MBioD

Multimodal Biometrics for Identity Documents [1]

State-of-the-Art

Research Report

PFS 341-08.05
(Version 2.0)

Damien Dessimoz
Prof. Christophe Champod

Jonas Richiardi
Dr. Andrzej Drygajlo

{damien.dessimoz, christophe.champod}@unil.ch
{jonas.richiardi, andrzej.drygajlo}@epfl.ch

UNIL | Université de Lausanne

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

June 2006

[1]This project was sponsored by the *Foundation Banque Cantonale Vaudoise*.

Contents

Chapter 1

Introduction

The issues associated with identity usurpation are currently at the heart of numerous concerns in our modern society. Establishing the identity of individuals is recognized as fundamental to the numerous administrative operations. Identity documents (IDs) are tools that permit the bearers to prove or confirm their identity with a high degree of certainty. In response to the dangers posed by theft or fraudulent use of identity documents and security threats, a wide range of biometric technologies is emerging, covering e.g. face, fingerprint and iris. They are also proposed to enforce border control and check-in procedures. These are positive developments and they offer specific solutions to enhance document integrity and ensure that the bearer designated on the document is truly the person holding it. Biometric identifiers - conceptually unique attributes - are today portrayed as the panacea for identity verification.

In many countries, identity document is increasingly associated with biometrics. Most modern identity cards include chips embedding biometric identifier. Under the impetus of the United States of America, a large number of countries (all EU countries) are developing biometric passports. ICAO (International Civil Aviation Organization, a United Nations specialised agency) issued specific recommendations for travel documents inviting its members to use facial images and optionally fingerprint or iris as a biometric modalities. The Swiss government is currently conducting a pilot study by testing and evaluating the passport of next generation developed according to ICAO recommendations.

This project has been triggered by the frenetic technological promises and claim of simplicity of biometric technology applied to identity documents. We believe that the deployment of such technology is a complex task that should receive proper attention. This research initiative (MBioID) addresses the following germane question: *What and how will biometric technologies be deployed in identity documents in the foreseeable future?* This research proposes to look at current and future practices and systems for establishing and using identity documents and evaluate their effectiveness in large-scale deployments.

Today, most research is focused on studying various biometric modalities independently. This renders comparisons between various biometric solutions difficult, thus a multi-modal approach will be favored in this initiative.

This report constitutes the *first milestone* of the MBioID project. At the outset of the initiative, it was felt that all relevant information should be gathered in a review document, in order to establish the current state-of-the-art. In such a rapidly evolving field, this step was of paramount importance to conduct research both for the elaboration of acquisition and evaluation protocols and for the establishment of a multimodal biometric research database. Discussion of the cost and whether or not the deployment of biometrics in this context will ensure adequate security or improve border controls is one that requires political involvement. Such considerations have been left out of this report.

This report is organised as follows:

Chapter 2 presents the main biometric definitions that are required when apprehending such a field. Emphasis is put on the generic properties (including a typology of errors), processing steps and architectures (including cryptography) that are shared regardless of the biometric attribute considered. Multimodal biometrics is also defined. It allows developing and reaffirming a common language that is sometimes missing in the literature and insist on the important distinction between using biometrics for verification purposes as opposed to using biometrics for identification purposes. Verification implies a 1 to 1 comparison between the acquired feature of a person claiming an identity and one template corresponding to that identity. Identification aims at finding an unknown individual in a database of N persons.

Interoperability for biometric passport is a key component to ensure all passports issued by each country are readable by the readers placed at borders. Chapter 3 offers a review of the main standards developed in the biometric industry and standardisation organisations (such as ISO) to ensure interoperability.

Biometrics and associated issues such as privacy and personal data protection are bound to get unprecedented levels of attention. Biometric information is personal data. Adding a biometric measure to identity documents cannot be envisaged without assessing the legal framework and the potential impacts on privacy and without raising questions regarding the relationship between the state and the citizen and the proportionality of the state's actions. *What will be collected, why and how* are questions that the state needs to address in a transparent manner. Following the 27th International Conference of Data Protection and Privacy Commissioners (September 2005), a resolution on the use of biometrics in passports, identity cards and travel documents calls for the implementation of effective safeguards and the technical restriction of the use of biometrics in passports and identity cards to verification purposes. Chapter 4 looks internationally at the tendencies on these issues. The option has been taken to leave out a full historical perspective, even though such a perspective is decisive to fully apprehend what is at stake. For that, we invite the reader to refer to the collective work edited by Caplan and Torpey [1] and to the recent

[1] Caplan J and Torpey J, Documenting Individual Identity - The Development of State Practices in the Modern World. Princeton: Princeton University Press, 2001.

issue of the *Cahiers de la Sécurité* (2005, No56, Police et identification).

Chapters from 5 to 9 summarise the state of affairs in terms of technological development for a range of biometric modalities (face, fingerprint, iris, on-line signature and speech) that can potentially play a role in identity documents. The choice of these modalities has been based on ICAO recommendations and availabilities. No doubt that the future may bring additional biometric solutions, for example ear morphology. Each technology has specific strengths and weaknesses that are reviewed. The framework of analysis is analogous for all chosen modalities. It encompasses an overview of the algorithmic approach, assessments of performance, available sensors, computational resources required and availability of systems and databases. The aim is to offer a structured compilation of information that is not actually found in such a format.

At present, biometrics in identity documents are mainly investigated with one biometric modality. Given that the accessibility of the biometric feature is not perfect (e.g. a few percent of the population cannot be enrolled using fingerprints or iris because of specific activities, age, ethnic background or disability) multimodality can be viewed as a mechanism to avoid penalising individuals who do not have the required biometrics. The opportunities and constraints offered by a combination of biometric features in this area are discussed in Chapter 10 with an emphasis on the description of existing multimodal databases.

Chapter 11 tackles the issues associated with the integration of biometric features in identity documents, by reviewing the ICAO and NIST (National Institute of Standards and Technology) technical requirements and presenting today's state of play in various countries and organisations.

To conclude this review document, we propose in Chapter 12 a short summary and outline of the future work that will be undertaken under the MBioID initiative. The deployment of biometrics in identity documents cannot be seen as a single technological challenge. The issues associated with it are technological, legal or societal, and call for a larger debate. Taking performance issues for example, the rate of failures to enrol forces to deal with exceptions procedure and discuss its fairness when compulsory enrolment is suggested. Choosing an adequate biometric technology for that task will indeed be guided by considering rates of false matches and non-matches. But setting the acceptable limits will require political decisions that are outside the strict technological arena.

We take this opportunity to thank the University of Lausanne, the EPFL and the Foundation BVC for the financial support to the research initiative.

Chapter 2

Definitions

2.1 Identity and identity documents

2.1.1 Identity

The term of *identity* is defined as "the quality or condition of being the same in substance, composition, nature, properties, or in particular qualities under consideration" [1]. The *personal identity* is thus a data set that allows to recognize a person and to distinguish her from another one, and that can establish the identity of this person. Identity always refers to a reference group or community. Indeed, our identity is function of this group or community in which we are in some point in time. According to Edmond Locard [166], this data set is at the basis of the identification process and allows to distinguish the *identical* from the *similar*.

> *"En police scientifique et en droit, l'identité est l'ensemble des caractères par lesquels un homme définit sa personnalité propre et se distingue de tout autre. Dans ce dernier ordre d'idées, établir l'identité d'un individu, est l'opération policière ou médico-légale appelée identification. Un homme peut être semblable à plusieurs autres, ou à un autre, au point d'amener des erreurs; il n'est jamais identique qu'à un seul, à lui même. C'est à discriminer avec soin les éléments de ressemblance des éléments d'identité que consiste le problème de l'identification".*

For Paul Kirk [158], this individualisation process is also essential to criminalistics:

> *"The real aim of all forensic science is to establish individuality, or to approach it as closely as the present state of the science allows. Criminalistics is the science of individualization.*

An *identity* is also defined as "a presentation or role of some underlying entity" [66]. In the case of a a human being, this *entity* can have some physical features such as its height, weight or DNA, called *attributes*. The *identity* of this *entity* has also some *attributes*, such as a username, a social security number or particular authorisations and permissions. The term *legal identity*, usually

assigned to every citizen, can be introduced here, referring to the fact that all human beings should be known and individualized by their registry office [182]. In the case of identity documents, it is this *legal identity*, associated to a particular *entity*, which can be verified.

Three approaches are available to prove a person's identity [194] and to provide "the right person with the right privileges, the right access at the right time" [291]. These identity proving approaches, which establish the genuineness of the identity, are:

Something you have The associated service or access is received through the presentation of a physical object (keys, magnetic card, identity document, ...), in *possession* of the concerned person.

Something you know A pre-defined *knowledge*, as a password normally kept secret, permits to access a service.

Something you are Measurable personal traits, such as *biometric* measures, can also be used for identity prove.

A combination of these approaches makes the identity proof more secure. In day to day activities, the combination of *possession* and *knowledge* is very widespread. The use of the third approach, in addition to the others, has significant advantages. Without sophisticated means, biometrics are difficult to share, steal or forge and cannot be forgotten or lost. This latter solution provides thus a higher security level in identity prove.

2.1.2 Identity Documents

An *identity document* (ID) is "something written, inscribed, etc., which furnishes evidence or information upon a subject" [1]. This piece of documentation is designed to prove the identity of the person carrying it. The document contains a data set that allows a person to be recognized and distinguished from another one. According to the Swiss law, an identity document, a passport or an identity card [70] [1], certify the Swiss nationality and the identity of the owner [69] [2].

The International Civil Aviation Organization (ICAO), an agency of the United Nations, recommends, in its technical report [125], the deployment of Machine Readable Travel Documents (MRTDs), containing also biometric measurements. The characteristics selected by this organisation to be used in the new generation of identity documents (facial, fingerprint and iris images) have to be stored on a contactless chip with specific technical constraints[3]. The choice of using MRTD was imposed by the willingness to improve the registration (entries and exits) at the borders. The use of biometrics came after, with thee purpose of facilitating the verification process and increasing security. Figure 2.1 presents an example of a machine readable part, line surrounded, of a

[1] Swiss federal prescription on identity documents available online at `http://www.admin.ch/ch/f/rs/1/143.11.fr.pdf`.

[2] Swiss federal law on identity documents available online at `http://www.admin.ch/ch/f/rs/1/143.1.fr.pdf`.

[3] Please note our remarks on contactless storage in Section 2.7.

Swiss identity document. A more complete description of the ICAO standards is presented in Section 3.5.

Figure 2.1: Machine readable part of a Swiss identity document.

According to the ICAO Doc 9303 [4] [124], a secure issuance process is described as follows:

- Criminal background checks in respect of document applicants and officials involved in the passport issuance process.
- Secure access to facilities and computer networks dedicated to document issuance.
- Detection and elimination of duplicate documents (in the registry).
- Identity verification of applicants who claim ownership of issued documents.

The current issuance process of an identity document without biometric information, as well as temporary documents, in Switzerland can be described as follows [5]:

- The applicant has to register personally his request with the competent municipal authorities.
- The applicant has to furnish several breeding documents to prove who he is, such as an old identity document, origin act or individual certificate of family status for single person and family book for married persons.
- The competent municipal authorities collect personal data, which will have to appear on the identity document, and biometrics, such as currently a recent photograph, fulfilling special conditions.
- Issuance accepted or denied.

[4] ICAO Doc 9303 available after ordering at `http://www.icao.int/mrtd/publications/doc.cfm`.

[5] Description of the Swiss issuance process available at `http://www.schweizerpass.admin.ch`.

After this process, the owner of this new document can prove and establish his identity and his nationality, and can use it for general purposes and daily activities in the society.

The issuance process of an identity document with biometric information in Switzerland, set up for the pilot project, will follow these steps [6]:

- The applicant has to register personally his request with the competent municipal authorities, furnishing the same breeding documents as the current issuance process.
- The applicant has to go in a biometric enrollment center five days or at most thirty working days after the registration. A facial image will be acquired and stored in the Swiss identity document's information system, called *ISA*.
- The new passport will be recieved at least after 30 working days. The applicant has the possibility to check in a biometric enrollment center if the passport is operational. Furthermore, the applicant has the possibility to consult in biometric enrollment centers the data stored in the chip.

In other countries, the issuance process is similar to the Swiss one. For example, Figure 2.2 describes the issuance process in the United States of America for a visa, including collection of biometric data.

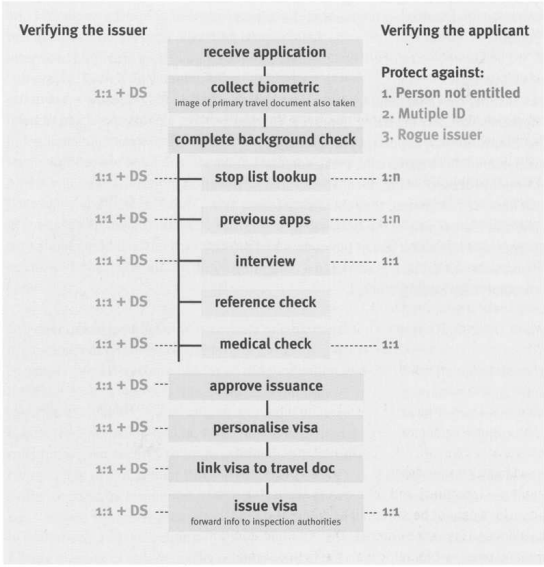


Figure 2.2: United States of America's identity document issuance process [52].

