Opportunities and Benefits - Vision of the Biometrics Working Group

Wu Jian Kang and Huang Weimin
Kent Ridge Digital Lab, Singapore

Dr Wu and Dr Huang participate in the Biometrics Working Group under the Security and Privacy Standards Technical Committee

Abstract

Biometrics is a challenging industry with a huge market potential. Technologies in the area are becoming mature, and various standards are about to be established. After a brief review of the status of international activities of biometrics standardisation, the activities of the Biometrics Working Group of the Security and Privacy Standards Technical Committee will be described. The article will concentrate on the problems and concerns in biometric applications. Opportunities and benefits for Singapore are highlighted. The analysis will cover aspects of related technologies, markets, and industries. The idea can be generalised to standardisation activities of other areas.

1. Introduction

Biometric techniques are designed to verify or identify people by their physical characteristics, including fingerprint, hand geometry, iris, voice, face image and handwriting signature. It provides an easy way to individual identification. Biometrics can offer a high level of protection against identity fraud.

According to Frost & Sullivan, as the demand for safeguards grows, the field of biometrics is expected to show impressive market growth of more than ten times its current size by 2006. The total biometric market generated US$66 million in 2000, and is expected to reach US$900 million by 2006.

On the other hand, governments around the world are responding to consumer concerns about the confidentiality of their personal information that is being stored or transmitted. By enacting strict privacy legislation, companies are accountable for all personal information they retain, and consumers will feel comfortable using biometric systems.

In order to demolish a long-standing obstacle to industry growth, it is necessary to establish standards. In this article, we will first analyse the problems encountered in the process of deploying biometric technologies, and then explain how standardisation can resolve these issues.

The main activities of the Biometrics Working Group in the previous year have concentrated on

1) tracking international activities and promoting awareness to related organisations in Singapore, and

2) studying the biometric technologies, industries and market in order to position ourselves and to identify opportunities at the right time.

Section 2 is devoted to existing standardisation activities of the Biometrics Working Group, while Section 3 analyses the biometric technologies, systems and applications. Our recommendations in Section 4 are based on the results of our analysis.

2. Existing Standardisation Activities

Biometric standardisation activities fall under the following areas: methodology, file format, application programming interface (API), and other security related standards. They are driven by various international groups. The Biometrics Working Group has been actively participating in those activities. A summary is given in Table 1. The rest of this section contains brief descriptions of these activities.

2.1 ANSI/NIST- ITL 1-2000 standard

The ANSI/NIST- ITL 1-2000 standard is a description of file format for some biometric traits. In this standard, the Biometrics Working Group participated as a Canvassee to review and ballot the draft. One feature of this standard is that it defines minutiae based fingerprint template in detail. That provides a baseline for other standardisation in this aspect. It also specifies image information for the non-fingerprint biometrics. It is mainly designed for the exchange of fingerprint, palmprint, facial/mugshot, and scar mark and tattoo (SMT) image information for government agencies.

Table 1 Standardisation Activities

ANSI/NIST-ITL 1-2000	A description of file format for biometric traits
CBEFF	A standard for "technology-blind" biometric file format
ISO/IEC JTC1/SC17	Smart card based biometric personal verification standard
Biometrics Standard Framework	A framework proposed for developers and users to adopt biometric standards for biometric system

2.2 Common Biometrics Exchange File Format

Effort is also made to design a standard for Common Biometrics Exchange File Format (CBEFF). It is designed to handle different biometric types, versions, and vendors in a common way. For the time being, there are no biometric data structures defined yet. The CBEFF's definition is achieved through a series of workshops sponsored by the National Institute of Standards and Technology (NIST), and the Biometrics Consortium.

2.3 BioAPI

Part of the format structures of CBEFF are used in BioAPI, a biometrics API standard developed by the BioAPI Consortium. Besides the data format, BioAPI also defines a high-level data structure, registry schema, error handling, operational functions and a service provider interface.

