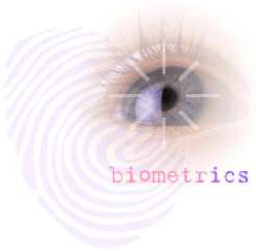
Biometric Systems



Igor Böhm
Department of Telecooperation
University of Linz
4040 Linz, Austria
Email: igor@bytelabs.org

Florian Testor
Department of Telecooperation
University of Linz
4040 Linz, Austria
Email: florian.testor@students.jku.at

***Abstract*— This paper covers the field of biometric systems with a special focus on biometric authentication systems. A short and general overview of biometric authentication systems gives some insight in how the various biometric data can be used for authentication. After that an abstracted view of biometric systems is given, followed by general performance evaluation techniques. The problems of varying biometric data, caused by noise respectively human nature and approaches to solve these problems with multi-biomteric systems in combination with information fusion, are also discussed. Since there is such a vast range of possibilities for the usage of biometric systems, some type of open system standardization is necessary. In connection to the need for open system standards a closer look at the BioAPI consortium which provides a widely accepted API serving for various biometric technologies, is taken.**

I. Introduction

First of all the term Biometrics should be more or less defined in order to have a common understanding of the subject. Both terms ”Biometrics” and ”Biometry” have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. The following are all examples which fall under the umbrella of ”Biometrics” as the term has been historically used:

- Statistical methods for the analysis of data from agricultural field experiments to compare the yields of different varieties of wheat.
- The analysis of data from human clinical trials evaluating the relative effectiveness of competing therapies for disease.
- The analysis of data from environmental studies on the effects of air or water pollution on the appearance of human disease in a region or country.

Recently the term ”Biometrics” has also been used to refer to the emerging field of technology devoted to identification of individuals on the basis of their biological traits, such as those based on retina-scans, iris-patterns, fingerprints or face recognition. The recent usage and meaning of the term ”Biometrics” will be the primary focus of this paper.

In todays world a wide variety of applications requires reliable and secure authentication methods to confirm the identity of an individual requesting their service. Some examples of such applications would include secure access to buildings, computer systems, laptops, cellular phones, memory such as USB sticks and many more. Furthermore it is possible to establish an identity based on ”who you are” rather than by ”what you posses” (e.g. identification cards) or ”what you remember”(e.g. passwords). [1]

II. Biometric System Examples

A. Fingerprint

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. The fingerprint itself consists of patterns found on the tip of the finger, thus making it a physical biometric. Fingerprints are known to be unique and immutable for each person and the basic characteristics of fingerprints do not change with time. The uniqueness of a fingerprint can be determined by the patterns of ridges and furrows as well as the minutiae points on the surface of the finger. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprints are routinely used in forensic laboratories and identification units all over the world and have been accepted in the court of law for nearly a century. Since the 1980’s the usage of fingerprints in civil areas has become more relevant because of increasing accuracy and decreasing prices of fingerprint devices. Some examples of the use of fingerprint devices in civil areas are:

- Fight the abuse of civil services like social security.
- Permitting logins based on fingerprints.
- Fight against illegal immigration.

B. Handscan

This biometric approach uses the geometric form of the hand for confirming an individual's identity. Specific features of a hand must be combined to assure dynamic verification, since human hands are not unique. Characteristics such as finger curves, thickness and length, the height and width of the back of the hand, the distances between joints and the overall bone structure, are usually extracted. Those characteristics are pretty much persistent and mostly do not change in a range of years.

The first handscanners were used more than 20 years ago and therefore it was one of the first biometric recognition systems. For scanning the hand a CCD *(Charge-Coupled Device)* camera is necessary. The camera takes two binary photos, one from above and one from beside the hand. Over 90 measurements are combined to form a template. A template is a binary file created from distinctive information from a biometric sample. Registration of a new user depends on the system but normally lasts less than 1 minute. The camera takes 3 times 2 shots and the system calculates the averages and stores the user with a special ID with his hand geometry code. The verification process requires the user to enter an ID in order to verify the claimed identity. After the user ID has been entered and the photos have been captured, the calculation of the feature set representing the biometric trait and the verification process lasts no longer than a second.