It is important to warn against potential breach of security at all the stages of this issuance process. Indeed, a security breach for the breeding documents

[6]Description of the Swiss issuance process for biometric identity document available at `http://www.schweizerpass.admin.ch`. Section 11.4 presents a complete description of the new Swiss biometric passport.

to be supplied can make useless a security increase, such as the use of biometrics, in the identity documents. So the documents establishing the identity in the first steps have to be genuine. It is then important that the administrative personnel involved in this process possess robust knowledge in the detection of forgery and have at their disposal original documents for comparison, as well as specialised knowledge on security elements integrated into documents to be submitted.

In this technical report, the term of *Identity Documents* is related to travel documents used for verifying the identity of the owner, as a visa, an identity card or a passport. Some documents are also available, for other purposes than border checking, for verifying the rights of the owner to some loans and authorisations, such as driver license, medical and allowance card and specific access to a protected place.

2.2 Biometrics

2.2.1 General Definition

Every human being has experience in recognizing a familiar person, in daily activities, by using his/her specific characteristics, like voice, face, gait, handwriting and signature. Some people, more than others, have even the ability to recognize unknown persons, after having seen or heard them.

The difficulties associated with person identification and individualisation have already been highlighted by the pioneers of forensic sciences. Alphonse Bertillon developed in the eighteenth century an anthropometric identification approach, based on the measure of physical characteristics of a person [24]. The term of biometrics used today is the scientific follow-on of this approach, abandoned in these days in favor of fingerprinting.

Biometrics is a term that encompasses "the application of modern statistical methods to the measurements of biological objects" [1]. However, by language misuse, the term biometrics usually refers to automatic technologies for measuring and analyzing biological and anthropological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for identity prove. *Biometrics* refers "to identifying an individual based on his or her distinguishing characteristics" [34]. Note that a legal definition of the term *biometrics* does not exist at the moment [110]. Actually, such technologies are used in several domains, person authorization examination in e-Banking and e-Commerce transactions or within the framework of access controls to security areas. Ideally the biometric characteristics used should satisfy the following properties [280] [7]:

Robustness Over time, the characteristic should not change (*Permanence*), and thus have a low *intra-class variability*.

Distinctiveness Over the population, a great variation of the characteristic should exist (*Uniqueness*), and thus have large *inter-class variability*.

[7] The corresponding terms used earlier by [64] for these ideal properties are indicated in brackets.

Availability Ideally, the whole population should possess the characteristic (*Universality*).

Accessibility The characteristic should be easy to acquire (*Collectability*).

The characteristics could be *physiological* or *behavioral* [194]. Characteristics, which can be measured on a part of the body at some point in time (passive), are physiological biometrics. On the other hand, characteristics, which are learned or acquired over time (active), are called behavioral. These last characteristics are produced by an individual with a special effort, and are hence dependent to some degree on his state of mind. For example, fingerprint, hand geometry and face are physiological biometrics, while dynamic signature, gait, keystroke dynamics and lip motion are behavioral onces. Biometric characteristics such as voice could even be viewed as a combination of physiological and behavioral traits [34, 146]. Indeed, the voice depends on physical features such as vibrations of vocal cords and vocal tract shape, but also on behavioral features, such as the state of mind of the person who speaks. Another class of characteristics can be added to the classification of biometrics [194]: the *biological* ones. The main biological characteristic is the Deoxyribonucleic Acid (DNA). It can be detected in biological material, such as blood, skin and saliva and is often cited as the ultimate biometrics [34, 146]. Biometrics of this category are never used, nowadays due to technological constraints, for instant automatic identity prove process, while those of the two other classes are often used for such purpose.

In this report, the term *modality* will be used to name these characteristics separately.

2.3 Use of biometrics

2.3.1 Biometric System

A *biometric system* is essentially a pattern-recognition system [146, 223]. Such a system involves three aspects [141]: data acquisition and preprocessing, data representation, and decision-making. It can thus compare a specific set of physiological or behavioral characteristics to the characteristics extracted beforehand from a person, and recognise this last one. The digital representation recorded in a database, which describes the characteristics or features of a physical trait, is defined as a *template*. It is obtained by a feature extraction algorithm. The complete process is described in Section 2.5. Biometric systems are traditionally used for three different applications [202]: *physical access* control for the protection against unauthorized person to access to places or rooms, *logical access* control for the protection of networks and computers, and *time and attendance* control.

An *authentication* procedure, a way "to let the system know the user identity" in information technology [173], can be performed in two modes by a biometric system [34, 146]:

Identification This method consists in selecting the correct identity of an unknown person from a database of registered identities (Figure 2.3). It is called a "one to many" matching process, because the system is asked to complete a comparison between the person's biometrics and all the biometric templates stored in a database. The system can take either the "best" match, or it can score the possible matches, and rank them in order of similarity [291]. Two modes are possible, positive and negative identification, as described in a taxonomy of uses in [280] (Figure 2.4 summarizes the differences between them). The *positive identification* tends to determine if a given person is really in a specific database. Such a method is applied when the goal is to prevent multiple users of a single identity. A *negative identification* determines if a given person is not in a "watchlist" database. Such a method is applied for example when the goal is to identify persons registered under several identities.

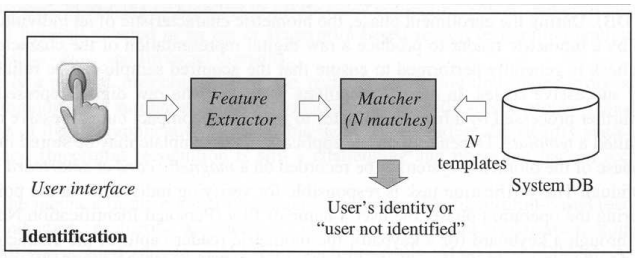


Figure 2.3: Identification task [173].

Positive	Negative
To prove I am someone known to the system	To prove I am not someone known to the system
To prevent multiple users of a single identity	To prevent multiple identities of a single user
Comparison of submitted sample to single claimed template – "one-to-one" under the most common system design	Comparison of submitted sample to all enrolled templates – "one-to-many"
A "false match" leads to "false acceptance"	A "false match" or a "failure to acquire" leads to a "false rejection"
A "false non-match" or a "failure to acquire" leads to a "false rejection"	A "false non-match" leads to a "false acceptance"
Alternative identification methods exist	No alternative methods exist
Can be voluntary	Must be mandatory for all
Spoofed by submitting someone else's biometric measures	Spoofed by submitting no or altered measures

Figure 2.4: Summary of the *taxonomy of uses* [280].

Verification This method consists in verifying whether a person is who he or she claims to be (Figure 2.5). It is called a "one to one" matching process, as the system has to complete a comparison between the person's biometric and only one chosen template stored in a centralized or a distributed database, e.g. directly on a chip for an identity document. Such a method is applied when the

goal is to secure and restrict specific accesses with obviously cooperative users.

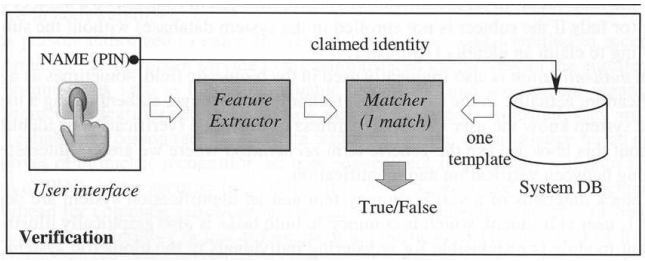


Figure 2.5: Verification task [173].

The application environments of biometric systems are variable, and thus a taxonomy has been proposed in this field [280]. They are classified in six categories:

Overt vs. covert If the user is aware about the acquisition of his biometric characteristics, the application is overt and declared; if not, the use is called covert.

Habituated vs. non-habituated If the user presents his biometric characteristic(s) every day, the application is considered as habituated (after a short period of time); if the frequency of use is low, the application is considered as non-habituated.

Attended vs. non-attended If the user is observed and guided by supervisors during the process, the application is called attended; if not, the use is called non-attended.

Standard vs. non-standard environment If all the conditions can be controlled and if the use takes place indoors within standard conditions, the application deployment is called within standard environment; if not, the use is called in non-standard environment.

Public vs. private If the users are customers of the system, the application is public; if the users are employees, the application is called private.

Open vs. closed If the system used works on completely proprietary formats, the application is called closed; if the system can exchange any data with other biometric systems used in other application, the use is called open.

2.3.2 Properties of biometric systems

Besides the basic properties that a biometric has to satisfy (see Section 2.2.1), some additional properties have to be considered in a biometric system [34, 64, 146]:

Performance All the factors that influence and affect the accuracy and the computational speed of a biometric system.

Acceptability The population should accept the fact that the characteristic is taken from them.

Circumvention The ability of a system to resist against potential threats and spoof attacks.

Exception handling The ability to complete a manual matching process in the case of an impossibility of features' extraction and modality use for certain persons.

System Cost All the costs of the system components, in adequate and normal use.

Some limitations, related to the properties described above, have been noticed when only a unique modality is used in biometric systems [146]:

Acquisition of noisy data The biometrics itself can be perturbed by noise, for example a scar on a fingerprint. The acquisition process can also be the reason of the background noise, for example, a fingerprint sensor maintained in a non-appropriate state, changing face's illumination during the acquisition, or background noise when a speaker recognition system operates.

Intra-class variability The data acquired during the enrollment can be different from the data acquired at the authentication process, because of changes in the technical characteristics of the sensor, an incorrect human-machine interaction, or simply day-to-day variability of the modality, affecting thus the matching process.

Distinctiveness While an ideal biometric trait should satisfy the property of uniqueness, the features extracted from real trait always possess some interclass similarities, making this property less specific. The term of *inter-class variability* can be used to describe this phenomenon.

Non-universality The desired property of universality of a biometrics means that everybody should have the specific trait. However, it is not the case. There are some people for which the system is not able to extract the features of their biometric, either due of the poor quality of the features, or because they can not present their trait at all. According to [146], about 4% of the population has not fingerprint ridges of sufficient quality to be enrolled. Recent research of the National Institute of Standard and Technology (NIST) tried to estimate the proportion of the population who have fingerprints that are hard to match [115], and the results were not so alarming. On a set of 6'000 frequent users of the US-VISIT programme (with 10 samples of each right and left index), the authors noticed that none of the subjects had fingerprint ridges that were *always* hard to match and less than 0.05% of the subjects had fingerprint ridges that were *usually* hard to match.

Spoof attacks Biometric systems have to resist against spoof attacks and detect impostors who want to circumvent the system. Biometrics that can be acquired surreptitiously are particularly vulnerable in that regard (voice and face can easily be covertly acquired, but with some degree of inventiveness signature and fingerprints can be as well). Biometric systems using physiological biometrics such as fingerprint and iris have also recently been proved likely to be spoofed [184, 185]. Spoof attacks can occur by using artificially created biometrics, by attacking via input port and at database [251], or by producing any data such as a noised facial image that allow to establish a fake identity [160]. Anti-spoofing measures can be the use of passwords or smart cards, a supervising acquisition process during the transactions, the use of multimodal biometric systems, the use of quality measures of the input signal and the use of liveness detection methods. Systems which have not any liveness detection countermeasure, whether it is for fingerprint or iris, can be fooled by using either artificial gummy fingers, or simple eye images printed on paper. For detecting spoof attacks through fingerprint sensors for example, distortion [12], perspiration [83] or odor [16] can be used. It should also be mentioned that some biometric characteristics are *revocable*, and other not. Indeed, there is a "life-long linking of the biometric characteristic to the data subject" [7]. The *revocation* means the possibility to change or modify the biometric characteristic if this latter is compromised by a spoof attack (i.e. in the case of an "identity theft"). The signature modality is the only biometric characteristic that can be modified completely if it is compromised. However, when fingerprints are used for identification or verification purposes, the possibility of choosing another finger for the recognition process remains, which is also the case for iris and hand geometry/palmprint modalities, but only to some extent.

2.4 Processing steps for biometric data

For all biometric modalities, biometric data will be transformed according to the processing steps described below and summarised in the activity diagram of Figure 2.6.

Capture or acquisition The biometric data (voice, on-line signature, fingerprint, ...), also called biometric presentation, is digitised via the input device (microphone, pen tablet, fingerprint scanner, ...) and stored in memory.

Preprocessing The signal-domain acquired data is prepared for feature extraction. This is typically used for normalising the signal-domain data and remove biases or sources of corruption in a systematic fashion. For speech, this will for instance include DC component removal as well as silence detection and removal. For signatures, this stage would include translating the signature to start at $(0, 0)$ coordinates and resampling the signature. For fingerprints, this may include rotation normalisation and thinning (skeletarisation).

