Biometric Authentication

Chiara Braghin
University of Helsinki
Department of Computer Science
cbraghin@cs.Helsinki.FI

Abstract

As people become more connected electronically, the ability to achieve a highly accurate automatic personal identification system is more critical. Biometric technology is a way to achieve fast, user-friendly authentication with a high level of accuracy. This presentation will highlight some of the benefits and the few limits of using biometrics for authentication. Emerging applications, both within the government and industry, will be discussed.

1 Introduction

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate automatic user identification and authentication.

Traditionally, two major types of automatic personal identification approaches [1] have been used: *knowledge-based* and *token-based*. Knowledge-based approaches use "something you know" to identify you, such as passwords. Token-based approaches use "something you have" to recognize you, such as smart cards, magnetic stripe cards and physical keys. The weakness of these systems is the fact that passwords can be forgotten, shared, or observed and tokens can be lost, stolen, duplicated, or left at home. In addition, they are unable to differentiate between an authorized person and an impostor using the token or the knowledge fraudulently acquired from the authorized person. The banking industry [5] reports that false acceptances at Automatic Teller Machines (ATM) are as high as 30 percent, resulting in worldwide financial fraud of $2.98 billion a year. MasterCard [5] alone reports over $1.2 million in fraudulent ATM losses every day.

Biometric technologies are automated methods of recognizing a person based on a physiological or behavioral characteristic. Examples of human traits physical characteristics used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. Using biometrics for identifying and authenticating human beings ensure much greater security, basing the identification on an intrinsic part of a human being. In a way, you are your own password.

Biometric techniques have been used a lot in the past for criminal identification and prison security, but since the technology is rapidly evolving, with low cost and high accuracy, it is currently in consideration for adoption in a broad range of civilian applications, like financial transaction and control access to secure areas. While biometrics is not an identification panacea, it is beginning to provide very powerful tools for the problems requiring positive identification. As the technology becomes more economically viable, technically perfected and widely deployed, we can expect biometrics to become the passwords of the twenty-first century.

The rest of this paper is organized as follows. In Section 2 we give a better definition of biometric authentication. In Section 3 we describe a biometric system. In Section 4 and Section 5 we give an overview of a selection of the emerging technologies whereas in Section 6 we list some of the current applications of the technologies described. Finally, Section 7 states the conclusions.

2 What is Biometric Authentication?

Biometrics is the science of using digital technology to identify individuals based on the individual's unique physical and biological qualities. Simply, biometrics is the technique of verifying a person's identity from a physical characteristic (i.e., fingerprint, hand print, face, scent, thermal image, or iris pattern), or personal trait (voice pattern, handwriting, or acoustic signature).

Biometric authentication can be used in two different modes:

- *biometric identification*: identifying a person from a database of persons known to the system ("Who am I?").
- *biometric verification*: authenticating a claimed identity ("Am I who I claim I am?").

3 Biometric Authentication Systems

3.1 What is a biometric system?

A biometric system is an automatic device for verifying or recognizing the identity of a person on the basis of a physiological characteristic. It can be seen as a special kind of pattern recognition system.

The database containing the expressive representation of the characteristic the biometric system is based on, can be either central or distributed. In the case of a distributed database, each individual has a magnetic or smart card in which his biometric characteristic is recorded.

The authentication process is performed in two different stages:

1. *Enrollment stage.*

   This phase is performed only once, since it inserts the specific biometric characteristic into the system database (central or distributed). During this phase three specific tasks are performed: first, the *scanning* of the biometric characteristic, then the creation of a compact but expressive *digital representation* of it, usually called a template. Finally, the template is then recorded in the database.

2. *Identification stage.*

   This phase is repeated at each transaction. During this phase, the system identify the person at the point of access. The tasks performed are three: again, the *scanning* of the biometric characteristic and the creation of an *optimized digital representation*, then the *matching* against the template(s) to establish the identity of the individual. Depending on the matching result, the user will be either accepted or rejected.

3.2 Performance measurements

The overall performance of a system can be evaluated in terms of its *storage*, *speed* and *accuracy*.

The size of a template, especially when using smart cards for the storage, can be a decisive issue during the selection of a biometric system. Iris scan is often preferred to fingerprinting for this reason.

Also the time required by the system to make an identification decision is important, especially in real-time application, such as ATM transactions.

