Biometric Authentication

- Technology and Evaluation -

Term Project CS574
Spring 2003
San Diego State University

Uwe Bubeck **Dina Sanchez**

Contents

Uwe Bubeck: uwe@ub-net.de
Dina Sanchez: semperfi22@hotmail.com

1. INTRODUCTION

This paper presents a survey of the use of biometrics in the field of computer security, with a focus on biometric authentication. We briefly outline the historical background on concepts related to biometrics, followed by the distinction between the use of biometrics for authentication and identification, and the advantages of the use of biometrics for both processes. The main part of the paper introduces the current biometric technologies and discusses their evaluation. The last part of the paper gives an overview of the major applications and briefly lists the most important industry standards.

1.1 Historical Background

The use of Biometrics is often regarded as a groundbreaking concept, coming straight out of modern science fiction literature. Nevertheless, there are numerous historical events that prove that the idea of using physical or behavioral characteristics for identification existed in ancient civilizations as well.

The first recorded historic incident is reported to have taken place in ancient Egypt, during the construction of the great pyramid of Khufu. Faced with a huge logistical challenge, the administrators in charge of providing food supplies to the workforce devised a system, by which every worker in a unit was assigned to go to the food warehouse once a month to receive his food allowance for that month. The administrators kept records of every worker's name, age, place of origin, work unit, occupation and the last date on which the worker received his allowance. The collected data was used for verification of identity, when a worker appeared in the food warehouse to claim his allowance. As violations were discovered (some workers claimed multiple/false identities), the administrators decided to include physical and behavioral characteristics on the record as well [1].

Another interesting technique was first used in the Babylonian era, where hand imprints were used to "prove the authenticity of certain engravings and works" [1], a concept that was revisited in 1823 by the Czech Jan Evangelista Purkinje, who noticed that unique patterns were formed by sweat excreted on a persons hand [1]. This concept was further refined in 1888, by Juan Vucetich, an Argentinean police officer, who was the first to take fingerprints on ink as an identification method. 1893, Sir Francis Galton finally demonstrated that no two fingerprints are alike, even in cases of identical twins [3].

1.2 The Use of Biometrics for Authentication vs. Identification

An authentication process addresses the question of "Am I who I claim to be?" In a system that uses biometrics, a user claims an identity, then his/her biometric data is captured, and compared against data already stored in the system, to return a match (thus authenticating the user to be who he/she claims to be), or a mismatch. Controlling physical access to military facilities is one example of the applications in which biometrics is used for authentication.

An identification process addresses the question of "Who am I?" Unlike authentication, in identification systems, a user is not required to claim an identity. In this case, the user's data is captured and compared against the data stored in the system to find the closest match(es), and thus possibly reveal the identity of the user.

Biometric identification is often used in large-scale systems for surveillance or screening purposes. This poses specific challenges to data acquisition and matching performance that are beyond the scope of this paper. We will instead focus on authentication systems.

1.3 Advantages of Biometrics

Using biometrics for authentication has obvious conceptual advantages when compared to the traditional use of passwords or PINs. In theory, biometric data cannot be guessed, stolen or shared among users, therefore providing increased security to a system. It also relieves the user from the burden of having to remember a password, or worse multiple passwords for different systems within an organization [2].

In addition to authentication, biometric applications are employed in large-scale identification systems, where they offer two important benefits: **fraud detection** and **fraud deterrence**. For example, one person can claim multiple identities, using fraudulent documents, to receive benefits from a public program. Without the use of biometrics, it would be extremely difficult to discover that the person has multiple registrations, considering the large volume of data stored in the system. Biometrics can therefore contribute to fraud detection. On the other hand, the presence of such a feature in a system introduces a psychological effect on people, as it dissuades individuals from attempting to register more than once, as they become aware of the fact the their unique physiological/behavioral characteristics are used to identify them. For this effect, biometrics provides the benefit of fraud deterrence [2].

2. Current Technology

In this section, we will briefly describe the current biometric technologies and present their strengths and weaknesses. Detailed evaluation can be found in chapter 3.

