Available online at www.sciencedirect.com
SCIENCE DIRECT®
NUCLEAR SCIENCE AND TECHNIQUES
Nuclear Science and Techniques, Vol.17, No.2 (2006) 97–105

Biometric technology overview

LI Yong-Ping *
(Biometrics Laboratory, Shanghai Institute of Applied Physics, the Chinese Academy of Sciences, Shanghai 201800, China)

Abstract Biometrics was identified as one amongst 10 emerging technologies which would change the world in the twenty-first century. Components and processes of biometric system and the relevant technologies are explained in this article. Examples of biometric applications and trends of biometric research, together with industry development, are introduced, which illustrate the challenges and opportunities of this technology.

Key words Biometrics, Personal identity authentication, Pattern recognition, Template, Smart card, Multi-biometrics fusion

CLC numbers Q983, Q984, D918.91

1 Introduction

Biometrics are drawing much attention since the 9/11 incident not only for anti-terrorism issues, but also for being a powerful authentication method to verify the identity of a person so as to restrict access to sensitive areas or systems. In their daily lives, people face many situations where there is a need to verify their personal identity by means of cards, passwords, or personal identification numbers (PIN), etc. Due to the limitations of these traditional techniques based on what we know (password, PIN, secure questions, etc.), or what we have (smartcard, token, ID cards, etc.), we are forced to carry many cards and have to remember many complex PIN or passwords. Therefore when we lose these cards or forget any password, we fail to prove our identities even if we are present there physically. That sarcastically means we have to use something that does not belong to us to prove who we are. Further, the instances of criminals capturing or decrypting all kinds of PIN and password are growing higher and higher. The U.S. Federal Trade Commission estimates the cost of a lost or stolen identity to be more than five billion US dollars every year. These kinds of thefts by criminals are increasing at an alarming rate in China, making huge loss to both individuals and organizations. New personal identity verification technologies are highly demanded to be a key ingredient of today's secure systems. Biometrics provides solution that satisfies the twin demands of security and convenience by making use of "what we are" instead of "something we have" or "something we know", thereby authenticating individual rather than device/password. Therefore biometric-enhanced authentication tops the pyramidal security infrastructures as shown in Fig.1.

2 Biometrics terminology

The most suitable definition of biometrics is the automated use of physical or behavioral characteristics to determine or verify the identity of an individual. Biometrics can be used in a variety of applications; to elaborate on this definition, physical biometrics are based on measurements and data derived from direct measurement of a part of the human body while behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body[1]. Biometric (noun) is one of various technologies that utilize

*E-mail: liyongping@sinap.ac.cn
Received date: 2006-01-24

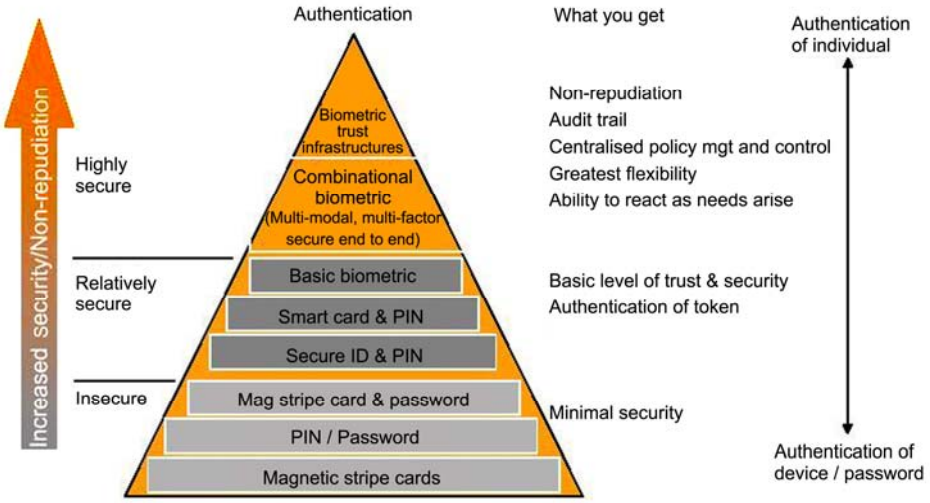

Fig.1 Biometrics and security infrastructures.

behavioral or physiological characteristics of an individual to determine or verify identity. Plural form of biometric is also acceptable but biometrics (noun) usually means the field relating to biometric identification. Biometric (adjective) is of or pertaining to technologies that utilize behavioral or physiological characteristics to determine or verify identity. Biometric system represents the integrated biometric hardware and software used to conduct biometric identification or verification.

