Automatic Signature Verification (ASV) in E-Commerce

Sharifah Mumtazah Syed Ahmad
Faculty of IT, Universiti Tun Abdul Razak (UNITAR), Kelana Jaya, 47301, Selangor
E-mail: sms2@unitar.edu.my

ABSTRACT

In the offline world, payments are often made over the counter with some levels of human inspections. However, such inspection does not exist in the online world. Online transactions are carried out virtually on a remote application server. Though other technical security measures have been introduced for online transactions such as the use of encryption, digital signatures and digital certificates, the issue of trust is still largely a major problem in e-commerce since actual authentication of users is not often established. A solution to this is to use biometrics Automatic Signature Verification (ASV) systems where human identification is carried out automatically based on their signatures. The main advantage of ASV over other biometrics technologies is that its applications are widely accepted and generally acknowledged by the public due to the fact that signatures have long been used as proof of identity in legal documents and financial transactions. Additionally, the ASV system allows the extraction of dynamic information that describes the way a signature is actually executed in terms of velocity, acceleration, pen pressure, pen inclination, etc. Many signature experts believe the dynamic information of the signing operation is generally consistent and stable throughout one's lifetime. This in turn is more secure simply because it is harder to imitate human signing operation than to reproduce signature images of another person. Since ASV allows for remote networked authentication, it appears promising to most e-commerce applications. This paper generally describes the ASV potentials, its current applications and impediments in e-commerce related activities. It also addresses areas for ASV improvements.

Keywords: *Automatic Signature Verification, biometrics, FAR, FRR, EER, feature sets, feature weights, feature thresholds.*

1.0 INTRODUCTION

Electronic commerce (e-commerce) can be defined as business transactions and processes which are carried out via the Internet [1, 2]. This includes the act of buying and selling of goods and services on the Internet, electronic fund transfers, as well as all online inter-company and intra-company functions (such as electronic document transfers for marketing, finance, and negotiation purposes) that enable this type of virtual commerce.

Though e-commerce appears promising and attractive to many business organizations, security and privacy are two issues that remain the prime concerns of the general public and organizations [1]. For example, customers engaging in e-commerce transactions need to feel confident that their credit card and personal details are secured and protected from prying eyes. Employees engaging in highly confidential e-commerce document transfers need to be positively assured that their electronic documents are not intercepted, read and altered by any unauthorized individuals.

In order to ensure that these security requirements are in placed, several technical measures have been introduced such as the use of passwords, encryption, digital signatures and digital certificates. However, such are only mere representations of users which may be lost, borrowed, stolen and consequently misused by others. For example, a study by Anne Adams [16] shows that most users tend to choose memorable passwords that are related to them (e.g. names, birthdays, favorite football clubs, etc), which are easy to guess, to break or to be cracked by a hacker. Should users been given system generated passwords or choose codes that are difficult to memorize, there is a high tendency that they write the passwords down, which in turn makes these more likely to de disclosed to others.

In addition, the notorious spy-wares that are usually downloaded automatically over the internet without users' knowledge and authorizations impose risks of users' keyed in passwords being transmitted illegally to unauthorized parties. On the other hand, in cryptography, one can only assumes that only genuine user posses the encryption keys, where as in reality encryption keys are just similar to any other tokens which can be borrowed and shared. Thus, the issue of trust arises, where one could not establish the true identity of a user based solely on these mere representations.

A solution to such trust issue is to use biometrics verification systems where user identification is carried out automatically based on his / her physical and behavioral traits. In other words, biometrics rely on 'something that you are', in order to make personal authentication. Biometrics traits are generally unique to individuals and cannot be borrowed, lost, or stolen, thus in principle providing for positive and reliable user authentication. Biometrics technologies include fingerprint, retina, iris, facial, hand geometry, voice, signatures and handwriting recognition.

2.0 BIOMETRICS REQUIREMENTS FOR E-COMMERCE APPLICATIONS

Not all of the available biometrics technologies suit e-commerce applications. There is a thorough report [4] issued by UK Biometric Working Group that advises on biometric product selection. Jain, Hong, and Pankanti [3] have also highlighted several critical factors that must be taken into considerations before deciding on which biometrics systems to be deployed. These reports can be used as general guidelines in order to select the most suitable biometric technology for e-commerce applications.

One of main requirements is biometric identification itself must be able to be carried out on a remote networked basis. In order to achieve this, it is critical that biometrics sensors / devices are feasible enough to be located at individual users' premises. This in turn, requires for cheap biometrics sensors / devices that can be easily installed into any standard PC, which can also be easily operated by any user without much complication. Thus, biometrics technologies such as retina and iris scanning that requires for expensive and bulky sensors, and careful handling of devices are not suitable for e-commerce authentications.

