An Adaptive Framework for Biometric Systems

Dr. Sitalakshmi Venkatraman
School of Information Technology and Mathematical Sciences,
University of Ballarat, PO Box 663
Ballarat, VIC 3353, Australia
Telephone: 61 3 5327 9074
Fax: 61 3 5327 9289
Email: S.Venkatraman@ballarat.edu.au

Abstract

This paper provides guidelines to classify biometric systems based on the level of privacy and security risks associated with their transactions. The classification of biometric systems as Basic, Medium or Advanced details how the transactions make use of biometric information for one or more purposes, such as, authorisation, accountability and analysis of sensitive data. An adaptive framework proposed here considers this classification as the fundamental building block in providing a step-wise implementation procedure for implementing biometric systems. It is believed that by adopting such an adaptive framework, societies, businesses and government would be able to harness the benefits of biometrics. This would pave way for a significantly faster diffusion of biometric systems in many everyday life scenarios.

Key Words: *Biometric Systems, Biometric Transactions, Privacy / Security Risk, Adaptive Framework*

1. Introduction

With the escalating increase in security breaches and transaction frauds being witnessed today, the need for highly secure identification and personal verification systems is warranted [1], [2], [3]. A biometric system, which is essentially a pattern recognition system, automatically recognises a person using physiological or behavioural traits such as fingerprints, hand geometry, signature, retina or voice [4]. This emerging technology could play a major role in addressing the prevalent security and information protection issues faced by a wide variety of everyday applications [1], [3]. However, biometrics is still in its early stage of adoption as it is surrounded by many issues related to cost, technology and privacy [5], [6], [7]. While much research studies have been done with regard to technology improvements and cost viability [3], [8], there is a paucity of research that focuses on addressing the privacy and security issues [5], [6]. Recent studies indicate that the privacy / security risk of biometrics is the predominant factor that has become the stumbling block for its diffusion today [8], [9].

In this paper, the main objective is to study the privacy and security issues / challenges faced by biometrics and thereby propose an adaptive framework that provides a step-wise guideline for a successful implementation of biometric systems. Section 2 of this paper highlights some related work found in literature that motivated this study. In Section 3, the impact of biometrics in societies, businesses and government are analysed in typical scenarios where biometric transactions could take place. With privacy / security risk as the major adoption factor, biometric transactions are classified based on the level of such risks. Section 4 describes the proposed adaptive framework that paves way towards successfully implementing a highly secured biometric system. Finally, Section 5 provides the conclusions and future research directions.

2. Literature Review

Research studies conducted on various biometric techniques indicate that fingerprint, face, iris, voice, signature, and hand geometry have matured well enough to become the de-facto authentication system to identify a person uniquely [2], [7], [8], [9]. Recently, biometric modalities such as DNA samples, gait, ear

978-0-7695-3521-0/09 $25.00 © 2009 IEEE
DOI 10.1109/ICCET.2009.98

contours and the like are being explored and are in the various stages of development and assessment [10], [11], [12]. It is envisaged that biometrics is capable of becoming part and parcel of everyday life as biometric identification and verification would increasingly be adopted in business transactions, public sectors, crime detection, law enforcement and other environments such as home and schools [13], [14]. However, one cannot identify any single biometric modality to be the best for all implementations as there are many influencing factors impacting on the success of biometric systems [2], [15], [16], [17].