It is worth noting that even though there are differences between the actual technologies, they mostly follow a common pattern. The basic processes of a biometric system are the following:

1. **Enrollment**: this is process through which the raw biometric data is captured. Depending on the technology being implemented, the data captured could be a facial image, a fingerprint, voice data, etc.
2. **Feature extraction**: in this stage, the raw data acquired during enrollment is processed to locate and encode the distinctive characteristics on which the system operates.
3. **Template creation**: a template is "a small file derived from the distinctive features of a user's biometric data" [2]. It is considered the building block of a biometric system, and in most cases templates are proprietary to each vendor and technology.

   Templates can occur in two forms:

   a. **Enrollment templates**: generated during the user's first interaction with the system, and stored in the enrollment database for future use.

   b. **Match templates**: generated during identification/authorization attempts, to be compared against enrollment templates, and generally discarded after the matching process.

4. **Biometric matching**: during this process, a match template is compared against an enrollment template to determine the degree of correlation. The matching process results in a **score** that is compared against a **threshold**. If the score exceeds the threshold, the result is a **match**; otherwise it is considered a **mismatch**. [2]

2.1 Physiological Biometrics

Finger Scan

This is a technology that uses the unique fingerprint patterns present on the human finger to identify or verify the identity of the individual.

Several acquisition techniques can be used (Details in [5]):

- optical scanning
- capacitive scanning (silicon chip)
- ultrasound scanning

This technology is very popular in the field due to a number of reasons:

- First and foremost, it is a “mature and proven core technology” [2] that has been vigorously tested, and delivers high accuracy levels.
- It is also a flexible technology that can be used in a wide range of environments.
- It has the advantage of employing “ergonomic, easy-to-use devices” [2]
- Finally, by performing multiple finger scans (of different fingers) for each individual, the system’s ease of use can be increased.

Nevertheless, the finger-scan technology has some weaknesses that prevent it from being useful in certain applications:

- It has been discovered that “most devices are unable to enroll some small percentage of users” [2]. This is attributed to hardware limitations as well as physiological reasons for special population groups.
- It has been reported that in systems which use the finger scan technology, performance generally tend to deteriorate over time (for example, fingerprints can change due to aging or wear or tear) [2].
- The last drawback is of a psychological nature. Since finger printing has always been used by law enforcement agencies, the technology is often “associated with forensic applications” [2].

Facial Scan

This technology is suited for both authentication and identification. It is based on the analysis of facial features and has a few strengths:

- The most obvious is that it can be easily integrated in an environment that already uses image acquisition equipment.
- It can also be used to "search against static images such as driver's license photographs" [2].
- In addition, it does not always require the user's cooperation to obtain the necessary data.

However, the technology has many drawbacks:

- The most obvious drawback is the presence of many variables which constitute an implementation challenge and which can greatly reduce the system's matching rate, for example, a change in the environment surrounding the individual, or changes in the individual's physiological characteristics.
- Also, the mere fact that the individual's cooperation is not required for gathering the data (a person's face might be scanned without his knowledge or consent), raises many privacy concerns.

Iris Scan

This is a technology based on using the unique features of the human iris for identification/authentication. So far, the technology has been successfully implemented in ATMs and is currently being promoted for desktop usage. The technology promises "exceptionally high levels of accuracy" [2], as the characteristics of the human iris maintain a high level of stability over the individual's lifetime.

Nevertheless, the challenges to the technology stem from the image acquisition process, which requires the use of proprietary devices and accurate positioning, and thus some specialized training. In addition, for some users, using an eye-based technology represents a major discomfort. [2]

Voice Scan

This is a technology that uses the unique aspects of the individual's voice for identification or authentication purposes. This technique is text-dependent, which means that the system cannot verify any phrase spoken by the user, but rather a specific phrase associated with that user's account. Voice scan is often coupled with speech recognition in systems that use verbal passwords. The processes of data acquisition and data storage represent the main obstacles to this technique. Gathering accurate voice data is entirely dependent on the quality of capture devices used and thus the absence of noise. In addition, voice data often generates relatively large templates, which constitutes a serious limitation to the number of applications this method is suitable for [2].

Hand Scan

This technology uses distinctive features of the hand, such as geometry of hand and fingers, for identity verification. Hand scan is "a more application-specific solution than most biometric technologies, used exclusively for physical access and time and attendance applications" [2]. The main advantages of this method are:

- It is based on a relatively stable physiological characteristic.
- It is generally considered to be non-intrusive from the user's perspective.

On the other hand, this technology is of limited accuracy and "the ergonomic design limits usage by certain populations" [2].