In addition, the identification process must be fast since e-commerce identification requires for real-time response. Hence, biometrics templates with small storage sizes are highly desirable in order to assist in achieving a fast authentication response time. This factor limits the use of facial recognition in e-commerce since it requires for a relatively high volume of processing which impose constraint on the processing speed and storage requirement.

It is also crucial that the use of the selected biometric technology being widely accepted and acknowledged by the international public. This is because a biometric authentication system which is highly rejected by users at several major[1] countries cannot be deployed in e-commerce applications which largely involve users from all over the world. This explains the widespread unpopularity of fingerprint identification, since it has strong associations with criminal means of identification, where such a biometric is strongly rejected in the many western countries [5, 6].

Accuracy also remains an important aspect in analyzing biometrics technologies. This includes the level of circumvention, which refers to how easy it is to fool the system by fraudulent techniques [7]. The accuracy of biometrics systems is often cited by its False Acceptance Rate (FAR) and False Rejection Rate (FRR), or by its Equal Error Rate (EER) (i.e. the equal point of FRR and FAR). Ideally, a biometrics system should produce a zero EER, that is, it should be able to accept all genuine users and reject all attempted forgeries. However, the performance of current biometrics technologies is still far from the ideal, despite impressive claims by some manufacturers. Biometrics systems that are based on human traits with a high degree of uniqueness and stability are usually highly accurate [8].

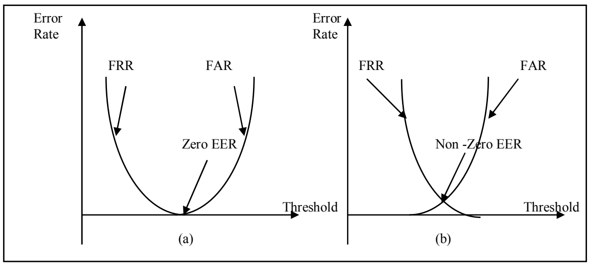

Figure 1(a): The Ideal Performance of Biometrics Systems

Figure 1(b): The Typical Performance of Biometrics Systems

3.0 ASV APPLICATIONS, POTENTIALS AND IMPEDIMENTS IN E-COMMERCE

Signatures have long been used as means of personal identification on official documents. Though signatures do evolve over time, for the case of the vast majority of users, once the signature style has been established the modification are usually slight, making the signature unique for each individual. Current credit card companies, banks and most financial institutions have used signatures as proofs of identity in financial transactions. Thus there is no argument about the role of signatures as a method for identity authentication, which is widely acknowledged by the public [9, 10, 11, 12, 13, 14, 19].

Online Automatic Signature Verification (ASV) is an automation of the traditional signature authentication which allows dynamic information to be derived from an input sample in addition to the static visual image that is more usually associated with visual human inspection. Dynamic information here describes the way a signature is actually executed in terms of velocity, acceleration, pen pressure etc. Currently, the use of an ASV system to verify the identity of a user is highly accepted by the public since they are used to writing down signatures as means of legal identification [14, 15].

For example, in Malaysia itself, ASV systems have been used over the counter to verify credit cards purchases. In November 2002, Nationwide, UK's biggest building society, has ruled out ASV systems for all of its customers' transactions and

[1] Major countries here are the countries where e-commerce activities mostly take place.

documentations[2]. SoftPro, one of ASV main system providers has supplied ASV systems to over 250 financial institutions worldwide[3]. Its latest developments allow e-commerce online user authentication. Mercedes-Benz AMG, a subsidiary of DaimlerChrysler Group is reported to use ASV systems in order to secure its electronic document transfers[4] in e-business. IBM research laboratory in Israel is currently reported to have started work on ASV system for commercial e-commerce purposes[5]. In 2003, CyberSign, a European ASV provider was announced[6] to provide ASV application plug-ins that seamlessly integrate with Adobe Acrobat 5.0 in order to enable users to quickly and easily make important electronic documents virtually tamper-proof.

Figure 2: CyberSign ASV system

ASV meets most of the requirements for e-commerce applications. Static information of signatures can be extracted by scanning 2-dimensional signed papers, while the dynamic information of signatures requires the use of digitizing graphics tablets that are able to capture the series of pen movements online. Digitizing graphics tablets are inexpensive and could cost less than US$100[7]. Both types of signature verification systems are fairly fast and simple to use. In addition, the ASV storage requirement is relatively low.

