USING BIOMETRICS AUTHENTICATION VIA FINGERPRINT RECOGNITION IN E-EXAMS IN E-LEARNING ENVIRONMENT

MSC WEB TECHNOLOGY/SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE/UNIVERSITY OF SOUTHAMPTON

SOUTHAMPTON/UNITED KINGDOM

Sara Jeza Alotaibi

sja2g09@ecs.soton.ac.uk

Alotaibi, S. (2010) Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. In: The 4th Saudi International Conference, Friday 30 and Saturday 31 July 2010, The University of Manchester, UK

Abstract

E-learning is a great opportunity for modern life. Notably, however, the tool needs to be coupled with efficient and reliable security mechanisms to ensure the medium can be established as a dependable one. Authentication of e-exam takers is of prime importance so that exams are given by fair means. A new approach shall be proposed so as to ensure that no unauthorised individuals are permitted to give the exams.

Keywords: e-Learning, biometrics authentication, fingerprint, e-exams

1. Overview

With the advent of computer technology, our lives have changed and provided them with a new dimension. The World Wide Web is also one of the inventions of computer technology which has changed the mode of communication and information for humans. A new concept which has emerged from the World Wide Web is education on the web: e-learning [2],[44]. As appealing as it sounds, it poses various threats, especially when exams are held online. There was a study held by King *et al*. in 2009 [1], which concludes that 73.6% of the students that were selected for the sample had the point of view that it is easier to cheat in an online environment rather than in a conventional one.

One of the main challenges facing the security of e-exams and the e-learning environment is to authenticate students so that no unauthorised individuals are permitted to upload submissions or access information, respectively [3]. Some other problems faced during e-exams are double submissions from the same students [4], and e-exams not being held in supervised locations, which therefore enables the individual to access unauthorised areas, etc. [6],[5].

2. Risk Analysis of Biometric System in E-exams in E-learning

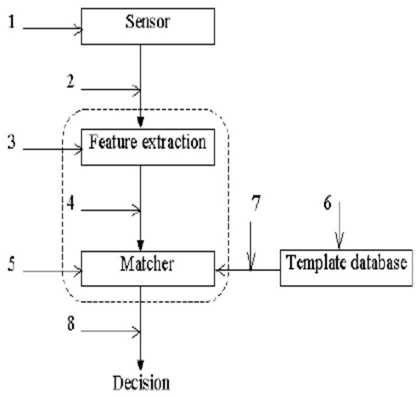

Figure 1: Eight different attack points in a biometric authentication system [7]

There are several problems and risks associated with the usage of biometrics in the authentication process. Some of them are:

2.1 Fake Input

One of the most common attacks on a fingerprint authentication system is of a fake input [9],[36], simply because this is the easiest mode of trying to gain access. It is a common practice for intruders to try to gain authentication by means of artificial fingers. Moreover, there has been much research on the subject of biometric systems accepting artificial biometric inputs (dummy fingers), with these systems being made more reliable [34],[35].

2.2 Low Quality Input

Fingerprint-matching techniques can be placed into two categories: minutiae-based. and correlation based. Minutiae-based techniques first find minutiae points, and accordingly map their relative placement on the finger. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality [15].

2.3 Modification to the Biometric Database

The first step in any biometric recognition system is to store the template of an individual's feature so that it can be later used for authentication purposes [43], [41]. The place where these templates are stored is known as a database in most systems, and the process whereby the student will register their fingerprints for the first time is called 'enrolment' [16],[17],[18],[19],[20].

2.4 Modifications to the Feature Extractor

The feature extractor may be attacked by intruders and modified, such that the legitimate fingerprint may be rejected and the unauthorized ones to be accepted [21].

3. Solutions

A new approach for authenticating individuals on the basis of their biometrics has gained name over the years [33], [39]. William *et al*. [8], for instance, explains that biometrics are unique physical features of an individual, such as fingerprints, iris, face, palm prints, etc. Fingerprint recognition systems are very common and popular due to their accuracy, ease, and proven track record [9],[38],[42]. However, like any other biometric system, fingerprints also pose various threats and risks to the process of authentication [10],[11].