2.4 Security-related standard

While CBEFF and BioAPI mainly deal with biometrics data interoperability, other standardisation activities cover issues such as security. Starting from ANSI X.509, CBEFF tried to integrate itself into the X.509 attribute certificate. With the coordination of efforts from CBEFF, BioAPI and Accredited Standards Committee (ASC) X9-financial services, a X9.84 Biometrics Information Management and Security was developed and published this year. It is observed that the combination of CBEFF and X9.84 can satisfy the security request for biometric systems.

2.5 Smart card standard and ISO/IEC biometric standard

Another effort is the cross development between ISO/IEC "Personal Verification Through Biometric Methods in Integrated Circuit(s) Cards" and CBEFF smart card data format. ISO/IEC is now working on the smart card based biometric personal verification standard and will look at other standards. The Biometrics Working Group was involved in the voting through the Cards and Personal Identification Technical Committee of ITSC by providing our reviews on the draft. With the coordination between CBEFF working group and ISO, more results are forthcoming for biometrics standardisation. The Working Group attended the first ISO/IEC meeting for biometrics standardisation and will follow the activities.

The Biometrics Working Group also proposed a Biometrics Standard Framework as a guideline for users and vendors to adopt and develop biometric standard. The Framework covers the area of biometric standards and related security standards. It is also a roadmap

to facilitate the development and adoption of biometric standards in Singapore. This will be discussed in greater depth in the following section.

3. Outstanding Issues In Biometric Applications

Although biometrics refers to methods of authenticating people by individual traits, biometric technology itself consists of many steps of capturing and processing of biometric data. At the system level in real applications, biometric techniques may be integrated with other techniques to form a complete solution. Many biometric applications are large scale, and can be national or international initiatives. Frequently, interoperability is required to cross applications. There is a need to study the problems that might be obstacles to the biometric industry. By doing so, we will understand the entire background, the issues that need to be addressed, existing solutions and outstanding issues of importance that require innovative work and persistent effort.

3.1 Issues at Biometrics System Level

A typical biometric system includes biometric data capture, processing, transmission, storage, and authentication. In this system, there are several issues to be addressed:

The first, and also the largest issue concerns the data. Taking fingerprints as an example, the following issues need to be addressed:

a) The resolution of the captured fingerprint image should be sufficiently detailed in order to support various applications. At the same time, redundancy should be minimized;
b) Determining the structure of the database. Biometric data processing methods are usually proprietary to each company. It is difficult to standardise these methods. A biometric template is a measure of biometric features that are extracted from the raw biometric data for final recognition or matching. Standardisation of templates will depend on the biometric type. Related standards include the ANSI/NIST 1-2000, and the CBEFF.
c) Deciding on the data format for interoperability when the data is shared among multiple systems.

Manufacturing robust and affordable biometric capturing devices is critical for the deployment of biometric systems. Meanwhile, it will be useful to have various devices compatible with each other. Biometrics API standardisation addresses this issue. It provides the common function for interfacing with capturing devices.

Security and confidentiality is another major concern. As soon as biometric data is captured, it is in a digital form. The advantages of being digital include convenience, speed, ability to be shared, and border-less. However, these advantages also apply to piracy and intrusion. As such, security now becomes a big concern. People are reluctant to accept biometric authentication applications because of possible security holes in

various steps of the system. There may be attacks at a certain stage of the system to illegally obtain the data, and reuse it. There is also possibility that the data in the database is not well managed and data is shared without proper concern of consequences.

3.2 Issues cross applications

Biometric technologies are used together with other technologies. Hence, a biometric system may be integrated with other existing applications. For example, if a bank decides to use voice as password for ATM system, the voice identification system needs to be integrated with the existing ATM system. Figure 1 shows issues that cross various applications. We have talked about Standard APIs, which will provide standard interface between any software and hardware modules, and making system integration easy. When APIs are standardised, software and hardware modules can be interchangeable, and each part is plug-and-play.