Feature extraction Discriminative features are extracted from the preprocessed data. Although features are very different for each biometric modality, the general underlying principle remains the same: this processing step typically reduces

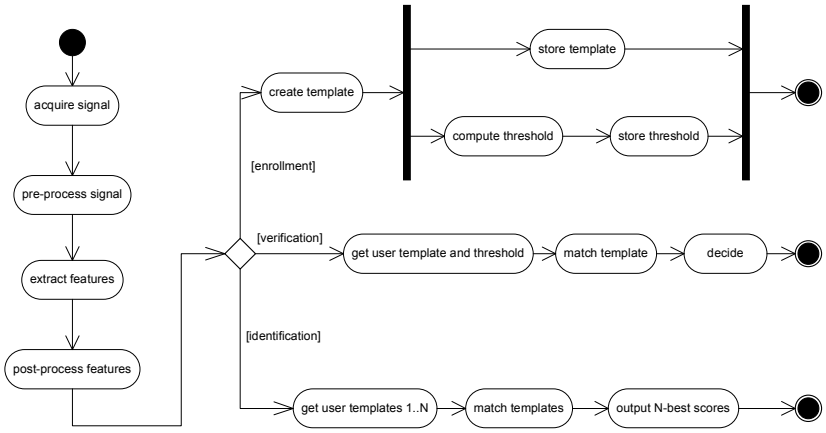


Figure 2.6: Processing steps for enrollment, verification, and identification.

the dimensionality of the input data to create a feature-level representation of input patterns that will be used by the classifier to perform pattern recognition. Typical examples of features include Mel Frequency Cepstral Coefficients or Perceptual Linear Prediction coefficients for speech, tangent angles and velocities for on-line signature, and minutiae locations for fingerprint: "In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features" [280].

Postprocessing Features are normalised to remove bias or adapt them to the classifier. An example of removing feature-domain bias is cepstral mean subtraction for speech, where transmission channel effects can be compensated for. Additionally, certain classifiers such as neural networks or support vector machines work best when their inputs have comparable dynamic ranges.

Template creation User models, also called templates, are created from training feature sets to obtain a generic representation of a user that will be used for future comparisons. Many algorithms and procedures can be used depending on feature and model class. For speech or signatures this can involve training Gaussian mixture models (GMMs) using an iterative procedure.

Background model creation A background model, also called world model or anti-model, is needed by some biometric algorithms to provide normalisation for user presentation scores. They represent an "average" of the users from the population of the system. They are typically created by pooling together features of many different users.

Template storage Once their parameters are estimated, user models are stored in a secure location for use in later biometric operations.

Template matching A biometric presentation is compared with a particular user's biometric template. This typically results in a presentation score which is somehow related to how likely it is that this particular user is the source of

that presentation. Depending on model and classifier types, this processing step will vary. For instance, GMM classifiers will use a likelihood-based score. For a given presentation, match scores are typically computed as the ratio of the score of the presentation with respect to a particular user's model to the score of the presentation with respect to the background model. Thus, this represents a kind of hypothesis testing, where the hypothesis is "is it more likely that this presentation was produced by this particular user rather than anyone else in the background population?".

Threshold computation Several presentations belonging to a particular user and several presentations not belonging to that particular user (impostor presentations) are matched to that user's model to determine a hard limit (the threshold) below which a presentation will not be considered as belonging to the user. Thresholds can be user-independent (system-wide) or user-dependent, which is largely reported to give lower error rates. Again, many threshold computation procedures exist but most do work in the presentation score domain. Not all biometric modalities need a threshold, for example fingerprint matching requires no threshold.

2.4.1 Biometric operations using the processing steps

The processing steps described above will be used in the following higher-level biometric *operations*.

Enrollment A user is added to the biometric system. A certain number of biometric presentation of a particular user are *acquired*, *preprocessed*, transformed into *features*, and *postprocessed*, then used to train a user *model* and adapt (retrain) the *world model* if necessary. The user model along with impostor presentations may be used to obtain a *threshold* for that user. The new model is then *stored*, along with the threshold for that user if needed.

Verification The claim to a user's identity causes the presented biometric data to be compared against the claimed user's model. Thus, the biometric data is *acquired*, *preprocessed*, transformed into *features*, and *postprocessed*, before being *matched* with the claimed user's model and the resulting score being compared with the stored *threshold* computed for the claimed user or a generic *threshold* value.

Identification A database of user models is searched for the most likely source of the biometric presentation. Thus, the biometric data is *acquired*, *preprocessed*, transformed into *features*, and *postprocessed*, before being *matched* with all the user models of interest. The user model that obtains the highest score with respect to the presentation is suggested to be the source of the presentation.

2.5 Performance metrics

The performance of biometric systems is measured, qualified and expressed using different rates. Some of these rates are also used to measure quantitatively the five properties, described in Section 2.3.2, for biometric systems [280].

During the enrollment, acquisition difficulties can appear with some people [34, 273], and can be quantified by rates called Failure to Acquire (FTA) and Failure to Enroll (FTE).

FTA Percentage of users for which the system has not the ability to present and acquire a usable biometric sample during the enrollment and the transactions. FTA hence cover FTE and the quality assessment of templates. For example, the images' quality of a fingerprint can be assessed by algorithms that will allow or otherwise refuse the creation of a template or the extraction of features (see Section 6.6 for more details on an algorithm developed by NIST).

FTE Percentage of users for which the system has not the ability to generate a template of sufficient quality for the enrollment because of limitations of the technology. (The FTE measures the *availability* of a biometric modality [280].)

Another measure that can dictate the performance of the enrollment process is the Time to Enroll rate, defined as:

TTE Duration of the enrollment process from capture the features of the physiological or behavioral trait to the creation of the biometric template.

Perfect error-free matches are never generated by systems [240]. In addition to the fact that uniqueness may not be achievable as such, the outcome of the enrollment process is influenced by factors [223], such as the acquisition conditions and the intra-variability of the features extracted from the modality. As the template and the physiological or behavioral trait are never exactly identical, the system has to estimate and quantify the similarity between them and then, according to the matching criterion, the threshold, a decision is taken by the system. This result may not be in adequacy with the truth of the matter and the system may generate two *decision errors* regarding a user's (or someone else) claim (verification mode), *False Rejection Rate* (FRR) and *False Acceptance Rate* (FAR), often called *type I* and respectively *type II errors*. If no claim is made (identification mode), two *matching errors* are generated, *False Match Rate* (FMR) and *False Non-Match Rate* (FNMR) [176]. The FNMR measures the *robustness*, while the FMR measures the *distinctiveness* of a biometric system [280]. Accordingly, we have the following definitions:

FRR Percentage of users who claimed a specific identity or on which a claim (such as "He is on a watchlist") was claimed or exclaimed, for which the system has either falsely rejected them during decision process, or does not have the ability at all to acquire their biometrics (whereas it was the case during the enrollment). Hence FRR also cover the FTA/FTE aspects outside enrollment.

FAR Percentage of users who claimed a specific identity, or on which a claim (such as "He is on a watchlist") was claimed or exclaimed, and that the system has falsely accepted them for this claimed identity during the decision process (FTA/FTE should have no bearing here).

FNMR Frequency of occurrance of non match rate (i.e the submitted template does not match the one from person already enrolled).

FMR Frequency of occurrance of match rate (i.e. the submitted template matches the one from another person already enrolled).

In negative identification systems, the *Binning Error Rate* (BER) and the *Penetration Rate* (PR) can be measured [176]. Indeed, some algorithmic approaches partition the data in subspaces, in order to minimise the number of samples to compare, and thus the duration of the matching process. But "the more partitioning of the database that occurs the lower the penetration rate, but the greater the probability of a partitioning error" [176]. That will impact on FNMR.

BER Number of matching template-samples pairs that the system has placed in different bins, with regard to the number of pairs assessed.

PR Average o number of comparisons needed - under the binning scheme - between each sample and the database, divided by the size of this latter.

FRR and FAR are dependent on FMR, FNMR, FTA, BER and PR [176]. Only if a single successful match influences the acceptance, the equations representing these dependences are:

$$FAR = PR \times FMR \times (1 - FTA) \tag{2.1}$$

$$FRR = FTA + (1 - FTA) \times BER + (1 - FTA) \times (1 - BER) \times FNMR \tag{2.2}$$

Other rates which can be used with those two mentioned above, is the *Equal Error Rate* (EER) and the *Half Total Error Rate* (HTER).

EER This rate refers to the threshold setting where FNMR and FMR (or FRR and FAR) are equal. This rate is often assigned as a summary performance measure.

HTER This rate refers to half of the addition of FRR and FAR.

A threshold is said to be set *a priori* if it is estimated only on the training data, and *a posteriori* if it is estimated based on results with test data. It is not a trivial problem to set the threshold *a priori*, and the EER figure with an *a-posteriori* threshold may be hard to reach with a threshold set a priori.

One way to represent graphically FNMR and FMR is to use a *Detection Error Trade-Off* (DET) curve [179]. The error rates are plotted on both axes and the relative performances of several recognition systems can be better distinguished. Figure 2.7 presents an example of DET curves, and thus the performances, of some biometric technologies on specific evaluation protocols [176].

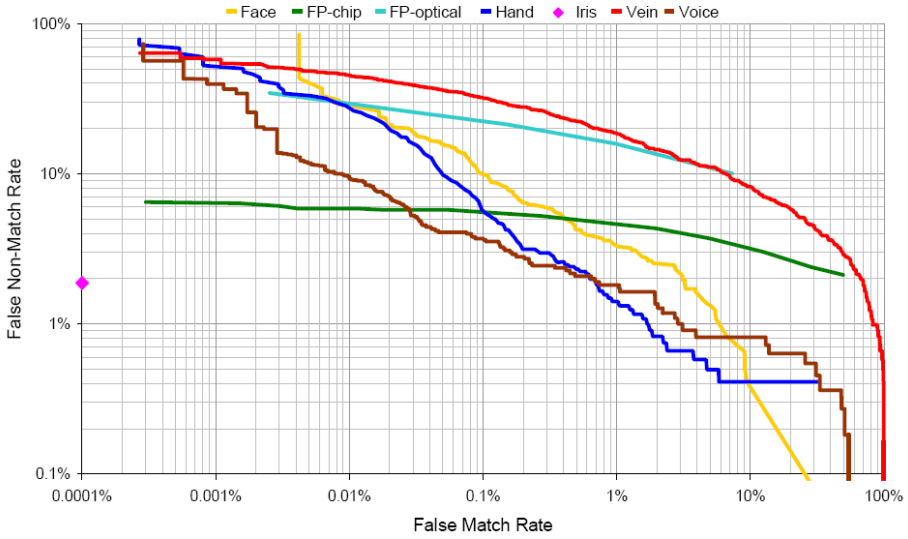


Figure 2.7: DET curves presenting the performances of the main biometric technologies [176].

Table 2.1 presents some figures for different modalities, which are taken from very different tasks, and therefore should not be construed as a direct comparison between biometric modalities.

Modality	**FMR (%)**	**FNMR (%)**	**References**
Face	1	10	[213]
Fingerprint	0.01	2.54	[172]
Iris	0.00129	0.583	[131]
On-line signature	2.89	2.89	[298]
Speech	6	6	[233]

Table 2.1: Performance examples of biometric systems.

A final way of estimating the performance of a biometric system is to focus on the matching process duration, called *Time to Match Rate* .

TTM Duration of the matching process since the end of the capture, until the system's decision.

2.6 Evaluation protocols for Biometric Systems

2.6.1 Evaluation scenarios

An evaluation of a biometric system should ideally be completed by independent organisations [214]. The complete detailed procedure, the evaluation protocol, the testing procedure, the performance results and representative examples of the data set, should be made available for the scientific community, in order to repeat the evaluation. Recommendations are also proposed to undertake successful evaluations, such as testing biometric systems on data not previously seen, completing not too hard or not too easy evaluations. Three evaluation tests can be conducted [214]: the technology evaluation, the scenario evaluation and the operational evaluation.

Technology evaluation It consists in comparing algorithms for a specific technology in typical conditions, in order to establish the current state of the art and to measure the progress of each kind of approach. These evaluations are the most frequent tests conducted on biometric systems. International competitions for fingerprint recognition (FVC), face recognition (FERET, FRVT), speaker recognition (NIST) and online signature (SVC) are examples of such evaluations [8].

Scenario evaluation It consists in measuring the system performance in a simulated application, combining sensors and algorithms. The scenarios tested should model real-world conditions as closely as possible. In [175], an example of a scenario evaluation is presented. Six modalities were used (face, fingerprint, hand geometry, iris, vein and voice) and the tests were conducted on 200 subjects over a three-month period. The objectives were to measure the performance of specific biometric systems, to promote and encourage evaluation tests.

Operational evaluation It consists in measuring the performance of a specific algorithm in a specific environment and on a specific target population.

2.6.2 Evaluation steps

An evaluation test can be characterized in 5 steps [176]: planning the evaluation, data collection, analysis, uncertainty of estimates and reporting of performance results.

Planning the evaluation The first step consists in determining what the evaluation will demonstrate and how it will be done. For an appropriate data collection procedure, all the information about the systems to be tested are needed. Then, the factors influencing the performance should be controlled, in order to observe or to minimize their effects. The subjects on which the experiments will be conducted should be fully informed and their identity should

[8] Chapters 5 to 9 contain a detailed description of international competitions for some biometric modalities.

never be released. The acquisition for enrollment and testing should be time-lapse. The test size will influence the accuracy of the results, the larger the samples, the more accurate the estimates will be. Two rules of thumb can be used for finding the test size: the *Rule of 3* and the *Rule of 30*. The rule of 3 allows to assess for a given number of comparisons N independent and identically distributed returning by chance no errors, which lowest error rate can be estimated. For a 95% confidence level, the error rate p is [9]:

$$p \approx 3/N \tag{2.3}$$

The rule of 30 proposes that the confidence interval (for 90% confidence) for the true error rate is within ± 30% of the observed error rate, when at least 30 errors are observed [10].

