

Biometrics at the frontiers, assessing the impact on Society
Technical impact of Biometrics

Bernadette Dorizzi

**Background paper for the Institute of Prospective Technological
Studies, DG JRC – Sevilla, European Commission**

January 2005

Legal notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

Disclaimer

The author of this report is solely responsible for the content, style, language and editing. The views expressed do not necessarily reflect those of the European Commission.

Reproduction is authorised provided the source is acknowledged
© European Communities, 2005

Preface

In June 2004, the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament (the LIBE Committee) asked the JRC to carry out a study on the future impact of biometric technologies. The report *Biometrics at the Frontiers: Assessing the Impact on Society* (EUR: 21585)¹ is the result of this request. The work was carried out by staff from the IPTS ICT Unit, in collaboration with a number of external experts.

Four experts were asked to contribute to the study, expressing their views on the technical, legal, social and economic implications of biometrics. They were respectively Professor Bernadette Dorizzi of the *Institut National des Télécommunications* (INT), FR; Professor Paul de Hert, of the faculty of Law, University of Leiden; Julian Ashbourn, chairman of the International Biometric Foundation and creator of the AVANTI non-profit on-line biometric resource (<http://www.avanti.1to1.org>); and Jonathan Cave, Senior Lecturer at the Department of Economics, University of Warwick, UK, and Project Leader at RAND Europe.

The above mentioned report *Biometrics at the Frontiers: Assessing the Impact on Society* contains the summarised contributions from these experts (in Chapter 3). More extended versions of their contributions are published on the IPTS website as background studies.

The present document is the extended version from Bernadette Dorizzi on *technological issues and implications*.

Available at: <http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm>

¹ Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodríguez, C., Ulbrich, M., Cabrera, M., Clements, B., Beslay, L., & van Bavel, R. (2005) *Biometrics at the Frontiers: Assessing the Impact on Society*. Study for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS, Sevilla, February 2005.

Available at: <http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm>

Biometrics at the frontiers, assessing the impact on Society

Technical impact of Biometrics

Bernadette Dorizzi

Contents

Introduction	4
1. Overview of technical challenges: An already established technology still under development	4
2. Description of different biometric modalities	7
3. Evaluation of biometric systems	13
Conclusion	19

Introduction

The proliferation of information access terminals and the growing use of applications (such as e-commerce, e-voting and e-banking) involving the transfer of personal data make it essential to provide reliable systems that are user-friendly and generally acceptable. With conventional identity verification systems for access control, such as passports and identity cards, passwords and secret codes can easily be falsified. Biometrics seem to provide a way of overcoming some of these systems' drawbacks, by basing verification on aspects that are specific to each individual.

For a long time the use of biometrics has remained limited to policing applications, but in view of its potential advantages, this technology is now being considered for many other tasks. Commercial applications have thus been developed, most often based on fingerprints or iris prints; these are currently considered to be the most reliable methods, but have the disadvantage of being intrusive, and are often disliked by users. This partly explains why their use remains limited at present to professional applications (e.g. airport personnel access control), and why, up to now, they have hardly ever been used for the general public, even though commercial products of this type are available.

Clearly, users are more familiar with methods based on face, voice or handwritten signature recognition, but the level of performance of such applications is not yet high enough for their large-scale use to be a realistic proposition. In view of this, combining several methods would seem to be a promising way forward, which remains to be validated.

Several American studies forecast a skyrocketing of the biometrics market, mainly as a result of the development of electronic data transfer, particularly on the Internet. At the European level, there are few studies available at present, and one of the EU's current concerns is to rapidly obtain reliable forward-looking studies.

What has changed recently is the ability to digitize, store and retrieve biometric patterns and have them processed by computers. Large scale deployments can thus be envisaged for example border control, voter ID cards, national ID cards, driver's license, welfare disbursement etc. In these types of applications, biometrics must be considered only as one element of a whole system that involves the use of sensors to acquire the biometric sample, the transmission of data from the sensor to a computer where matching will be performed after access to a huge database of stored templates. It means that biometrics should not be evaluated alone but it is this system that must be designed and evaluated in its entirety.

1. Overview of technical challenges: An already established technology still under development

1.1 Architecture of a biometric system

Generally speaking, there are two phases in a biometric system (see Fig. 1): a learning phase (enrolment) and a recognition phase (verification). In all cases, the item considered (e.g. finger print or voice) is recorded using a sensor and digital data are then available (a table of pixels, a digital signal, etc.). In most cases the data themselves are not used directly; instead the relevant characteristics are first extracted from the data to form a **template**. This has two advantages: the volume of data to be stored is reduced, and greater anonymity is achieved in data storage (because it is not possible to recover the original signal by referring to these characteristics).

The role of the **learning** module is to create a model of a given person by reference to one or more recordings of the item considered. Most of the models used are statistical models, which make it possible to allow for a certain variability in individual data.

The **recognition** module enables a decision to be taken. In identification mode, the system compares the measured signal with the various models contained in the data base and selects the model corresponding most closely to the signal. In verification mode, the system will compare the measured signal with just one of the data base models and then authorise the person or reject him. Identification may be a very difficult task if the data base contains thousands of individuals. Access time problems then become crucial.

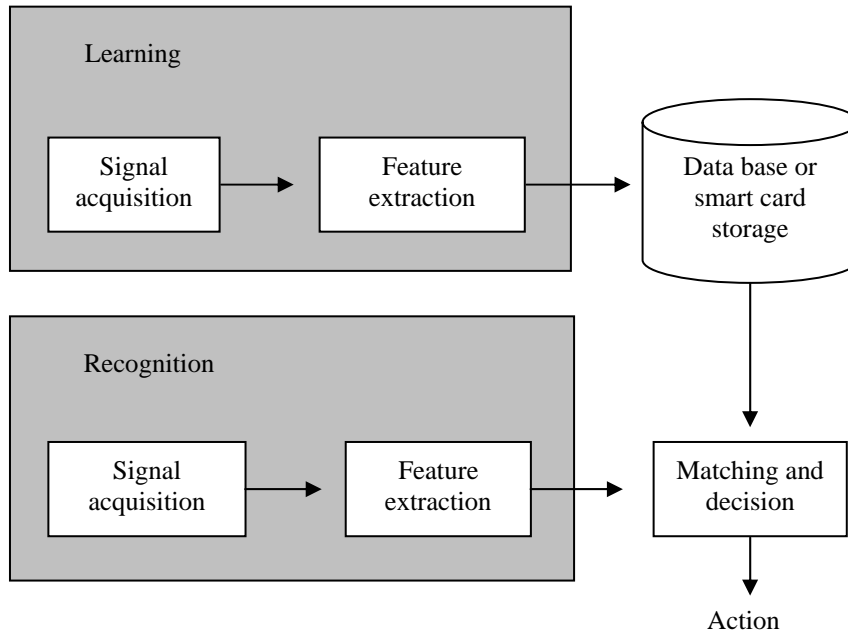


Fig. 1: The various modules of a biometric system

1.2 What are the different types of errors a biometric system can make?

Biometric systems are often evaluated solely on the basis of recognition system performance. But it is important to note that other factors are involved in the deployment of a biometric system. One factor is the quality and ruggedness of the sensors used. Clearly the quality of the sensors used will affect the performances of the associated recognition algorithms. What should be evaluated is therefore the sensor/algorithm combination, but this is difficult because often the same sensors are not used in both the enrolment and test phases. In practice therefore the evaluation is made on the basis of the recognition algorithm's resistance to the use of various types of sensor (interoperability problem). Another key factor in determining the acceptability of a biometric solution is the quality of the associated communication interface. In addition to ease of use, acquisition speed and processing speed are key factors, which are in many cases not evaluated in practice.

