Journal of Organizational and End User Computing, 18*(3), 1-25.

United States Department of Education, National Center of Educational Statistics (NCES) (2005). *Mini-digest of educational statistics*. Retrieved September 20, 2006, from http://nces.ed.gov/pubs2005/2005017.pdf

Williams, J. M. (2002). New security paradigms. *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, 97-107.

Yang, S., & Verbauwhede, I. M. (2003). A secure fingerprint matching technique. *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, California, USA 89-94.

Yu, C., & Tsao, C. C. (2003). Web teaching: Design, security, and legal issues. *Delta Pi Epsilon Journal, 45*(3), 191-203.

ENDNOTE

1 Source: http://www.jaypeetex.com/products/Biometrics/Fingerprints/Scanumatch.htm

2 Source: http://www.jaypeetex.com/products/Biometrics/Fingerprints/Authenteon.htm

3 Source: http://www.secugen.com/products/pk.htm

4 Source: http://www.onclickbiometrics.com/ebusiness/ocbioweb.nsf/wcontent/productsviacard?opendocument

5 Source: http://bssc.sel.sony.com/Professional/puppy/products.html