Handscan applications have proven their practical use which is shown by the 30-60% market share of biometric identification applications. The following listing should give some examples in real world areas where handscan identification is or was used:

- Personel at the olympic games 1996 were identified with handscans.
- In a lot of cases access to military plants is granted upon successful handscan identification.
- Airport personel at the San Francisco Airport is identified by handscans.

C. Signature

Signature verification is the process used to recognize an individual's hand-written signature. Dynamic signature verification uses behavioral biometrics of a hand written signature to confirm the identity of a person. This can be achieved by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing. On the other hand there is the simple signature comparison which only takes into account what the signature looks like. So with dynamic signature verification, it is not the shape or look of the signature that is meaningful, it is the changes in speed, pressure and timing that occur during the act of signing, thus making it virtually impossible to duplicate those features.

Devices which enable dynamic signature verification store the behavioral factors and the captured signature image itself for future comparison in their database. These devices account changes in one's signature over time by recording the time and the dynamic features each time a person uses the system.

The major difficulty with this technology is to differentiate between the consistent parts of a signature, these are the characteristics of the static image, and the behavioral parts of a signature, which vary with each signing. Comparing many signatures made by one individual reveals the fact that an indivduals signature is never entirely the same and can vary substantially over an individual's lifetime. Allowing these variations in the system, while providing the best protection against forgery is a big problem faced by this biometric technology.

The financial industry sometimes uses signature verification for money transactions. The Manhattan Bank was the first bank to test such an approach by using a biometric signature application for their money transaction system.

D. Iris

Iris scan biometrics employs the unique characteristics and features of the human iris, which remains unchanged throughout an individual's lifetime, in order to verify the identity of an individual. The iris is the area of the eye where the pigmented or colored circle, usually brown, green, grey or blue, rings the dark pupil of the eye. The iris is well protected cause of the human anatomy and therefore injuries are rare.

Typically the iris scan process begins with a photograph which is taken with a special camera close to the subject. The user has to be in between a maximum distance of about 1 meter to the reading device. The camera uses an infrared imager to illuminate the eye and capture a very high resolution photograph. The inner edge of the iris is located by an iris-scan algorithm which maps the iris distinct patterns and characteristics.

Systems using iris biometrics even work with glasses and this technology is one of the few biometric technologies that can work well in identification mode.

Iris patterns are extremely complex, carrying an astonishing amount of information and have over 200 unique spots. Unique spots are categorized into the tissue, which gives the appearance of dividing the iris in a radial fashion, rings, furrows, freckles and the corona. The fact that an individual's right and left eyes are different and that patterns are easy to capture, establishes iris-scan technology as one of the biometrics that is very resistant to false matching and fraud.

E. Retina

Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. It is also among the most difficult to use and requires well-trained, and is perceived as being moderately to highly intrusive. The users have to be cooperative and patient to achieve a proper performance.

Basically the retina, a thin nerve on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain. Blood vessels used for biometric identification are located along the neural retina which is the outermost of the retina's four cell layers.

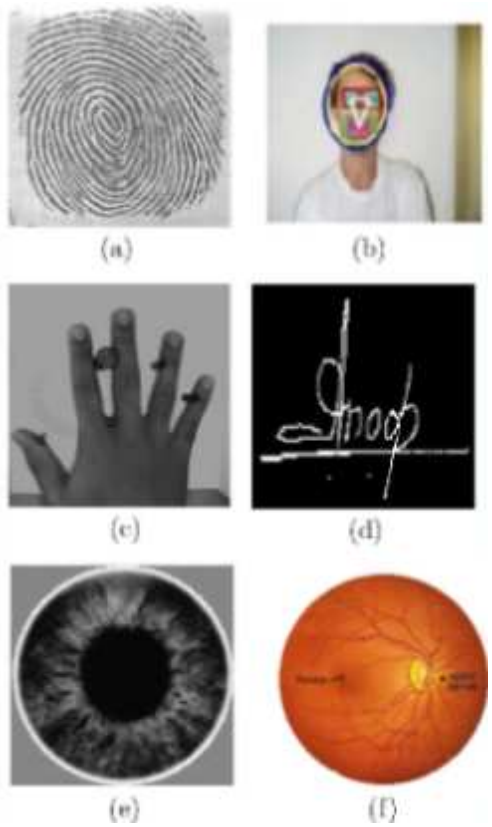


Fig. 1. Examples of some of the biometric traits associated with an individual: (a) fingerprint, (b) face, (c) hand geometry, (d) signature, (e) iris and (f) retina.