In the case of a verification system, two error rates are evaluated which vary in opposite directions: the **false rejection rate FRR** (rejection of a legitimate user called “the client”) and the **false acceptance rate FAR** (acceptance of an impostor). In Figure 2 are drawn the distributions of clients and impostors according to the response of the system which in general is a real number (likelihood) (see [1]). The decision of acceptance or rejection of a person is thus taken by comparing the answer of the system to a threshold (called the decision threshold). The values of FAR and FRR are thus dependent on this threshold which can be chosen so as to reduce the global error of the system

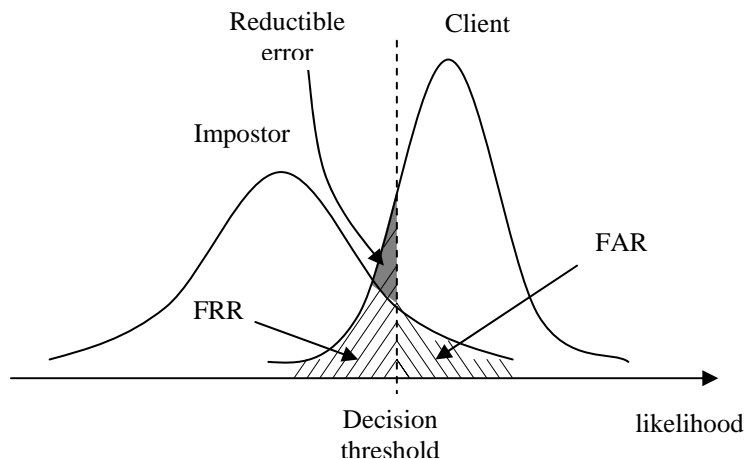


Fig. 2: False rejection rate and false acceptance rate of a biometric verification system

The decision threshold must be adjusted according to the desired characteristics for the application considered. High security applications require a low FAR which has the effect of increasing the FRR, while Low security applications are less demanding in terms of FAR (see Figure 3). EER denotes Equal Error Rate ($FAR=FRR$). This threshold must be calculated afresh for each application, to adapt it to the specific population concerned. This is done in general using a small database recorded for this purpose.

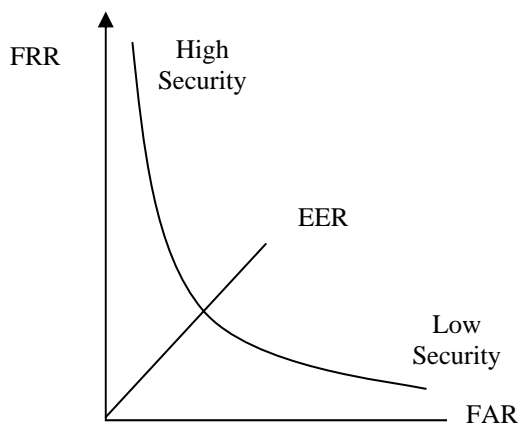


Fig. 3: ROC (Receiver Operating Characteristic) curve

1.3 Different problems with different scopes and challenges

We refer to [2] to identify three different ways of using a biometric system:

(i) Positive Identification (“Is this person truly known to the system?”).

Biometrics can verify with high certainty the authenticity of a claimed enrolment based on the input biometric sample. For example, a person claims that he is known as Mr. X within the authentication system and offers his fingerprint; the system then either accepts or rejects the claim based on a comparison performed between the offered pattern and the enrolled pattern associated with the claimed identity. Commercial applications such as computer network logon, electronic data security, ATMs, credit card purchases, physical access control, cellular phones, PDAs, medical records management, and distance learning are sample authentication applications. Authentication applications are typically cost sensitive with a strong incentive to be user friendly.

(ii) Large Scale Identification (“Is this person in the database?”). Given an input biometric sample, a large-scale identification determines if the pattern is associated with any of a large number (e.g., millions) of enrolled identities. Typical large-scale identification applications include welfare-

disbursement, national ID cards, border control, voter ID cards, driver’s license, criminal investigation, corpse identification, parenthood determination, missing children identification, etc. These large-scale identification applications require a large sustainable throughput with as little human supervision as possible. In this case, the data base must include data that can characterise each of the people in the base, and the system must then search for the person that best corresponds to what it observes.

(iii) Screening (“Is this a wanted person?”).

Screening applications covertly and unobtrusively determine whether a person belongs to a watch-list of identities. Examples of screening applications could include airport security, security at public events, and other surveillance applications. The screening watch list consists of a moderate (e.g., a few hundred) number of identities. By their very nature, these screening applications do not have a well-defined “user” enrolment phase, can expect only minimal control over their subjects and imaging conditions and require large sustainable throughput with as little human supervision as possible.

Neither large scale identification nor screening can be accomplished without biometrics (e.g., by using token-based or knowledge-based identification).

Service	Device	Storage	Database size	Accuracy
1:N Large Scale Identification	PC or smart card	Local or central database	Millions of people	Low FAR
1:1 Positive Identification/ Verification	PC or hard disks	Smart card or local database	No database needed	Low FRR
Screening	PC or hard disk	Local or central databases	Few hundred of people	Low FAR

Table 1 : Summary of some characteristics associated to the above mentioned 3 types of applications

Table 1 summarizes different characteristics associated to the three situations depicted above. Note in particular that Large Scale Identification involves the storage of the data on a central database, contrary to verification applications with which the information concerning the person can be recorded, for example on a smart card held by the user, which ensures a higher degree of confidentiality, but offer the disadvantage of potential theft or loss.

2. Description of different biometric modalities

Even if some modalities like iris or fingerprint can be considered as "sufficiently efficient", it is interesting to also envisage other inputs as the choice of one modality is linked to acceptability or usage purposes. In this report, we describe in more details 4 modalities: iris, fingerprint, DNA and face, even if there are other possible choices such as voice, signature or gaiting.

2.1 Iris recognition

How does iris recognition work?

The iris (see Fig.4) is an overt body that is available for remote (non invasive) assessment. Unlike other modalities, face for example, the variability in appearance of any iris might be well enough constrained to make an automated system possible based on currently available machine vision technologies [3].



Fig. 4: Iris image

J.Daugman is a pioneer in the iris recognition area. He published his first results in 1993[4], relying on the use of Gabor wavelets in order to process the image at several resolution levels. An iris code composed of binary vectors is computed in this way and a statistical matcher (XOR, logical exclusive OR operator) analyses basically the average Hamming distance between two codes (bit to bit test agreement). This works has been patented by a US Patent (No. 4,641,349 entitled "Iris Recognition System") held by Iridian Technologies, Inc (Ex Sansar and IrisScan).

Another approach, in the framework of iris verification, introduced by Wildes [3], consists of measuring the correlation between two images using different small windows of several levels of resolution and Linear discrimination analysis to make the decision. Also, other methods for iris verification have been proposed, in particular relying on ICA : Independent Component Analysis (a lot of research is now conducted in ASIA on this modality).