The leading physical biometrics includes fingerprint, facial recognition, iris scan, retina scan, and hand geometry. Voice recognition and signature scan are leading behavioral biometric technologies. Physical biometric can use the static image as a metric whereas one of the defining characteristics of a behavioral biometric is the incorporation of time as a metric---the measured behavior has a beginning, middle and end. The distinction between behavioral and physical is slightly artificial. Behavioral biometrics is based in part on physiology, such as the shape of the vocal chords (voice recognition) or the dexterity of hands and fingers (signature scan) while physical biometric technologies are similarly informed by user behavior, such as the manner in which a user presents a finger or looks at a camera. However, the distinction is a helpful tool in understanding how biometrics work and how they can be applied in the real world. The primary biometric disciplines include the following:

- Fingerprint (optical, silicon, ultrasound, etc.)
- Facial recognition (optical and thermal)
- Voice recognition (also referred as speaker recognition)
- Iris scan, retina scan
- Hand geometry
- Signature scan, keystroke scan

3 Basic components and processes of biometric system

Biometric systems generally include the classical pattern recognition components data acquisition, preprocessing, feature extraction and classification[2]. The result is that biometric decision-making is very rapid, and in most cases, in real time. Biometric systems convert data derived from behavioral or physical characteristics into templates, which are used for subsequent matching. Their components and processes can be generally illustrated in Fig. 2. This is a multi-stage process as described below.

Enrollment: The process through which a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system. Enrollment takes place in both 1:1 and 1:*N* systems. If users are experiencing problems with a biometric system, they may need to re-enroll to gather higher quality data.

Submission: The process through which a user provides behavioral or physiological data in the form of biometric samples to a biometric system. A submission may require looking in the direction of a camera

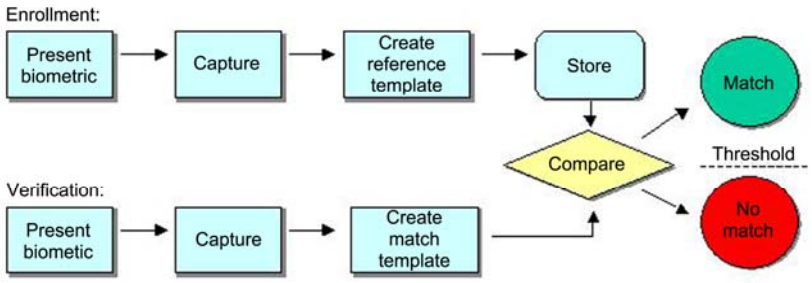

Fig.2 Diagram of biometric system components and processes.

or placing a finger on a platen. Depending on the biometric system, a user may have to remove eyeglasses, remain still for a number of seconds, or recite a pass phrase in order to provide a biometric sample.

Acquisition device: The hardware used to acquire biometric samples.

Biometric sample: The identifiable, unprocessed image or recording of a physiological or behavioral characteristic, acquired during submission, used to generate biometric templates.

Feature extraction: The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template. The feature extraction process may include various degrees of image or sample processing in order to locate a sufficient amount of accurate data. For example, voice recognition technologies can filter out certain frequencies and patterns, and fingerprint technologies can thin the ridges present in a fingerprint image to the width of a single pixel. Furthermore, if the sample provided is inadequate to perform feature extraction, the biometric system will generally instruct the user to provide another sample, often with some type of advice or feedback.

The manner in which biometric systems extract features is a closely guarded secret, and varies from vendor to vendor. Common physiological and behavioral characteristics used in feature extraction include the following:

Technology	Feature extracted
Fingerprint	Location and direction of ridge endings and bifurcations on fingerprint, known as minutiae
Voice recognition	Frequency, cadence and duration of vocal pattern
Facial recognition	Relative position and shape of nose, eyes, and mouths, position of cheekbones
Iris scan	Furrows and striations in iris
Hand scan	Height and width of bones and joints in hands and fingers
Signature scan	Speed, stroke order, pressure, and appearance of signature
Keystroke scan	Keyed sequence, duration between characters

Template: A comparatively small but highly distinctive file derived from the features of a user's biometric sample or samples, used to perform biometric matches. A template is created after a biometric algorithm locates features in a biometric sample. Template is one of biometric technology's defining elements, but not all biometric systems use templates to perform biometric matching, for example, some voice recognition system utilize the original sample to perform a comparison.