Research has proven that the patterns of blood vessels on the back of the human eye were unique from person to person. It has even been proven that these patterns, even between identical twins, were indeed unique. This pattern also doesn't change over the course of a lifetime.

Retinal scanners require the user to place their eye into some sort of device and then ask the user to look at a particular spot so that the retina can be clearly imaged. This technology involves using a low-intensity infrared light source through an optical coupler to scan the unique patterns of the retina. The reflection of the vascular information is being recorded. Retina scanning works well in both modes, identification and verification. Additional advantages include the small template size and good operational speed.

F. Voice

Of the many types of biometric technologies available today, voice identification and authentication solutions have a unique edge over much of the competition, because customers typically don't need to purchase new hardware to implement the solutions. Most of the voice biometric solutions can be used through a typical telephone or microphone hooked up to the computer.

In order to identify or authenticate users, most voice biometric solutions create a voice print of the user, a template of the person's unique voice characteristics created when the user enrolls with the system. During enrollment the user has to select a passphrase or repeat a sequence of numbers. The passphrase should be in the length of 1 to 1.5 seconds. The problem with shorter passphrases is that they have not enough data for identification. Longer passphrases have too much information. The user has to repeat the passphrase or the sequence of numbers several time. This makes the enrollment process lasting much longer than with other biometric technologies. All subsequent attempts to access the system require the user to speak, so that their live voice sample may be compared against the pre-recorded template. A voice biometric sample is a numerical model of the sound, pattern and rhythm of an individuals voice.

A problem considering the voice is that people's voices change over time along growth, or when someone has got a cold or an other desease. Background noise can also be an disturbing factor.

G. Face

Human face detection plays an important role in applications such as video surveillance, human computer interfaces, face recognition, and face image databases [8]. To enable this biometric technology it requires to have at least a video camera, PC camera or a single-image camera. Nevertheless, this biometric approach still has to deal with a lot of problems and can not work with acceptable identification rates unless certain restrictions are being considered. Finding a face in a picture where the position, the orientation, the background and the size of a face is variable, is a very hard task and many algorithms have been worked on to solve this problem. Other problems with face detection occur whenever faces are partially covered, as with beards, glasses, hair style or hats, because a lot of information just stays hidden.

III. Biometric Authentication Systems

Looking at biometric systems in a more general way will reveal certain things all biometric-based authentication systems have in common. In general such systems work in two modes:

- *Enrollment mode:* In this mode biometric user data is acquired. This is mostly done with some type of biometric reader. Afterwards the gathered information is stored in a database where it is labeled with an user identity(e.g. name, identification number) to facilitate authentication [2].
- *Authentication mode:* Again biometric user data is acquired first and used by the system to either *verify* the users claimed identity or to *identify* who the user is. While *identification* involves the process of comparing the users biometric data against all users in the database, the process of *verification* compares the biometric data against only those entries in the database which are corresponding to the users claimed identity.

In general one can consider the verification of the identity of a person a two-class problem:

- either the person is who he/she claims to be (*client*)

- or the person fails to be the one he/she claims to be (*impostor*)

So we are basically dealing with a binary-decision scheme where we either accept or reject a person. Simple biometric systems usually consist of the following four components:

1) *Sensor modules:* This modules acquires biometric user data. Examples of sensor modules would be an retina-scanner or a fingerprint sensor.
2) *Feature extraction modules:* This modules is responsible for extracting feature values of a biometric trait. If hand geometry would be used as a biometric trait then feature values would include width of fingers at various locations, width of the palm, thickness of the palm, length of fingers etc.
3) *Matching modules:* The matching modules compares the acquired biometric features against those stored in a database.
4) *Decision-making modules:* The users identity is either established or a claimed identity is accepted or rejected. This is done based on the results of the matching modules.

Since we are dealing with a binary decision scheme it is obvious that the *decision-making module* can make two kinds of errors. The errors, which can be made in the process of verification, are called:

- **False Rejection (FR)**: when an actual client gets identified as an impostor.
- **False Acceptance (FA)**: when an actual impostor gets identified as a client.