Retina Scan

This technology uses the distinct features of the retina for identification and authorization. It is considered one of the least used technologies in the field of biometrics, almost only used in highly classified government and military facilities. Even though this technique delivers very high levels of accuracy, yet its unpopularity is attributed to the difficulty of usage, in addition to the user's discomfort [2].

DNA Matching

A relatively new technology that relies on the analysis of DNA sequences for identification and authentication. The technology raises many concerns over "privacy issues, invasiveness and data misuse." [2] and currently cannot be done fully automated.

Vein Identification

Another fairly new technology that uses the vein patterns on the back of the hand for identification and authentication. The technology has the potential of delivering high accuracy, in addition to the advantage of being non-intrusive to the user [2]. Vein identification has been recently implemented in commercial products, such as VeinID.

2.2 Behavioral Biometrics

Signature Scan

This technology uses the human written signature for identity verification. This technique is non-invasive to the user and flexible in the sense that it can be changed by the user (unlike most of the other biometric technologies), yet the error rates can be very high due to inconsistencies in one's signature [2]. This static analysis can be extended to incorporate dynamic features (e.g. velocity, acceleration, pressure), claiming increased accuracy and reduced privacy concerns [4].

Keystroke Scan

This technology uses a person's distinctive typing patterns for verification. This technique is combined with the traditional password scheme for increased security. It doesn't require any special hardware for data acquisition, since all data is gathered from the keyboard. Furthermore, the process is practically invisible to the user, since the user is merely asked to type his/her password. In addition, the technique is highly flexible, as it accommodates to password changes [2].

However, the method is fairly new, and the underlying concepts have not been fully developed. In addition, keystroke scan inherits all the flaws of password-based systems [2].

Gait Recognition

A technology based on the analysis of the "rhythmic patterns associated with walking stride" [2]. This is another new concept, currently under development.

3. EVALUATING BIOMETRICS

3.1 Motivation

Over the last 3-5 years, the biometrics industry has seen an enormous growth. In particular, the call for more security following the events of September 11, 2001, has created a big hype in biometric technology. This has led to the development of a variety of different methods and even more vendors waiting for customers. Those, however, seem to be reluctant to invest in a technology that is still emerging and therefore features a bewildering diversity of products and companies. As a recent article in the Washington Business Journal brought it to the point, "biometrics is the next evolution in security, but it's a very fragmented industry, with lots of companies trying different things" [6].

Comparative testing can provide valuable orientation. Considerable research has been conducted recently on developing standardized biometric evaluation methodology to reflect real-world performance. The most active research organizations in this area are:

- The “UK Biometrics Working Group” (BWG)[1], a UK governmental organization, has developed the widely recognized “Best Practice” standards for testing and reporting on biometric device performance [7].
- The “International Biometric Group” (IBG)[2], an independent consulting firm, has conducted comparative biometric testing since 1999 [10].

We will give an overview of the techniques developed and discuss actual test results for various biometric systems.

3.2 Metrics and Performance Criteria

Just as in other areas of computer security, vendors of biometric systems are constantly promising near-perfect security. Adverts are full of technical buzzwords and good-looking performance values. For example, a renowned vendor of fingerprint sensors claims on his website that his “sensor achieved 0.0% false acceptance and 0.0% false rejection rates”. Sounds great to the unaware customer, but the following definitions will soon allow us to understand the exact testing conditions (they were described on a separate web page) and reveal that those numbers are not as impressive as they seem at first glance.

[1] UK Biometrics Working Group Website: http://www.cesg.gov.uk/technology/biometrics/

[2] International Biometric Group Website: http://www.biometricgroup.com/

The following three key metrics are commonly used to assess the performance of a biometric authentication system (definitions according to [7]):

- The **False Match Rate (FMR)** is the probability that the system will match a user's verification template with a different user's enrollment template. It can be understood as the likelihood of an impostor being recognized as a legitimate user. In general, this is the most critical accuracy metric, as it is imperative in most applications to keep impostors out.
- The **False Nonmatch Rate (FNMR)** is the probability that a user's verification template is not matched with his enrollment template. So it is the likelihood of a legitimate user not being recognized as such. While not as critical as the FMR, high false match rates can still lead to lost productivity or user frustration.
- The **Failure-to-Enroll Rate (FTE)** denotes the probability that the system will not be able to extract distinctive, consistent and replicable characteristics from the sample presented during the enrollment process, i.e. this is the likelihood of the system being unable to create an enrollment template for a new user. This might have behavioral reasons, e.g. user moving during data acquisition, as well as physical reasons, e.g. faint patterns because of wear or aging.