Standardization

There is no international iris standard, only a preliminary report was proposed including : Image acquisition (near infra red images), image compression (Using a low JPEG compression level), image pre-processing including boundary extraction, the used coordinate system, rotation uncertainty, image quality, grey scale density, contrast (50 grey level separations between pupil and iris, and 90 grey level separations between iris and sclera) and up to now only the UK group has rejected this report making comments about ID devices: the Japanese, German and US groups have accepted this report with some comments about iris size, iris quality measurement, and the iris compression format. The US group has asked to include some normal light image acquisition standards (instead of only near infra red images).

Summary

The iris code obtained in the corresponding encoding process is the most precise print of all existing biometric techniques, at the expense of rather constrained acquisition conditions (the camera must be infra-red, the eyes must be at a very precise distance from the camera). These elements provide a very good quality of the initial image which is necessary to ensure such a high level of performance. On the other hand they may generate a long time during the enrolment phase and the necessity of personal assistance [2]. This method also requires a relatively expensive acquisition system and necessarily involves the scanning of the eye, which can initially prove offputting to users. The resulting reliability means it can be successfully used both for identification and authentication, an advantage which few other techniques can offer.

2.2 Fingerprint recognition

State of the art

Most fingerprint processing approaches use specific features called minutiae as a description of the fingerprint. These minutiae are composed of big details like starting lines, splitting lines and line fragments and smaller ones like ridges ending, incipient ridges, bifurcation, pores, delta and line-shapes (see Fig. 5).

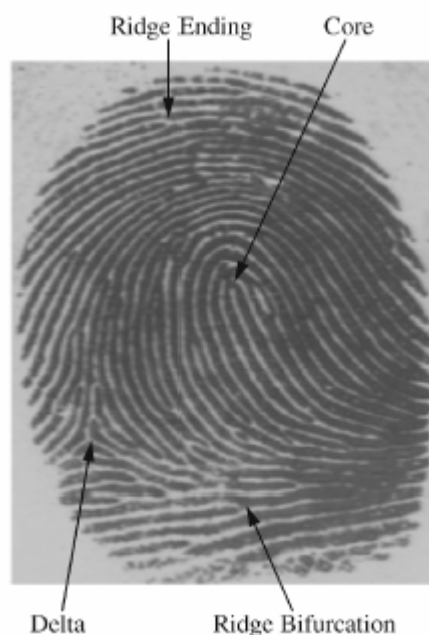


Fig. 5: Minutiae of a fingerprint

Automatic minutiae detection is an extremely critical process, especially in low-quality fingerprint images, where noise and contrast deficiency can originate pixel configurations similar to minutiae or hide real minutiae.

Several approaches to automatic minutiae extraction have been proposed [5]: Although rather different from each other, most of these methods transform fingerprint images into binary images. The images obtained are submitted to a postprocessing which allows the detection of ridge-lines. The different fingerprint authentication systems can be classified by their level of accuracy. The greater the accuracy needed, the more complex and naturally the more expensive the system is. The classification of a system is based on the number of features (minutiae) that it can deal with. The high-tech systems are able to exploit up to 80 points and also to distinguish between a real fingerprint and a forged one (synthetic fingerprint). The most widely used in general use employs some 20 particular points. Since the fingerprint is never captured in the same position, the verification algorithm must perform rotation and translation of the captured fingerprint in order to adjust the fingerprint minutiae with the template minutiae.

The final stage in the matching procedure is to compare the sampled template with a set of enrolled templates (identification), or a single enrolled template (authentication). It is highly improbable that the sample is bit-wise identical to the template. This is due to approximations in the scanning procedure, misalignment of the images and errors or approximations introduced in the process of extracting the minutiae. Accordingly, a matching algorithm is required to test various orientations of the image and the degree of correspondence of the minutiae, and it assigns a numerical score to the match. Different methods exist for processing fingerprints:

- The direct optical correlation is practically not used, because it is not very efficient for large databases.
- The general shape of the fingerprint is generally used to pre-process the images, and reduce the search in large databases. This uses the general directions of the lines of the fingerprint, and the presence of the core and the delta. Several categories have been defined in the Henry system: whorl, right loop, left loop, arch, and tented arch.
- Most methods use minutiae, the specific points like ridge endings, bifurcations, etc. Only the position and direction of these features are stored in the signature for further comparison.
- Some methods count the number of ridges between particular points, generally the minutiae, instead of the distances computed from the position.
- Other Pattern matching algorithms use the general shape of the ridges. The fingerprint is divided into small sectors, and the ridge direction, phase and pitch are extracted and stored.
- Very often, algorithms use a combination of all these techniques.

Standardization

The international ISO norm for the finger Pattern is still under discussion.

There are several American standards for the fingerprints [6]:

- ANSI/NIST-ITL 1-2000 Revision of ANSI/NISTCSL 1-1993 and ANSI/NIST-ITL 1a-1997

This standard defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial, and SMT information that may be used in the identification of a subject. Exchanged information consists of several items, including record data, digitized characteristic information, and compressed or uncompressed fingerprint, palmprint, facial, and SMT images.

This standard forms the basis for interoperability between federal, state, local, and international users of Automated Fingerprint Identification Systems (AFIS) in the interchange of fingerprint search transactions. All agencies involved in the electronic transmission of fingerprint, palmprint, facial, and SMT images and related data must adhere to the format described by the standard. Dissimilar vendor equipment belonging to agencies submitting fingerprint images to the FBI must also adhere to the standard. In addition to being able to successfully submit fingerprint search transactions to the FBI, agencies that adhere to the standard can also effectively exchange fingerprint search transactions among themselves even though their systems are manufactured by different vendors. The FBI has been a supporter during the development of this standard and they required that their AFIS system vendors comply with the provisions of this standard.

- ANSI INCITS 377-2004 Published in 2004: "Information technology - Finger Pattern Based Interchange Format":

This standard specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data.

- ANSI INCITS 378-2004: Published in 2004: "Information technology - Finger Minutiae Format for Data Interchange":

This Standard specifies a concept and data format for representation of fingerprints using the fundamental notion of minutiae. The data format is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. No application-specific requirements or features are addressed in this standard. This standard contains definitions of relevant terms, a description of where minutiae shall be defined and a data format for containing the data and conformance information.

Summary

Fingerprint is, up to now, the modality that allows the best compromise between price, acceptability and accuracy [5] and a lot of systems based on this modality are already operational. However, the latest evaluation results [7] show that the performance of such a system deeply relies on the quality of the acquired images, in particular during the enrolment phase. Moreover it seems that a not so negligible part of the population cannot be enrolled through fingerprints (manual workers, persons with too wet or too dry hands etc...); the percentage is estimated at up to 1 or 2 % but it seems that this number can be decreased with the use of two or more fingers and adequate specific enrolment processes for persons who present problems. Another point is the existence of a great number of different sensors associated with various technologies which make the interoperability problem more difficult to solve because it is the coupling of sensor and algorithms that is optimized by the designer of the biometric system and dissociating them may lead to a noticeable decrease in performance. Fingerprint is in general rather well accepted even if it has some forensic connotations and it allows both identification and verification.

2.3 Face Recognition

State of the art

In more than twenty years of research, several methods have been tested with the aim of recognizing people from the image of their face. Some of them are dealing with local features [8] like eyes, nose and mouth, while others consider the appearance of a face (Eigen face [9] and Fisher face [10] methods) but no method up to now performs sufficiently well, which means that a lot of research is still going on.