When templates are created upon the user's initial interaction with a biometric system, they are referred to as enrollment templates, and are stored for usage in future biometric comparisons. Matching templates are generated during subsequent verification or recognition attempts, compared to the stored template, and generally discarded after the comparison. Multiple samples may be used to generate an enrollment template---facial recognition, for example, will utilize several facial images to generate an enrollment template. Matching templates are normally derived from a single sample—a template derived from a single facial image can be compared to the enrollment template to determine the degree of similarity.

Matching: The comparison of biometric templates used to calculate their degree of similarity or correlation. A match attempt results in a score that is compared against a threshold. A match means the score exceeds the threshold whilst a non-match indicates the score falls below the threshold.

Biometric comparisons are algorithm-dependent. These algorithms manipulate the data contained in the biometric template to make valid comparisons, accounting for variations in placement, background noise, etc. The matching process involves the comparison of the match template, created upon sample submission, with the reference template(s) already in file. In 1:1 verification systems, there is generally a single-match template matched against a reference template. In 1:*N* identification systems, the single-match template can be matched against dozens, thousands, even millions of reference templates.

In most systems, reference and match templates should never be identical. An identical match is an indicator that some sort of fraud is taking place, such as the resubmission of an intercepted or otherwise compromised template.

Score: A number indicating the degree of similarity or correlation of a biometric match. Traditional verification methods---passwords, PINs, keys, and tokens---are binary, offering only a strict yes/no response. This is not the case with most biometric systems. Nearly all biometric systems are based on matching algorithms that generate a score subsequent to a match attempt. This score represents the degree of correlation between the match template and the reference template. Regardless of the employed scale, this verification score is compared to the system's threshold to determine how successful a verification attempt has been.

Incidentally, many systems return a score during enrollment, referred to as an enrollment score or quality score. This score refers to how successful the extraction process was at finding distinctive features in the biometric sample. If the sample was rich in information, there will likely be a high enrollment score. This score is not used in the matching process, but might be used to determine whether a user can enroll successfully. A low-quality score may indicate that the user cannot be verified in a reliable manner.

Threshold: A predefined number establishing the degree of correlation necessary for a comparison to be deemed a match. If the score resulting from template comparison exceeds the threshold, the templates are a "match". When a biometric system is set to low security, the threshold for a successful match is more forgiving than when a system is set to high security.

Decision: The result of the comparison between the score and the threshold. The decisions a biometric system can make include match, non-match, and inconclusive, although varying degrees of strong matches and non-matches are possible. Depending on the type of biometric system deployed, a match might grant access to resources, a non-match might limit access to resources, while inconclusive may prompt the user to provide another sample.

One of the most interesting facts about most biometric technologies is that unique biometric templates are generated every time a user interacts with a biometric system. As an example, two immediately successive placements of a finger on a biometric device generate entirely different templates. These templates, when processed by a vendor's algorithm, are recognizable as being from the same person, but are not identical. In theory, a user could place the same finger on a biometric device for years and never generate an identical template.

Therefore, for most technologies, there is simply no such thing as a 100% match. This is not to imply that the systems are not secured---biometric systems may be able to verify identify with error rates of less than 1/100,000 or 1/1,000,000. However, claims of 100% accuracy are misleading and are not reflective of the technology's basic operation.

4 Applications

Biometric techniques are increasingly being integrated into the security strategies of existing applications [2]. There are diverse biometric applications such as IT/Network Security, e-Commerce, Identification Systems, Access Control, etc. Specific skills and experience are required for different biometric applications---in many cases the biometric solution is a small part of the overall technology challenge. Requirements for accuracy, ease of use, response time, legacy integration, security, and privacy differ widely across

these applications.

4.1 Identification systems

Biometrics integrated into large-scale systems are utilized for drivers' licensing, surveillance, health and identity cards, and benefits issuance. The need for singular identification and transactional verification has emerged in various public and private sector environments such as

- Smart card integration
- Interfaces between 1:1 and 1:N systems
- Capabilities of leading AFIS, facial recognition, and iris-scan scan solutions positioned for identification systems
- Vendor-neutral system design
- Multiple device integration
- Ensuring accurate enrollment processes
- Integration of biometric systems and decisions into legacy systems
- Privacy-sympathetic system design
- Image processing and optimization
- Encryption of biometric data and match decisions

Identification systems are among the most complex biometric systems, with detailed requirements for acquisition devices, matching algorithms, fallback procedures, and privacy-sympathetic design.