In the event of a false nonmatch or a failure to enroll, it is likely that the system will offer to retry a number of times. Analogously, an impostor is likely to try again after a failed attempt to get access. It is therefore useful to extend the metrics presented above to reflect the possibility for a final error after multiple attempts (a complete transaction). According to the "Best Practice" testing standards [7], three attempts should be allowed and the following naming conventions be used: the extension of the FMR is usually called the **False Acceptance Rate (FAR)**, the extension of the FNMR is the **False Rejection Rate (FRR)** and the extension of the FTE is the **System Failure-to-Enroll Rate**. The latter two present a biometric system in a better light, whereas the first one will reveal a higher error rate.

Modifications to the parameters of the system, especially the threshold value, allow to lower either FMR or FNMR – unfortunately not both at the same time, as research conducted by the BWG [9] has shown there is an inverse relationship between the two criteria. This is why many available systems tolerate enormous false rejection rates just to keep the false match rates as low as possible. For many applications of biometrics, this is not a problem, as it is often possible to find a suitable balance between susceptibility to false matches and false nonmatches. However, especially some of the more popular possible areas of application, like the financial sector, are quite susceptible to both. This has been a definitive knockout for many experiments with biometrics and has caused the technology to lose credibility in the eyes of potential customers.

3.3 Evaluation Methodology

Biometric characteristics may change over time. For many technologies, this is a major challenge and can lead to dramatic increases in false nonmatches. The IBG tests [10] are therefore broken into two parts: a first round (called the primary visit) immediately after enrollment and a second round (second visit) under identical test conditions, but after a time of six weeks.

We can now demystify the initial example of a vendor claiming 0.0% false acceptance and 0.0% false rejection rates: a couple of mouse clicks away from the product description, they reveal on a separate web page that those numbers were achieved in IBG's primary visit test. Furthermore, as we already know from the last section, false rejection means a false nonmatch after up to as much as three attempts. And all of a sudden, those numbers have largely lost their impressiveness. Nanavati/Thieme [2] bring it to the point with the following conclusion: "Verifying a user immediately after enrollment is not highly challenging to biometric systems. However, after six weeks, testing shows that some systems' error rates increase tenfold."

Depending on the actual technology used, biometric systems are more or less sensitive to environmental changes. Comparative testing therefore has to follow very strict protocols to ensure that all systems are evaluated under equal conditions. Furthermore, systems tend to be susceptible to changes in user presentation. For real-world performance testing, it is important to randomly select a volunteer crew that reflects the user population for the anticipated area of application, including users which are unfamiliar with enrolling and verifying on biometric systems, or even scared. Different ethnic and age groups should also be represented. This is not always easy, as BWG admit in their test report [9].

3.4 Test Results

Based on the criteria and methodology presented in the previous sections, the BWG has conducted a large-scale comparative test [9]. Over a period of 3 months, a volunteer crew of slightly over 200 participants has used authentication systems based on 7 different biometric technologies in a normal office environment. The test was back in late 2000, but it is still widely referenced in the biometric community. To our knowledge, there have not been any more recent (and publicly available!) tests that incorporate a comparable diversity of technologies.

Except for retina scanning (which, because of its difficult acquisition process, is mainly limited to military use) and DNA matching (which currently cannot be done fully automated and is still in experimental stages), all physiological biometrics presented in chapter 2 have been tested.

In the following, we present the most important results. The data is cited from the final test report [9]. For more detailed results and an exact description of test scenario and methodology, please refer to the report.