By 1993 several algorithms were claimed to have accurate performance in minimally constrained environments. To better understand the potential of these algorithms, DARPA and the Army Research Laboratory established the FERET program with the goals of both evaluating their performance and encouraging advances in the technology [11].

The FERET database testing employs faces with variable positions, scales, and lighting in a manner consistent with mug shots or driver's license photography. On databases of fewer than 200 people and images taken under similar conditions, all algorithms produce nearly perfect performance. Interestingly, even simple correlation matching can sometimes achieve similar accuracy for databases of only 200 people [12]. This is strong evidence that any new algorithm should be tested with databases of at least 200 individuals, and should achieve a performance over 95% on mug shot-like images before it can be considered potentially competitive.

The latest face verification competition FAT 2004, held in conjunction with the 17th International Conference on Pattern Recognition has shown that the best performance is obtained with a method based on independent feature analysis rather than those working with either Eigen or Fisher face methods. It also showed that by degrading the recording conditions (leading to images of lower quality), the results dropped from 1.39 to more than 13% of EER, for a database of only 52 persons. Aging also significantly degraded the performances [14].

Standardization

There is an international standard for face recognition, adopted in August 2004 "ISO/IEC JTC 1/SC 37 Biometric data Interchange Formats: Part 5: Face Image Data".

It defines the Facial Image Record Format with the following organization

- A fixed-length (14 byte) *Facial Record Header* containing information about the overall record, including the number of facial images represented and the overall record length in bytes;
- A *Facial Data Record* for each facial image. This record consists of :
 - o A fixed length (20 byte) *Facial Information* block describing discernable features of the subject such as gender, eye colour, hair colour, pose angle.
 - o Multiple (including none) fixed length (8 byte) Face Definition Parameter *Feature Points* (from MPEG4) (with position of eyes and nostril) for the purpose of feature position interchange.
 - o A fixed length (12 byte) *Image Information* block describing digital features of the image such as facial image type (Jpeg, JPEG 2000, frontal images) and dimensions such as width and height as well as source type (camera or scanner).
 - o *Image Data* consisting of a JPEG or JPEG2000 encoded data block.

There are some scene requirements for the Frontal Image Type, for example the full-face frontal pose shall be used. But the specification of the background is not normative for the creation of frontal images. Lighting shall be equally distributed on each side of the face and from top to bottom. There shall be no significant direction of the light from the point of view of the photographer. If the person normally wears glasses then they should wear glasses when their photograph is taken. Care shall be taken that the glasses' frames do not obscure the eyes.

The token face image is used to store the extracted face information from any other image source. The Token face image inherits properties from the Frontal face image format. It can be generated at any resolution using only the pixel positions of the centre of the eyes relative to the upper left corner of the full image. The purpose of the Token face image is to standardize the position of the eyes in an image and define the minimal amount of image area around the eyes. Using a token face image representation may help to reduce the amount of data stored for facial images while retaining the information needed for automated face recognition applications.

The standard is associated to best practise informations regarding face images acquisition.

Summary

Face is considered at this moment as a relatively non accurate modality due to the presence of a lot of variability (from 1.39% to more than 13% EER). Some are due to the different changes that can occur to the person over time, like aging, wearing bears or not, glasses, hair etc. while others are related to environmental conditions (illumination, textured background, poses, facial expressions).

Therefore the performance highly varies depending on the recording conditions and the context of application (static images or video, with uniform background or not, with constant lighting conditions or not).

Face recognition is not efficient enough at this moment to deal with Large Scale Identification but it can be useful in the context of verification or limited access control with constrained acquisition conditions. It means that, during enrolment, the person must face the camera at a fixed distance and that the background is uniform. This will ease the verification process while remaining acceptable for the user. In the video context, no system can be considered as sufficiently developed [11, 12] but there are promising new efforts using 3-D modeling in order to cope with the problem of pose [15, 16]. Of course this may mean the use of sophisticated 3-D scanners in place of standard medium-cost cameras, therefore increasing the cost of the global system which otherwise remain practicable.

However, due to the fact that this modality is well accepted and natural for the users, and that it has been introduced as a standard in travel documents by the ICAO, a lot of research is being conducted to improve the accuracy of the systems. A big increase in performance can be expected in the next 5 years but this modality can never be expected to be as accurate as fingerprint or iris due to its intrinsic variability and behavioral character.

Nevertheless for comfort applications (like access control to car, home or personalisation of environment) which imposes limited FAR constraints, using the face is still very interesting as it can be transparent but in this case an association with other modalities has to be considered in order to reduce the error rates or to do a preselection of the database.

2.4 DNA in Forensic Authentication

State of the Art

DNA Sequencing: DNA sequencing consists in the ordering the bases (A, T, G or C) of the DNA or of a fragment of the DNA. This procedure is quite error-prone, depending on the quality of data.

In 1970, the dot matrix or diagram method was proposed by A.J.Gibbs and G.A. McIntyre to analyze the similarity of the nucleotide or protein sequences (but not the whole DNA sequence)[17].

At the same time, Needleman and Wunsch used a dynamic programming algorithm to compute the similarity between 2 DNA fragments. The disadvantage of this method is that it is time consuming, therefore it is impossible to compare two sequences of 300 proteins (10^{88} comparisons, Waterman 1989) [17].

For this reason, the comparison of DNA segments is not used for the forensic applications, but DNA sequencing is useful to store the DNA in a computer for further research.

DNA fingerprinting: the main type of forensic DNA testing consists of DNA fingerprint: DNA fingerprinting is based on Restriction Fragment Length Polymorphism (RFLP) or Polymerase Chain Reaction (PCR).

Obtaining DNA fingerprinting is the result of a complicated laboratory procedure [18], which consists of taking DNA from a cell, cutting it into many DNA segments by using appropriate enzymes, separating DNA segments on a gel by using electrophoresis, attaching a colored probe (a small piece of DNA) to the gel and a pattern is produced. This procedure makes a single probe's DNA fingerprint.

The final DNA fingerprint is built by using several probes (5-10 or more) simultaneously. Figure 6 shows the first DNA fingerprint constructed by Professor Jeffreys using 11 probes.

As a conservative estimate in [19], when using one probe to make the DNA fingerprint, the chance that two people have the same fingerprint is 25% (in reality, this probability is less than 0.05).

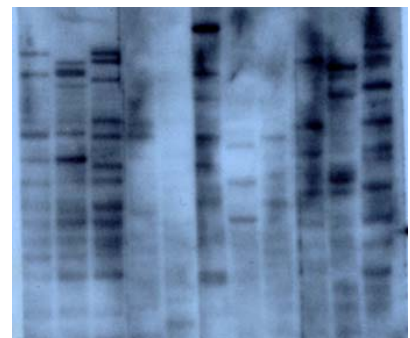


Fig. 6: The first DNA fingerprint, produced by P. Jeffreys, September 1984.

But, if we use 14 probes, the chance that two people have the same final DNA fingerprint is about $(0.25)^{14}$ or 1 per 268 million.

The set of probes, which is thus the DNA fingerprint, is visualised as a 1 D “bar code » and the DNA fingerprint matching is just a numerical comparison which allows large-scale identification.

While effective at producing highly discriminatory patterns, this technology is slow, cumbersome and manual – it couldn't be automated.

Standardization

There are many DNA sequence databases like GenBank [20], FASTA [21]. Each database has its own sequence format but conversions are possible.