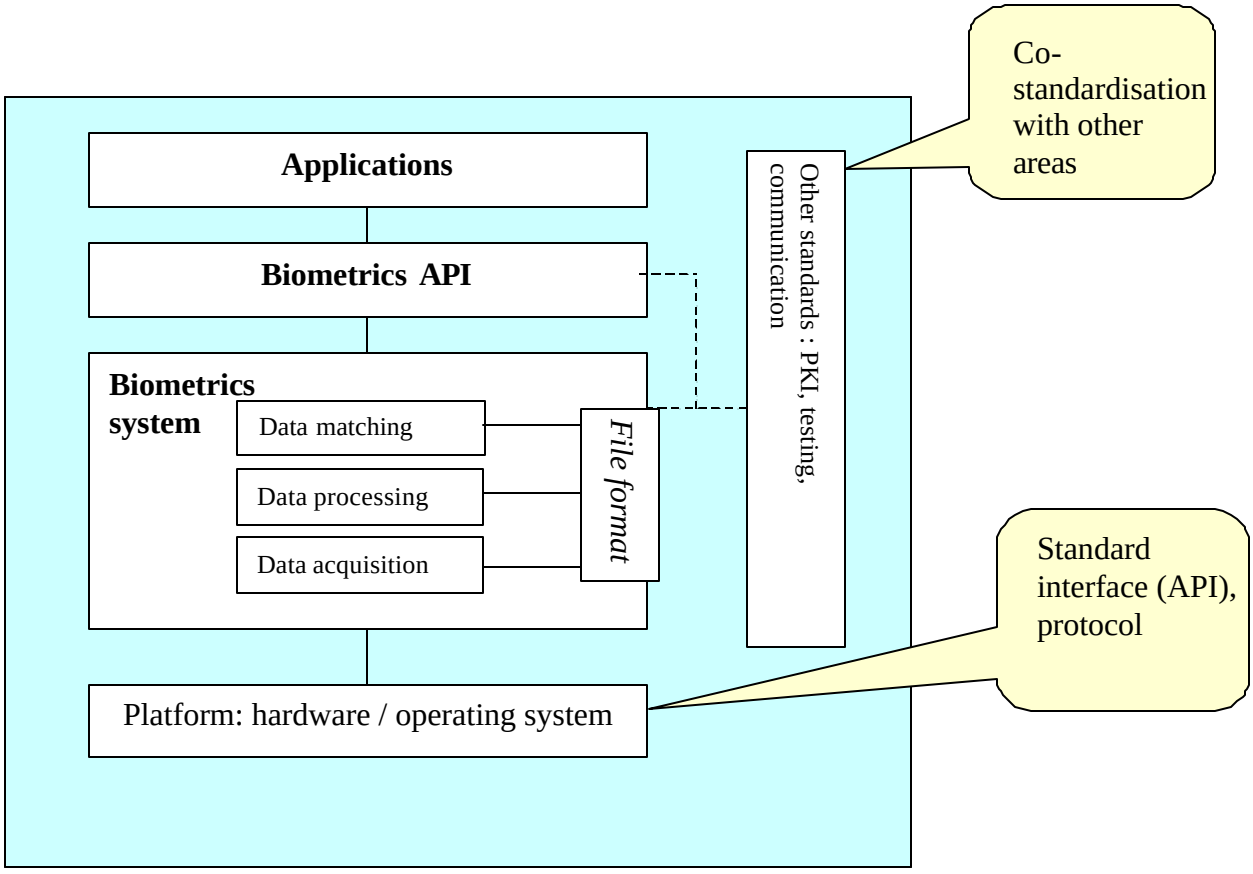

Figure 1. Framework for biometrics

Biometric authentication is one aspect of secure applications. For example, in Public Key Infrastructure (PKI), digital certificate is used for personal identification. Effectively linking a person to his digital certificate is not as simple as putting a face image on a person's Identity Card (IC). In the case of an IC, physical inspection of the face image on the IC is a reliable means for authentication. As far as digital certificate is concerned, the