The accuracy is critical for determining whether the system meets requirements and, in practice, how the system will respond. It is traditionally characterized by two error statistics [7]: the *False Accept Rate (FAR)* (sometimes called False Match Rate), percentage of impostors accepted, and the *False Reject Rate (FRR)* (sometimes called False Non-Match Rate), percentage of authorized users rejected. These error rates come in pairs: for each false-reject rate there is a corresponding false-alarm. In a perfect biometric system both rate would be zero. Unfortunately, no biometric system today is flawless, so there must be a trade-off between the two rates. Usually, civilian applications try to keep both rates low. The error rate of the system when FAR equals FRR is called the *Equal Error Rate* and it is used to describe the performance of the overall system. The better biometric systems have low equal error rates of less than 1%. This should be compared to the error rates in the current methods of authentication, such as passwords, photo IDs, handwritten signatures, and so forth. Often we forget how many errors can occur in these types of systems.

In *On the Error-Reject Trade-Off in Biometric Verification Systems* [3], the authors attempt to derive two simple and affordable statistical expressions for calculating theoretically the false accept and false reject rates in any system prototype. Although this is feasible in theory, practical comparison between different biometric systems, when based on different technologies, is very hard to achieve.

In *Best Practices in Testing and Reporting Performance of Biometric Devices tries* [8], the Biometric Working Group (founded by the Biometric Consortium) tries to provide a guideline for reliable and repeatable independent testing of biometric devices and systems.

According to the WG, the three basic types of evaluation of biometric systems are: technology, scenario, or operational evaluation.

The goal of a *technology* evaluation is to compare competing algorithms from a single technology. The use of test sets allows the exact same test to be given to all participants.

The goal of *scenario* testing is to determine the overall system performance in a single prototype or simulated application, to determine whether a biometric technology is sufficiently mature to meet performance requirements for a class of applications.

The goal of *operational* testing is to determine the performance of a complete biometric system in a specific application environment with a specific target population, to determine if the system meets the requirements of a specific application.

3.3 What makes a biometric system usable?

While all possible biometric technologies have their own advantages and disadvantages, there are some common characteristics needed to make a biometric system usable. The most important are:

uniqueness – the biometric system must be based upon a distinguishable trait, no two persons should be the same in terms of the characteristic the system is based on.

universality – each person should have the characteristic the system is based on.

permanence – the characteristic should neither change not could be altered during lifetime.

user-friendly – people must be willing to accept the system: the scanning procedure does not have to be intrusive and the whole system must be easy of use.

cost – cost is always a concern, in this case also the life-cycle cost of system maintenance must be taken into account.

accuracy – there is the need to achieve an appropriate balance between the false accept rate and false reject rate (see Section 3.2), depending on the use the system is intended to.

3.4 Benefits of using biometric identification

- **Biometrics assure you about the identity of the person performing the transaction.** Password or card-based systems only tell you that whoever performed a given transaction possessed the needed card and/or PIN, leading you to believe it was probably the account owner. These methods of identification do not provide any proof about who actually performed the transaction. A biometric provides positive identification of the individual who performed a given transaction.

- **Biometrics enhance customer service.** Many forms of customer identification, such as signature verification, photo ID, even PIN numbers are perceived by customers as providing no additional convenience and even as something that "slows down" the process of performing a transaction. Biometrics, on the other hand, enhances customer service by providing quick and easy identification. There is nothing to remember, no risk of leaving a card or ID at home. Even if their paper credentials are lost or stolen, customers can continue to transact business quickly and easily. And they have the added peace of mind of knowing that their lost or stolen credentials cannot be used to access their personal accounts.

- **Biometrics are not easily compromised.** Most identification systems in use today employ either a password/PIN or a token, such as a card, or some combination of the two. These types of systems are easily compromised, usually by stealing the token or password. A biometric identification system is based on something you are, which cannot be stolen or compromised. In the case the biometric feature is stored on a microchip in a credit card, for example, and the card is stolen, when the impostor will try to use the card he will be rejected because his biometric feature will not match the one recorded in the card.

- **Biometrics require no teller or operator interpretation.** Some systems in use today, such as signature verification and photo ID, require an employee to examine the documents and make a judgment about whether the signatures, photos, etc. match. As these operators are not trained experts in fields such as handwriting analysis, errors can and do occur. Biometric identification depends on computer algorithms to make a yes/no decision.