Much research has addressed the tangible factors such as, technology, reliability and cost that could impact the development of biometric systems [15], [17]. Many studies concentrate on reducing possible errors in biometric matching systems, such as, False Acceptance Rate (FAR) and False Rejection Rate (FRR) and in reliable encryption methods [3], [8]. However, studies indicate that privacy / security risk is the key intangible factor that has a major influence on the user acceptance of such systems [16], [18], [19], [20]. The following factors identified from the literature survey conducted in this study have been the motivating factor for this research work:

I. There is a false fear prevailing among the public that biometric sensors could potentially hinder their health and safety [22].
II. Information security policies and compliance statutes have undergone considerable changes over the last few years both locally and globally and this has affected biometric diffusion [9], [12].
III. Different biometric technologies are at different stages of maturity and there is no single modality that could become the standard for all applications [21], [10], [11] and this could impact very much on their commercial adoption.
IV. The easiness of biometric enrollment and its permanence (tolerant or non-tolerant) varies among different biometric modalities [23], [24]. Frequent and multiple biometric enrollments for different situations pose a major inconvenience to the users [25].
V. User confidence is also affected based on the extent to which biometric data is used, whether the system allows exchange of biometric data with other systems and leads to function creep [12], [26].

It is, therefore, important to understand the purpose and to what extent any information processing transaction uses biometrics. In view of these findings from literature, in the next section, this research takes the first step to classify biometric transactions based on the level of privacy / security risk involved.

3. Classification of Biometric Transactions

Research studies indicate that privacy / security risk is the key factor for society to be slow in adopting biometrics [9], [12], [16]. Hence, this research considers various types of biometric transactions that are possible in commercial and non-commercial scenarios so as to classify them based on the level of privacy / security risk associated with them. This is summarised in Figure 1 with the following three main privacy / security risk levels under which any biometric transaction would be classified:

I. Basic-level – Biometric transactions fall under this category if they are mainly authorisation-based transactions that have minimum privacy risk as the biometric data is normally used only for verification of identity. Common scenarios where such biometric transactions take place are, access to physical locations (laboratories, bank lockers, membership premises, etc.), authorisation of payments (online payments, ATMs, etc.) or even regulating certain physical controls (power supply, heaters, etc.) at office or at home. Such transactions have a low level of privacy / security risk as biometric data is not stored anywhere while being processed.
II. Medium-level - As a next level to identification are accountability-based transactions that record biometric identities of individuals to determine when (time-based) or for what purposes (resource-based) tasks have been accomplished by them. Such transactions could typically prevail in societies that make use of biometrics, say in fee calculation based on time spent or in other public service based on resource utilisation. Businesses and government services could use biometric identities for determining the time of approvals or completion of tasks (e.g., online purchase approvals, aircraft boarding, etc.). Such transactions have a medium level of privacy / security risk as the biometric data is stored as part of the history of transactions for future reference.
III. Advanced-level – Transactions at this level access and process sensitive information using an individual's biometric identity. Such personal information retrieval-based transactions are used to perform behaviour analysis (e.g., profiling customers or employees, crime detection, etc.) or health analysis (e.g., patient treatment, employee recruitment, etc.). These would have the highest

privacy risk as the biometric data is not only stored as part of the transactions but could also be used to retrieve their personal information to extrapolate the physical and mental faculties of individuals.

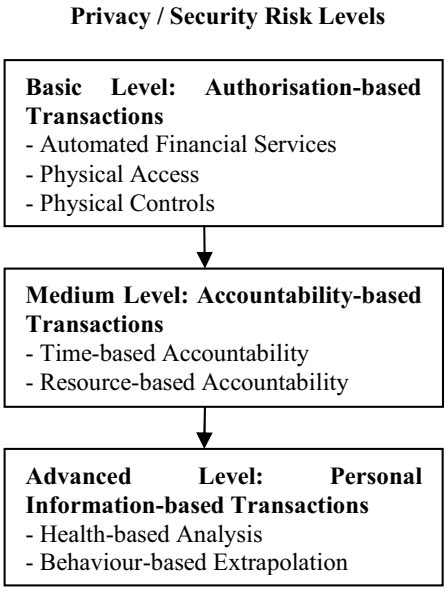

Figure 1. Risk-Based Classification of Biometric Transactions

Overall, privacy / security risks could be identified with biometrics during the very first interaction with the user, namely, the enrollment process, when biometric data is collected and stored as signatures or normalised as templates. Next, it is the verification stage, when risks could be associated at the time of matching or data transmission. Finally, at the application level, risks are associated based on the type of transaction as described above. Hence, the abovementioned classification of all the biometric transactions that are required for an application would help in determining and addressing the associated privacy / security risk levels. The next section uses this classification methodology to arrive at an adaptive framework for successfully implementing biometric systems.