System	**Failure-to-Enroll Rate**
Face	0.0%
Fingerprint – Chip	1.0%
Fingerprint – Optical	2.0%
Hand	0.0%
Iris	0.5%
Vein	0.0%
Voice	0.0%

Table 1: Failure-to-Enroll Rate (Source: [9])

System	**FAR 0.001%**	**FAR 0.01%**	**FAR 0.1%**	**FAR 1.0%**
Face	–	FRR 40%	FRR 30%	FRR 15%
Fingerprint – Chip	FRR 2.7%	FRR 2.3%	FRR 2.1%	FRR 1.7%
Fingerprint – Optical	–	FRR 16%	FRR 12%	FRR 10%
Hand	FRR 13%	FRR 9.0%	FRR 1.2%	FRR 0.25%
Iris	FRR 0.25%			
Vein	FRR 13%	FRR 13%	FRR 12%	FRR 10%
Voice	FRR 12%	FRR 4.5%	FRR 0.5%	–

Table 2: FAR vs. FRR, 3 attempts (Source: [9])

We can conclude that iris scanning and capacitive fingerprint systems achieve good overall performance. Unfortunately, those technologies appear to have the highest failure-to-enroll rates. One percent does not seem to be much, but in a company with 500 employees, it means five of them won't be able to enroll – an alternative authentication method would have to be provided, raising cost and potential security problems. It will be interesting to see whether improved acquisition devices and algorithms will be able to overcome this problem in the near future.

3.5 Overcoming Biometric Systems

In the past, researchers have focused on analysing the accuracy of authentication achieved by biometric systems. Technologies have improved over the years, and some of them are already able to combine reasonable accuracy with acceptable ease of use. It has therefore become more likely that an attacker will try to get around the biometric system itself or to overcome it.

With buzzwords like "Live and Well" Detection, the industry tried to disperse doubts. In May 2002 however, two interesting articles appeared:

- T. Matsumoto, a Japanese mathematician (!), demonstrated how to fool fingerprint devices with artificial gelatine fingers [11].
- The renowned German computer magazine c't featured an article on fooling a variety of different commercial biometric devices using simple tricks. Although only intended for the print edition of the German-language magazine, this article has stirred so much interest worldwide that it was translated into English and made available on the web [12].

Both of them are based on rather informal studies, but can nevertheless be considered scientific. In the following, we present some of the most astounding results.

c't identifies three different attack scenarios:

- Presenting artificially created samples to the regular sensor
- Eavesdropping the communication between the sensor device and the system (e.g. using USB sniffers or hardware analyzers)
- Exploiting poorly protected template databases

The first scenario has proven to be the easiest und most successful. But the other two can help to obtain the data required to create an artificial sample. It has turned out that poorly protected databases are surprisingly common, even for expensive systems. If the attacker has already access to the system (but perhaps on a lower privilege level), he might be able to read templates belonging to other users. Especially for privacy concerns, the industry has always denied that it is possible to reconstruct sufficient sample data from an enrollment template. In practice, however, this is possible for some systems.

Matsumoto and c’t found even easier ways to get sample data belonging to other users and to “fool” several technologies:

- The **capacitive fingerprint scanners** in the test allowed an attacker to restore latent images on the surface of the scanner using graphite powder and adhesive film. This technique also allows to capture residual fingerprints on other objects. Matsumo managed to produce gelatine fingers out of the captured fingerprints. Using these gummy fingers, he was able to fool 11 different types of fingerprint systems.
- **Face recognition** systems could be fooled by displaying (secretly captured) photos or video clips on a notebook screen presented to the camera. Even systems that claimed to have “live detection” could be taken in by video clips.
- **Iris Systems** were fooled using a high-quality photo of a human iris printed on special paper. A hole was cut in the middle, and the attacker held the photo in front of his eyes, such that his own pupils were visible through the hole. That was sufficient to overcome the “live detection” of the tested systems.

What’s amazing about those results is that the attackers used very easy and inexpensive means – no cut off fingers or artificial eyes, as shown in Hollywood movies. Vendors were quickly to point out that the systems tested were not high-security devices. Nevertheless, some of them came with hefty price tags, so one should expect them to be resistant to attacks like these.

What can we learn from those discoveries? As in other areas of computer security, we have to consider the security of a biometric system as a whole. The most sophisticated algorithms and technologies are useless if communication channels, template databases or acquisition devices itself are not resistant to attack.

If a conventional password-based authorization system happens to be compromised, it is possible for users to start over again on a clean system with new passwords. In a physiological biometric system, you cannot simply get a new fingerprint or a new iris! This is a major concern and explains why templates and the original biometric data need the highest possible degree of protection.

4. BIOMETRIC APPLICATIONS

According to the International Biometric Group's "Biometric Market Report 2003-2007" [13], total biometric revenues are likely to reach the magic number of $1 billion in the year 2003. In this chapter, we give a brief overview of this rapidly growing market.