3.5 Problems of using biometric identification

- **Lack of a single standard supported by the entire industry.** For example, if my bank allows me to protect my various cards (or single function smart card) with an eye scan of some type, my ATM card will only be usable at other ATMs supporting this same device and not at ATMs supporting fingerprinting, voice printing, or no biometric identification at all. My checks and credit card will only be accepted at points of sale supporting that form of eye scanning. For the shop owner, the diversity of biometric methods would require perhaps a dozen data collection devices at every cash register. Even if a single biometric measure such as fingerprinting were accepted as the standard, there are dozens of proprietary formats for data storage and analysis.

  Since 1998, at least four organizations have been trying to define a biometric API [14]: BAPI (Biometric API), Bio API Consortium, HA-API(Human Authentication API), SVAPI (Speaker Verification API). In March 1999, they agreed to merge their efforts into a new Bio API organization, and a complete specification is due by the end of this year.

- **Most of the technologies work well only for a “small” target population.** Only two biometric technologies, fingerprinting and iris scanning, have been shown in independent testing to be capable of identifying a person out from a group exceeding a thousand people. Three technologies, face, voice and signature, have been shown in independent testing to be incapable of singling out a person from a group exceeding a thousand [15]. This can be a big problem for large-scale use.

- **The level of public concern about privacy and security is still high.** Public resistance can a big deterrent to a widespread use of biometric-based identification. See Section 3.6 for a discussion on the privacy issues related to biometric authentication.

- **Biometric technologies do not fit well in remote systems.** If the verification takes place across a network (the measurement point and the access control decision point are not co-located), the system might be insecure. In this case, the attacker can either steal the person's scanned characteristic and use it during other transactions, or inject his characteristic into the communication channel. This problem can be overcome by the use of a secure channel betwwen the two points.
- **Biometric systems do not handle failure well.** If someone steals your template, it remains stolen for life. Since it is not a digital certificate, or a password, you cannot ask to your bank or to some trusted third party to issue you a new one. Once the template is stolen, it is not possible to go back to a secure situation.

3.6 Privacy issues

The issue of privacy is central in biometrics. Public is concerned about possible uses and abuses of the information gathered by biometric systems. The question that always arises when talking about biometrics is: "What about my privacy?". The primary concern seems to be "They will find me, track me or correlate my personal data". "They" is commonly thought to be some government agency or some hacker on the Internet.

Let's first define *privacy* in a legal context [5], and then examine the two major issues that raise when talking about biometric technologies. Privacy is different things to different people. Most importantly for the context of biometrics, privacy includes a control aspect *"control we have over information about ourselves"*, *"control over who can sense us"*, *"...control over the intimacies of personal identity.*"

A basic criticism from the standpoint of privacy is that we, as individuals, **lose our anonymity** whenever biometric scanning systems are deployed. Controlling information about ourselves includes our ability to keep other parties from knowing who we are. However, there are many examples of a honest person losing control over his personal account information because a criminal has gained unauthorized access to his information by stealing the person's password. The use of biometrics prevents from this. In some cases, the benefits of establishing a person's identity outweigh the costs of losing anonymity. If a biometric system is accurate, you are the only person that can have access to your sensitive personal information.

In *Biometric yet Privacy Protecting Person Authentication* [20], the author suggests a solution which uses biometric technologies but is still acceptable from a privacy point of view. The solution is to equip people with personal devices (called *wallet*) that can run a trusted local biometric verification process (called *observer*). The system is depicted in Figure 1.

The scope of the observer is to verify that the person holding the wallet is the right owner. When the wallet is issued, the observer is "personalized" for the particular biometric identity of its owner and inserted in the owner's personal wallet. The observer has no communication link other than to its hosting wallet. Once personalized, there is no way to re-personalize it, thus there is no harm in having it stolen: the stealer cannot use it and it is possible to have the observer re-issued.