Concerning the DNA fingerprint, the normalization problem is much more serious. In Europe, there are about 150 laboratories practicing DNA testing [22]. There is no common protocol and standard when making DNA fingerprints. For this reason, the DNA fingerprints of the same person made by 2 laboratories may be completely different. It makes the cross comparison of laboratories' DNA fingerprints impossible. In 1989, about 15 European laboratories decided to work together to produce some standard protocols.

Summary

Except for identical twins, each person's DNA is unique. It can thus be considered as a “perfect” modality for identity verification. However, the human DNA length is too big to allow the examination of the whole DNA sequence; in general identification techniques look at some specific areas of DNA, which are known to vary widely between people. The accuracy of this technique is thus very high allowing thus both identification and verification. Enrolment can be done from any cell that contains a structure called the nucleus. This includes blood, semen, saliva or hair samples. Acquiring these data may thus be felt as intrusive by people. At this moment, DNA analysis is performed in specialized laboratories and is cost and time-consuming (roughly 4 or 5 hours for the whole procedure). Moreover there is a complete lack of standardization which means that we are very far from being able to produce interoperable systems.

DNA usage is mainly forensic. Anyhow, future introduction, if possible, of a rapid, cheap DNA biometric authentication technique will face acceptability problems as, unlike iris or fingerprint which just correspond to performing some internal measure of the man, DNA is something that's intrinsic to, and very detailed about, the person. Anyhow, when using DNA for authentication, only a very small part of the genetic information is coded and this information is insufficient to go back to the initial genetic heritage of the person.

So, it seems that it will be a long time before DNA printing can become a real time routine for biometric authentication. However, a Canadian Laboratory recently announced a proprietary DNA extraction process which would need only simple equipment and need a time of only 15 minutes.

According to James F. Crow [23], the technical improvements in the future will be of two types : more automation and more accuracy in the existing processes. The author even foresees that DNA analysis could be made in real time. The other improvement concerns the building of new systems requiring very small amounts of material to provide an identification. Future DNA forensics are likely to involve plants and animals, they will not be confined to human DNA as each of us carries a unique constellation of viruses, bacteria and other parasites.

3. Evaluation of biometric systems

First, one can try to compare the error rates of different systems in each modality, using estimations of FAR (False Acceptance Rate) and FRR (False Rejection Rate), but these results are only indicative as only some systems in a restricted number of environments per application have been tested. In fact, the performance of the systems is highly dependent on the test conditions and very

often, the systems are evaluated in laboratory conditions with a small database and relatively good quality data. Moreover fair evaluation should include forgeries (natural or simulated) in the database and this is very rarely the case. Fingerprints and face are the subject of yearly independent international evaluation [7, 11, 24] which now aims at testing more operational situations while no open evaluation on iris is being conducted.

One must also notice that new systems show up continuously and that the performance is thus going to improve continuously. This is in particular true for face authentication, the performance of which is still insufficient for a real applications.

When trying to compare the results of different systems one has to note that the test results do not use similar test methodology or datasets of similar scale. It would be fairer to provide the global ROC curves, instead of FMR or FNMR. The technologies may not be directly comparable in the extent of specific applications.

As an illustration, we report in Table 2 what we consider as the most accurate table available at this moment in the literature [2]. FNMR denotes rejection rates also quoted as FRR in the literature. FMR are also called FAR (False Acceptance Rates) in the literature. n/a denotes data non-availability.

Biometric	Face	Finger	Iris
FTE % failure to enroll	n/a	4	7
FNMR % rejection rates	4	2.5	6
FMR1 % verification match error rate	10	<0.01	<0.001
FMR2 % large-scale identification for database sizes of 1 million	40	0.1	n/a
FMR3 % screening match error rates for database sizes of 500	12	<1	n/a

Table 2. Typical biometric accuracy performance numbers reported in large third party tests.

The face recognition results are based on FRVT 2002 [25] and its extrapolation using Eyematic data. The fingerprint authentication errors are from [26] and assume use of right index fingers with no failures-to-enroll.

Both fingerprint screening and identification assume the use of 2 fingers. Fingerprint identification performance reflects the state of the art AFIS (Automatic Fingerprint Identification System) performance based on 2 fingers against a 6 million person database with no failures-to-enroll [26]. Iris FTE is from [27] and fingerprint FTE is from [28]. Iris error rates are from ([29], p. 121). These numbers are based on what the authors [2] believe to be order of magnitude estimates of the performance of the state of the art systems.

Concerning iris, Table 2 gives no results on Large Scale Identification and Screening because there is unfortunately, at the date of writing, no public data base which enables the free evaluation of the algorithms that are commercially available. The only independent known evaluation comes from [30] which indicates an FMR of 0% with a database of roughly 2,000 people. Only Iridian [31] computed Large Scale Identification with 0% FMR and a Database of roughly 10,000 persons.

More generally, in the evaluation of operational biometric systems, other criteria than performance have to be taken into account, such as robustness, acceptability, facility of data acquisition, ergonomy of the interface, enrolment and identification time. For example one has to take into account while choosing a practical fingerprint system, the robustness of the sensor to impacts, wrong or clumsy manipulation, dirtiness[5]. Likewise, the high constraints imposed for the acquisition of irises may significantly increase the global enrolment or verification time capable of producing compression problems in some applications. Moreover, wearing contact lenses or glasses may produce errors.

Note, that for any modality a relatively large part of the population is unable to enroll and this has to be taken into account when facing a specific application. Alternative processes have always to be envisaged.

Resistance of the system to forgeries

A major characteristic of biometric recognition methods, against knowledge- and possession based methods is that it is more difficult to reproduce or steal our biometric data than to try to guess a password or to steal an object. Nevertheless, fraudulently reproducing biometric data is possible, but is very dependent on the modality, application and resources being considered and availability of the data to be reproduced.

Different points should be considered in order to answer the question: Is it possible to fool a biometric system? : the technical possibility to reproduce them artificially; the availability of the biometric data (with or without the cooperation of the person); the possibility to design biometric sensors that are resistant to this kind of imposture.

Let us consider the case of fake fingerprints: it is possible to reproduce artificially a fake fingerprint. Producing a gummy clone of an available real finger is technically possible. [32] and [33] have shown that it is possible to fool commercially available fingerprint scanners. While reproducing the ridge and valley structure is relatively easy, simulating all the physiological properties of the finger becomes more complicated, without being impossible. Considering the finger vitality detection problem, fingerprint sensors could be designed to detect physiological characteristics, such as the pulse, the blood pressure, the sweating process. But, based on the knowledge of which of these characteristics is checked in the sensor it is always possible to create a fake finger with these characteristics. [33] argue that many scanners can be fooled by heating up, flashing, humidifying. But as pointed out in [5] a fake finger that will fool all the vitality detections barriers implemented in a fingerprint sensor, can still be built given enough resources.

As far as the availability of the biometric data, it is not easy to have a good three dimensional image of the finger, while it is possible to use latent fingerprints left on different surfaces and objects by the person. However, reconstruction of a fake finger built from latent fingerprints remains quite complicated, and is less reliable.

Concerning iris, [34], it is also possible to introduce liveness tests into the cameras, but J. Daugman himself quotes that “Some low-cost, consumer-oriented, handheld iris cameras do not incorporate any effective liveness tests, as Professor Matsumoto demonstrated”. In fact, living tissue differs in many respects from artificial objects made of plastic, or printed images on paper. In the case of the eye, there are aspects of physiology, and of the optics of a working eye, that can be exploited. There are also behavioural tests of liveness. Some of these tests rely only on software, but some require special hardware as well, to detect by means of physics that this is living tissue and not fake.