3.1 Solution for low Quality Input

Puiri *et al*. [22] propose a method in which a pre-processing function is performed on the data to reduce the blur on the image. Subsequently, a pre-filtering operation is also performed so that the background can be reduced to a minimum. Along with these operations, segmentation of the fingerprint is also conducted by identifying the region of interest (ROI) [12],[13],[14].

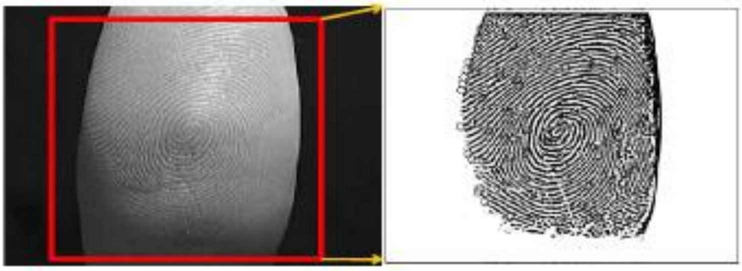

Figure 2: Fingerprint scan after pre-processing operation [22]

In this approach, the authors propose that a webcam or a low-cost biometric sensor can also be used for the input, but the finger needs to be positioned only a few centimetres away from the objective lens, with the focal length of the lens needing to be tuned accordingly [22]. Prabhakar *et al*. [15] also propose a solution aimed at improving the quality of the image.

3.2 Solution to Overcome Fake Input

Derakshani *et al*. [24] propose a method for handling the fake input for fingerprint recognition system—'live-ness detection'. This term is also used by [23],[25],[26],[27],[37]. Perspiration from the fingers is considered to be a sign of life which is obviously not present in the case of fake (dummy) fingers.

3.3 Solution to Overcome Modifications in the Database

A method was proposed by Ratha *et al*. [23] and Connell *et al*. [28] to protect templates from fraudulent usage, which it involves using a distorted version of the biometric signal or the feature vector: if a specific representation of template is compromised, the distortion transform can be replaced with another one from a transform database. Data hiding and watermarking techniques have also been proposed as means of increasing the security of fingerprint images, by detecting modifications [29], and by hiding one biometric into another [30].

4. Proposed New Security System

After a comprehensive study of the solutions that have been proposed so far, a new approach has been devised—fingerprint biometrics solution for e-exam takers' authentication with the use of intelligent security agent. The intelligent agent will use the following devices:

a) Mouse Applications

There are several fingerprint-scanning mouse available, which will take the exam taker's fingerprints during the examination. For example, Digent offers a wide range of mouse including IZZIX FM 1000, IZZIX FD1000 [31].

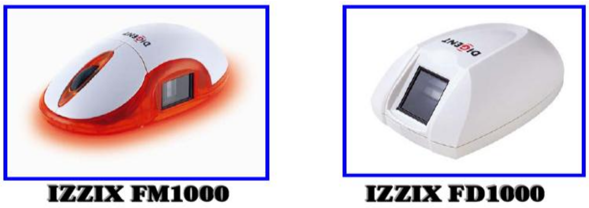

Figure 3: Fingerprint scan enabled mouse [31]

b) Keyboards

There are some keyboards also available in the market which can scan the fingerprint of the user whilst he is working, without any extra effort of getting his fingerprint scanned [32].

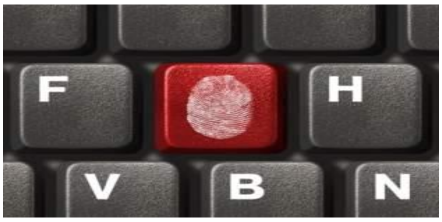

Figure 4: Fingerprint scan enabled keyboard [32]

4.1 Proposed Method

The first process in any biometric recognition system is ‘enrolment’, whereby all students who are supposed to appear for the e-exam will have to ‘enrol’ their fingerprints so that they are stored in the relevant e-learning server database and biometric server database. All the fingerprint scans will be saved in an encrypted form to avoid any modifications.