The inspection of the person at the point of access (called *verifier*) is based only on the wallet (token-based approach), but if the observer verification of the biometric identity of

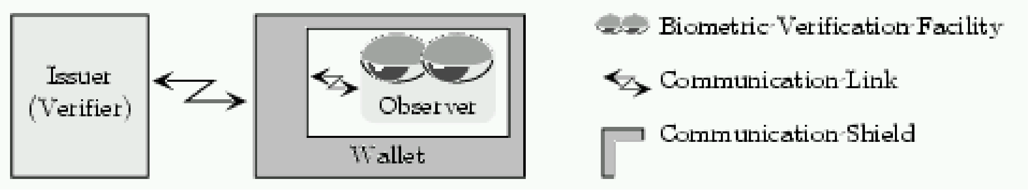

Figure 1: Wallet with observer architecture

the person performing the action at the checkpoint fails, the whole process fails. Since there is no outflow of information from the observer to the checkpoint, the system is able to preserve privacy. Unfortunately, this approach has been proved theoretically but it has not been implemented yet.

People also argue that the use of biometric systems would **enable the state to monitor the actions and behavior of citizens**. Actually public and private organizations already have the ability to gather substantial amounts of information about individuals by tracking, for example, credit card use and consumer spending. In the case of biometric technologies, what is certainly required to safeguard the public interest is a regulation of the electronic databases containing the personal identification information. We agree with Ziemmerman saying [10] "...privacy law should focus more on identifying and protecting information that warrants it at the points of origin, rather than continuing the practice of imposing liability only after the information is disseminated to the public." Organizations using biometric identification information must be required by law to safeguard their databases and to permit the individual to correct any mistakes in the data collected.

Currently, in "real life" there are just small single systems, which keep the information in limited contexts, thus seeming less dangerous. Consequently, government legislations address each specific system. For example, in Connecticut (USA) the Federal Highway Administration is using biometric identification for commercial driver's license to avoid concurrent licenses. The legislation states that [10]:

> "...the information obtained from the identification process is the proprietary information of the Department of Motor Vehicles, and cannot be released or made available to any agency or organization, or used for any purpose other than identification or fraud in this or any state. One exception is that information may be made available to the office of the chief state's attorney, if necessary, for the prosecution of fraud."

4 Different Biometrics Technologies

In this Section we give a brief overview of some of the emerging biometric technologies.

Facial Recognition and Thermogram – Facial recognition [11] systems are based on the distance between facial attributes (from pupil to pupil, for instance) or on the dimensions of the attributes themselves (such as the width of the mouth). At each transaction, a tiny camera feeds a live image of the person to a database which compares the image to the one stored. This technology has a good impact on the user, since it seems natural and intuitive, is not expensive and works well under constrained conditions. The weakness is that it is very sensitive to variations in illumination, faces with different positions or expressions, and it performs poorly when database size increases. Identical twins are hardly distinguished; other identification methods, such as iris scan or fingerprint, can be more accurate. Some of the problems will be overcome in the next future with the improvement of the algorithms used during the image generation process.

Facial thermograms are based on the blood vessel pattern of the face. It is not proved that this technology is discriminative enough with big databases, and it can be sensitive to the emotional state of the subject or to body temperature.

Fingerprints – Fingerprints are unique, they are distinct even in identical twins and they don't change over time. They also have some limits: dry skin and dirt can affect performance, sometimes they are not usable because of cut or scars, they often have a bad impact on the user since in the past they have been used for criminals. Finally, they require a large amount of computational and storage resources, so they are not so easy to implement with the general population.

Hand Geometry and Vein – Hand geometry measures the shape of the hand. The system looks at both the top and sides of the hand using a video camera. Hand recognition has several advantages over fingerprinting: it requires less bytes to store the template, the whole system is cheaper and it encounters less psychological resistance. But the technology has some shortcomings too: people do not want to place their palms where so many others have placed theirs, performance can depend on weather conditions or cleanliness of the hand, the shape of the hand may not be invariant during lifetime and, actually, test with “simulated hands” (gloves) have not been performed. One problem that will never be overcome is the fact that the size of the sensor is quite big, so the technology is not suitable for certain applications such as laptop computers.

Iris and Retinal Scan – Iris scan [13] is the most promising technology. It is based on the scanning of the colored ring that surrounds the pupil in the human eye. After DNA, irises are the most individualized feature of the human body, even identical twins have different irises. This technology uses video cameras during the scanning procedure, it does not require contact between the subject's eye and the biometric device and it is cheap. Finally, irises are less susceptible to injury than many other parts of the body, the template requires just few bytes and the system works even if the person is wearing glasses.

Retinal scans shoot a low-intensity beam of light into the eyeball and record the pattern of veins in the eye. Users are required to stand close to the device and focus on a target, which makes the systems unattractive. In addiction, the sensors are still quite expensive and retinas change during a person's life.