In order to increase the number of transactions (genuine and impostor) and keep the number of volunteers reasonable, the biometric characteristic of each subject can be acquired multiple times. The test size should nevertheless be as large as practicable and the number of samples should correspond to the requirements of the rules of 3 and 30. After collecting and analysing the data, the uncertainty in the observed error rates should be estimated, in order to determine if the data set was large enough.

Even if the data collection is demanding, several operational evaluations should not be conducted simultaneously. However, the same data set can be used for technology evaluations, while for scenario evaluations, the presentations' order of the subjects to the sensors may be randomised, for decreasing the influence that the volunteers became familiar with the sensors.

Data collection During the data collection of the *corpus* (collected biometric samples) and the *database* (information about the samples and the volunteers), errors should be avoided, for example an incorrect use of the system or the acquisition of corrupted samples, a wrong PIN for a specific subject or the presentation of the wrong body part during the enrollment.

Ideally, the system should automatically allow the recording of the biometric information and log enrollments and transactions, such as the claimed identity, the quality and the matching scores. This approach will permit a full cross-comparison of the samples, thus increasing the number of impostor scores, an improvement evaluation of new algorithms based on the same set of samples, an examination of the transactions log for checking errors in the corpus and the database, and a decrease of transcription errors. If the system evaluated returns only a binary decision, DET curves should be plotted in changing the security settings of the system. If the system allows only online testing, each subject should complete transactions at each of these security settings.

The enrollment, conducted only once for each subject, has to be made in adequacy with the evaluation scenarios. The conditions should be the same for each enrollment in a technology evaluation, similar to the target application conditions and consistent throughout the process in a scenario evaluation, and

[9] For a confidence level of 90%, this equation becomes $p \approx 2/N$.

[10] For a confidence level of 90%, the confidence interval is within ± 10% of the observed error rate, when at least 260 errors are observed.

should not be controlled in an operational evaluation. The quality of the biometric information should be checked during the enrollment. The elapsed time and/or the number of attempts for enrolling should be pre-determined, in order to determine the FTE regarding these criteria. The quality threshold of the acquisition procedure will also affect the failure to acquire rate in scenario and operational evaluation.

The elapsed time between the enrollment process and the technology evaluation, influencing the *template ageing* phenomenon, should be determined regarding the required application: the longer the elapsed time, the more difficult the matching process will be. In scenario evaluation, this elapsed time should be as close as the relevant target application, while in operational evaluation, this frequency of use should be balanced with frequent and non frequent subjects. In order to evaluate the template ageing and the fact that the user gets accustomed to the system, multiple samples should be acquired over time in different sessions.

Whether or not the samples acquired during the evaluation matched with any template already enrolled, these samples should be included in the corpus.

The presentation and channel effects have to be either uniform or randomly varying across the subjects during the enrollment and the testing process in technology and scenario evaluations, while these effects should not be controlled in the operational evaluation.

Online transactions, samples of a subjects' set compared against the templates of an other part of the database (randomly selected), or offline transactions, a full cross-comparison between every sample and every non-corresponding template, can be conducted for evaluating impostor attacks. Some conditions are nevertheless required. With partitioning systems, the templates against which the samples will be compared online should belong to the same bin (i.e. same general shape for fingerprints and same gender for voice). The use of a background database (large database containing biometric samples from different environment or population than the reference population) for online impostor transactions is not recommended, as these transactions should be made in the same environment as the genuine transactions. When the templates are dependent, the subjects used for the online impostor transactions should not be enrolled in the database. In an offline generation of impostor transactions, the samples of each subject are compared to a subset of the database, which does not contain the corresponding template. The offline impostor transactions should also not contain within-individual comparisons, such as between fingers of a same subjects. These latter transactions should thus not be included in the impostor transactions, as "within-individual comparisons are not equivalent to between-individual comparisons" [176].

Analysis The analysis of the evaluation can be completed using the rates presented in Section 2.5, such as FTE, FTA, FMR, FNMR, FAR, FRR, BER and PR.

Uncertainty of estimates The uncertainties in the performance of biometric systems can be generated by two errors types. The natural variations, called *systematic errors*, can be decreased by increasing the test size. The bias in test procedures, called *random errors*, can be evaluated and measured in changing

the environment conditions. For estimating the variance of the performance measures, some assumptions have to be made:

- The subjects used in the tests are representative of the target population.
- The transactions of different subjects are independent.
- The transactions are independent of threshold.
- The error rates vary across the population.
- The observed errors are not too limited in numbers.

Some equations are proposed in [176] for measuring the variance of false match and false non-match transactions, whether there were single or multiple transactions for each subjects.

For confidence intervals estimation, the errors observed can be approximated by parametric distributions or by non parametric methods, such as bootstrap. Bootstrap values of FMR, obtained by sampling with replacement (more than one occurrence of the same item available) from original samples allow the creation of confidence intervals on the distribution of these values. At least 1000 bootstrap samples for 95%, and 5000 for 99%, are generally required for a correct estimation of confidence intervals.

Reporting performance results In addition to all performance metrics measured during the analysis, the reporting should disclose all information about the system, the type and the size of evaluation, the demographics of the subjects, the test conditions, the elapsed time between enrollment and testing, the quality and decision thresholds used during the acquisition, the factors influencing the evaluated performance, the test procedure, examples of abnormal cases, the estimated uncertainties and the deviation from the requirements of [176].

2.7 Biometric systems architecture

Biometric systems can be implemented in different ways depending on the application scenario. These different implementations can be described in terms of the processing steps defined in 2.4. Essentially, *distributed* architectures split processing tasks between different hosts (or computers, or machines) over a wired or wireless network and typically make use of a verification or identification server, while *centralised* architectures keep all biometric processing tasks on one host, typically at the access point. Centralised architectures can be implemented on standard personal computers or embedded microprocessors such as smart cards (see 2.7.1). In the case of smartcards, a host computer to which the smartcard reader is attached can perform some processing steps such as feature extraction.

Biometric systems architectures can also be described in terms of where the template storage and matching take place. Figure 2.8 provides an overview of different storage architectures according to these two processing steps.

We stress that biometric template and/or raw biometric data storage should be handled with the utmost care, having security and privacy in mind first and

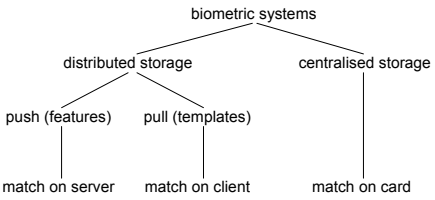


Figure 2.8: Taxonomy for biometric systems storage architecture.

foremost. Unlike a PIN number, a compromised biometric template cannot be changed (although for fingerprints it is possible to switch to other fingers).

Centralised databases containing personal information such as biometric data or templates are very likely to become focal points of attack due to their high value, and contribute to increasing (biometric) "identity theft" rather than deterring it. Numerous recent stories about large consumer database serve to highlight the problems inherent with centralising valuable data for a large number of users. For example, ChoicePoint, possibly the largest US-based identification and credential verification company, has over a period of one year leaked information about 145'000 people to fraudsters from its database [188]. More recently, on April 12th, 2005, LexisNexis admitted to a breach concerning approximately 310'000 US citizens[11], which was earlier announced to concern "only" 32'000 people. To make matters worse, LexisNexis' subsidiary Seisint had been in charge of running the MATRIX (Multistate Anti-Terrorism Information Exchange) database together with the state of Florida. Even more recently, Citigroup lost track of backup tapes containing data for 3.9 million customers[12].

Therefore, distributed storage architecture, where biometric templates and/or data is only stored on the identity document, seems the most reasonable way to prevent such large-scale security breaches, as the effort expounded to fraudulently access one person's biometric template would need to be repeated for each user.

Due to concerns about easy covert acquisition and subsequent possible recovery of the secret cryptographic key [38] or indeed, any data stored, the use of Radio-Frequency IDentification (RFID) chips or other contactless media for storing biometric data in passports should be avoided. In 2005, the Californian Senate proposed a bill (called the "Identity Information Protection Act of 2005") to forbid the use of contactless chips in identity documents [255]:

> The act would prohibit identification documents created, mandated, purchased, or issued by various public entities from containing a contactless integrated circuit or other device that can broadcast personal information or enable personal information to be scanned remotely, except as specified.

The proposal to store biometric data on a RFID chip has also come under criticism from human and civil rights organisations worldwide [225].

Furthermore, the *Swiss Federal Data Protection Commissioner* has recommended in his Annual report, that adequate measures ought to be taken in order

[11] `http://www.lexisnexis.com/about/releases/0789.asp`.
[12] `http://www.informationweek.com/story/showArticle.jhtml?articleID=164301046`.

to avoid any illegal processing of personal data if RFID are used [228]. Indeed, the persons have to be informed "about the objective of the data processing and have to know which data are processed, when, where and how".

2.7.1 Smart Cards

Smart cards are most frequently made of flexible plastic (PVC), and embed an integrated circuit micromodule containing read-only memory (ROM), random access memory (RAM), application memory (often electrically erasable programmable read only memory or EEPROM), microprocessor, and input/output controller. In addition, a card operating system or chip operating system (COS) is present, which provides basic functions such as data management, access control, and cryptographic operations.

Three prominent COS are JavaCard [13], MULTOS [14] and the ISO 7816 COS [133], but countless other COS (including the short-lived Windows for smartcards) exist in the industry. Both JavaCard and MULTOS allow applications on the card to be changed if needs be, facilitating software upgrades. JavaCard applications are developed in Java, while MULTOS applications can be written in C or native language for the underlying hardware. Both these COS provide the concept of a firewall between on-card applications to prevent one application from accessing data reserved to another application. Convergence is under way in the form of the Global Platform specifications [15], which draws from both Visa's Open Platform specification and the MULTOS specification.

In recent years, smartcard hardware has become quite powerful and versatile, with for example the ST Microelectronics ST22 family offering 32 bits RISC-type microprocessors with 32 KB of RAM, 364 KB of ROM and 256 KB of EEPROM, as well as hardware encryption functions, and supporting JavaCard 2.1 programs without recompilation. Thus, it seems that generic-purpose smartcards would provide sufficient computing power to run biometric applications.

Lately, standards have emerged to integrate smartcards and biometric data, such as the JavaCard biometric API [16] and the MULTOS Biometry C API [177], which is compatible with the JavaCard biometric API.

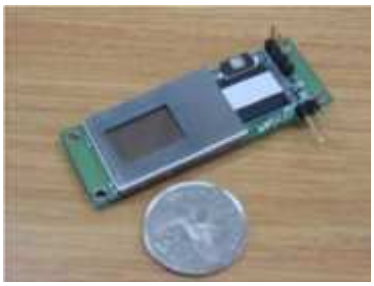


Figure 2.9: Integrated fingerprint sensor-smartcard assembly from RiTech International ltd. (RiTech website).

[13] `http://java.sun.com/products/javacard/`.
[14] `http://www.multos.com/`.
[15] `http://www.globalplatform.org/`.
[16] `http://www.javacardforum.org/Documents/Biometry/biometry.html`.

Numerous biometric-enabled smart cards are proposed by many vendors, and sensor-on-card solutions (Figure 2.9) exist for the fingerprint modality in a wide array of form factors (USB sticks, PDAs, smartphones, mice...). Match-on-card is an attractive solution also because it offers very good scalability - no matter how many users are issued with biometric identity documents, the matching time will be the same as it is performed locally.

2.7.2 Template storage

For parametric classifiers[17], a model of the user's data will need to be stored to enable verification.

Template storage is an important issue because its compromission would enable an attacker to generate very effective synthetic attacks. Furthermore, template data can be reversible to some level, meaning the original biometric or some information about the user can be gained from the template. As an relatively benign example, for a GMM-based speaker model, formant frequencies can be estimated [77], meaning the gender or accent of the user can be inferred, albeit not easily. For face images, user templates (weights) based on eigenfaces are perfectly reversible from the eigenfaces and the mean face, which means the original face image can be perfectly reconstructed (or a very good approximation if only the first few eigenfaces are used, as these contain most of the distinctive features). Therefore, template information must be considered sensitive data and stored and protected accordingly.

It should be noted that some classifiers (typically those used with the fingerprint modality) do not need background models and thus will require less storage space.

Templates can be stored in plain or encrypted form (see section 2.8), using a variety of media.

Printed storage Printed storage comprises 1-dimensional and 2-dimensional barcodes. These typically have low storage capacity compared to other forms of storage (up to about 500 bytes per square inch for 2D), but are sufficient for most biometric template storage. They may be inappropriate to store multiple biometric templates unless care is taken to choose an efficient encoding for the templates. They are well suited to be embedded in identity documents. Axtels' QR code[18] has a maximum storage capacity of 2953 bytes, or about 2.88 kB. Their DataMatrix and PDF417 barcodes have similar or lower storage capacities. Datastrip's 2DSuperscript[19] barcodes can store from 90 to 9615 bytes (8.41 kB) depending on the size of the barcode area. De La Rue International has proposed a high-density 2D barcode which can store up to 32 kB of data [264].

Optical storage Optical storage such as compact discs or digital versatile discs benefits from large storage capacities (in the low GB range) but suffer from relatively low transfer rates and large size. For these reasons they are not well suited for embedding in identity documents.