4.2 IT/Network security

As more and more valuable information is made accessible via LAN and WAN, the risks associated with unauthorized access to sensitive data grow larger. Protecting networks with passwords is problematic, as passwords are easily compromised, lost, or inappropriately shared. Biometrics are proving to be an effective solution for IT/Network Security by their safety, convenience and cost reduction. Major challenges in deploying biometrics in this environment include accuracy and performance, integrating biometric-match decisions with existing systems, interoperability across proprietary technologies, and secure storage and transmission of biometric data.

4.3 e-Commerce and Internet

Biometrics are being adopted as a solution for e-Commerce and Internet security, designed to ensure that only authorized individuals can access sensitive data or execute transactions. From the perspective of commercial or government institutions, however, building effective e-Commerce and Internet solutions is more complicated than replacing a password and secure question dialog with a biometric interface [3]. Whether with authenticating customers, employees, or citizens, institutions must consider the following factors:

- Providing compatibility across the range of incompatible fingerprint technologies deployed at the desktop level,
- Accommodating individuals who cannot enroll or verify successfully, requiring fallback procedures,
- Integrating biometric match decisions into payment and clearance systems,
- Defining accuracy requirements for biometric systems,
- Location of biometric data storage and processing for maximum availability,
- Integrating biometric acquisition processes into existing interfaces,
- Administrative and auditing functionality to manage biometric accounts and transactions,
- Secure transmission of biometric information,
- Compatibility with Windows and Unix web-servers,
- Processes for verifying initial identity claims,
- Incorporating iris scan, voice recognition, and other biometric technologies for account access.

4.4 Access control

Biometrics have proven to be an effective solution for high-security access control to ensure that only authorized individuals are able to access protected or secure areas. However, there is more to deploying biometrics than replacing or complementing existing proximity or swipe systems. Biometric systems require controlled and accurate enrollment processes, careful monitoring of security settings to ensure that the risk of unauthorized entry is low, and well-designed interfaces to ensure rapid acquisition and matching. Poor system design and implementation can slow down the authentication process and expose new vulnerabilities.

Complex access control installations require independent expertise to ensure that security levels, in-

gress and egress processes, and system administration capabilities meet deployer's expectations.

5 Considerations of biometric projects

The pattern recognition task is a hard problem in the case of biometrics, since biometric data are statistical data, typically drawn from too few examples. Test patterns in use are never identical due to variability in the biometric data itself as well as the variability generated by the user interface. Furthermore, biometric features are derived from living organisms, and thus underlie changes due to acquisition, profession and activities. Still, the decision of the biometric system shall be reliable over time. Majority of accuracy rates of biometrics are only relevant in laboratory settings. When considering "what is the best biometric technology" for a project, there is much more to finding the right biometric device than accuracy. The following factors come into play with all biometric technologies:

- **Requirement gathering, integrating, and training** all of the components that goes into determining what biometric technology. A lack of training will almost certainly derail accuracy and user acceptance. Proper training ensures a quality enrollment, consistent submission, and the highest level of accuracy.
- **Location of devices**: Placing an optical fingerprint device in a sunlit, outdoor physical access installation, or placing a face recognition in a room with inconsistent or poor lighting, or using voice verification in a noisy environment are all recipes for poor performance. Location of the device and the immediate surrounding environment are essential criteria for deciding which device to use.
- **People using the device**: The type of device implemented will vary significantly depending on whether you are authenticating customers, students, citizens, prisoners, or employees. The level of intrusiveness, the ease-of-use, and the accuracy requirements are weighed differently in each situation. After selecting, implementing, and successfully training employees on your ideal biometric system, you'll have people falsely rejected. It is essential to devise procedures for times when authentication is impossible. Backup passwords are one option for logical (PC) access, as long as the passwords do not remain static. Ideally, the use of a password for authentication should be flagged, so that IT administrators can track and monitor those sessions. For physical access, the same protocol can be implemented, as long as the device has a keypad-style interface along with the biometric.