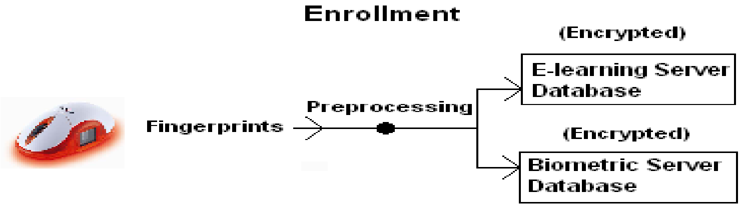

Figure 5: Enrolment

When the client initiates the e-exam, the intelligent agent assigns the student ID with an IP address so that the student cannot log-in from any other PC [4]. The intelligent agent will then start extracting the fingerprint scans from the hardware devices mentioned above at every second, and the following steps will then be performed:

- **Pre-processing operations** shall be performed on these scans so as to ensure that there is minimal blur and noise present in the images.
- **Test A**: Additional live-ness detection tests will be performed by the intelligent agent to ensure that no dummy fingers are being used to pose as another student’s identity.
- **Test B**: After these initial operations, these scans will then be matched with the ‘enrolled’ scans which have been saved in the two server databases.

- If either Test A or B do not pass at any point of time, the exam will then be immediately stopped for that specific student, and notification will be sent to the authorities for further action. This process will continue for the duration of the exam.

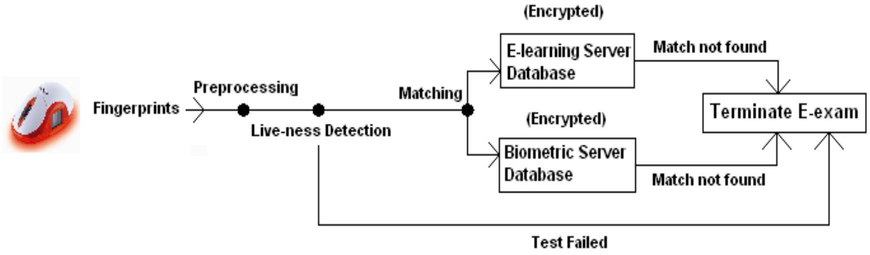

Figure 6: Proposed Method

4.2 Advantages of the Proposed Solution

1. Since the fingerprints will be extracted whilst the user in working on the keyboard or the mouse, the pace of his work will not be affected.
2. The interval at which the fingerprints will be scanned is one second, which ensures that no other individual can take the exam on another student's behalf.
3. The scanned fingerprints will be saved in the two databases in an encrypted form to mitigate attacks from intruders.

4.3 Disadvantages

1. The interval at which the fingerprints are being scanned can prove to be very small and can cause storage problems for such a huge amount of data.
2. This approach requires an initial investment of providing students with the fingerprint scanning enabled devices.

4.4 Steps to Handle Barriers

As soon as the e-exam is complete, the fingerprint scans should be completely analysed for the last time and then deleted so that the space can be available for the next exam. Another method of handling this can be to increase the time interval to at least three seconds so that the amount of data decreases to a reasonable degree.

5. Conclusion

A solution has been proposed to ensure a secure e-learning environment in which e-exams can be held in an ethical manner. It is very important to properly authenticate the e-exam takers so that no unauthorised individuals are permitted access to the e-learning environment.

References

[1] C.G. King, R.W. Guyette, C. Piotrowski, ‘Online exams and cheating: An empirical analysis of business students’ views’, The Journal of Educators Online, 6(1), 2009, http://www.thejeo.com/Archives/Volume6Number1/Kingetalpaper.pdf.