It is important to notice that, in general, the performance of the systems in verification mode (in terms of FAR) are not published taking into account deliberate forgeries. The impostors are simply the other people in the database but not those who deliberately try to imitate the real trait of the person (except for signature verification where the database contains imitations). So there is almost no way to predict the behavior of a biometric system in the presence of deliberate impostors.

Multimodality

The use of several modalities can be considered in order to :

- Improve the efficiency of the global system

A single modality biometric system can be subject to a certain number of defaults leading to an expected or unexpected high level of errors.

Some errors can be due to *some noise* associated with the sensed data. It may be introduced in such data in many different ways: by sensors (for example, a dirty fingerprint), by ambient conditions (for instance, poor illumination for capturing someone’s face), or by the user (the voice of someone having a cold is a noisy input to the system). As a consequence, when comparing the sensed data to a client’s references (the stored templates of such a client), the biometric input may be incorrectly matched, and the user may be falsely rejected.

A high level of errors can also be related to *Intra-class variability*. Biometric data may be variable from one acquisition to another (depending for instance on the emotional state of the person). This intra-class variability may be stronger for some individuals, especially when talking about behavioral biometrics (like signature or voice or gaiting). Therefore, the biometric data acquired during authentication may be very different from the data acquired during enrolment. This affects, of course, the matching process and may lead the system to failure.

A biometric trait is expected to be *differential across clients*, i.e. it has to vary significantly from one person to another. Some modalities do indeed permit the identification of a person (fingerprints, iris), because of their high discrimination capability while others are less effective .

Impostor attacks /liveness. A biometric system may be attacked with forged data, or genuine data of a dead person may be presented to the sensor. Generally, behavioral biometrics (signature, voice) is more susceptible to attacks since it is easier for forgers, but physical biometrics is also the object of such attacks (there is extensive literature on how to make fake fingers) [33].

Using several **different modalities together** should help to deal with the points mentioned above, mostly when using complementary biometrics such as behavioral and physical, discriminative or not etc. [35]. Indeed, multimodality has a clear impact on performance: research works have shown that multimodal systems enhance authentication systems' performance significantly, relative to unimodal systems. Such systems have by construction a higher discrimination capability and are more difficult to attack by impostors. Indeed combining fingerprint with hand shape, or face recognition may circumvent the usage of fake fingerprints, as faces and hands are more difficult to imitate than fingers. This is also the case for voice and lip movements which are naturally correlated.

- Provide an alternative

Considering two (or more) modalities does not mean using them at the same time. Indeed if we build a biometric system relying on both fingerprint and face and if a person cannot enroll its fingerprint, because of the bad quality of his finger, then it will be possible to use only his face image for verification. Non availability of a biometric trait can also be temporary. Imagine a system functioning with iris and fingerprints. If one person during a short period has a problem with his eye, so that it is impossible to perform the iris scan, the fingerprint system can be used instead. The same thing occurs with people which would refuse to use a specific modality (for religious or health purposes for instance). So the multimodality of the system allows a flexibility by providing an alternative to the identification process.

When the modalities are considered at the same time, the fusion of the information provided by the different modalities can be done at several different levels [36]: At the decision level : in this case each system takes a decision and only at the end, the two (eventually contradictory decisions) are combined in general by a simple AND or OR operation, leading to a lot of errors or rejection. In this framework, the performance of a "bad" system can degrade those of the bi-modal system. More interesting is the case of fusion of scores. In this case, the combination concerns the scores produced by the system before producing its final decision. In this framework, the performance is always increased provided that the fusion scheme is adequately chosen [37, 38, 39]. In particular this scheme allows the reduction of the importance of a less accurate modality to the benefit of a more accurate one (case of face and fingerprint for example). In certain cases, the two modalities that are combined may be very correlated. This is the case for example, of lip movement and voice recorded together when a person is speaking. In these cases, it is possible and interesting to fuse the information at an even earlier stage, namely just after feature extraction and to build a unique system taking as input a combination of these features.[40].

Application Issues

One has to distinguish between "Mass Identification" applications (border control, National ID cards, Visas etc.) which demand a great level of security (very low FAR) and domestic, personal applications (ambient intelligence, personal accesses to computers) for which the constraints are low FRR and friendly interfaces.

Mass identification involves:

- Storage of the data on a central Database

- High accuracy level
- User constraints for high quality enrolment

The size of the population may be a problem, when considering access times to database, fluidity of the entire process.

Interoperability is another issue : if we want a border control system to be used in several Schengen area entry points, either we have to use the same system all over Europe, or we need the different systems to be interoperable (which means the ability of software and hardware on multiple machines from multiple vendors to communicate). Interoperability between different systems is achieved by using common standards and specifications. At this moment, the standardization of the data formats (for iris, face, fingerprint) is in rapid progress in the ISO- SC37 commission.

As far as only raw data are considered, these formats will indeed assure interoperability but some propositions are also made concerning the standardization of templates (like minutiae for fingerprints or face images with explicit position of the eyes). Storing templates instead of raw data presents the advantage of compressing the information and insuring more security in case of attack. However, it will not allow complete interoperability. Moreover, as soon as functional interoperability is wanted (interchange of algorithms from different vendors), there is a need for some software interchange formats. The BioAPI specification language has been introduced for this purpose, but its use burdens the whole identification system. It seems that such constraints are essentially suitable for verification systems (1:1) while in the context of Large Scale Identification systems, they increase the processing time which can be prejudicial for an operational system. Very few tests have been conducted so far concerning real interoperability issues which thus remain a fundamental question. Let us just quote here from [41] that with the cooperation of organizations representing seafarers and shipowners, the International Labour Office ILO has just completed a six-week test involving 126 volunteer seafarers on the M.V. Crystal Harmony, a vessel operated by Crystal Cruises. The seafarers included men and women from 30 countries and covered a wide distribution of ages and a diverse set of seafaring job categories.

The testing exercise involved seven biometric products submitted by various manufacturers. The ILO has found that two of them met the requirement of global interoperability.

In the second type of applications, the focus is on transparency and comfort for the user. So non-intrusive biometrics may be used such as video recording. In this case one can recover from a sequence of images, different types of correlated information such as gaiting [42], voice in correlation with the face images. As none of these modalities is effective enough by itself they cannot be used alone. However, the redundancy that the joint use of all this information will provide, will be an important tool to insure a final good reliability in the identification of the people.

Biometrics can therefore be seen as a way to simplify everyday life, reducing the number of keys, passwords and pin codes that we have to memorize.

Biometrics as a way to increase privacy and anonymity and security

Biometrics presents users with the ability to protect and secure their privacy despite the ubiquitous nature of the Internet and almost all forms of commerce, but due to the fact that in general, biometric data are stored in Large Data Bases, one can also consider that privacy and security issues are not satisfied by the actual implementations of biometrics. One interesting issue to this problem is to consider Biometric Encryption which is defined in [43] by Dr. George Tomko as the use of the unique pattern in a person's fingerprint as one's private encryption or coding key. Fingerprint is only an example but iris or other stable biometrics can be envisaged. This way, the fingerprint of one person can be used to code the PIN allowing access to a bank machine. The coded PIN has no connection whatsoever with the finger pattern. What is stored in the database is only the coded PIN. The finger pattern only acts as the coding key of that PIN, any PIN. The fingerprint pattern, encrypted or otherwise, is not stored anywhere during the process. It stays on the finger, where it belongs.