Voice Recognition – Voice verification [16] is considered to be the least accurate, but is favored by users and can provide access to secure data over telephone lines. Voice recognition can be text-dependent or text-independent. In the first case, the speaker says a predetermined phrase; in the second, less accurate, the speakers just says something. There are many weaknesses: the speaker may achieve a great variety of inflexions due to the variations in environment –such as stress and disposition–, background noises and the quality of a telephone connection can greatly reduce the performance. Based on limited testing, twins (and siblings, to a lesser extent) are more difficult to distinguish than the general population and, therefore, are responsible for higher error rates. This technology does not achieve large scale recognition.

Signature recognition – It is based on the fact that each person has a unique style of handwriting. The problem is that even two signatures of a same person are never exactly the same. Thus, it is less reliable, more expensive and it is used only with small target population. It can be static and dynamic. The dynamic method uses also the acceleration, velocity and pressure of the person's handwriting to improve in accuracy.

As this brief overview should have highlighted, each biometric technology has its own advantages and disadvantages. There is not an all-purpose technology, even if iris scan is very promising.

Then, what will the future of biometric be? Will there be a sort of *biometric centralization*, whereby one biometric would dominate multiple applications; or will we see *biometric balkanization* [5], where multiple biometrics are used for multiple applications? It is hard to tell.

Another possible solution, if sensor cost will continue to fall, is integration between different technologies. A multi modal identification system achieves much greater accuracy than single-feature systems: if one characteristic is unusable, the other two will lead to a correct identification. BioID [12] is an example of a multi modal identification system, using face, voice and lip movement to get the correct identification.

5 Case study: an iris-recognition system

In this Section we analyze the features that make iris scan technology promising and very accurate. We will focus on the processes of features extracting and matching.

The human iris, the colorful organ surrounding the pupil, is rich in features that can be used to quantitatively and positively distinguish one from another. Among the clearly visible features of the iris are contraction furrows, collagenous fibers and filaments, crypts, coronas, striatlons, a serpentine vasculature, freckles, rifts and pits. The iris scan process typically uses about 200 of these measurable variables to create the iris code.

The properties of the iris that render it potentially superior to the other biometric technologies include:

Uniqueness – During the course of examining large numbers of eyes, ophthalmologists and anatomists have noted that the detailed pattern of an iris seems to be highly distinctive. Even two irises with the same genetic genotype (as in identical twins, or the pair possessed by one individual) have uncorrelated iris minutiae. The statistical probability that two irises would be identical by random chance is calculated at approximately 1 in 10^{52}.

Stability over time – The features of the iris, their placement, size, shape and orientation is fully developed from the age of twelve months and remains stable for life. In addition, the iris is protected from the external environment behind eyelid, cornea, frequently eyeglasses or contact lenses (which have negligible effect on the identification process).

Hardly alterable – It is impossible to surgically modify the iris without unacceptable risk to vision. In addition, its physiological response to light and the small continuous fluctuations of the pupil, provide a natural test against artifice.

Ease of registering – The system captures images of the iris from a distance of 15-46 cm, without physical contact, using a conventional zoom camera, with a 20-watt quartz-halogen light, operated at approximately 7 watts and filtered with a magenta acrylic filter to provide a comfortable amount of light without harshness or irritation.

Once the system has located the iris in the video image, it delineates eight zones of analysis of the iris based on a polar coordinate system. The iris code is calculated using these *eight circular bands* (see Figure 2) that have been adjusted to conform to the iris and pupil boundaries. The Daugman system [19], which is the one currently used in commercial applications, makes use of a decomposition derived from application of a two-dimensional version of Gabor filters to the image data. By quantizing its filter outputs, the representational approach that is used in the Daugman system yields a representation with a size of 256 bytes.

