Biometrics ‘Big Brother Exposed’

Michael McKenzie, Marbyte Limited, MikeMck37@aol.Com

Hossein Jahankhani, School of Computing & Technology,
University of East London, h.Jahankhani@uel.ac.uk

Abstract

This project will investigate the development of biometrics as a viable security approach to counter terrorism and identity fraud. Related issues on privacy, performance assessments, deployment and standardization are discussed. Finally; the future directions of biometric systems development are explored.

Introduction

The explosion of interest in and use of biometrics technology is the quest for an ever more efficient and fraud proof means of authentication. Another has been the drive for better means of identifying criminals and terrorist suspects for law enforcement reasons. Biometric technology is potentially hard to forge and it uniquely identifies a person, the contemporary solution to put to slay security frailty. Moreover biometric technologies have the advantage that they are tightly bound to the individual and cannot be easily used by an impostor.

The term “Biometrics” and “Biometry” is derived from the words bio (meaning life) and metric to (measure) that have been in use since the early 20th century. Biometrics is divided into two types: behavioral (the traditional signature and voice) and physiological (face, fingerprint, hand, and iris recognition).

It is evident that biometric solutions are finding places in various industries due to a litany of reasons ranging from ease of use to stronger security. However there is an enormous debate over the accuracy and benefits as well as the intrusive nature of some biometric technologies into people's privacy. Furthermore there is an element of uncertainty to this new approach; the question could be raised that companies or government agencies may have a hidden agenda to use these same monitoring technologies to monitor the private lives of law-abiding citizens? Password and personal identification numbers can be illicitly acquired by direct covert observation by an intruder. There is no way of linking the usage or service to the actual user thus there is no means of protection against repudiation by the user identification owner. Passwords are by far the most used and most easily subverted method of personal authentication. This type of authenticity can be compromised in many ways, it can be forgotten, or carelessly written down on a yellow- post it note. The Smart card on the other hand uses methods that identify the user by a possession of a physical object that is unique to that user, or group of users. These are usually encoded with information used in the authentication process on a magnetic strip, a bar code, or a chip. However this can be easily exploited, be lost, forgotten, stolen, given away, or duplicated. Both methods may be used independently or in conjunction with one another, to further increase the security level of the system.

There are a multitude of information security and authentication technologies to choose from and the selection process is often overwhelming to the customer. Selecting the right authentication technology or a combination thereof is indeed a complex matter. The decision in terms of functionality occurs on different levels. The following chart shows the different levels and one possible decision path see fig. 1.

The key to a successful selection is flexibility and modularity; there is simply no single path - technology, biometrics, algorithm, interface or sensor - that works for all.

One of the main drawbacks is that biometric as a contemporary solution is not clear enough to meet the needs of the companies’. They need biometric solutions that can be delivered quickly and can be easily installed.