But there is another benefit to all of this, and that is, true privacy: the operation of successfully decoding the PIN confirms my eligibility for a service without having to reveal any personal identifiers. Since I'm the only one that can decode the PIN, it is not based on trust. It is "absolute" privacy.

There is also an indirect benefit to privacy. We can continue to have a multitude of PINs and passwords, thereby achieving "safety through numbers" versus one single identification with which to link everything.

The development of biometric encryption techniques is not an easy task because the image of the finger pattern itself is "plastic" and does not remain stable. Each time that you place the fingerprint on a finger scanner, from a holistic view, it may appear to be the same, but there are actually small differences in the pattern due to dryness, moisture and elasticity conditions of the skin. In addition, cuts and scratches can change the pattern. It is somewhat like "fuzzy" decryption. That is the challenge that developers of this new technology face. Furthermore, the system must be built so that these PINs or keys can only be decoded with a "live" finger pattern. It must be immune from a latent print lifted off an object, or a 3-D silicone replica of someone's finger pattern. Some [44] solutions have been already proposed and some patents [45] applied for, but this still remains a research topic as the fact that biometric patterns are never exactly the same while doing different acquisition, renders the production of a private key, that needs to be similar at each stage, very difficult.

Biometric data storage

As soon as only verification is requested, the biometric data can be stored on smart cards kept by the user, which provides him with the insurance that the data cannot be used without his own authorization, contrary to what happens with a centralized database. Biometric verification/identification can also be realized through remote access, in this case there is a need for a transmission of the biometric image or template through a network. This means having a highly secure connection. Watermarking may also be used in this case to insure that the transmitted data have not been corrupted.

Of course smart cards can be lost or stolen. For this reason, the data that it contains must be encrypted but if the information has been retrieved by a robber, it is necessary to be able to revoke it and to produce another template which could be used for further identification. Revocation is easy when dealing with pin codes or passwords but not with biometric traits as we cannot change our iris or our fingerprint. Cancellable biometrics is a new research field and some preliminary propositions have been made.

One method of cancellable face biometrics is described in [46]. Considering a face image of a person, it is possible to generate new images obtained after a filtering of the original image. The coefficients of the filter are randomly generated thanks to a PIN code. Changing the PIN code means changing the filter and therefore changing the new face image generated. It has been demonstrated that for face recognition and if the matching algorithm relies on correlations this process does not affect the result of recognition. More research is needed to confirm these results on other face recognition methods.

The use of such filtering is not straightforward for fingerprint or iris recognition, because it affects the quality of the images and the accuracy of the minutiae detection (fingerprint) or texture analysis (iris). For iris, one solution is to extract from the 2048 bit length code a smaller length and to use only this information in the matching process.

Much work has been made in the framework of encryption and watermarking in which the concern is how we can protect the stored data. Even if the aims are different, cancellable biometrics can adapt some of watermarking or encryption method. The two most known techniques in watermarking or encryption are those developed by Rathan Connell and Bolle [47] and Jain et al [48]. The first one, which is more interesting for cancellable biometrics, relies on the use of special deformations on an image (face, fingerprint) like grid morphing or random transformation like block permutation. This watermarking technique can be easily adapted and turned into a cancellable biometric technique by introducing a PIN code to generate the grid morphing coefficients or the block permutation parameters.

The second watermarking technique consists of embedding face information into the fingerprint one. In the recognition process, the system reconstructs the face and the fingerprint image from the embedded fingerprint image.

It seems, at this stage of research, that cancellable biometrics can't work without introducing a PIN code. We can use the right iris instead of the left iris, or one of our ten fingerprints in order to

introduce some cancellation in our biometrics data, provided that enrollment has been realized with a large set of data, but it is not a completely satisfactory solution.

From my point of view, there are still a lot of unsolved problems in the first type of applications (interoperability, storage, accuracy). At this moment, different experiments are being undertaken by several entities (Africa, Asia, US, Europe, EU member-states, etc..) without any coordination. Let's quote for example, the Nigerian National ID card where fingerprints have been stored on 2D bar codes. 50 millions people were enrolled in 4 months, two years ago. A project of a National ID card is now in progress in the Arab Emirates. The fingerprints will be stored on a smart card and the check will be on the card itself (match on card).

Malaysia is developing a multi-usage biometric smart card while Large Scale Experiments of a system relying on iris identification for border control are in progress. It will concern 2 million of air passengers. No smart card is envisaged, the checking will be through identification in a database (1:n). Australia is developing an access checking application for the flying staff relying on face verification from the chip included in the passport (which means, with the ICAO standard, the storage of the face on a contactless chip inserted in the passport). Interoperability is requested[ref SAGEM, private communication]. France will introduce the principle of INES (Identité Nationale Electronique Sécurisée) National Electronic Secured Identity, which will be certified by the government and necessary to obtain either the CNIe (National electronic ID card) and/or the passport. This "identity" will associate alphanumeric data from the civilian state and physical data (photo, fingerprint, signature).

In the second type of application, some products are already available (see for example [49] for a list of products and companies) but there is a lack of certification procedures for the market to develop widely. Use of videos (face, gaiting) in the home environment is still an open issue and a potentially good topic for research which should lead to interesting results in the near future. Note that the corresponding results will be also useful in a wider field than purely biometrics, namely videosurveillance and tracking.

Conclusion :

The introduction of biometric elements in a global identity authentication system is often seen as a way to increase security. There are still challenges considering biometric systems for large scale identity verification. Large scale experiments have been conducted in the past in non-european countries (Africa, Asia) and some are now being conducted in Europe but it seems that this is done without any coordination and that the results are not widely spread and directly reusable.

There is still a lack of independent evaluations and testings. NIST (National Institute of Standards) in the US and CBAT (Centre for Biometric Authentication & Testing)² in China are working in this direction. The BioSecure Network of Excellence³, aims at becoming such an European Center for evaluation and testing of biometrics algorithms and systems.

Biometrics can also be seen as a way to increase privacy and anonymity when considering personal security needs. It would be nice to increase the education of the future users and operators in order to demystify this topic which is still considered to some extent as science-fiction, as well as to continue to develop technical research in relation to the actual needs of the citizens and the states.