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

[3] W. Huang, D. C. Yen, Z. X. Lin, J. H. Huang, ‘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, 2004

[4] K. M. Apampa, G. B. Wills, D. Argles, E. Marais, ‘Electronic Integrity Issues in E-assessment Security’, 2007

[5] E. Marais, D. Argles, ‘Security issues specific to E-assessments’, 8th Annual Conference on WWW Applications. Conference proceedings, Bloemfontein, South Africa, 2006

[6] IS Blackboard team, (2003), ‘Online Assessment’, Aberystwyth Learning & Teaching Online, http://alto.aber.as.uk/caa/issues.asp

[7] D. Argles, A. Pease, R. J. Walters, ‘An Improved Approach to Secure Authentication and Signing’, IEEE, 2007

[8] J. M. Williams, ‘New security paradigms’, *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, 97-107, 2002

[9] U. Uludag, A. K. Jain, ‘Attacks on Biometric Systems: A Case Study in Fingerprints’, *Proceedings of SPIE-EI*, 2004

[10] N.K. Ratha, J.H. Connell, R.M. Bolle, ‘An analysis of minutiae matching strength’, *Proc. AVBPA 2001*, *Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228, 2001.

[11] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, ISBN 0-387-95431-7, 2003.

[12] T. Putte and J. Keuning, ‘Biometrical fingerprint recognition: don’t get your fingers burned’, *Proc. IFIP TC8/WG8.8*, Fourth Working Conf. Smart Card Research and Adv. App., pp. 289-303, 2000.

[13] S. Jung, T. R, Scheiter, K. F. Gorser, ‘A Low-Power and High-Performance CMOS Fingerprint Sensing and Encoding Architecture’, *IEEE Journal of Solid-State Circuit*, Vol. 34, No. 7 (1999).

[14] S. Shigematsu, H. Morimura, Y. Tanabe, T. Adachi, K. Machida, ‘A Single-Chip Fingerprint Sensor and Identifier’, *IEEE Journal of Solid-State Circuit*, Vol. 34, No. 12, 1999

[15] S. Prabhakar, A. Jain, Fingerprint Identification, http://biometrics.cse.msu.edu/fingerprint.html

[16] National science and technology council (NSTC). Fingerprint recognition

[17] I. Maghiros, Y. Punie, S. Delaitre, ‘An Introduction to Biometrics - Fingerprint Recognition’, 2005, http://cybersecurity.jrc.ec.europa.eu/pages/ProjectlibestudyBiometrics.htm

[18] N. Yoshiura, Y. Onozato, H. Kimura, ‘Application of one way function to biometric authentication’, *Transactions of the Institute of Electical Engineers of Japan*, vol. 124-C, 2004.

[19] A. K. Jain, ‘Biometric Recognition: How Do I Know Who You Are?’, Department of Computer Science and Engineering, Michigan State University, 2004.

[20] Y. Sutcu, H. T. Sencar, N. Memon, ‘Authentication protocols: A secure biometric authentication scheme based on robust hashing,’ 7th Workshop on Multimedia and Security at ACM Multimedia, New York, USA, 2005.

[21] S. Walton, (2005), ‘KS3 ICT Onscreen Test Project’, Qualifications & Curriculum Authority, *BETT 2005*, http://www.qca.org.uk/downloads/6967_ks3_ict_bett_2005.pdf.

[22] V. Piuri, F. Scotti, ‘Fingerprint Biometrics via Low-cost Sensors and Webcams’, IEEE, 2008.

[23] N.K. Ratha, J.H. Connell, and R.M. Bolle, ‘Enhancing security and privacy in biometrics-based authentication systems’, *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001.

[24] R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, ‘Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners’, *Pattern Recognition*, vol. 36, pp. 383-396, 2003.

[25] S. Hoshino, H. Matsumoto, T. Matsumoto, ‘Mapping a Fingerprint linage to an Artificial Finger’, *Technical Report of IEICE*, ISEC2001-60, pp. 53-59, 2001.