IV. Performance Evaluations

The performance of a biometric authentication system can be measured as the *False Acceptance Rate FAR* Equation (2), or the *False Rejection Rate FRR* Equation (1) which are defined as:

$$FRR = \frac{number\ of\ false\ rejections}{number\ of\ client\ accesses} \quad (1)$$

$$FAR = \frac{number\ of\ false\ acceptances}{number\ of\ client\ accesses} \quad (2)$$

A perfect biometric authentication system would have a $FRR = 0$ and a $FAR = 0$ which is a little bit unachievable in reality. It is also interesting that any of the two values FRR and FAR can be reduced to an arbitrary small number, with the drawback of increasing the other value.

Another interesting value is the *TotalErrorRate TER* Equation (3) which is defined as:

$$TER = \frac{number\ of\ FA + number\ of\ FR}{total\ number\ of\ access} \quad (3)$$

At this point it is important to emphasise the fact that these measures could be heavily biased by one or either type of errors (FAR or FRR) depending only on the number of accesses which have been used in obtaining these respective errors. This means that the **TER** will always be closer to that type of error which has been obtained with the largest number of accesses.

The overall performance of a biometric authentication system should not be measured by the *TER* but rather by the **Receiver Operation Characteristic ROC**, which represents the **FAR** as a function of the **FRR**. So wherever there is a tradeoff of error types, a single performance number is inadequate to represent the capabilities of a system. Such a system has many operating points and is best represented by a performance curve. The **ROC** curve has been used for this purpose. Generally false alarm is plotted on the horizontal axis whereas the correct detection rate is plotted on the vertical axis.

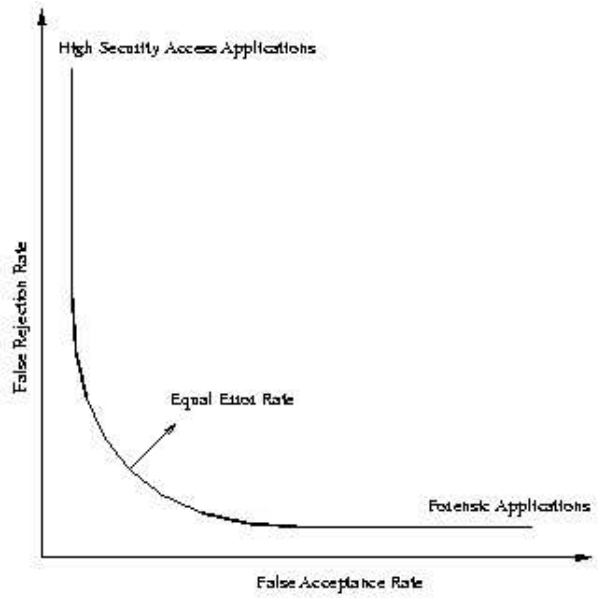


Fig. 2. Examples of operating points of different application types.

In some applications though the *Detection Error Tradeoff* **DET** curve has been found to be more useful since both types of errors are plotted on the **DET** curve. Typically one can observe approximately straight lines, which do correspond to normal likelihood distributions, in **DET** plots. This method is especially useful in speech applications. For further information see [5] and Figure 3.

Some high security applications tend to keep the **FAR** as small as possible when they operate at the point on the **ROC**. Forensic science operates with a very low **FRR** and a very high **FAR** since they desire to catch a criminal even at the expense of examining large numbers of false accepts. Civil applications try to work at a level where **FRR** and **FAR** are both as low as possible *(see Figure 2)*.

V. Problems with Biometrics

In theory collecting and verifying biometric data is no problem but in todays demanding real-world applications there are a lot of problems with biometric systems. One of those