[17] Non-parametric classifiers such as k-nearest neighbours store examples of the biometric presentation instead and use no explicit modelling.

[18] `http://www.axtel.com/QRCode.htm`.

[19] `http://www.datastrip.com/english/products_detail.asp?id=268`.

Figure 2.10: Example 2D QR barcode (Axtel's website).

Solid-state storage Solid-state storage refers to integrated circuit chips or the memory found in smart cards, and a large variety of removable storage media used in digital photography such as CompactFlash, SmartMedia, Memory Stick, etc. Their capacity (32 kB is common for algorithm storage, and 256 kB can be obtained in small form factors, for example see Fig. 2.11), low access times and small form factors make them well suitable embedding in identity documents. The interface needed to read data from the chip can necessitate contact or not. In the case of RFID contactless transmission, it should be noted that problems will arise when an RFID biometric passport is appended with a RFID biometric visa and that this solution is currently not feasible [55].

Figure 2.11: Solid-state micro-controller from Samsung (S3CC9EF) with 256 kB storage and ISO 7816 compliance (Samsung website).

Magnetic storage Magnetic storage refers to magnetic substrate whose surface can be encoded to store digital information, as is the case in hard disks or DAT archive tapes. Their large capacity is counterbalanced by their relative susceptibility to mechanical problems due to moving parts. While some solutions like IBM's Microdrive go down to relatively small form factors, their cost may present an obstacle to widespread use.

Because solid-state and printed storage offer low footprints and sufficient storage, they are well suited for use in biometric identity documents.

The ICAO has defined a standard for storing biometric data, known as "logical data structure" or LDS [126]. It comprises a series of data elements such as date of birth, name, and optionally[20] face or other biometrics.

2.7.3 Processing locations

Depending on the hardware where the processing take place, we define several solutions and their acronyms in Table 2.2. We assume a limit of 32 kB memory

[20]For ID issuing authorities, the use of biometrics is optional, but if a biometric is included, it must follow the LDS.

for the smartcard solution and 32 kB for 2D barcode storage, so the DOC, FOC and TOC options also apply to 2D barcodes. This table is made to the best of our knowledge.

Acronym	Meaning	2D face	FP	Iris	Sig.	Speech
DOC	data on card	√	√	√	√ [a]	×
FOC	features on card	√	√	√	√	√
TOC	template on card	√	√	√	√	√
MOC	match on card	√	√	√	√	√
SOC	sensor on card	×	√	×	×	×

Table 2.2: Processing locations in a smart card-based architecture.

[a] Depends on signature duration.

Recently, three major biometric companies and one smart card supplier have presented a multimodal match-on-card solution, with facial, iris and fingerprint data [23]. The images of this three biometric data are stored on one high-specification Jav-based smart card and the matching process is performed on the card itself.

2.8 Cryptography

Cryptography is the art and science of making messages very difficult to read to unauthorised parties. *Encryption* refers to the operation by which a plaintext message is converted to ciphered form, making it very difficult to read, while *decryption* refers to the operation by which the original plaintext message is recovered from the ciphertext. Conversion to and from ciphertext occurs through the use of a secret piece of information called the *key*, which is a bit string of a certain length (a ballpark figure being from 64 to 4096 bits).

Two broad algorithms families can be distinguished in cryptography: *symmetric* algorithms, where the same key is used for encryption and decryption, and *public-key* algorithms, where different keys are used for encryption and decryption. Symmetric algorithms can be denoted as follows [250]:

$$\begin{aligned} E_k(M) &= C \\ D_k(C) &= M, \end{aligned} \tag{2.4}$$

where E is the encryption function using key k, M is the plaintext message, C is the cyphertext and D is the decryption function. Public-key algorithms can be denoted as follows:

$$\begin{aligned} E_{k_1}(M) &= C \\ D_{k_2}(C) &= M, \end{aligned} \tag{2.5}$$

where k_1 is the *public key*, which is publicly available and can be stored on a public-access key server, and k_2 is the *private key* known only to the intended recipient of the message. Often, private keys are protected by passwords, but can also be protected by biometric access control (see Section 2.8.1).

Another application of cryptography is for producting one-way *hash functions*. Hash functions, also called message digests or cryptographic checksums, are mathematical functions that can be applied to messages to produce unique and shorter output strings. Since no two different messages should produce the same hash value if the hash function is *collision-free*, hashes allow interested parties to verify that a message has not been modified.

Digital signatures allow a user to sign a message (or a hash thereof) to prove its authenticity. One amongst many possible algorithms based on public-key cryptography involves encrypting a hash of the message with the user's private key. By encrypting the hash with her private key, the user has proved her identity because only she knows the password to unlock the private key. At the other end, the recipient can verify the authenticity of the message by generating a hash for it using the same hash function as the sender, then decrypting the hash sent with the public key of the sender. If the locally generated hash and the sent hash match, the message has not been modified and has genuinely been signed by the sender.

2.8.1 Integration of biometrics with cryptographic techniques

Private keys of users are typically protected against misuse by a password or passphrase. If the correct password is provided, the key is *released* and can be used to decrypt a message. If the password is compromised, an unauthorised user may be able to use the private key and decrypt the message.

Thus, a first possibility for integrating biometrics and cryptography is to use biometric matching to protect the secret key. This means biometric verification and key release are two separate processes. A problem of this approach is that a biometric template still has to be stored to verify the identity claims. This mechanism has been applied to smartcard-based systems for fingerprints [63].

A second possibility is to use the biometric data directly in cryptographic key generation. This can be done by combining biometric data and other random data to create a private key. It has been applied to fingerprints [259], face [105], palm [71], and iris [112].

One of the main issues to solve in this context is that for cryptography, all bits must match exactly otherwise the data cannot be decrypted (avalanche property); unfortunately, two biometric presentations never match bit-for-bit (which is one motivation for using statistical models). Possible solutions involve the use of error-correcting codes, as for instance in [112], where the authors use two error correction codes that can withstand up to 20% bit errors.

Vielhauer *et al.* [275] have used computations based on global features of the signature to form a 24-components hash vector. This could likely be used to generate keys. While to the best of our knowledge no other research deal with this issue, it is likely that the signature modality is suitable for biometrics-based key generation.

Tuyls and Goseling have proposed a generic cryptographic framework for privacy-protective biometric authentication [269].

2.8.2 Cryptographic techniques for identity documents

The ICAO has issued a technical report concerning protection of data stored on biometric identity documents using cryptographic techniques [157]. A brief summary is provided in [156].

The ICAO technical report proposes passive and active authentication. In passive authentication, the chip holding the data does not perform any computation. A data security object contains a hash of the contents of each data group of the LDS (see Section 2.7.2), to ensure that they have not been tampered with.

In active authentication, the chip in the identity document has some capacity to perform computations and a challenge-response mechanism is put in place to ensure the chip itself has not been substituted.

The report also defines key management standards and other aspects of implementation.

Juels, Molnar and Wagner [148] provide a good overview of security and privacy risks related to the use of ICAO-based passports.

2.9 Vulnerability of biometric systems

Standard information security concerns apply to the biometric identity document case, perhaps even more stringently because of the very confidential nature of the data processed. Security issues with distributed systems (denial of service, sniffing, man-in-the-middle, replay attacks...) are also present in distributed biometric architectures.

Tuyls and Goseling [269] propose an algorithm that protects privacy and achieves secure biometric authentication, using the following reasonable assumptions about distributed biometric systems security:

- Enrollment is performed at a trusted Certification Authority (CA). The CA adds a protected form of the user data to a database.
- The database is vulnerable to attacks from the outside as well as from the inside (malicious verifier).
- During recognition an attacker is able to present synthetic biometric sources at the sensor.
- All capturing and processing during authentication are tamper resistant, e.g. no information about raw biometric data or features can be obtained from the sensor.
- The communication channel between the sensor and the verification authority is assumed to be public and authenticated, i.e. the line can be eavesdropped by an attacker.

All these assumptions can be taken as given in real-world deployment of biometric identity documents, except that the sensor/feature extraction device may not be fully tamper-resistant.

Centralised architectures such as match on card, where all processing steps are performed internally, offer the highest system security because the user's biometric data never leaves the card. Existing industrial processes for smart

cards can be adapted to the biometric case [211].

As mentioned by Albrecht [21], "the security of biometric systems depends largely on the protection of the reference data and the comparison mechanisms" [6]. Indeed, the data acquired during the enrollment and the verification/identification transactions may be genuine. Furthermore, the acquisition process has to be secured, in order to avoid any interception, replacement without the consent of the subject.

The main places of a biometric system in which attacks may occur [34, 230] are as follows (Figure 2.12):

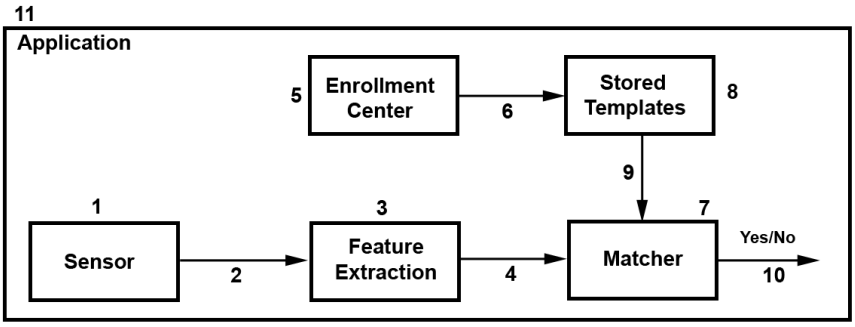


Figure 2.12: Possible vulnerable points of a biometric system [34, 230].

1. **Presenting fake biometrics at the sensor:** A true biometric representation is presented to the device, but obtained in an unauthorized manner, such as a fake gummy finger, an iris printout or a face mask.
2. **Resubmitting previously stored digitized biometrics signals (replay attack):** The digitised biometric signal, which was previously enrolled and stored in the databases, is replayed to the system, circumventing thus the acquisition device.
3. **Overriding the feature extraction process:** A pre-selected template is produced in the features extraction module using a Trojan horse.
4. **Tampering with the biometric feature representation:** During the transmission between the feature extraction and the matching module, a fraudulent feature set replaces the template acquired by the device.
5. **Attacking the enrollment center:** The enrollment module is also vulnerable to spoof attacks, such as those described in the previous points 1 to 4.
6. **Attacking the channel between the enrollment center and the databases:** During the transmission, a fraudulent template replaces the template produced during the enrollment.

[21] Member of the *German Federal Office for Information Security* (BSI) and Head of TeleTrustT Working Group Biometrics, Germany.

7. **Corrupting the matcher:** A pre-selected score is produced in the matching extraction module using a Trojan horse.
8. **Tampering with stored templates:** A template, previously stored in the database (distributed or not), can be modified and used afterward as corrupted template.
9. **Attacking the channel between the stored templates and the matcher:** During the transmission between the databases and the matching module, a fraudulent template replaces the template previously stored.
10. **Overriding the final decision:** The result of the decision module can be modified and replace the output obtained previously.
11. **Attacking the application:** The application is also a point of attack and all existing security system should be used to reduce the vulnerability at this level.

2.10 Multibiometrics

2.10.1 Generalities

In real-world applications, some limits of monomodal biometric systems have already been reported (see Section 2.3.2). Indeed some biometrics have only little variation over the population, have large intra-variability over time, or/and are not present in all the population. To fill these gaps, the use of multimodal biometrics is a first choice solution [146, 242]. In [119], Hong, Jain and Pankanti demonstrated empirically the performance improvement in integrating multiple biometrics. It seems that *multibiometrics* systems increase their robustness [238] and are more reliable [146, 241]. Indeed, multimodality approaches provide appropriate measures to resist against spoof attacks, as it is difficult to counterfeit several modalities at the same time, to circumvent a system. They also provide an adapted solution to the limitations of universality, as even if a biometrics is not possessed by a person, the other(s) modality(ies) can still be used.

2.10.2 Fusion scenarios and levels

As described in Section 2.3 and 2.4, biometric systems have four main components: *sensor*, *feature extraction*, *matching-score* and *decision-making* modules. The combination of single biometrics and the fusion of several modalities can be completed at every stage of this process. Multimodal systems can be designed to operate in five different ways [146, 242] (Figure 2.13). Some of them may not involve multiple modalities but imply a fusion at some points. They are given here for sake of completeness.

Single biometric, multiple sensors The same biometric is acquired by different sensors and combined to complete and improve the recognition process.

Multiple biometrics Different biometrics of a same person are acquired and combined to complete and improve the recognition process. This approach is the only well-named multimodal biometric fusion scenario.

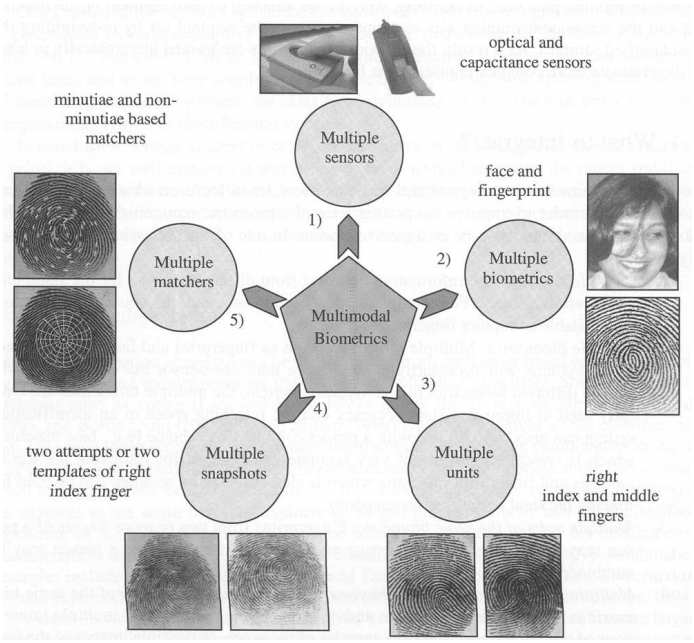


Figure 2.13: Combination schemes [146].