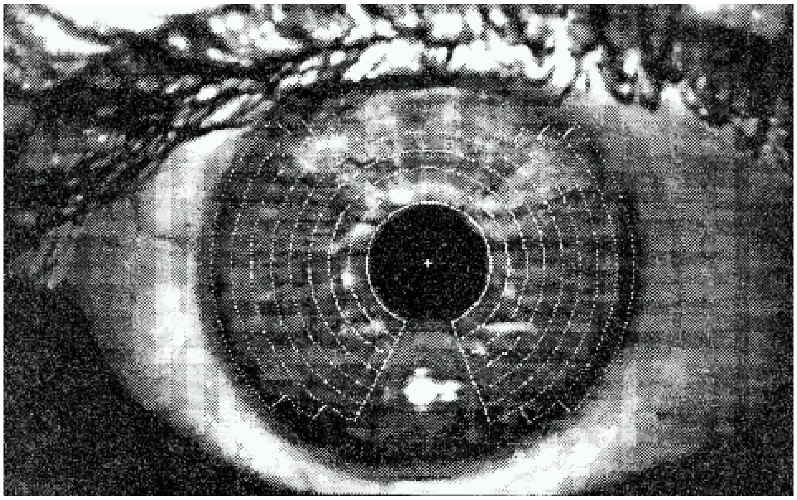

Figure 2: Illustration of iris detail, with the eight zones of analysis highlighted

The *difference* between two iris codes (the presented one and the template recorded in the database) is expressed as the fraction of mismatched bits, termed as a *Hamming distance*. To calculate the Hamming distance, each of the 2048 pairs of bits are compared: if two bits are alike, the system assign a value of zero to that pair comparison; if two bits are different, the system assigns a value of one to that pair comparison. After all pairs are compared, the assigned values are summed and divided by the total number of pair comparisons. For two identical iris codes, the Hamming distance is zero; for two perfectly unmatched iris codes, the distance is one. For two different irises, the average distance is about 0.5, which indicates 50 percent difference in the codes. For two different images of the same iris, the distance ranges from approximately 0.05 to 0.1, a variation that includes contributions from video noise as well as variations in the position of the user's eye with respect to imaging optics. Generally, a threshold of 0.32 can reliably differentiate authentic users from impostors.

The Daugman system has been subject of preliminary empirical evaluations [18]. The most interesting results are:

- Computations and decisions are accomplished at extremely high rates of speed, resulting in processing times of less than two seconds.
- Dark eyes were handled with identical speed and accuracy as others.
- Conventional contact lenses (clear or tinted) posed no problem in either enrollment or identification/verification phase. Enrollment without contacts could be followed by identification with the lenses, and vice versa, without impacting accuracy or speed. Similarly, the system handles imprecisely positioned lenses (not in same exact position on the eye every time) and colored contacts without difficulty.
- No false accepts were recorded. In the typical recognition case, the false accept probability is expected to be one in about 10^{31}.

6 Examples of Biometric Applications

Currently, both the public and private sectors are making extensive use of biometrics. Applications range from the elaborate security of the Winter Olympics in Nagano, Japan, two years ago, up to physical access control to computer systems containing sensitive information. There are also significant applications for biometrics in the commercial sector. Some of the biggest potential applications include the use of biometrics for access to Automated Teller Machines (ATMs) or for use with credit cards. MasterCard will begin using fingerprints as a substitute for a signature [17]. Many types of financial transactions are also potential applications; e.g., banking by phone, banking by Internet, and buying and selling securities by telephone or by Internet. Fraud on cellular telephone systems has increased dramatically and is estimated by some sources at over $1 billion per year. Biometrics are being considered to reduce this fraud. Telephone credit card fraud is also a significant problem that may benefit from the use of biometrics.

The following list of current "real world" application is not exhaustive, but might give an idea of the high potential of this new approach to identity authentication.

- Since 1994, the University of Georgia [4] at Athens has been using **hand recognition** to restrict cafeteria access to the students enrolled in its meal plan.
- Since 1992, the Colombian Legislature has been using **hand geometry** to confirm the identity of the members of its two assemblies immediately prior to a vote.