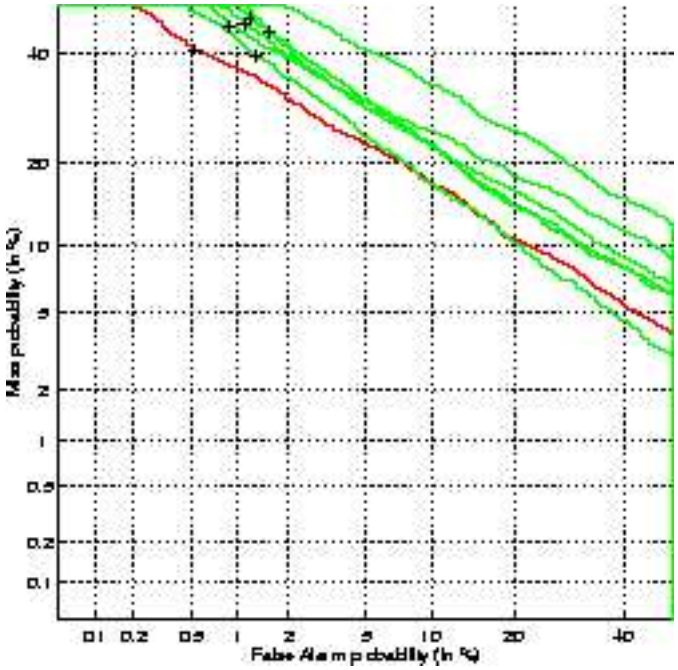


Fig. 3. DET-curve example.

problems is that biometric traits extracted from persons tend to vary with time for one and the same person and to make it even worse, this variation is itself very variable from one person to another. Most of the other problems are caused by extreme or constantly changing surroundings and the nature of certain biometric measures.

A. Noise

Noisy biometric data like a person having a cold(voice recognition), a simple cut on ones finger(fingerprint scan) or different lighting conditions(face detection) are some examples of noisy inputs. Other examples are misconfigured or improperly maintained sensors or inconvenient ambient conditions like dirt on a sensor for fingerprints or voice recognition with loud background noise. The problem with noisy biometric data is that authorised personnel may get incorrectly rejected(*FR*), if the noisy data affects the extracted features so much, that no match can be found in the biometric database. The other extreme situation would occur if noise would change the extracted features in such a way, that the result feature set would match to another person(*FA*).

B. Distinctiveness

While a biometric trait is expected to vary significantly across individuals, there may be large similarities in the feature sets used to represent theses traits. Thus, every biometric trait has a theoretical upper bound in terms of discrimination capability [1].

C. Non-universality

The problem of non-universality arises when it is not possible to acquire certain biometric traits from all users. That means that even though a person has a fingerprint, it still may be impossible to acquire that trait because of the poor quality of the ridges which make up the fingerprint.

VI. Multi biometric Systems

Most of the problems and limitations of biometrics are imposed by unimodal biometric systems. Unimodal biometric systems rely on the evidence of only a single biometric trait. Some of these problems may be overcome by multi biometric systems and an efficient fusion scheme to combine the information presented in multiple biometric traits. It is evident that problems like non-universal traits, distinctiveness and security problems are easier and better to deal with if more biometric traits are present.

So if a persons fingerprint can not be acquired by a sensor, other biometric methods like voice recognition and retina-scans are taken into account and the resulting data is validated against the biometric database. Spoofing of biometric data also becomes harder since it is far easier to spoof only one biometric trait whereas with multi biometric systems it would be necessary to spoof several traits simultaneously.

A. Fusion of Biometric data

In general there are three possible levels of fusion for combining two or more biometric systems to a multi biometric system:

- *Fusion at the feature extraction level:* Feature sets are acquired from each sensor where each feature set is represented as a vector. Then the vectors are concatenated which results in a new feature vector with higher dimensionality representing a persons identity in a different hyperspace.
- *Fusion at the matching score level*: Each biometric system provides a matching score which indicates the proximity of the feature vector with the template vector. Fusion at this level would mean combining the matching scores in order to verify the claimed identity. In order to combine the matching scores reported by the sensors, techniques such as logistic regression is used. The logistic regression model is simply a non-linear transformation of the linear regression. The logistic distribution is an S-shaped distribution function similar to the standard-normal distribution, but it is easier to work with in most applications because the probabilities are easier to calculate. These techniques attempt to minimise the **FRR** for a given **FAR** [7].
- *Fusion at the decision level:* The resulting feature vectors from each sensor need to be classified into two classes - reject or accept. Afterwards a majority vote scheme can be used to make a final decision.