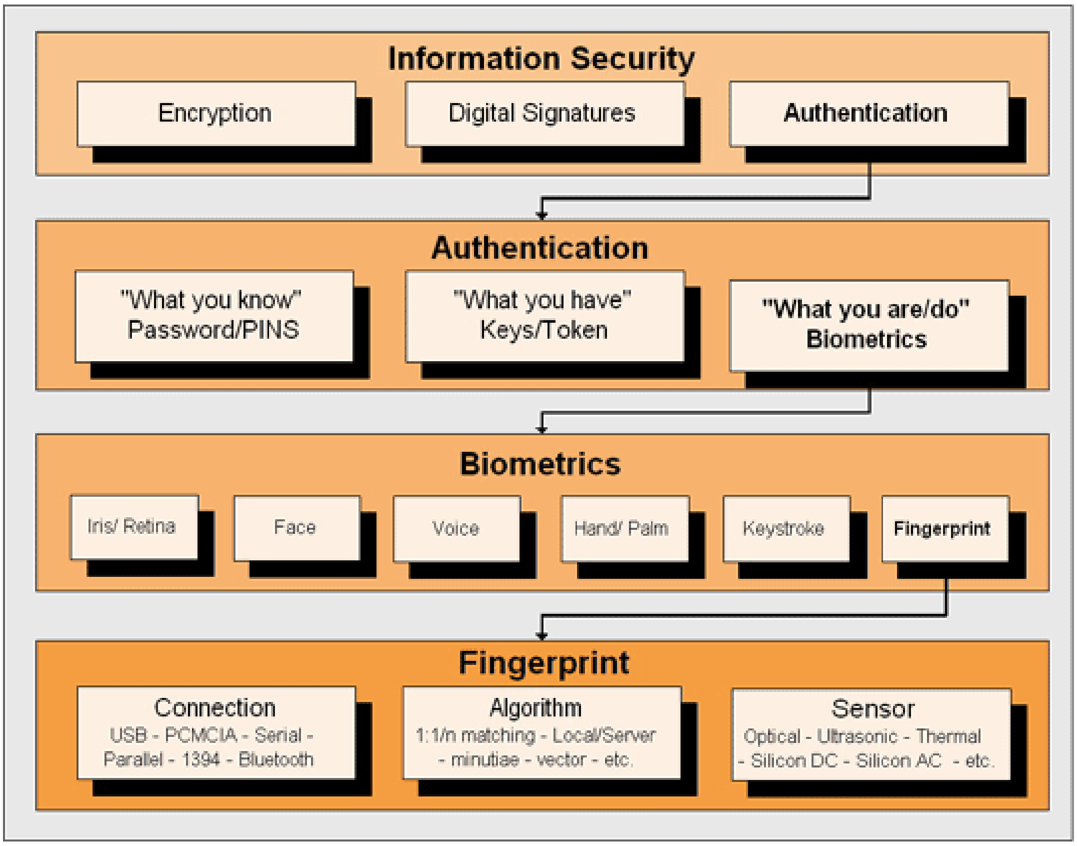

Information Security
Encryption
Digital Signatures
Authentication
Authentication
"What you know" Password/PINS
"What you have" Keys/Token
"What you are/do" Biometrics
Biometrics
Iris/ Retina
Face
Voice
Hand/ Palm
Keystroke
Fingerprint
Fingerprint
Connection
USB - PCMCIA - Serial - Parallel - 1394 - Bluetooth
Algorithm
1:1/n matching - Local/Server - minutiae - vector - etc.
Sensor
Optical - Ultrasonic - Thermal - Silicon DC - Silicon AC - etc.

Fig. 1 Various types of information security showing one possible decision path
Source: Adopted from iosoftware.com [5].

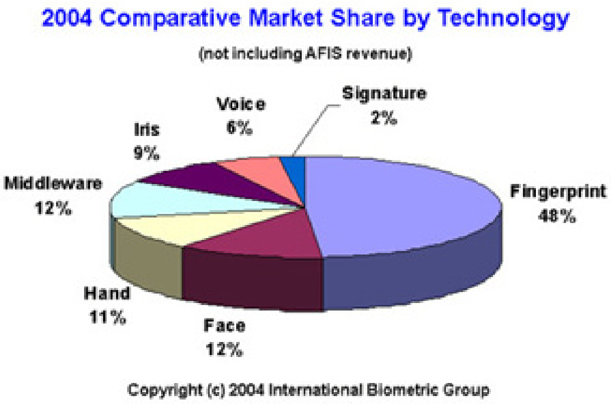
Companies require a biometric solution that is compatible with existing infrastructure this will streamline cost when integrating biometric solution. Previous deployments that have been incompatible with the existing infrastructure have eradicated the companies IT budgets during development process therefore it is imperative to have the right biometric solution that is ready to be deployed with minimum in house development work.