4. An Adaptive Biometric Framework

An adaptive framework for implementing biometric systems is proposed here with the goal of enhancing user adoption through minimizing privacy / security risks. This is achieved as the framework aims at promoting multimodality and pseudonym operations using an encrypted one-stop database that ensures high security and reliability levels at the same time, leverages on the simplicity of "enroll once" policy. Such a framework, on one hand incorporates the desired flexibility and convenience for the users, and on the other hand caters to the privacy / security risk issues as well. This framework addresses the complexity of potential biometric systems so that specific implementations of biometric technology could follow the guidelines specified here to customize the deployment for different scenarios effectively.

The framework consists of the following four components to be considered as building blocks for a successful biometric implementation:

I. Biometric Technology Component – This component addresses the technology issues surrounding the possible biometric system considered for implementation. It considers techniques relating to the different biometric modalities that could be considered for the enrollment process. Based on the biometric modalities considered, suitable pseudonym operations could be identified for the verification as well as application level transactions. This component also determines the. encryption techniques that could be adopted for data storage or while transmitting data during enrollment, verification and application-level transaction processing.

II. Privacy / Security Risk Component – This component addresses the user concerns with respect to privacy and security fears. Apart from identifying the risks associated with the sensors used and the templates created during the enrollment process, it also considers the risks associated during the verification and transaction processing stages in biometrics.

III. One-Stop Database Component – This component deals with the various methods of biometric data storage and retrieval. It considers the importance of "enroll once" facility to reduce the burden of multiple enrollments for different applications at different points of time. Such a one-stop database component could also cater for storing the necessary biometric data (signatures and meta-data) gathered from national and international sources as well as agencies that could aid in developing the centralised database.

IV. External Factor Component – This component addresses the external factors that could affect the implementation of the biometric system. It ensures that appropriate international biometric standards are considered and that the local government policies / laws are adhered to.

These four components of the framework have an impact on one another and their relationships are summarised in Figure 2.

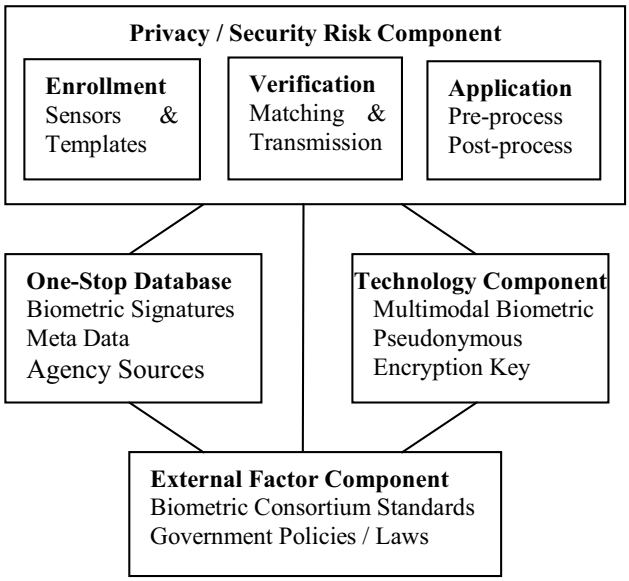

Figure 2. Components of the Adaptive Biometric Framework

The following seven steps (Figure 3) provide a guideline for adopting the adaptive biometric framework for organisations venturing into biometrics:

Step 1: Determine the transaction classification (refer to Section 3) where the biometric system would possibly fit into. This would be based on the goals and objectives of the biometric system.

Step 2: Identify the risks associated with enrollment, verification and application transactions. Identify those transactions that are under low-level, medium-level and advanced-level privacy / security risks.