The major issue of ASV system is in terms of its accuracy. Human signatures can be effectively forged giving rise to False Acceptance Rate (FAR), especially if it is based solely on the static visual information extracted from a signature. However, signature execution is considered as a 'ballistic motion', which literally means rapid practiced motions that are not driven by feedback, and instead are predetermined by the brain [9]. Given the ballistic nature of signature writing, a good forgery that has both the shape and motion of the genuine signature is unlikely to be produced without considerable amount of practice, hence making ASV systems that are based on dynamic signing information more resilient to fraud and impersonation [3, 9, 19].
Second limitations of ASV is that signatures of an individual often suffer from a high level of intra-user variability which can directly influence the system False Rejection Rate (FRR).This means that, though a person generates similar signatures, he / she can never produce two identical sets of signatures [18, 19]. Each signature feature varies within each natural variation range. This specific range may not be easily recognizable to the signer. However, if the range is large enough it could result in a user being falsely rejected in an ASV system. There is a through report that describes means to overcome such a problem, where the optimization methods are generic enough to be implemented in any target user populations [19]. Amongst the methods investigated are optimization tools at the feature level, such as feature selection and feature weighting, optimization tools at the decision level, such as the use of multiple classifiers, and optimization tools on the human signing characteristics which requires extensive study on a subset of users with a high level of False Acceptance Rate (FAR).

Automatic Signature Verification (ASV) has always been and still remains an important and challenging area of research interest, particularly with the aims to improve its error rates performance. Many have attempted to personalize the ASV process to individual user signature characteristics such as by using personalized feature sets [13, 20, 21, 22], personalized feature weights [23], and personalized feature thresholds [24] which have been proven to be more accurate in identifying genuine individuals and discriminating forged signatures. The logic explanation behind this is that though signatures of a given person varies slightly from one sample to another, there is a common subset of his / her signature characteristics which are highly distinguish and consistent that assists in accurate verification, where such a subset differs from one person to another.

In addition, signature verification algorithms with higher levels of accuracy are constantly being developed and introduced as time progress. Such ongoing research findings can be implemented in ASV, making it more accurate for e-commerce applications. There are also suggestions to use encryption on biometrics templates, in order to enhance the security of biometrics data [16, 24, 25]. Biometrics standard such as Common Biometric Exchange File Format (CBEFF) includes an additional encryption facility in its specifications [26]. Thus, if ASV can be incorporated together with other existing e-commerce security measure such as encryption and digital certificates, the outcome would be more reliable and more secured e-commerce

[2] News on the 8th November, 2002 at http://news.bbc.co.uk entitled "Hi-Tech Signatures to Fight Fraud".
[3] News at http://www.group-data.com/ entitled "Solution Integration – Signature Verification".
[4] News on the 6th September, 2003 at http://www.prweb.com/releases/2003/9/prweb78900.htm entitled "Capturing of Biometric Characteristics Secures Electronic Documents – SignDoc Makes MercedesBenz AMG even faster"
[5] IBM Image Processing Laboratory, Israel research site http://www.haifa.il.ibm.com/projects/image/sv/index.html
[6] News by CyberSign Press at http://www.cybersign.com/news_press8.htm
[7] As quoted by PriceGrabber.com at http://geek.pricegrabber.com/search_attrib.php/page_id=53

applications that provide true identifications and verification of individuals.

Another major impediment to ASV implementation in e-commerce is lack of standards. Standards assure worldwide interoperability between different competitive software and devices in the market. Open standards are also vital in order to increase users' confidence by preventing the sole source lock-in and by indicating the maturity of ASV technology. Though, there are ongoing efforts amongst organizations, vendors, manufacturers and research consortiums towards developing and exercising common biometrics standards [7, 27, 28], it would be beneficial to have a dedicated international standard for a specialized ASV implementation in e-commerce B2B and B2C applications. In addition, incentives can be introduced either on an implicit or on an explicit basis in order to promote deployment of ASV in e-commerce.

4.0 CONCLUSION

Automatic Signature Verification (ASV) systems provide for positive user verifications which are based on signature characteristics that belong to individual users and not just mere users' representations. The main attractiveness of ASV over other biometrics technologies is that it is widely acknowledged and accepted by the general public. In addition, ASV appears promising to e-commerce applications since it allows for remote networked authentication, due to its relatively simple and fast identification process which requires for inexpensive devices that can be easily installed into any standard PC. Currently, ongoing active research is carried out in order to improve the accuracy level of ASV. In addition, the possibility of the integration between ASV and encryption may lead to a more secured and more reliable e-commerce applications. An effective incentive towards promoting the use of ASV in e-commerce is by developing dedicated international standards which support such applications.

REFERENCE

[1] 'Electronic Commerce', Third Annual Edition, Gary P. Schneider, Thomson Course Technology 2002

[2] The Internet Dictionary http://www.nref.com/dictionary.html

[3] Anil Jain, Lin Hong, Sharath Pankanti, "Biometric Identification", Communications of the ACM (42, 2), February 2000, page 91 – 98.