[26] J. Mainguet, P. Pegulu, J. B. Harris, ‘Fingerprint recognition based on silicon chips’, *Future Generation Computer Systems*, Vol. 16, No.4 pp.403-15, 1999

[27] L. O'Gorman, ‘Fingerprint Verification, in Biometrics: Personal Identification in Networked Society’, The Kluwer Academic Publishers, *International Series in Engineering and Computer Science*, Vol. 479, Chapter 2, pp. 43-64, 1999

[28] J. Connell, N. Ratha, ‘Cancelable Biometrics’, Biometric Consortium 2000 Conference, Sept. 13-14, 2000.

[29]. S. Pankanti, M. M. Yeung, ‘Verification watermarks on fingerprint recognition and retrieval’, *Proc. of SPIE EI*, vol. 3657, pp. 66-78, 1999.

[30] A. K. Jain, U. Uludag, ‘Hiding biometric data’, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, 2003.

[31] Bayometric.Inc, 2009,http://www.bayometric.com /products/griaule-fingerprint-sdk.htm

[32] Wayne Parslow, ‘Identity and access management in the NHS — improving efficiency and security around’, BJHC & JM, 2008,http://www.bjhcim.co.uk/features/2008/ 809001.htm

[33] N. Green, G. W. Romney, ‘Establishing Public Confidence in the Security of Fingerprint Biometrics’, ITHET 6th Annual International Conference, IEEE, 2005

[34] R. Raitman, L. Ngo, N. Augar, W. Zhou, ‘Security in the Online E-learning Environment’, *Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT’05),*2005

[35] T. M. Gualberto, S. D. Zorzo, ‘Incorporating Flexible, Configurable and Scalable Security to the Education Collaborative Environments’, 39th ASEE/IEEE Frontiers in Education Conference, San Antonio, TX, 2009

[36] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, ‘Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems’, Optical Security and Counterfeit Deterrence Techniques IV, *Proceedings of SPIE Vol. #4677*, 2002 http://www.spie.org/Conferences/Programs/02/pw/confs/4677.html

[37] D. Pishva, ‘Spectroscopic Approach for Liveness Detection in Biometrics Authentication’,IEEE, 2007

[38] G. Aggarwaltt, N. K. Rathat, T. Y. Jeat, R. M. Bollet, ‘Gradient based Textural Characterization of Fingerprints’, IEEE, 2008

[39] R. W. Frischholz and U. Dieckmann, ‘Bioid: A Multimodal Biometric Identification System’, *IEEE Computer*, vol. 33, no. 2, pp. 64-68, 2000.

[40] A. K. Jain, A. Ross, S. Prabhakar, ‘An Introduction to Biometric Recognition’, *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, Vol. 14, No. 1, 2004.

[41] R. K.Rowe, K. A. Nixon, S. P. Corcoran, ‘Multi spectral Fingerprint Biometrics’, *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy*, West Point, NY, 2005

[42] I. Ali, U. Ali, M. I. Shahzad, A. W. Malik, ‘Face and Fingerprint biometrics Integration Model for Person Identification Using Gabor Filter’, IEEE, 2006

[43] S. Shafaei, T. Inanc, L. G. Hassebrook, ‘A New Approach to Unwrap a 3-D Fingerprint to a 2-D Rolled Equivalent Fingerprint’, IEEE, 2009

[44] Y. Takahashi, T. Abiko, E. Negishi, ‘An Ontology-based System for Network Security’, IEEE, 2006

[45] S. Mitra, M. Savvides, A. Brockwell, ‘Statistical Performance Evaluation of Biometric Authentication Systems Using Random Effects Models’, IEEE, 2007

Bibliography

[46] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, ‘Personal Verification using Palmprint and Hand Geometry Biometric’, *4th International Conference on Audio- and Video-based Biometric Person Authentication*, Guildford, UK, June 9-11, 2003.