- INSPASS [9], Immigration and Naturalization Service's (INS) Passenger Accelerated Service System (INSPASS) has been using **hand geometry** to verify the identity of the traveler at an automated inspection station since 1993. It has been used at John F. Kennedy Airport in New York and Newark International Airport in New Jersey to provide prompt admission for frequent travelers (at least three times a year) to the US. There is also a Canadian version, similar to INPASS, except that it uses **fingerprint biometric**.
- PORTPASS [9] uses **voice recognition** to monitor people in vehicles at borders (only US/Canada). It requires the vehicle to stop.
- Walt Disney World [5] in Orlando (Florida) is using **finger geometry** with the season passes.
- Woolworth's supermarket [5] in Australia uses **fingerprints** to monitor time and attendance for about 100000 employees.
- Since September 1997, Langkawi Airport in Malaysia has been using **face recognition** to reconcile passengers with their luggage from check-in to boarding to prevents terrorists from checking luggage and not boarding the plane.
- At Charlotte/Douglas International Airport [6] in North Carolina **iris scan** has been used to identify airport employees and U.S. Airways Group Inc. The use will be extended to frequent airline passengers. Flughafen Frankfurt Airport in Germany is using the same system.
- Bank United Corporation [6] in Houston in May 1999 converted three supermarket automated teller machines, at a cost of $5,000 each, to use **iris scan** to identify customers before they conducted transactions. Right now it seems to be the lone player in its industry to go live with the technology in the United States.
- Since October 1996, in Tokio (Japan) some banks [5] have been using **iris-recognition**-based ATM systems. Alternatively, fingerprint is also used.

7 Conclusions

For years biometrics has been used by only few government and military agencies, law enforcement fingerprinting, and an occasional James Bond movie.

As biometric sensors continue to become less expensive and the technology improves, biometric systems will be used for access control to sensitive spaces and computers, airport security, automated border crossing, information security, automated teller machines and electronic commerce.

Since there is no the "perfect" biometric system that fits all needs, it is likely that more than one biometric technology or an integration of different technologies will emerge.

The major impediment to universal implementation is the public concern about privacy, but appropriate policymaking can greatly increase public acceptance of this technology.

References

[1] Anil Jain, Lin Hong and Sharath Pankanti. Biometric Identification, *Communications of the ACM*, February 2000.

[2] Bruce Schneier. Biometrics: Uses and Abuses, Inside Risks 110, *Communications of the ACM*, vol. 42, no. 8, Aug 1999. available electronically http://www.counterpane.com/insiderisks1.html

[3] Matteo Golfarelli, Dario Maio and Davide Maltoni. On the Error-Reject Trade-Off in Biometric Verification Systems, *IEEE Transactions on pattern analysis and machine intelligence*, vol. 19, no.7 july 1997.

[4] Dave Sims. Biometric recognition: our hands, eyes, and faces give us away, *IEEE Computer graphics and applications*, 1994.

[5] John Woodward. Biometrics: Privacy's foe or privacy's friend?, *Proceedings of the IEEE*, vol. 85, no.9, September 1997.

[6] Michael Meehan. Iris scans take off at airports, (July 17, 2000). available electronically http://www.computerworld.com/

[7] Weicheng Shen, Marc Surette and Rajiv Khanna. Evaluation of automated biometrics-based identification and verification systems, *Proceedings of the IEEE*, vol. 85, no.9, September 1997.

[8] Biometrics Working Group. Best Practices in Testing and Reporting Performance of Biometric Devices - Version 1.0, 12 January 2000

[9] Hays and Ronald. INSPASS. Jan 1996. available electronically http://www.biometrics.org/REPORTS/INSPASS.html

[10] James Laban. Privacy issues surrounding personal identification systems, April 1996.

[11] Alex Pentland and Tanzeem Choudhury. Face recognition for smart environments, *IEEE computer*, special issue, February 2000.

[12] Robert Frischholz and Ulrich Dieckmann. BioID: a multimodal biometric identification system, *IEEE computer*, special issue, February 2000.

[13] Michael Negin and Theodore Camus. An iris biometric system for public and personal use, *IEEE computer*, special issue, February 2000.

[14] Catherine Tilton. An emerging biometric API industry standard, *IEEE computer*, special issue, February 2000.

[15] James Wayman. Biometric identification and the financial services industry, available electronically http://www.house.gov/banking/52098jlw.htm

[16] Steven Boll. Biometrics and the Future of Money, May 20, 1998. available electronically http://www.house.gov/banking/52098dsb.htm

[17] Pamela Sherrid. You can't forget this password, available electronically http://www.usnews.com/usnews/issue/990517/17biom.htm

[18] Gerald Williams. Iris Recognition Technology, Security Technology, 1996. *30th Annual 1996 International Carnahan Conference*, 1996.

[19] John Daugman. High Confidence Recognition of Persons by Rapid Video Analysis of Iris Texture, *European Convention on Security and Detection*, May 1995.

[20] Gerrit Bleumer. Biometric yet Privacy Protecting Person Authentication, *AT&T Labs-Research*, January 1998.