Step 3: Choose suitable modalities of biometrics so as to address the enrollment, verification and application risks.

Step 4: Adopt appropriate levels of encryption for templates, data transmission and data storage and identify the processes where pseudonymous biometrics could be applied.

Step 5: Design and implement a one-stop database of biometric signatures and other meta-data that could possibly be collected from agencies and local enrollments conducted by national as well as international bodies.

Step 6: Verify that the system and processes conform to consortium standards, government laws and policies.

Step 7: Perform post-evaluation of technologies and risks. Determine any risks that are not addressed in the above steps. Introduce new modalities of biometrics as the situation warrants and as new technologies emerge.

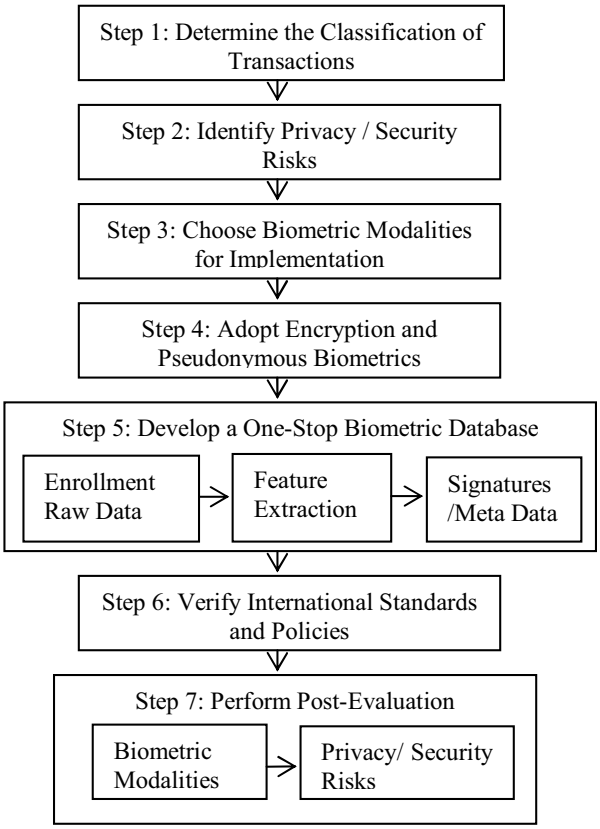

Figure 3. Step-wise Adaptive Framework for Biometric System Implementation

5. Conclusions and Future Research

Biometrics, a fast growing emerging area with latest robust technologies such as DNA fingerprinting and vein-sampling, is still slow in its adoption due to the privacy / security risks associated with their transaction processing. Hence, this paper takes the first step to classify the biometric transactions based on the level of privacy intrusion so that one could understand the risk level to be addressed before venturing into biometrics. Next, the proposed adaptive framework with four components follows a generic model with a seven-step guideline that could be adopted for specific deployment of biometrics in business, government and society. Future research would be to apply this framework for a case scenario in Australia. This paper is another step forward paving the way for further research in

implementing each of the components of the proposed biometric framework for any future scenario.

6. References

[1] Jain, A., Ross, A., and Pankanti, S., "A Biometrics: Tool for Information Security", *IEEE Transactions on Information Forensics and Security*, 2006, 1(2), pp. 125-143.

[2] Condon, R., "New Biometrics See Right through You", *Information Security*, 2007, 4 (1), pp. 24-26.

[3] Clarke, N.L. & Mekala, A.R., "The Application of Signature Recognition to Transparent Handwriting Verification for Mobile Devices", *Information Management & Computer Security*, 2007, 15(3), pp. 214 – 225.

[4] Jain, A., Ross, A., and Prabhakar, S., "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, *Special Issue on Image and Video-based Biometrics,* 2004, 14(1), pp. 4-20.

[5] Prabhakar, S., Pankanti, S., and Jain, A., "Biometric Recognition: Security and privacy concerns", *IEEE Security and Privacy*, 2003, 1(2), pp. 33-42.