Single biometric, multiple units The same biometric, but different units (e.g. two different fingers), are acquired and combined to complete and improve the recognition process.

Single biometric, multiple representations The same biometric unit is acquired several times by a same sensor and combined to complete and improve the recognition process.

Single biometric, multiple matchers The same biometric is acquired ones by a single sensor and different approaches of features extraction and matching are combined to complete and improve the recognition process.

From the scenarios described above and the four important components of biometric systems, the combination and the fusion of the information acquired in each stage is possible (Figure 2.14).

Features extraction This fusion mode consists in combining the features extracted from biometrical traits, into a unique features vector, if the modalities or the features extracted are independent between them.

Matching score level This fusion mode consists in combining the scores, which describe the similarities between the biometrics acquired and their templates, obtained by each biometric system. This mode requires a scores' normalization, as the scores have to belong to a common domain before the combination

[241, 242]. A two-step process can be completed: statistical estimation of the scores distribution and translation into a common domain.

Decision level This fusion mode consists in combining the decisions taken by each biometric system, to obtain a final decision.

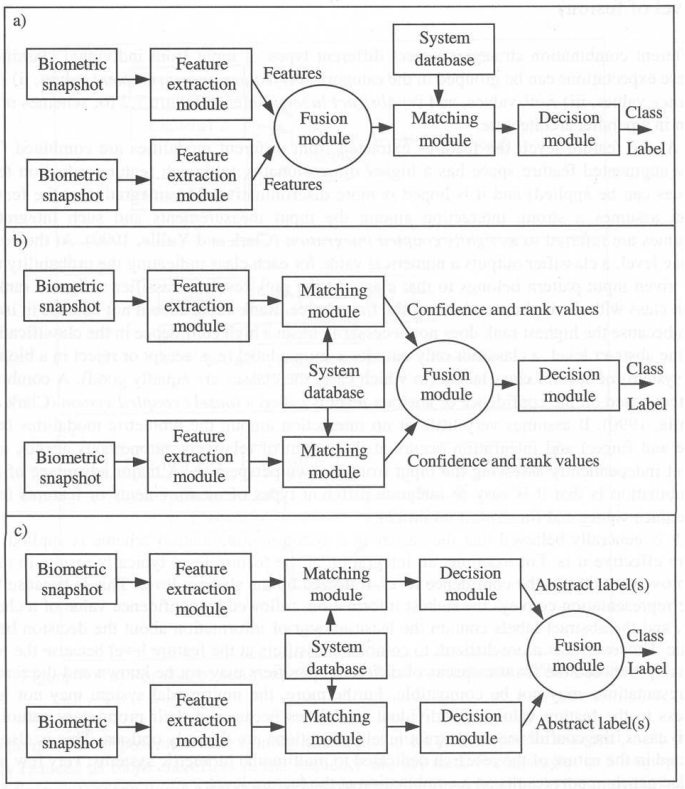


Figure 2.14: Fusion levels possibilities [241].

The earlier the fusion is operated, the more biometric systems are believed to be effective [242]. Indeed, fusion at a features extraction level is expected to provide better accuracy. However, the difficulties to complete this kind of fusion, as state of the art biometric systems generally do not allow access to this stage, the next level, the matching score level, is usually preferred. But reliable and robust biometric systems require suitable decision-level fusion approaches [238].

2.10.3 Fusion methods

In this Section, some fusion methods will be described. In the matching score level, methods such as simple *sum rules* [242], *weighted averaging* [146], *product rules, k-NN classifiers, decision trees* and *Bayesian methods* [241] can be used to combine scores obtained by biometric systems. Such approaches provide significant performance improvement. In [238], Roli et al. have subdivided the

decision fusion methods in two main categories: *fixed* and *trained* rules. Fusion strategies such as *majority voting* and *sum rule* are fixed rules, and should perform well when different systems with similar performance are combined. On the other hand, techniques such as *weighted averaging* and *behavior knowledge space* are trained rules and should perform well when systems with different performances are combined. *User-specific parameters* can be used to improve further the performance of biometric systems, with techniques such as user-specific thresholds and weights [145, 242].

2.10.4 Operational modes

Furthermore, from an operational aspect, biometric systems can perform in three different modes: (a) *parallel*, (b) *serial* and (c) *hierarchical* mode [146, 242] (Figure 2.15).

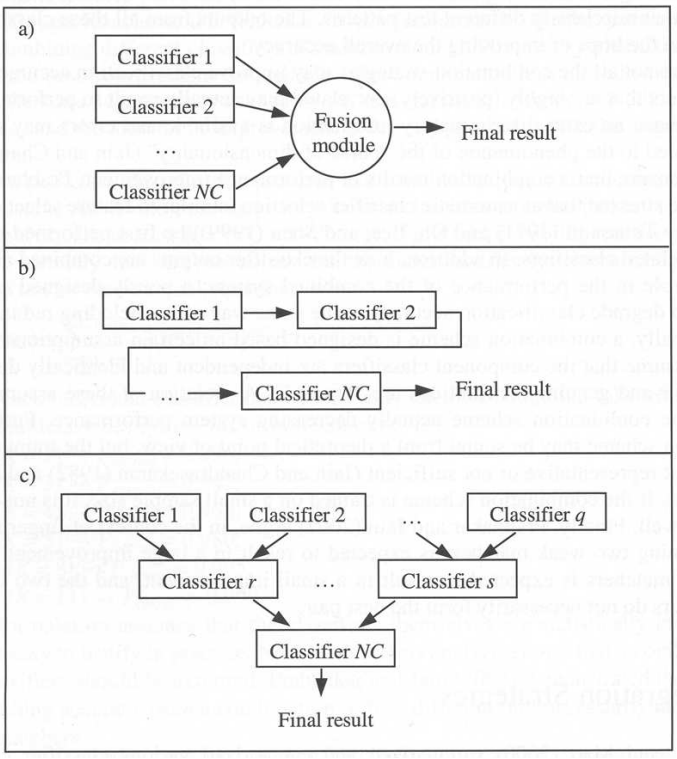


Figure 2.15: Classifier schemes [173].

Parallel mode This operational mode consists in completing the combination of the modalities simultaneously.

Serial mode This operational mode consists in completing the combination of the modalities one after the others, as it permits to reduce at the start the initial population before the following modality is used. The decision could thus

be taken before all the remaining biometrics are acquired, reducing considerably the processing duration (Time to Match rate).

Hierarchical mode This operational mode consists in completing the combination of the modalities in a hierarchical scheme, like a tree structure, when the number of classifiers is large.

Chapter 3

Standards

International standards relating to biometrics are maturing quickly, and many are already available. They support interoperability and data exchange between applications and systems, thus avoiding problems and costs stemming from proprietary systems. See [30] for a quick overview of future biometric standards which are still not approved at an international level, but may be soon approved.

For identity documents such as passports, international standards are essential so that biometric verification can be performed.

An example of interoperability is the capacity of all ePassports issued by each country to be readable by the readers placed at borders. Recently a passport - passport readers interoperability test was conducted in Japan on 8-10 March 2005 [29]. The main objective of the test was "to ensure that all passports can be read at all borders points, regardless of who has manufactured the passports and the readers", accordingly to the ICAO specifications and requirements. 16 reader vendors and 30 passport vendors (providing about 100 different passports) have participated to these tests. The tests demonstrated that on average, 82.9% of all passports could be read, while each reader could read 79.5% of all passports. Furthermore, Java-based solutions needed the slowest time to read the data contained on the chip in a *passive authentication* mode: 2 seconds with a 20Kb picture on the chip. If *Basic Access Control* is used besides, the reading time increased up to 20 seconds.

In November 2005, another passport interoperability test was conducted in Singapore [1]. The organisers had 140 ePassports specimens and 45 readers for the test, but only the results from 95 ePassports and 29 readers were published. 22 readers out of 29 had an interoperability percentage higher than 90% and only 1 reader out of the 7 remaining had an interoperability percentage below 79% (about 55%). At the end of May 2006, another international passport interoperability test will be conducted and will focus principally on cross over tests and conformity tests [2].

Another example of interoperability is the efficiency of biometric system to work with interchange formats. The MIT (Minutiae Template Interoperability Testing) project [3] will test and impove the interoperability of fingerprint

[1] See `http://www.securitydocumentworld.com` for more information.
[2] See `http://wg8.de/interoptest-berlin` for more information.
[3] See `http://www.MITproject.com` for more information.

biometrics. The main objectives of the MIT project are:

- define criteria for interoperability testing;
- develop a database of fingerprint images to enable testing;
- develop a test bed enabling the automated and repeatable testing of fingerprint minutiae interoperability, and also investigation of how factors such as image quality are important for interoperability;
- incorporate an improvement step, whereby the interoperability of the tested systems can be improve;
- provide for testing if interoperability of future systems from further vendors.

3.1 BioAPI

The BioAPI specification version 1.1 [10] intends to promote interoperability between vendors. The BioAPI 1.1 specification defines two APIs: an Application Programming Interface (API), which exposes framework functionality to the application, and a Service Provider Interface (SPI), which exposes biometric functionality to the framework. Biometric Service Providers (BSP), essentially recognition engines for a given modality also responsible for managing their user interface, implement SPI functionality. The API exposes three high-level methods: `enroll`, `verify`, and `identify`. These in turn rely on lower-level *primitives*: `capture`, which acquires the biometric signal, `process`, which extracts the features and performs pre/post-processing, `match`, which compares data to a user model, and `createTemplate`, which trains user models from supplied data. BioAPI defines a number of function signatures in C which must be implemented for the BSP or application to be BioAPI compliant.

More recently, the newer BioAPI specification (BioAPI v2.0) has been published [139]. It extends and generalises the BioAPI 1.1 framework. An interesting change is that it breaks down BSPs into sub-units called Biometric Function Providers (BFPs). These are

- Sensor BFPs, which manage sensors
- Archive BFPs, which manage access to template databases (whether stored locally on a smartcard-type device or remotely on a database).
- Processing-algorithm BFPs, which can perform pre-processing and feature extraction
- Matching-algorithm BFPs, which actually perform the match and return a score

To these functional level correspond "unit" levels, which replace the concept of "device" found in BioAPI 1.1. Thus, it is now possible for a BioAPI 2.0 BSP to use several sensors (sensor units).

As much of the SC37 standardisation efforts (see section 3.4) are based on BioAPI 2.0, it is likely that BioAPI 1.1 applications and components will migrate towards BioAPI 2.0

3.2 CBEFF

The Common Biometric Exchange File Format (CBEFF) [219] is a standard to exchange biometric data between systems and organisations. CBEFF does not provide for a standard template format, but merely for a storage format, and thus is not meant to address template sharing between applications. The BioAPI Biometric Information Record (BIR) conforms to the CBEFF specification.

This format specifies that biometric data must be encoded in three parts: the Standard Biometric Header (SBH), the Biometric Specific Memory Block (BSMB) which contains the biometric data payload, and the Signature Block, which is typically a hash of BSMB and parts of the header.

The SBH contains information such as encryption flags (if the payload is encrypted), CBEFF or patron version number, BSMB format owner and type, data length, and so on for each modality available to the application.

The BSMB is a memory block whose format can be defined by the format owner. It may contain raw (signal), intermediate (features or pre-processed data), or templates, to be used for enrollment or matching. The BSMB may also contain non-biometric data.

3.3 ANSI X9.84

The ANSI X9.84 standard [11], *Biometric Information Management and Security for the Financial Services Industry*, describes the security features needed to implement biometric verification for financial services. The Core Security Requirements are summarised here:

1. The integrity of biometric data and verification results must be guaranteed between any 2 components using software techniques such as hashes and physical measures such as tamper-resistent assemblies.

2. The source and receiver of biometric data and verification results must be authenticated, again using software or physical methods where appropriate.

3. The confidentiality of biometric data may be ensured between any 2 components.

X9.84 also describes secure enrollment, verification, storage, transmission, and termination procedures.

3.4 ISO/JTC1/SC37

The *International Organization for Standardization* (ISO) and the *International Electrotechnical Commission* (IEC), created in early 1980's the *Joint Technical Committee One* (JTC1), which has several active subcommittees, amongst other three subcommittees interesting for the biometric area [4]. The *SC17*, for Cards and Personal Identification, the *SC27* for IT Security Techniques and the *SC37* for Biometrics. All these committees have working groups, and for instance the

[4] JTC1 homepage at `http://www.jtc1.org`.

six *SC37 WGs* are in the areas of harmonized biometric vocabulary (WG 1), biometric technical interfaces (WG 2), biometric data interchange formats (WG 3), biometric functional architecture and related profiles (WG 4), biometric testing and reporting (WG 5) and cross-jurisdictional and societal aspects (WG 6).