[4] Communications-Electronics Security Group (CESG), "Biometrics for Identification and Authentication Advice on Product Selection", Version 2.0, March 2002. http://www.cesg.gov.uk/technology/biometrics/media/Biometrics%20Advice.pdf

[5] John D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?", Proceedings of the IEEE (85, 9), September 1997, page: 1479 – 1491.

[6] Ann Cavoukian, "Privacy and Biometrics", Information and Privacy Commissioner, Ontario, Canada. http://www.pco.org.hk/english/infocentre/files/cakoukian-paper.doc

[7] Farzin Deravi, JSIC Technology Application Programme (JTAP), "Audio-Visual Person Recognition for Security and Access Control". http://www.jtap.ac.uk/reports/htm/jtap-0.38.htm

[8] Ben Miller, 'Vital Signs of Identity', IEEE Spectrum (31,2), February 1994, page 22-30.

[9] Chris Allgrove, University of Kent at Canterbury, PhD Thesis, "A Study of Automatic Signature Verification Techniques in The Context of a Practical Document Processing Application", 1999.

[10]Anil K. Jain, Friederike D. Griess, Scott Connell, "On Line Signature Verification", Pattern Recognition (12,35), December 2002, Page: 2671-3017.

[11]Paul St. John Brittan, University of Kent at Canterbury, PhD Thesis, " High performance Parallel Image Analysis Architectures Applied to Handwritten Signature Verification", 1992.

[12]Gopal K Gupta, Alan McCabe, Department of Computer Science, James Cook University, "A Review of Dynamic Handwritten Signature Verification", Technical Report, September 1997. http://citeseer.nj.nec.com/cs

[13]Sue Gnee Ng, University of Kent at Canterbury, PhD Thesis, "Optimisation Tools for Enhancing Automatic Signature Verification",2000.

[14] F. LeClerc, R. Plamondon, "Automatic Signature Verification: The State of The Art", IEEE International Journal of Pattern Recognition, (8, 3) 1994, page 643 – 660.

[15]University of Kent at Canterbury, BT Technology Group Ltd, "KAPPA Summary Report", May 1994.

[16]Anne Adams, Martina Angela Sasse, "Users Are Not The Enemy", Communications of the ACM (42,12), December 1999, page 41 – 46.

[17]Vaclav Matyas Jr., Zdenek Riha, E-Commerce Monitor (Ecom-Monitor) "Biometric Authentication System", 2000. http://citeseer.nj.nec.com/cs

[18]Jim.R.Parker, "Simple Distances between Handwritten Signatures", The 15th International Conference on Vision Interface, 2002. http://www.cipprs.org/vi2002/pdf/s4-6.pdf

[19]Sharifah Mumtazah Syed Ahmad, University of Kent at Canterbury, PhD Thesis, "Automatic Signature Verification Optimization Tools", 2004.

[20]Luan L. Lee, Toby Berger, Erez Aviczer, "Reliable On Line Human Signature Verification Systems", IEEE Transactions on Pattern Analysis and Machine Intelligence (18,6), June 1996.

[21]H D Crane and J.S Ostrem, "Automatic Signature Verification Using a Three Axis Force Sensitive Pen", IEEE Transactions on Systems, Man and Cybernetics (13, 3), 1983, page 329 – 337.

[22]F. Bauer, B. Wirtz, "Parameter Reduction and Personalised Parameter Selection for Automatic Signature Verification", Proceedings on the International Conference on Document Analysis and Recognition (ICDAR) Volume 1, August, 1995.

[23]Seong Hoon Kim, Myoung Soo Park, Jaihie Kim, "Applying Personalised Weights to a Feature Set for Online Signature Verification", 3rd International Conference on Document Analysis and Recognition, August, 1995.

[24]Anil K. Jain, Friederike D. Griess, Scott Connell, "On Line Signature Verification", Pattern Recognition (12,35), December 2002, Page: 2671-3017.

[24]John D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?", Proceedings of the IEEE (85, 9), September 1997, page: 1479 – 1491.

[25]Gael Hachez, Francois Koeune, Jean-Jacques Quisquater, University Catholique de Louvain, Belgium, "Biometrics, Access Control, Smart Cards: A Not So Simple Combination". http://citeseer.nj.nec.com/cs

[26]Fernando L. Podio, "Biometrics – Technologies for Highly Secure Personal Authentication', National Institute of Standards Technology (NIST), May, 2001. http://www.itl.nist.gov/lab/bulletns/bltnmay01.htm

[27]Catherine J. Tilton, "An Emerging Biometric API Industry Standard", IEEE Computer (Special Issue), February 2000.

[28]BioAPI Consortium, "BioAPI Specifications", Version 1.1, March 2001. http://www.bioapi.org/