possible authentication means are using password and tokens such as smart cards. There are proposals to use fingerprints or handwriting signatures as part of a digital certificate. That is, instead of using only a public key as a means of identifying that person, his fingerprint and/or handwriting signature are also incorporated. The uniqueness of the fingerprint and handwriting signature provides very secure means for authentication. Of course, in order to incorporate this in an infrastructure, there must be a standard, defining aspects of this proposal with respect to existing PKI related standards. For standardisation to take place, many issues need to be solved. This includes: registration, secure management of fingerprint and hand signatures and verification process.

Application oriented standards are also possible. While PKI is an across-the-board standard for security, to provide an electronic means to authenticate individuals or organisations within a computer network, we may also propose standards for both physical and electronic identity for individuals. An example is smart passports. This naturally falls within the realm of biometrics – a smart passport needs to have photograph of a face on it. If an international standard on smart passports can be established together with biometrics extended digital certificate system, the PKI would be much more feasible, and trust-worthy: Certificate Authorities (CA) would then be government authorities who issue passports. This guarantees the quality of the digital certificate, and cuts down the cost of existing CAs.

While talking about the advantages of biometric technologies, we have to bear in mind that customer acceptance is a key. Although people complain all the time about remembering passwords, yet, it is the simplest and most popular means for personal authentication. Biometrics must address this challenge and try to co-exist with password systems. As such, more creative technologies and standards are expected to emerge rather than biometric processing methods themselves.

Standard biometric testing database and testing procedures are important in any biometric applications. A standard database and a standard testing procedure will provide users a comprehensive understanding of a biometric system, and guide users to the right choice.

Most biometric standards will be standalone standards. But as suggested in the IT Security framework, the legal framework has an important impact on implementing security services, architecture, secure process and the adoption of best practices. The legal acts affecting security aspects including biometric application are the Electronic Transactions Act, the Banking Act and Computer Misuse Act.

4. Opportunities and Our Strategy

As of now, the biometric industry is relatively small. There is no significant international initiative dedicated to biometrics standardisation issues. Rather, it is scattered into several small efforts, each addressing different aspects.

In the coming years, the Biometrics Working Group will continue to track existing international standardisation activities, and organise seminars to facilitate and promote

biometric research and industries in Singapore. On the other hand, we will actively pursue the following three initiatives:

- To strategically plan and organise our effort in order to contribute to an international standard. To this end, we will identify opportunities and develop a proposal that is very likely to be accepted by society. While pushing for standardisation, we must develop technologies to support the implementation of those standards. Our technologies and products will be ready for the market when those standards emerge, though they may not be initiated by us.
- Actively collaborate with biometrics standardisation organisations in other countries. The Biometrics Working Group has a collaboration with NIST, and plans to establish links with the Biometrics Association of UK and Australia. This is very important because the status of biometrics standardisation is such that there is no strong international organization so far. As such, we should actively pursue collaboration with individual organisations in each country, especially NIST in the U.S. and others.
- To provide databases and protocols for testing and guidelines for choosing these databases and protocols for various applications. This is critical for government tenders and private industrial projects.

References

[1] ANSI/NIST-ITL 1-2000 American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, and Scar Mark & Tattoo (SMT) Information, 2000.

[2] CBEFF - Common Biometrics Exchange File Format, NISTIR 6529, NIST, 2001

[3] BioAPI Specification Version 1.00, the BioAPI Consortium, 2000.

[4] ISO/IEC CD 7816 11, Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 11 : Personal Verification Through Biometrics Methods, 2000.

[5] ISO/TEC JTC1/SC17 N 1793, Usability of Biometrics in Relation to Electronic Signatures EU Study, 2000.

[6] ITU-T Recommendation X.509 Digital Certificates, "Information technology - Open Systems Interconnection - The directory: Authentication framework", 1993.

[7] ANSI X9.84, Biometrics Management and Security for the Financial Services Industries, 2001.