The biometric data interchange formats, concerning fingerprint, face and iris images, proposed by the *ISO/IEC JTC1/SC37*, are presented in this section. The parts 2, 4, 5 and 6 are already approved to date [30].

Part 1: Framework This part is still not available at the time of the publication of this report.

Part 2: Fingerprint Minutiae Data The ISO/IEC SC37 working draft on fingerprint minutiae data specifies the main requirements about the extraction of minutiae features from fingerprint images and defines the data format for storage and transport and for a card-based use [134]. The minutiae are specified by a location (horizontal x and vertical y positions, with the origin at the upper left corner of the image), a direction (angle between the tangent and the horizontal line, starting on the right and going counter-clockwise) and a type (ridge ending, ridge bifurcation and other). The placement of the minutiae is function either of where the three legs of the thinned valley (ridge ending) or of the thinned ridge (ridge bifurcation) intersect, or of the ridge skeleton end or bifurcation point. The latter will be used in the *record formats*, while the *card formats* will use one of the two localizations. For the matching process, the type "other" can match with all the types and the "ridge ending" and "ridge bifurcation" type can match either with itself, or with the type "other". All these features are intended to be embedded in a *CBEFF*-compliant structure in the *Biometric Data Block*.

Part 3: Fingerprint Pattern Spectral Data The ISO/IEC SC37 working draft on fingerprint pattern spectral data specifies the main requirements about the exchange of local or global spectral features from fingerprint images and is characterized by two main steps [135]. Re-sampling of the data to a lower resolution, and dividing a portion of the image into a grid of (non-)overlapping cells for creating the fingerprint pattern spectral interchange data. Each cell can be decomposed into a 2D spectral representation (Discrete Fourier Transform) with complex spectral components characterized by a wavelength in the x and y direction, an amplitude and a phase. All these features are intended to be embedded in a *CBEFF*-compliant structure in the *Biometric Data Block*.

Part 4: Fingerprint Image Data The ISO/IEC SC37 working draft on fingerprint image data specifies the main requirements about the exchange of fingerprint images within a *CBEFF* data structure [136]. The scanner used to acquire to fingerprint image should have a minimum resolution of 500 dpi, with each pixel gray level quantized to 8 bits. Latent print scanners should have a minimum resolution of 1000 dpi. Such images with high resolution should be compressed with the JPEG 2000 standard. The signal-to-noise ratio ought to be equal to or greater than 125. The dynamic gray-scale range of image data ought to 200 gray levels for at least 80% of the captured image, and 128 gray levels for at least 99% of the captured image. The fingerprint center should be

located approximately in the center of the image capture area. For multi-finger capture, half of the fingers should be located to the left, while the other half should be to the right of the image center.

Part 5: Face Image Data The ISO/IEC SC37 working draft on face image data specifies the main requirements about a face image format for recognition applications [137]. It specifies the record format within a *CBEFF* data structure, scene constraints, photographic properties and digital attributes of the facial images. Indeed, the pose angles with respect to the frontal view of the subject as well as the geometric characteristics of the full frontal image are defined. The minimum image width should be 240 pixels, which corresponds to an image height of 320 pixels. The distance between the two eyes' centers should be about 120 pixels. The image minimum resolution should be about 300 dpi. The standard passport photo size (width x height) is 416 x 536 pixels at 300 dpi, and the average size of the uncompressed image is about 669kB (about 71kB after compression with JPEG standards). Some guidelines for travel documents' facial images are also presented: subject looking directly at the camera with opened eyes, appropriate brightness and contrast for the image without any shadows or flash reflections, a light-coloured background, image printed at a high quality resolution, face taking up 70-80 % of the photograph, with the top of the shoulders visible, showing clearly the eyes with no flash reflection if wearing glasses, without covering the face and wearing hats or caps, and have neutral expression. This working draft contains also data areas for 3-dimensional information, for example x, y and z coordinates of some feature points, such as eye location and nose length and position. But an amendment was submitted to the SC37/WG3 in order to include, additionally: to these feature points, the 3D image information and the range data in the CBEFF Header. These data will be stored using a canonical or cylindrical coordinate system.

Part 6: Iris Image Data The ISO/IEC SC37 working draft on iris image data specifies some requirements about the exchange of iris images and proposes two interchange formats, a raw data (compressed or not) and a polar image, intended to be embedded in a CBEFF-compliant structure in the CBEFF Biometric Block [138]. Each pixel of the raw image shall be represented by 256 gray levels (8 bits). During the acquisition, near-infrared wavelengths (700-900 nm) should be use for the illumination. The minimum requirement for the image resolution is that the iris diameter is between 100 and 149 pixels, but for high quality images, this diameter should be about 200 pixels or more. For the contrast, a minimum of 90 gray levels should separate the iris and the sclera, while a minimum of 50 gray levels should separate the iris and pupil. Furthermore, 70% of the iris should be visible on the image and at least 70 pixels should separate the vertical and horizontal edges of the image and the iris. The signal-to-noise ratio should be equal to or greater than 40 dB. For the lossless compression and the compressed formats, they should be in accordance respectively with the JPEG-LS and JPEG compression standards. Some pre-processing steps can be applied to the image, such as rectilinear image pre-processing (image rotation angle and uncertainty) and polar image pre-processing (boundary extraction, iris occlusions, scan type, orientation correction and polar conversion). Some requirements are also indicated for the presentation of the iris during the ac-

quisition process: vertical positioning of the head, opening the eyes as wide as possible, presenting an iris with a pupil size of 7 mm or less, removing eyeglasses and contact lenses.

Part 7: Signature/Sign Behavioural Data] This part is still not available at the time of the publication of this report.

Part 8: Finger Pattern Skeletal Data This part is still not available at the time of the publication of this report.

3.5 ICAO

The International Civil Aviation Organization (ICAO) and the International Organization of Standardization (ISO) joined their competences for publishing the Doc 9303 specifications in three separate parts with common structure [124]: Part 1 for *Passports*, Part 2 for *Visas* and Part 3 for *Official Travel Documents (Cards)*. These parts are structured as follows:

- The first two sections contain an introduction about the organisations ICAO and ISO, some definitions and references.
- The third section contains technical specifications for all MRTDs, as physical requirements, security safeguards and a standardized layout.
- Specifications unique to the MRTD under discussion.
- Specifications for additional size variant to the MRTD under discussion (only for Part 2 and Part 3).

The ICAO made some recommendations about the deployment of biometrics in machine readable travel documents [125]. Here are presented the most important requirements regarding biometrics [5]:

- Incorporation of an "optimally-compressed" facial image, and additionally, according to the will of states, a fingerprint and/or an iris image. The main advantages observed by the ICAO for the use of facial recognition in this purpose, is that this approach is socially and culturally accepted, already used for identity documents issuance and control, and non-intrusive.
- The minimum storage sizes per image in the Logical Data Structure (LDS) are about 12 to 20 kB for the facial image, about 10 kB for the fingerprint image and about 30 kB for the iris image.

3.6 Wavelet Scalar Quantization

The FBI proposed the Wavelet Scalar Quantization (WSQ) image compression algorithm as a way to standardize the digitization and compression of gray-scale fingerprint images [44]. To archive the large FBI fingerprint database (more than 40 million fingerprint cards!), an efficient compression algorithm was required

[5] Section 11.1 presents the main *technical specifications* for biometric Identity Documents.

which retained the fidelity of ridge details [121]. The fingerprint images scanned at 500 dpi (8 bits of gray-scale) are compressed with the WSQ algorithm and an "archival-quality images at compression ratios of about 15:1" are thus produced [44]. The specifications of the WSQ encoder/decoder are as follows [44] (Figure 3.1):

WSQ Encoder It consists in a discrete wavelet transform (DWT) decomposition, a scalar quantization, and a Huffman entropy coding.

WSQ Decoder It has to be able to decode these three processes and all variants of them that are allowed under the general specifications.

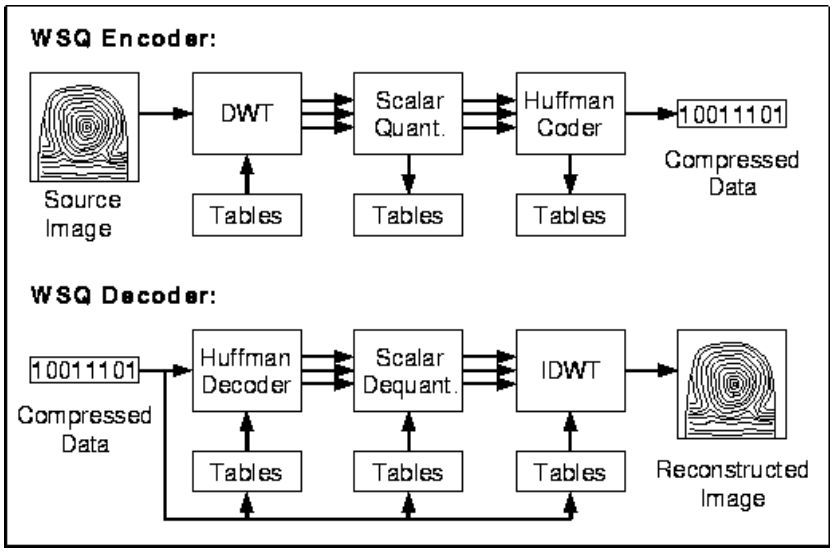


Figure 3.1: Overview of the WSQ algorithm [44].

The specifications for a WSQ certification complying by the FBI's recommendations are as follows: the commercial vendors' implementations have to be tested and thus have to belong to a category of encoders and to a single decoder with sufficient generality that any compressed images can be decoded [44]. The certification guidelines for this standardized compression algorithm are available on-line [6].

3.7 JPEG2000

The Joint Photographic Experts Group (JPEG) [7] proposed since 1988 a popular image compression standard, which efficiency was increased with the adoption of the new JPEG-2000 standard, used amongst other for digital archiving applications. Previously, the JPEG standard used Discrete Cosine Transforms, while

[6] Certification guidelines available at `http://www.itl.nist.gov/iad/vip/fing/cert_gui.html`.
[7] JPEG homepage at `http://www.jpeg.org/`.

wavelet technology are used for the new generation of compression standard, which can achieve much higher compression ratios [174]. Some features of this new algorithm are presented in [178]: state-of-the-art bit-rate compression performance; progressive transmission by quality, resolution, component, or spatial locality; lossy and lossless compression; random access to the bitstream; pan and zoom; compressed domain processing; region of interest coding by progression; limited memory implementations.

The JPEG 2000 standard is organized in twelve parts, amongst which six were adopted as ISO standards [174].

Part 1 This part defines the *core* JPEG 2000 image coding system was adopted as an ISO standard (royalty and license-fee free, but not patent free).

Part 2 This part defines various *extensions* to the base-line core system (part 1).

Part 3 This part, adopted as an ISO standard, specifies a file format for *motion* sequences of JPEG 2000 images.

Part 4 This part, adopted as an ISO standard, tests the *conformance* to the part 1, and thus the test's procedures for the encoder and the decoder processes.

Part 5 This part, adopted as an ISO standard, consists in a *reference software*, which implements in C and Java the core JPEG 2000 image coding system, described in part 1.

Part 6 This part, the *Compound image file format* adopted as an ISO standard, provides a framework for encoding compound document images.

Part 7 Abandoned.

Part 8 This part consists in *security aspects*, which specified standardized tools and solutions, such as encryption, source authentication, conditional access, and ownership protection.

Part 9 This part, the *interactive protocol*, defines solutions for delivering image and metadata

Part 10 This part defines the encoding of *3D* data.

Part 11 This part specifies additional tools for protection and errors detection for *wireless* multimedia applications.

Part 12 This part, the *ISO Base Media File Format*, is a common initiative between JPEG and MPEG, to create a base file format for future multimedia applications.

Chapter 4

Legal framework, privacy and social factors

At the 26th international conference of the data protection and privacy commissioners, the Swiss Federal Data Protection Deputy Commissioner [276] has highlighted that

> The collection and processing of biometric data must be conducted only in accordance with the requirements of data protection regulations and especially with the basic principles (lawfulness, good faith, purpose-link, data security, proportionality and rights of the persons concerned).

Here, we summarise these basic principles as per [276]. In the private sector, biometric data can in principle only be used with the approval of the person concerned, and the approval must be free, specific, and informed (*lawfulness*).

The process of collection and processing of biometric data should be transparent, and not happen without the knowledge of the subject (*good faith* principle).

The *purpose-link* principle states that if a less privacy-invasive technique such as verification instead of identification can achieve the stated goal (e.g. access control), it should be used.

The *proportionality* principle means that personal data can only be collected if they are necessary with respect to the purpose for which they should be collected and processed. As such, the question should be asked whether the desired goal could not be achieved without using personal data. Applied to biometrics, this means that putting in place an identification system is not necessary where a verification system is sufficient, and that anonymisation and encryption methods that would allow authentication without identification should be preferred. The proportionality principle is applied differently according to the country, and each country's data protection commissioner is consulted on a case-by-case basis.

According to the *data security* principle, the security of biometric systems data is essential. In case of "identity theft", the victim will be hard put to demonstrate that she has not commited the wrongdoings perpetrated by the

usurper. Thus, security measures should be put in place starting with the data acquisition process.