Choosing the right technology

In the course of a year, millions of individuals pass through check-in desks at a large domestic or international airport, and many millions more pick up and drop off friends, family, and co-workers. In comparison, the set of airport employees is relatively small and constant therefore it is important to determine the right type of biometric technology used to authenticate the identities of people within these two different groups. For example, fingerprint/hand scanning can be use to identify/authenticate a relatively small flow constant group of employee at a control access point. Similarly, another usage for the finger scanning technology is to have the device built into a computer mouse (biometric mouse) with the software support for network security logons. However this will be expensive as it has to be implemented on to several computers [6]. Conversely, the advantage of voice recognition software is that it is centralized and able to support and manage up to several secure logon machines. Undoubtedly, face recognition has an overwhelming advantage over other biometric technologies, by being a touch-free biometric, and allies itself more easily with the human element of intelligence.

Until recently the only way to attack security problems was adding expensive screening and administrating procedures steps include maintaining accurate databases, reviewing identity documents and administrating password systems these methods have proven to be too costly and can be easily overcome by impostor. Biometrics offers more effective low cost solution that streamlines these conventional methods. Biometric Technology may be used to provide new services while maintaining high security, there are a number of vertical markets using biometrics such as government department deploying biometrics in passports national identification cards voter card and driving licenses. During the past ten years the science of biometrics has matured some what into an industry that offers real world solution to security problems [8].

Below is a comparative market share amongst the biometric technologies in 2004 which is compiled by the international biometric group.



Biometric comparative market share showing finger scanning as the current leaders.

Source: Adopted from the International Biometric Group [7].

Types of Biometric System and Processes

There are two distinct of phases of operation for biometric systems; they are enrolment and verification /identification. The template is created during enrolment process, the enrolment process may require the individual to provide multiple instances of biometrics trait for example, the unique identifier may be scanned or copied three or four times for comparison or to create a composition comparison template. Identification commonly defined as a one-to-many (1:N) matching of a single biometric sample set against a database of samples, this entails that the users biometric trait is matched against all previously enrolled samples. Scores are generated for each comparison, and an algorithm is used to determine the matching record, if any. Generally, the highest score exceeding the threshold results in a match. The most comprehensive usage of these application devices occurs within the law and enforcement agencies in order to identify criminals and passport fraud. Finally verification is defined as a one-to-one (1:1) matching of a single biometric sample set biometric identifier record against another; this could be placing your finger on the touch pad or looking into the lens of the camera. Generally, the first sample is newly captured and the second is the enrolled identifier on file for a particular subject. The file sample is retrieved from the database based on a unique subject identifier such as a User ID. In a user authentication environment, a score exceeding the threshold would return a ‘match’, resulting in the authentication of the user. A score below the threshold would return a ‘no-match’, resulting in the denial of access.

An important issue for the acceptance of biometric technologies is to measure the performance of individual biometric technologies in a credible and objective way; this is done through the use of sensors and algorithms. Matching is always based on probability, and the accuracy is generally measured by establishing the values for the following four criteria: FRR (False Rejection Rate), FAR (False Acceptance Rate), FER (Failure to Enrol Rate), and ERR (Equal Error Rate). These rates are usually expressed as events per 1,000 or 10,000 uses therefore each biometric technology would need to adopt the following condition [1, 2, 3, 4, 10].

False Rejection Rate and False Acceptance Rate are complementary in determining how stringent a biometric device is in allowing access to individuals. As a result, biometric devices include features to allow for variable threshold or sensitivity settings for each biometric technology and solution intended. For example, if the false acceptance rate threshold is increased to make it more difficult for impostors to gain access, it also will become harder for authorized people to gain access. As FAR goes down, FRR rises. On the other hand, if the false acceptance threshold is lowered as to make it very easy for authorized users to gain access, then it will be more likely that an impostor will slip through.

Vendors usually provide a means for controlling the threshold for their system in order to control the trade-off between FRR and FAR. The Equal Error

Rate (EER) is the threshold level for which the FAR and the FRR are equal [9]. The EER is often quoted as a single figure to characterize the overall performance of biometric systems. From the tests carried out on finger, voice and face scanning it is evident that luminescent lighting, time and positioning of the face will affect the performance and accuracy of face recognition between different face acquisitions of the same image. Additionally, for voice recognition to remain optimal, the same handset, speaker and telephone number is needed for performance and accuracy to remain constant over a set time. Finally, finger scanning device must ensure that the scanning plate is kept clean so as to provide the necessary quality and standard to help reduce both false and accept error rates. Another area of concern is the high error rate that comes with the different fingerprint impressions from the same finger; this could prove to be problematic for all permissible users.