Biometric applications can be categorized in horizontal categories as well as vertical markets. Biometrics are most frequently used in the following horizontal categories ([2], [13], in descending order of estimated annual revenues generated 2003-2007):

- **Citizen Identification:**
  identify/authentify citizens interacting with government agencies
- **PC / Network Access:**
  secure access to PCs, networks and other computer resources
- **Physical Access / Time and Attendance:**
  secure access to a given area at a given time
- **Surveillance and Screening:**
  identify/authentify individuals present in a given location
- **Retail / ATM / Point of Sale:**
  provide identification/authentication for in-person transactions for goods/services
- **E-Commerce / Telephony:**
  provide identification/authentication for remote transactions for goods/services
- **Criminal Identification:**
  identify/verify individuals in law enforcement applications

In each of those applications, biometric systems can be used to either replace or complement existing authentication methods.

The key vertical markets are the following ([13], in descending order of estimated annual revenues generated 2003-2007):

- **Government Sector**
- **Travel and Transportation**
- **Financial Sector**
- **Health Care**
- **Law Enforcement**

Among the technologies, finger scan is the undisputed leader with more than 50% market share (Source: [13]):

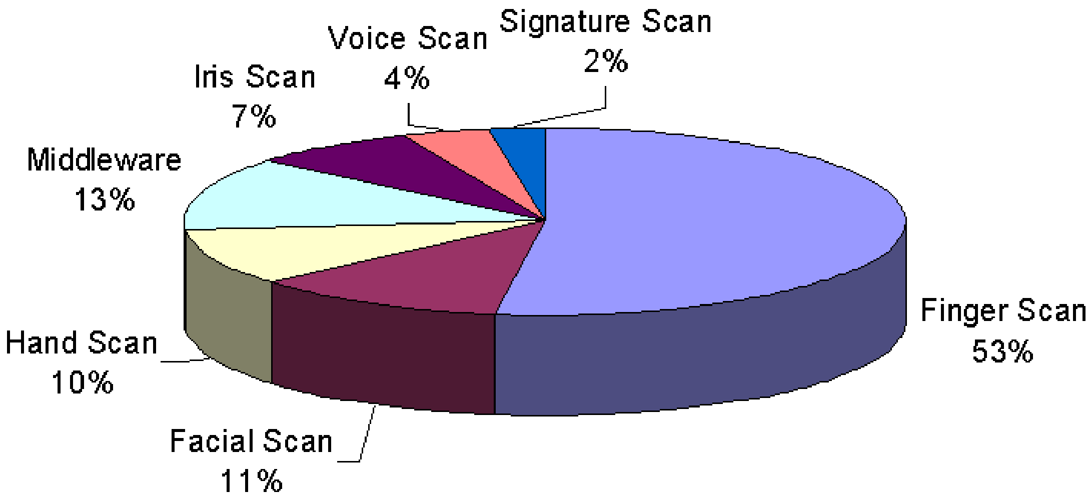

Figure 1: 2003 Market Share by Technology (Source: [13])

5. STANDARDS

Recently, the computer industry leaders have dedicated serious efforts to create standards for the fields of biometrics. The lack of standards, which forces companies to adhere to a certain technology, is regarded as one of the main reasons that biometric applications have not been widely adopted in business environments. The availability of an industry standard would allow software vendors to develop so-called biometric middleware which could use a variety of data input devices, even combining multiple technologies into one platform.

5.1 BioAPI

BioAPI is a consortium formed by 50 organizations in 1998 to "develop a widely available and widely accepted API that will serve for various biometric technologies".[3] As stated on the BioAPI consortium website (http://www.bioapi.org), the goals of the BioAPI are to:

- Work with industry biometric solution developers, software developers, and system integrators to leverage existing standards to facilitate easy adoption and implementation.
- Develop an OS independent standard.
- Make the API independent of biometric details.
- Support a broad range of applications.

Earlier standardization efforts such as BAPI (Biometric API) and HA-API (Human Authentication API) have merged into BioAPI by March 1999 [14].

Version 1.0 of the specification was published in March 2000, and version 1.1 of both the specification and the reference implementation was released in March 2001. BioAPI is now an ANSI Standard ANSI/INCITS 358-2002. Recently, vendors have started rolling out products that are BioAPI compliant.