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to definitely state if a biometric submission will be successful, it is possible to locate factors that can reduce the effect on the system performance. Take examples of fingerprint and face recognition research projects, the main biometric objects in our laboratory, technology aspects that work against a successful verification are listed below:

Fingerprint project

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)
- Cuts to fingerprint
- Manual activity that would mar or affect fingerprints (construction, gardening)

Facial recognition

- Change in facial hair/hairstyle
- Lighting conditions
- Adding/removing hat
- Adding/removing glasses
- Change in weight
- Change in facial aspect (angle at which facial image is captured)
- Too much or too little movement
- Quality of capture device
- Change between enrollment and verification cameras (quality and placement)
- 'Loud' clothing that can distract face location

An additional strike occurs when a long period of time has elapsed since enrollment or since one's last verification. For the most part, a single strike will probably not materially affect the performance of a

given system. However, as you have more and more strikes for a given submission, your chances of a successful verification diminish. These strikes do not include inherent characteristics such as age, ethnicity, or gender, which can also affect system accuracy. The performance of many biometric systems varies for specific populations.

6 Developing trends and outlook of biometric technologies

6.1 Multiple-biometric fusion

A biometric system that utilizes more than one core technology for user authentication is referred to as multimodal (in contrast to mono-modal). It is recognized today that biometric identification can be better performed if more than one biometric is involved in the matching process. This can relate to multiple samples of the same biometric, or to the use of different biometrics (such as a fingerprint combined with a facial image).

There are three types of multimodality in the biometric world: synchronous, asynchronous, and either/or.

Either/or multimodality describes systems that offer multiple biometric technologies, but only require verification through a single technology. For example, an authentication infrastructure might support facial, voice, and fingerprint at each desktop and allow users to verify through any of these methods. A number of vendors have developed enabling middleware that allows for authentication by means of various biometrics. The benefit of this system is that biometrics, instead of passwords, can be used as a fallback. To have access to either/or multimodality, a user must enroll in each technology. To use finger, face, and voice, for example, one must become familiar with three devices and three submission processes. As a key performance indicator in biometrics is ease-of-use, requiring familiarity with multiple processes can be problematic.

Asynchronous multimodality describes systems that require that a user verify through more than one biometric in sequence. Asynchronous multimodal solutions are comprised of one, two, or three distinct authentication processes. A typical user interaction consists of verification on fingerprint, then of face, if the finger is successful. The advantage of added security---it is highly unlikely that a user will break two systems---is offset by a reduction in convenience. In addition to the time required to execute these separate submissions correctly (such verification can require 10 seconds of submission) the user must learn multiple biometric processes, as in either/or systems. This can be a challenge for both physical and logical access scenarios.

Synchronous multimodality involves the use of multiple biometric technologies in a single authentication process. For example, there are biometric systems that use face and voice simultaneously, reducing the likelihood of fraud and reducing the time needed to verify. Systems that offer synchronous multimodality can be difficult to learn, as one must interact with multiple technologies simultaneously.

6.2 Biometric standardization

Standards are market enablers as well as a sign of industry maturity. They foster widespread usage of a technology by facilitating the integration into existing applications, reducing time-to-market and the risk of individual applications. Standards offer standardized interfaces to existing technology and thus facilitate interoperability and interchangeability of the technologies involved. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC established a Joint Technical Committee 1 (ISO/IEC JTC 1) on Information Technology; then, JTC 1 setup a new Subcommittee 37 on Biometrics.

With respect to biometrics, several levels of standardization have to be involved as shown in Fig.3.

Standards addressed include BioAPI, BAPI, CDSA/HRS, CBEFF, X9.84, ANSI/NIST ITL 2000, ANSI B10.8, ICAO (SC17), biometrics and card technologies, biometrics and cryptographic systems (x.509), and M1 activities and SC37 activities (including interoperable template formats, interoperable data formats, biometric performance testing, biometric

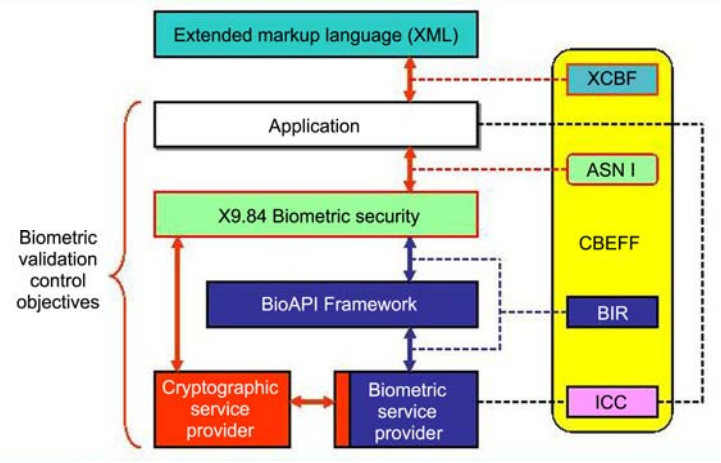

Fig.3 Standardizations with biometric architecture.