So in the context of biometrics, fusion can take the following forms:

- *Single biometric multiple representation:* This approach involves a type of fusion which uses multiple representations on a single biometric indicator. Each representation

has its own classifier and the similarity scores reported by these classifiers are then consolidated [2].
- *Single biometric multiple matchers:* Another possibility is to combine multiple matching strategies in the matching module of a biometric system and combine the scores generated by these strategies.
- *Multiple biometric fusion:* The combination or fusion of multiple biometric traits is used in order to achieve an improvement of speed, reliability and accuracy of a biometric system.

VII. Standards

The biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. Standards are emerging to provide a common software interface, to allow sharing of biometric templates, and to permit effective comparison and evaluation of different biometric technologies [9].

The BioAPI consortium has released an open system standard called the BioAPI which defines a common method for interfacing with biometric applications. Today the BioAPI has been accepted as an ANSI standard - ANSI/INCITS 358-2002. The BioAPI is implemented in the C programming language and it is intended to provide a high-level generic biometric authentication model suited for any form of biometric technology. It covers the following basic functions:

- enrolment
- verification and identification
- a database interface is also provided in order to manage the identification population for optimum performance

The BioAPI also provides primitives that allow the application to manage the capture of samples on a client, and the enrolment, verification and identification on a server [10].

VIII. Biometric Application Scenarios

A. Biometrics applications and plans in the United Kingdom

The United Kingdom passport service *(=UKPS)* started a six month trial in 2004 to test the recording and verification of facial recognition, iris and fingerprint biometrics. Approximately 10000 participants will take part in the trial. Results from the trial will help to inform the government's plans to introduce biometrics to support improved identity authentication and help prevent identity fraud [11].

The participants will receive a card with their photograph on the front. The chip embedded in the card will contain an electronic photograph and the person's biometrics. The card is issued solely as a demonstrator and cannot be used for travel or identification purposes *(see Figure 4)*.

All the biometrics obtained from the participants will be destroyed at the end of the trial. All process recordings and the participants questionnaires will be anonymous and analysed by the UKPS [11]. The main objectives are:

- Test the use of biometrics through a simulation of the passport process.
- Include exception cases, e.g. people who may have difficulties in enrolment.
- Measure the process time and hence estimate costs.
- Assess customer perceptions and reactions.
- Assess practical aspects of incorporation of biometrics into a biometric database.
- Identify issues and risks and produce an outline for an implementation plan.

In the middle of 2005, the government of the United Kingdom plans to introduce biometric technology, especially the electronical scanning of the iris, at the Heath-row, Gatwick and Stan-stead airport in London and the airports in Manchester and Birmingham. A faster entry and exit procedure should be achieved with this innovation.

Another example of the use of biometric technology in the United Kingdom is the London City Airport. It has become the first airport in Europe to establish terminal wide biometric security access for its 1600 employees. Fingerprint recognition and a photo ID card is used to identify a person. The system is used across all areas at the airport and even though its usage was only planned for staff members, it is possible to extend the system to also handle entry and exit procedures of travellers [15].

Fig. 4. United Kingdom passport service trial ID card.

B. Biometric applications and plans in the U.S.

US-VISIT is part of a continuum of security measures that begins overseas, when a person applies for a visa to travel to

the United States, and continues on through entry and exit at U.S. air and seaports and, eventually, at land border crossings. The US-VISIT program should enhances the security of U.S. citizens and visitors by verifying the identity of visitors with visas [12].

Biometric technologies, especially the scanning of fingerprints in combination with taking a digital photograph, are being used during entry and exit procedures to verify the identity of a person. This process is applied to persons between the age of 14 to 79 who are travelling with visas.

This project started at January 5, 2004 at the Airport in Atlanta, U.S., and should be extended to the 115 greater airports and 14 seaports until the end of 2004.

Additionally, in May 2004, the United States Embassy in Buenos Aires began electronically scanning the fingerprints of all visa applicants. Today more than a 100 U.S. visa-issuing consular sections are scanning fingerprints. By October 2004, every U.S. consular section in the world, should be able to electronically capture the fingerprints of visa applicants [13].

In 2005, the United States will also begin to issue machine-readable passports with biometric identifiers. At least fingerprints will be included to the U.S. citizen's passports. Other "visa-waiver" countries like Germany, France and Japan will also develop biometric passports within the next years, but the governments of these countries were not able to meet a concrete deadline for issuing biometric passports for travellers.