² <http://www.sinobiometrics.com/pdf/xuchenghua.pdf>

³ <http://www.biosecure.info>

References

- [1] B. Dorizzi, P. Lamadeleine, C. Guerrier, J.L. Les Jardins : Biométrie : Techniques et usages, Revue des sciences et techniques de l'ingénieur, Avril 2004
- [2] Anil K. Jain et al : "Biometrics: A grand Challenge", Proceedings of International Conference on Pattern Recognition", Cambridge, UK., August 2004
- [3] R.P. Wildes, "Iris recognition: an emerging biometric technology", Proceedings of the IEEE , Volume 85, Issue 9, pp. 1348 -1363, September 1997.
- [4] J. Daugman, "High confidence recognition of persons by rapid video analysis of iris texture", European Convention on Security and Detection, pp. 244 -251, 16-18 May 1995.
- [5] Maltoni D., Maio D., Jain A.K., Prabhakar S., Handbook of Fingerprint Recognition, Springer, 2003.
- [6] ANSI Homeland Security Standards Panel: Biometric Workshop Report April 2004
www.itl.nist.gov/iad/highlights/2001/fingerprint.html
www.ncits.org/tc_home/m1htm/docs/m1040266.pdf
www.incits.org/tc_home/m1htm/docs/m1030014.pdf (see part 2 Scope)
- [7] FINGERPRINT VENDOR TECHNOLOGY EVALUATION 2003 <http://fpvte.nist.gov/>
- [8] Kazunori Okada, Johannes Steffens, Thomas Maurer, Hai Hong, Egor Elagin, Hartmut Neven, and Christoph von der Malsburg. The Bochum/USC Face Recognition System And How it Fared in the FERET Phase III test. In H. Wechsler, P. J. Phillips, V. Bruce, F. Fogeman Soulié, and T. S. Huang, editors, Face Recognition: From Theory to Applications, pages 186–205. Springer-Verlag, 1998.
- [9] M. A. Turk and A. P. Pentland. Face Recognition Using Eigenfaces. In Proc. of IEEE Conference on Computer Vision and Pattern Recognition, pages 586 – 591, June 1991.
- [10] J. Ross Beveridge, Kai She, Bruce Draper, and Geof H. Givens. A nonparametric statistical comparison of principal component and linear discriminant subspaces for face recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 535 – 542, December 2001.
- [11] FERET Database. <http://www.itl.nist.gov/iad/humanid/feret/>. NIST, 2001.
- [12] P.J. Phillips, H.J. Moon, S.A. Rizvi, and P.J. Rauss. The FERET Evaluation Methodology for Face-Recognition Algorithms. T-PAMI, 22(10):1090–1104, October 2000.
- [13] vismod.media.mit.edu/tech-reports/TR-516.pdf
- [14] International Conference on Pattern Recognition, Cambridge, UK, August 2004
- [15] C. Xu, Y. Wang, T. Tan and L. Quan, "A New Attempt to Face Recognition using 3D Eigenfaces". In 6th Asian Conference on Computer Vision (ACCV), Vol. 2, pp.884-889, 2004.
- [16] Chang, Bowyer and Flynn "Face recognition using 2D and 3D Facial Data", IEEE international workshop on analysis and modeling of faces and gestures, pp. 187-194, October 2003.
- [17] David W. Mount. "Bioinformatics, Sequence and Genome Analysis", Cold Spring Harbor Laboratory Press, 2004
- [18] http://www.alumni.ca/~fren4j0/dna_fingerprinting.htm
- [19]] <http://users.rcn.com/jkimball.ma.ultranet/BiologyPages/R/RFLPs.html>
- [20] <http://www.psc.edu/general/software/packages/genbank/genbank.html>
- [21] <http://www.biosci.ohio-state.edu/~genomes/mthermo/>
- [22] <http://europa.eu.int/comm/research/success/fr/soc/0356f.html>
- [23] James F. Crow , "DNA Forensics : Past, present and Future", Genetic Identity Conference Proceedings, Tenth International Symposium on Human Identification, 1999

- [24] Duane M. Blackburn, Mike Bone and P. Jonathon Phillips. Facial Recognition Vendor Test 2002., <http://www.dodcounterdrug.com/facialrecognition/frvt2002/frvt2002.htm>, DOD, DARPA and NIJ, 2002.
- [25] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J.M. Bone, "FRVT2002: Evaluation Report", http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf, March 2003.
- [26] Jain-29. C. Wilson, M. Garris, and C. Watson, "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints" NISTIR 7110 , May, 2004, http://www.itl.nist.gov/iad/893.03/pact/ir_7110.pdf
- [27] BBC News, "Long lashes thwart ID scan trial", 7 May 2004, news.bbc.co.uk/2/hi/uk_news/politics/3693375.stm
- [28] NIST report to the United States Congress, "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability." Available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf, November 2002.
- [29] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, *Guide to Biometrics*. Springer, 2003.
- [30] National Physical Laboratory, UK, CESG contract X92A/4009309 (2001), Biometric Product Testing Final Report. Available on-line at <http://www.cesg.gov.uk/technology/biometrics>. For comparisons against 8 competing biometrics, see Figure 6, page 12 of the NPL report.
- [31] J. Daugman (2003), "The importance of being random: Statistical principles of iris recognition", *Pattern Recognition*, vol. 36, no. 2, pp. 279-291.
- [32] Putte T, Keuning J.; Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned"; in Proc. Working Conf. on Smart Card Research and Advanced Applications (4th); Proc. TC8/WG8.8, pp.289-303, 2000
- [33] Matsumoto T., Matsumoto H., Yamada K., Hoshino S.; Impact of artificial ""gummy"" Fingers on Fingerprint Systems; Proc. of SPIE, vol. 4677, pp. 275-289, Feb. 2002
- [34] http://www.findbiometrics.com/Pages/feature_daugman_camuk.htm
- [35] A. K. Jain & A. Ross, Multibiometric Systems, *Communications of the ACM*, January 2004/Vol. 47, N°1
- [36] J. Kittler, M. Hatef, R. Duin and J. Matas, "On combining classifiers, *IEE Trans. On Pattern Analysis and Machine Intelligence* 20, 3 (Mar. 1998), IEE, NY, 226-239.
- [37] S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J. Leroux-Les Jardins, J. Lunter, Y. Ni, D. Petrovska-Delacretaz, "BIOMET: a Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand and Signature Modalities", Proc. of 4th International Conference on Audio and Video-Based Biometric Person Authentication, pp. 845-853, Guildford, UK, July 2003.
- [38] B. Ly Van, R. Blouet, S. Renouard, S. Garcia-Salicetti, B. Dorizzi, G. Chollet, "Signature with text-dependent and text-independent speech for robust identity verification", pp. 13-18, Workshop on Multimodal User Authentication, Santa Barbara, USA, 2003.
- [39] C. Sanderson, S. Bengio, H. Bourlard, J. Mariéthoz, R. Collobert, M.F. BenZeghiba, F. Cardinaux, S. Marcel, "Speech&Face Based Biometric Authentication at IDIAP ", IDIAP Research Report 03-13, February 2003.
- [40] Brown, C. C., X. Zhang, R.M. Mersereau & M. Clements "Automatic Speech Reading with Application to Speaker Verification". ICASSP International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2002
- [41] <http://www.ilo.org/public/english/bureau/inf/pr/2004/53.htm>
- [42] Baseline Algorithm and Performance for Gait Based Human ID Challenge Problem, <http://gaitchallenge.org>
- [43] George Tomko, Data Protection Authorities Workshop, Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy? Hotel Reyes Catolicos, Santiago de Compostela, Spain, September 15th, 1998, <http://www.dss.state.ct.us/digital/tomko.htm>
- [44] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", *Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management*, Vol. 92, No. 6, June 2004.

- [45] Colin Soutar, Danny Roberge‡, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar « Biometric Encryption »™, Bioscrypt Inc. , The content of this article appears as chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nichols, McGraw-Hill (1999)
- [46] “Cancelable Biometric Filters For Face Recognition”, Marios Savvides, B.V.K. Vijaya Kumar and P.K. Khosla, International Conference of Pattern Recognition, ICPR 2004, Cambridge.
- [47] Ratha, Connell, Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, vol. 40,no. 3, 2001, pp. 614-634.
- [48] Jain,Uludag, Hsu, "Hiding a Face in a Fingerprint Image", Proc. of ICPR, Aug., 2002
- [49] <http://www.alibaba.com/>