[3] http://www.bioapi.org/index.html

5.2 CBEFF

The Common Biometric Exchange File Format (CBEFF) is a result of the collaboration of the National Institute of Standards and Technology (NIST) and the Biometric Consortium, as both organizations sponsored a workshop in February 1999 to define standardized template formats. During this workshop, “the participants identified the need for a “technology-blind” biometric file format that would facilitate the handling of different biometric types, versions, and biometric data structures in a common way”[4]. As listed on the CBEFF section of the NIST website (http://www.itl.nist.gov/div895/isis/bc/cbeff/), CBEFF is intended to provide the following features:

- Facilitate biometric data interchange between different system components or between systems
- Promote interoperability of biometric-based application programs and systems
- Provide forward compatibility for technology improvements
- Simplify the software and hardware integration process

CBEFF was published by NIST in January 2001 as NISTIR 6529, and is being adopted by biometric vendors.

As reported in [15], there is a very close relationship between BioAPI and CBEFF, with CBEFF being the preferred file format of BioAPI.

[4] http://www.itl.nist.gov/di5/isis/bc/cbeff/background.htm

6. Conclusion

There's no doubt about it: biometrics has come a long way from the first experimental devices to recent commercial systems featuring a reasonably balanced combination of matching performance and ease of use.

However, there is still much to be done: customers are scared off by high failure-to-enroll and false nonmatch rates as well as incompatibilities. Furthermore, system security as a whole needs more care to be taken of.

Future improvements in acquisition technology and algorithms as well as the availability of industry standards will certainly assure a bright future for biometrics. Will this be the end of traditional password- or token-based systems? Certainly not – biometrics is not the perfect solution either, it is just a good trade-off between security and ease of use. Future security solutions will therefore be likely to feature combinations of different technologies, for example tokens and biometrics.

References

General Biometrics References

[1] Ashbourn, Julian. "Biometrics: Advanced Identity Verification".
Springer, London, 2000

[2] Nanavati, Samir et al. "Biometrics: Identity Verification in a Networked World".
Wiley Computer Publishing, New York, 2002

[3] Baird, Stephen. "Biometrics". The Technology Teacher, February 2002

[4] Jain, Anil et al. "Biometric Identification".
Communications of the ACM v43 n2, 2000

Recent Developments

[5] Kroeker, Kirk L. et al. "Graphics and Security: Exploring Visual Biometrics".
IEEE Computer Graphics and Applications July/August 2002

[6] Martin Kady II. "Sept. 11's imprint on biometrics industry still unclear".
Washington Business Journal, April 26, 2002,
URL: http://washington.bizjournals.com/washington/stories/2002/04/29/focus2.html

[7] Mansfield, A. J. and Wayman, J. L. "Best Practices in Testing and Reporting Performance of Biometric Devices". UK Biometrics Working Group, 2002,
URL: http://www.cesg.gov.uk/technology/biometrics/media/Best Practice.pdf

[8] "Biometrics for Authentication and Identification - Advice on Product Selection".
UK Biometrics Working Group, 2002,
URL: http://www.cesg.gov.uk/technology/biometrics/media/Biometrics Advice.pdf

[9] Mansfield, T. et al. "Biometric Product Testing Final Report".
UK Biometrics Working Group, 2001,
http://www.cesg.gov.uk/technology/biometrics/media/Biometric Test Report pt1.pdf

[10] “Comparative Biometric Testing”. International Biometrics Group, 2002,
http://www.biometricgroup.com/Comparative Biometric Testing –Test Plan 2.11.pdf

[11] Matsumoto, Tsutomu. “Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies”. Yokohama National University, 2002,
URL: http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf

[12] Thalheim, Lisa et al. “Body Check: Biometric Access Protection Devices and their Programs Put to the Test”. c’t 11/2002,
URL: http://heise.de/ct/english/02/11/114/

[13] “Biometrics Market Report 2003-2007”. International Biometrics Group, 2002,
URL: http://www.biometricgroup.com/reports/public/market_report.html

[14] Tilton, Catherine J. “An Emerging Biometric API Industry Standard”.
IEEE Computer v33 n2, 2000

[15] Pero, Jennifer. “Biometric standards pave the way for greater implementation”.
Government Security, July 23, 2002,
http://govtsecurity.securitysolutions.com/ar/security_biometric_standards_pave/