C. Automated Fingerprint Identification Systems

Many law enforcement agencies often use fast fingerprint identification systems based on a huge amount of fingerprints stored in a database. These systems are called AFIS *(Automated Fingerprint Identification Systems)*.

The FBI's Integrated AFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding history information for more than 47 million subjects. This system is running the whole time. As a result of an electronically submitted fingerprint, the agencies receive responses to a criminal ten-print fingerprint submission, which contains ten-rolled fingerprint impressions and a corresponding flat fingerprint impression, within 2 hours and within 24 hours for a civil fingerprint submission [14].

But the IAFIS supports both, electronic and hard copy submissions of latent fingerprints. Special laboratories have been deployed in order to enhance the search capabilities using databases especially designed for matching latent fingerprints.

IX. Conclusion

Biometric systems and especially multi biometric systems have a huge potential of growth. By using biometric technologies, access procedures should be made simpler, faster and more secure. Especially governments, law enforcement agencies, military and industrial companies, already make partial use of this technology.

In the future biometric devices will surely become more involved in many civil areas. Maybe in a couple of years access to ones private home or car will be granted upon a successful iris scan, thus making the traditional house or car keys obsolete. Maybe money, credit cards and cheques will become obsoleted by leaving ones fingerprint instead of a certain amount of monetary value.

But in spite of all the advantages coming along with the broader usage of biometric technology in our every day lives, this technology also brings up a whole new range of difficulties and problems. So it will not suffice to study factors like cost versus performance tradeoffs, or usability and security issues before deploying biometric systems. Very special care must be taken what may be done with the acquired biometric data and who may use it for a certain purpose.

References

[1] A. K. Jain, A. Ross. "Mutlibiometric Systems", *Communications of the ACM*, Vol. 74, pp. 34-40, 2004.

[2] A. K. Jain, A. Ross. "Information fusion in biometrics", *Pattern Recognition Letters*, Vol. 24, pp. 2115-2125, 2003

[3] P. Verlinde, M. Acheroy. "A Contribution to Multi-Modal Identity Verification Using Decision Fusion", *Decision Fusion.* ENST-Paris Ph.D. Thesis, 1999.

[4] R.-L. Hsu, M. Abdel-Mottaleb, and A. K. Jain. "Face detection in color images", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 696–706, May 2002.

[5] A. Martin, T. K. G. Doddington, M. Ordowski, and M. Przybocki. "The DET curve in assessment of detection task performance", *In Proceedings of EuroSpeech '97,* volume 4, pages 1895–1898, 1997.

[6] M. Roach, J.D. Brand, and J.S.D. Mason. "Acoustic and Facial Features for Speaker Recognition", *ICPR*, 2000.

[7] A.K. Jain, S. Prabhakar, S. Chen. "Combining multiple matchers for a high security fingerprint verification system", *Pattern Recognition Letters*, Vol. 20, pp. 1371-1379, 1999

[8] Rhien-Lien Hsu, Mohamed Abdel-Mottabel, Anil K. Jain. "Face Detection in Color Images", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 696–706, May 2002.

[9] S. Liu, M. Silverman. "A Practical Guide to Biometric Security Technology", *www.computer.org/itpro/homepage/Jan_Feb/security3.htm*, 2000

[10] The BioAPI Consortium. "BioAPI Specification 1.1", *The BioAPI Consortium*, March 2001.

[11] The United Kingdom Passort Service (UKPS). "The UKPS biometrics enrolment trial", *http://www.ukpa.gov.uk/docGallery/17.pdf*, April 2004

[12] U.S. Department of Homeland Security, "U.S. VISIT", *http://www.dhs.gov/dhspublic/display?theme=91*, 2004

[13] U.S. Government, "Biometric U.S. Visas", *http://usembassy.state.gov/posts/ar1/wwwhbiometricinfo.html*, May 2004

[14] The FBI "IAFIS (Integrated Automated Fingerprint Identification System)", *http://www.fbi.gov/hq/cjisd/iafis.htm.* U.S.A., 2004.

[15] London International Airport "Security arrangements at the Airport", *http://www.lcacc.org/operations/#Security*, U.K., 2003