security evaluations). All those evaluations are related to definite users or biometric database and correlative protocol. Algorithm evaluation and scenario evaluation are premature testing of detailed biometric technologies that can usually be illustrated by the Receiver Operational Characteristic (ROC) curve while operational evaluation is solution/product-oriented performance testing that can only be represented by a few ratios such as False Match Rate/False Acceptance Rate (FAR), False Non-Match Rate/False Rejection Rate (FRR), etc.

6.3 Smart cards

Biometrics is an authentication technology, whereas smart cards can be a storage, processing, and/or authentication technology. The two technologies are increasingly deployed in conjunction, strengthening each other's capabilities. Typically, biometric data is stored on a smart card, matching can take place on a local PC or central server, on the reader itself, even within the smart card's internal memory. The result of a biometric match can be used to unlock a protected area of a card, such as account information, or to release a card-based PIN or certificate to an external application.

Major smart card platforms and key standards and infrastructure issues (the use of biometrics in smart card applications) are listed below:

- Java Card, Multos
- EMV, Mondex
- PC/SC, OCF
- ISO 7816-x, ISO 14443-x (contact-less)
- Cryptographic cards: Gemplus, Schlumberger, VISA Cash, Mondex, Proton
- SAM design and implementation
- Match-on-card architecture
- Card management systems and middleware
- Card issuance and lifecycles

One of the most important applications of biometrics on smartcard is the Machine Readable Travel Documents (MRTD) which is advocated by the International Civil Aviation Organization (ICAO) to ensure standardization and global interoperability of the identity confirmation process. The Technical Advisory Group on MRTD developed specifications, which have been included in the new editions of each Part of Doc 9303, aimed at governing the use of an MRTD when performing machine-assisted identity confirmation, the generic personal identification features that apply, and the locations and technologies wherein the required identity details would be recorded (or derived).

Facial recognition was selected as the globally interoperable biometric for machine-assisted identity confirmation with MRTDs because the face rated highest in terms of compatibility with key operational considerations, followed by fingers and eyes. The face has long been used by border-control authorities and airline staff at airports to confirm identity with a "photo ID". Facial recognition technology automates this process, using a camera to capture the image of the face, while a computer validates facial characteris-

tics. ICAO also has selected high-capacity, contact-less smartcard to store identification information in MRTDs--- passports, visas and identity cards.

ICAO has set the deadline of April 1, 2010, for all 188 State Members to adopt a worldwide, standardized biometric-enhanced passport. Currently about 45 countries have already been issuing this kind of passports. Many others including China need to accelerate the steps for developing ICAO-MRTDs.

7 Concluding line

Both the biometric technology and the industry are maturing well, getting increased user-acceptance. There will be significant growth in multimodal biometrics. The outlook of biometric applications and the market are very promising. Total biometric revenues are growing at the speed of nearly 50% per year as shown in Fig. 4 according to the forecast of International Biometric Group (IBG) [4].

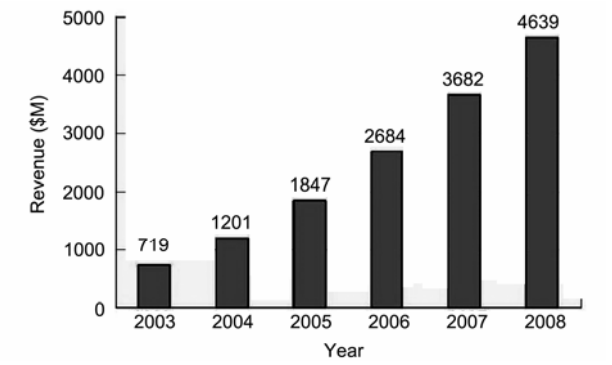

Fig.4 Total biometric revenues 2003-2008.

References

1 Bolle R, Connell J, Pankanti S, *et al*. Guide to biometrics, Springer, November 6, 2003

2 Ashbourn J, Practical biometrics: From aspiration to implementation, Springer; November 18, 2003

3 Nanavati S, Thieme M, Nanavati R, Biometrics: Identity verification in a networked world, Wiley; March 15, 2002.

4 International Biometric Group (IBG), http://www.biometricgroup.com