It is important to note that some techniques, such as retinal scanning or finger print recognition, may offer high accuracy especially retina scanning whose accuracy is second to none, has a high data collection error rate and low user acceptability in both cases their deployment may not be appropriate for some applications. This is due to the high level of co-operation required by the user or the social or psychological factors that may prove unacceptable to potential users. Psychological factors include fingerprints, hand geometry, eye patterns, and facial features. Both voice and face recognition is considered to be easy to use and normally acceptable by potential users. However, their accuracy is currently less than some other biometric technologies, especially in unconstrained environments such as where the background sound and illumination is variable.

Performance of a verification system uses the False Reject Rate (FRR) and the False Accept Rate (FAR). The perfect biometric system will produce zero error rate on both FAR and FRR measurements. On the other hand, if the system denies everyone the false-rate will be one and the false accept will be zero. Typically, systems operators can adjust a system parameter to achieve the desired FAR & FRR. Typically it is true to say that the desired measurement depends on the application and not the biometric device deployed. For a bank’s ATM, where the concern may be to avoid irritating permissible customers the FRR should be set low, on the other hand for a systems that provide access to secure area then the FAR should be of overriding concern. Typically biometric devices uses different FAR therefore it is difficult to compare systems that provide performance measurement [11].

Standardization

In recent years, a lot of time and effort has been spent to put together a set of standards for the integration of biometric technologies in the form of Application Programmers Interfaces (APIs). The quest to hide the unique aspects of individual biometrics types is now forthcoming. The task of the API is to provide a generic interface between a software application that uses biometric technology and the technology itself. A set of standards was drawn up known as the Common Biometric Exchange File Format to help describe and interchange a set of data elements necessary, to support biometric technologies in a common way independently of the application (e.g., mobile devices, smart cards, protection of digital data, biometric data storage)[11].

The set of standards ensures system integrators that the pervasive adoption of biometrics science will no longer be locked into a single biometric technology, vendor, or product. Conversely some system integrators undergo extensive evaluations to be sure they pick the right biometric, and others adopt a wait and see approach.

A standard API would allow an integrator to go forward with a tentative selection and programming facilitated by the API. Should the integrator later decide that another biometric would be more suitable, it could be substituted with minimal changes to the calling application. In addition to allowing substitution of biometrics, a common API would also provide for leveraging of a single biometric technology across multiple applications as well as allowing one application to integrate multiple biometric technologies using the same interface [11].

Human Authentication Application Programmers Interface- HAAPI

The Human Authentication API was first introduced at the Tenth US Biometric Consortium meeting in December 1997. The specification was originally developed by the National Registry Inc. under contract to an agency of the US Department of Defence. The API was then placed in the public domain in hopes that the adoption of a generalised biometric API would lead to the interchange of biometric technologies and encourage the widespread distribution of biometrics in general.

The HA-API attempts to hide, to the degree possible, the unique features of individual biometric types and products by providing a toolbox of biometric functions, which is accessed via a standard interface. The HA-API supports the deployment of multiple and layered biometrics and both local and server based verification. Currently, HA-API is defined for the Microsoft Win-32 environment, with plans to expand it to other environments. The HA-API specification has 11 function calls in 3 categories, as follows:

- **Biometric Technology Functions**. There are many tasks carried out by the biometric technology function one of which lists the biometric devices i.e. (finger scanning iris scanning, face technologies etc) installed on a system. Another identifies which specific biometric technologies are available for use by the application. Additional function is used to initialize or release the biometric technologies. Furthermore the biometric technology that was released can subsequently be used again by calling the getBio function.
- **Biometric Authentication Functions.** This function captures raw biometric data, specified by the Biometric technology. A sub function of biometric authentication functions carry's out the tasks of processing the raw biometric data captured indiscriminate of its size. The raw data captured differs per technology, for example: Finger Imaging could be – a raw greyscale finger image; Facial Recognition could be a video image of a face; Speaker Verification could be a digitized speech waveform. The resulting biometric identifier record contains processed data and data size. The authentication functions also summarize the functionality of Capture, Process, and Verify in a continuous manner until a match is found or a timeout is reached. Another task includes enrolment and batch enrolment, which is facilitated by a wizard that provides the means for the application to ensure a successful enrolment.
- **Biometric Utility Functions.** Biometric Utility Functions include the interface for the application developer to get and set parameters specific to a biometric device and releases memory used by a previous biometric function. The Utility function also displays the biometric properties dialog box, if it is available, to read and set parameters, which are specific to a biometric and their input devices [12].

This technology must be entered in the registry to make the HA-API aware of its existence. To register a technology, a vendor must first generate a unique biometric identifier (BUID). The BUID is a 128 bit Global Unique Identifier (GUID). This value, along with the technology module (BSP) name and the technology name, must be stored in the system registry.

Standards currently under development

- Project 1603 ANSI/INCITS 395-information Tel-signature/sign image based interchange format for Data Interchange.
- ANSI/INCITS (M1/103-0620) -information technology -hand Geometry Format for Data interchange.
- ANSI/INCIS (M1-03-0351) Information Technology-biometrics performance Testing and reporting standard.
- Recommendation for Electronic Authentication based on draft NIST special publication 8000-63.
- ANSI/INCCITS 358-2002 information technology _ BIOAPI SPECIFICATON.
- Federal information Processing standard (FIPS) -FIPS 197 advanced encryption standard (PES)-November 2001.
-

Source: www.ncits.org/tc-home/m1.htm(docs/m1 docreg.htm [14].

Discussion and Conclusion on the future of biometrics

The European Commission has produced draft regulations to introduce, by 2005, biometric data (fingerprints and facial images) on visas and resident permits for non-EU nationals. The information would then be stored on national and EU databases that will be accessible through the Visa Information System held on what is called the Schengen Information System.

Perhaps it could be argued biometrics has little to do with combating terrorism and a lot to do with the demands of the law enforcement agencies for the surveillance of individuals where everyone is a suspect. Nevertheless, there are areas that need to be addressed such as cost in card production and the need for specialist readers, for registration. The worry of rejection rate, privacy advocacy groups advocating their concerns about who will be allowed access to the ID card database and Scalability, the use of biometrics on this scale has never been attempted before.

Against these motivations for tight social control, and an efficient identification scheme to support it, it is necessary to balance the interests of individuals in the various aspects of civil liberty. Analyzing the very principle of our democratic society's there is noticeable excessive and overall surveillance which cannot be accepted for long, as private spaces in which people can move around freely from intrusions are being rapidly invaded by data surveillance technologies. These are the burning issues of concerns involving the deployment of biometrics and also in the light of international acknowledgment can compromise personal data and privacy principle as well as other fundamental values in our democratic societal order.

One further aspect that our attention must be drawn to is how foolproof is biometrics? Biometrics work well only if the verifier can verify two things: one, that the biometric came from the person at the time of verification, and two, that the biometric matches the master biometric on file. If the system can't do that, it can't work. Let's draw your attention to performance indicator namely the FAR and FRR error rates, an important barrier to active and passive biometrics technologies. A false negative rate of even one percent could allow at least one bad person to board a jet flight. Conversely one percent false positive rate could result in one innocent person on every flight being falsely matched to someone in a database of suspicious people. Another drawback is that optical scanners can't always distinguish between a picture of a finger and the finger itself, and capacitive scanners can sometimes be fooled by a mole of a person's finger. Furthermore this may seem bizarre but which cannot be dismissed is the possibility that people may mutilate other people's body parts in order to use someone else's biometric identity for criminal purposes, for example, access to money, or buildings. We may have hygiene issues; the need to place a hand or finger on a sensor plate can prompt fear about the spread of disease a requirement that makes some people uneasy. Viewing privacy as a human right not only reflected in the European Data Protection Directives 95/46/EC and 97/66EC or in Article 8 of the European Convention on Human Rights it is dealt in a wide range of areas and circumstances which includes video surveillance, telephone interception and bugging.