[6] Crosbie, M., "Biometrics for Enterprise Security", *Network Security,* 2005, 12(11) 4-8.

[7] Capoor, S., "Biometrics as a Convenience", *Security*, 2006, 43(12), pp. 48-50.

[8] Song, O. T., Jin, A. T. B. and Connie, T., "Personalized Biometric Key Using Fingerprint Biometrics", *Information Management & Computer Security,* 2007, 15(4), 313-328.

[9] International Biometric Group 2007, "Biometrics Market and Industry Report 2007-2012", *Biometrics Report & Research,* 2007 http://www.biometricgroup.com

[10] Silva, L. M, Montes O. H, Diniz C. R, Fortes-Dias C. L., "Fingerprinting of Cell Lines by Directed Amplification of Mini Satellite-region DNA", *Brazilian Journal of Medical and Biological Research*, 2001, 34 (11), pp. 1405-1410.

[11] Chang, K., Bowyer, K., W., Sarkar, S., and Victor, B., "Comparison and Combination of Ear and Face Images in Appearance-Based Biometrics", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2003, 25(9), pp. 1160-1165.

[12] OECD, "Biometric-based Technologies. Working Party on Information Security and Privacy",2004,www.oecd.org/sti/security-privacy

[13] Strohm, C., "A New Identity", *Government Executive*, 2005, 37(3), pp. 63-69.

[14] Costanzo, C., "Suddenly, Biometric ID doesn't Seem Like Science Fiction", *American Banker*, 2006, 171(107), pp. 6-11.

[15] Kittler, J., Hatef, M., Duin, R., and Matas, J., "On Combining Classifiers", *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 1998, 20(3), NY, pp. 226-239.

[16] Chandra, A., and Calderon, T., "Challenges and Constraints to the Diffusion of Biometrics in Information Systems", *Communications of the ACM,* 2005, 48(12), pp. 101-106.

[17] Camlikaya, E., Kholmatov, A., and Yanikoglu, B., "Multi-biometric Templates Using Fingerprint and Voice", *Proceedings of SPIE Conference on Biometric Technology for Human Identification,* 2008.

[18] Alterman, A., "A Piece of Yourself: Ethical Issues in Biometric Identification", *Ethics and Information Technology,* 2003, 5(3), pp.139-150.

[19] Barton, B., Byciuk, S., Harris, C., Schumack, D., and Webster, K., "The Emerging Cyber Risks of Biometrics", *Risk Management*, 2005, 52(10), pp. 26-31.

[20] Lysecki, S., "Federal Facial Recognition Project Raises Privacy Fears", C*omputing Canada,* 2006, 32(13), www.itbusiness.ca/it/client/en/Home/News.asp?id=40881.

[21] O'Gorman, L., "Fingerprint Verification: Personal Identification in a Networked Society", Dordrecht: Kluwer Academic Publishers. Edited by Bolle, R., and Pankanti, S., 1999, pp. 43-64.

[22] Bromme, A., "A Risk Analysis Approach for Biometric Authentication Technology", *International Journal of Network Security*, 2006, 2(1), pp. 52–63.

[23] Jain, A., and Ross, A., "Multibiometric Systems", *Communications of the ACM*, 2004, 47(1), pp. 34-40.

[24] Xia, X. and O'Gorman, L., "Innovations in Fingerprint Capture Devices", *Pattern Recognition,* 2003, 36(2), pp. 361-369.

[25] Phillips, P. J, Martin, A, Wilson, C. L. and Przybocki, M, "An Introduction to Evaluating Biometric Systems", *IEEE Computer*, 2000, 33(2), pp. 56-60.

[26] Song, O. T., Teoh, A. B., and Ngo, D. C-L., "Application-Specific Key Release Scheme from Biometrics", *International Journal of Network Security*, 2008, 6(2), pp. 127-133.