Today's solution for tomorrow problems

The pervasive nature of biometric is becoming more noticeable in critical areas such as homeland security, finance and banking. The following are today's solutions being developed or under discussion for deployment.

Heathrow will be the first UK airport to carry out a large-scale trial of the iris recognition technology the aim is to speed up the movement of passenger through the terminal and detect illegal immigrants. It is reported that a Rap Scan Secure 1000 body scanner, a low-energy X-ray that goes beyond today's metal detectors by beaming through a passenger's clothes to reveal the outline of foreign objects next to their skin. It can detect metal, as well as anything inorganic. A school in Sunderland plans to use a retina scanning device to charge student for lunches in an attempt to make the school cashless and protect poor children who receive free food from being ridiculed. Bank of Tokyo Mitsubishi reported that it will introduce a new biometric security system for cash machines which can identify customers from the pattern of veins in their hands. A credit card sized passport with biometric chip to be developed as a prototype ID card, the trail to determine technical solutions and business case by mid 2004. The UK Passport Service is to develop a passport book that stores biometric details of the passport holder. A chip will contain a digitized photograph to improve security a six month roll out is due in 2005.

The content of this project is extremely general, for this reason the project did not delve deep enough into the theoretical and practical aspects of FAR and FRR these are widely used methods to measure accuracy. Additional, more research was needed to establish a standard way for comparing two products of biometric authentication in an unbiased way. Also there is a pressing need to expedite the process of standardization for both testing and the deployment of biometrics technology hence leverage security to counter real world security problems in both finance and homeland security sectors. Finally, addressing the issues surrounding biometrics and the effect it has on privacy we must accept that both are not conflicting aims but parallel goals worth fighting for.

References

1. Ashbourn, J M (Oct 2000), '*Biometrics: Advanced Identify Verification: The Complete Guide'*, Springer Verlag.

2. Phillips, P.J. et al., (1998), '*The Feret Evaluation Methodology for Face-Recognition Algorithms,'* NISTIR 6264, Nat'l Institute of Standards and Technology.http://www.itl.nist.gov/iaui/894.03/pubs.html#face.

3. Wayman, J, Jain, A, Maltoni, D & Maio, D (July 2004), '*Biometric Systems: Technology, Design and Performance Evaluation*', PaperBack, Springer Verlag.

4. Yen, et al, (2002),'*Biometric authentication: assuring access to information'*,Information Management & Computer Security, volume 10, No. 1.

5. www.iosoftware.com./(accessed 10 Dec 2004).
6. http://www.biometritech.com/features/shen031903.htm (accessed 15 Mar 2004).
7. http://www.biometricgroup.com/reports/public/market_report.html (accessed 21 Apr 2004).
8. http://www.datastrip.com/ (accessed 15 Mar 2004).
9. Golfarelli, M, Maio, D & Maltoni, D (1997)'*On The Error-Reject trade off in Biometric Verification Systems*', IEEE Transactions on Pattern Analysis Machine Intelligence, Vol. 19, No. 7, pp. 786-796.

10. Egan, JP 1975 '*Signal Detection Theory and ROC Analysis'*, Academic Press, New York.

11. http://www.biometrics.org/REPORTS/HAAPI20/ (accessed 30 Mar 2004).

12. http://csdl.computer.org/comp/mags/co/2000/02/r2056abs.htm (accessed 13 Apr 2004).

13. www.statewatch.org (accessed 13 Mar 2004).

14. www.ncits.org/tc-home/m1.htm(docs/m1 docreg.htm)