4.1 Legal framework

As mentioned in Section 2.2.1, no legal definition of biometrics exists at the moment, neither in Europe, nor at the international level [110]. Even if security takes more and more importance, the right for the private life and the respect of the human body are in force in most countries. This right for private life means also the protection of any sensitive personal data, as it is the case with biometrics. Legal issues for some countries will be presented in this part, beginning with Switzerland, the European Community and then with the USA, which has influenced most the international legal framework since 2001.

4.1.1 Switzerland

In Switzerland, even if there is no special law on biometrics, the *Swiss Federal Constitution* [1] protects the right to privacy and against the misuse of personal data (Art. 13). The *Swiss Federal Data Protection Act* [2] has for main objective to protect the personality and the fundamental rights of those individuals about whom undergoes a data processing. The *Swiss Federal Data Protection Commissioner* [3] has warned (in his annual reports, data protection act and information sheets and guides) about the introduction of biometric systems. He argued that the use of such systems has to respect amongst other things the proportionality and decisiveness rules. In 2002 [4], biometric information was already considered as personal sensitive data, and the use of biometric system ought only to be accepted and approved when technical security problems related to its introduction were resolved. In his last annual report [5], the *Swiss federal data protection commissioner* has mentioned that the use of biometrics has to respect some principles accordingly to data protection rules, in order to avoid risks about liberties and fondamental rights [228]. These considerations are as follows:

- Biometrics can be used if no other less intrusive mean is available.
- Biometrics can be used if the main objective is the protection and security of data.
- The finality of the processing has to be respected.
- Clear information has to be given to the concerned persons.
- The collection process of the biometric data should be explained to the concerned persons (overt collection).

[1] Swiss Federal Constitution available online at `http://www.admin.ch/ch/f/rs/1/101.fr.pdf`.

[2] Swiss Federal Data Protection Act available online at `http://www.admin.ch/ch/f/rs/c235_1.html`.

[3] Swiss Federal Data Protection Commissioner homepage: `http://www.edsb.ch/`.

[4] Press release at `http://www.edsb.ch/d/doku/pressemitteilungen/2002/2002-07-01c.htm`.

[5] The 2004/2005 annual report of the swiss federal data protection commissioner is available online at `http://www.edsb.ch/e/doku/jahresberichte/2005/index.htm`.

- Alternative choices have to be planed for people who have not the possibility to use a particular biometric.
- The identification of biometric data should only be conducted by comparing data acquired directly from the concerned person.
- The original biometric data have to be destructed after the enrollment procedure.
- Methods using biometric templates, instead of raw data, stored in decentralised databases should be privileged.
- A centralised database of biometric data, which can also be found outside the system as traces left by individuals, such as fingerprints, can only be created in the case of a "dominating interest" (i.e. security).
- Without such an interest, other modalities, such as hand geometry, have to be chosen.
- Adequate measures, such as encryption of data or the use of templates, have to be taken in order to prevent any diversion of the finality if biometric data that can be found as traces are stored in a centralised database.
- Biometric data should not be used as a unique universal identifier.
- Information about the health of the person should not be gathered from the biometric data.
- Anonymous authentication should be privileged in order to avoid the revealing of the person's identity.
- In a verification mode, the biometric data should not be used for other purposes, except if the legal framework has allowed this finality.
- A biometric system should be securised with additional identification / verification means, such as an access code.
- Starting from the enrollment, the biometric data have to be encrypted, as well as the communication in the network.
- A periodical re-enrollment is necessary in order to verify the reliability of the stored biometric data, and to avoid the ageing of the biometric information.
- The persons ought to have the possibility to control how their biometric data are used.
- Certification and audit procedures should be conducted with biometric systems. Furthermore, the risks related to their use have to be evaluated before the introduction of such systems.

4.1.2 European Community - Council of Europe

In 1981 the *Convention 108 for the protection of individuals with regard to automatic processing of personal data* [72] [6], was adopted by the Council of Europe. Its main objective is to protect personal data in general. The European Parliament and the Council of Europe proposed the *Data Protection Directive 95/46/EC* [7], which has for main objectives the protection of individuals with regard to the processing of personal data and the free movement of such data. The core values of this directive are as follows [7]: "reduction of the processing of personal data to the unavoidable extent, maintain the highest transparency possible, institutional and individual control of processing of personal data as efficient as possible". The *G29*, a consultative group of the European Community composed by representatives of national authorities of control, has warned about the danger of the conservation of biometric information in databases [108] [8].

4.1.3 United States of America

Since 2001, the USA have thought about ways to introduce legislation to enhance control of citizens and protect their territory. Three important laws have thus been introduced. The *US Patriot Act* [9] has for main objectives "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes". The *US Public Law 107-71 (the Aviation and Transportation Security Act)* [10] has for main objective the use of emergent technology in aviation security, such as the access control system for airports employees. The *US Public Law 107-173 (the Enhanced Border Security and Visa Entry Reform Act of 2002)* [11] has for main objective the enhancement of the border security of the United States, such as the introduction of biometric information in travel documents. In the recent US *National Intelligence Reform Act of 2004* (*US Public Law 108-458 / S.2845*) [12], the use of biometric technology is mentioned as a way to increase the security of the United States (e.g. the use of a biometric entry and exit data system for verifying the identity of passengers in airports and for collecting the biometric exit data, the development of an integrated biometric screening system, the use of biometrics to improve the security of travel documents and pilot licenses, the establishment of competitive centers of excellence at the national biometric laboratories and the promotion of research and development of biometric technology applications to aviation security). The *US-VISIT* program [13] belongs to these security measures for enhancing the control at US borders, and has for main objective to verify the identity of visitors with visas by collecting amongst other biometric information: the two index fingers and a photography of the face. The

[6] Available online at `http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm`.

[7] Data Protection Directive 95/46/EC available online at `http://www.dataprivacy.ie/6aii.htm`.

[8] Available online at `http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm`.

[9] US Patriot Act available online at `http://www.epic.org/privacy/terrorism/hr3162.html`.

[10] Aviation and Transportation Security Act available online at `http://www.access.gpo.gov/nara/publaw/107publ.html`.

[11] Enhanced Border Security and Visa Entry Reform Act of 2002 available online at `http://www.access.gpo.gov/nara/publaw/107publ.html`.

[12] National Intelligence Reform Act of 2004 available online at `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s2845pp.txt.pdf`.

[13] US-VISIT homepage at `http://www.dhs.gov/dhspublic/display?theme=91&content=3768`.

fingerprints collected are compared against a watchlist, against a database of individuals already enrolled by the program, and against the biometric information contained on the identity documents for verification purposes. The US *Real ID Act*, approved by the house of representatives in the beginning of February 2005, has for main objective to "establish and rapidely implement regulations for State driver's license and identification document security standards" [14]. This act will impose the use of anticounterfeiting features, machine-readable technology for all driver's licenses and other identity cards. Furthermore, this act requires that States' Department of Motor Vehicles databases should be linked and all the information shared with the federal authority.

It is important to highlight that the United States has no data protection laws, only codes of conducts or recommendations, no data protection commissioner and that the term of privacy doesn't exist in the U.S. Constitution [290].

4.1.4 France

In France, as there is no legal definition of biometrics, only the *French Data Protection Board CNIL* [15] can allow the use of biometric information, accordingly to the *French Data Protection Act* [16]. Several guidelines regarding the use of biometric technology for protecting privacy was proposed by the CNIL, such as using preferably a decentralized database and the respect of proportionality and decisiveness rules. In the future, the CNIL will evaluate, within the INES project (creation of a new biometric identity card called *CNIE* [17]), the problems generated by a centralized database for identity documents and strike an appropriate balance between the risks and the advantages of such an application. The CNIL has given its approval for the French Biometric Passport.

4.1.5 Germany

In Germany, the *Federal Data Protection Act* [18] has for main objective to protect the individual against the impairment of his/her right to privacy through the handling of personal data. Indeed, the right to *informational self-determination* which is "the power of the individuals to basically decide for themselves whether their personal data should be divulged and used" [7], is at the base of data protection in Germany. The *Federal Data Protection Commissioner* ensures that the *Data Protection Act* is implemented. Furthermore, as all European countries, Germany has to implement the *Data Protection Directive 95/46/EC* in federal law. The *German Federal Office for Information Security* (BSI) [19] also plays a role in the domain of data protection: this federal institution has the responsability to "support the *federal data protection commissioner* in issues relating to the technical implementation of statutory requirements" [7].

[14] Real ID Act available online at `http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.418:`.
[15] CNIL homepage: `http://www.cnil.fr`.
[16] French Data Protection Act available online at `http://www.cnil.fr/index.php?id=301`.
[17] Chapter 11)presents more information about the INES Program.
[18] Federal Data Protection Act available online at `http://www.bfdi.bund.de`.
[19] *Bundesamt für Sicherheit in der Informationstechnik*'s home page: `http://bsi.bund.de`.

4.2 Biometrics as sensitive personal data

A study in the Netherlands concluded that biometric information must be considered as personal data, if the template is associated to other personal data [273] (which is most likely to be the case). Furthermore, if racial and religious information can be obtained from the collected data, such as facial images, these must also be considered as sensitive. Canada's standing committee in citizenship and immigration reports likewise that biometric data is information *of* the person, rather than information *about* the person [96]. The swiss federal data protection act specifies in article 3 that any information relating to an identified or identifiable person is considered as personal data and that any data relating to religious, health or racial origin is considered as sensitive data. Raw biometric data is considered as sensitive personal data according to these definitions as it can always be linked to the source and can include sensitive elements [197].

It should also be noted that raw biometric data, and in some cases biometric features, may contain medical information. For example, fingerprints can allow to some degree inference about ethnicity, chromosomal aberrations [195, 274], and mental disorders (skin and brain develop from the same ectoderm during gestation) [272], and retina scans can reveal information concerning diseases such as diabetes, brain tumors, or AIDS [35].

A recent draft report of the Council of Europe considers that biometrical data constitute a specific category of personal data [73] [20]. Accordingly, these data have to be used only for "specific, explicit and legitimate" purposes, and involve adequate protection measures. The appropriate architecture of the biometric system has then to be chosen depending on its purpos. This report recommends that the complete information about the purpose of the system should be made available to the person whose biometric will be enrolled. This person should also be entitled to access and rectify data set upon request. Accordingly to the *International Conference of Data Protection Commissioners* cited in [227], a complete transparency of the biometric system is necessary, especially if the system is designed for a large-scale use.

4.3 Privacy

The term of *privacy*, defined as "the state or quality of being private" [1], appears also largely in the literature in relation to biometrics. *Privacy* is "the ability to lead your life free of intrusions, to main autonomous, and to control access to your personal information" [223]. This term also includes an aspect of autonomy, as well as "a control over the quantity of information abroad" [290]. An elegant definition of privacy is provided in [9]:"[...] privacy is control over how and when we are represented to others".

The International Biometric Group [21] subdivides privacy risks in two general categories [130]. The *personal privacy* concerns people who find the use of biometrics as invasive and inherently offensive. The *informational privacy* concerns the impact of a misuse (unauthorized collection, use, retention and disclosure) of biometric data.

[20] As best practices, the BioVision project recommends also "to always treat biometric data as personl data" [6].

[21] IBG homepage at `http://www.biometricgroup.com`.

The relation between a biometric system and privacy can be described as a continuum according to the BioPrivacy framework [130], from privacy enhancing to privacy intrusive:

Privacy-Protective A biometric system is *privacy-protective* if it is used to protect or restrict the access to personal information or if this system is a mean for establishing a trusted identity.

Privacy-Sympathetic A biometric system is *privacy-sympathetic* if it is used in a limited way, or if the system is designed to ensure the protection from unauthorized access and usage.

Privacy-Neutral A biometric system is *privacy-neutral* if its use has low privacy impact.

Privacy-Invasive A biometric system is *privacy-invasive* if it is used without knowledge or consent, or if it is used for undisclosed purposes.

Regarding biometrics, using a part of a human being ("something you are") during a transaction is considering as "giving information about himself!" [290]. Additionally, because biometric technology is recent, people may have of a negative *a priori* for its use and may thus be reticent to the introduction of such systems. The implications for privacy, every time biometrics is used, is a very important element that people want to know about [280].

The inlet of new technologies has always required setting-up new laws and policies [290]. Indeed, each time a new technology emerges, the legal framework becomes outdated and has to be rethought according to this new reality or to set societal acceptable boundaries for its usage. It is exactly what is happening now with the introduction of biometrics in daily activities and in its implementation in identity documents. Legal experts have to explore from their perspectives "what is required to safeguard the public interest and to ensure optimal results for society", without excluding scientific experts from this analysis [290].

As with all emerging technologies, there is potential for abuse [240]. The main danger is that the information transmitted with or without permission is misused (in respect to the use allowed for a defined application). The main concerns regarding biometrics are as follows [240]:

- Information gathered without permission.
- Information used for other purposes.
- Information disseminated without permission.
- Creation of a complete picture about people.
- Real-time surveillance and profiling.

These concerns are legitimately caused by the fact that the biometrics collected by a system can be linked to personal information or can allow to track the movements of a person [280] or proceed to background checks against law enforcement databases. What is also highlighted by Wayman et al., is that this

new technology "can only link a person to a biometric pattern and any identity data and personal attributed presented at the time of enrollment in the system" and that an authentication's anonymity can be guaranteed when no link is possible between the biometrics and the personal information. Indeed, if no other personal information is stored during the enrollment process at the same time as the biometrics, this latter cannot be linked to the concerned person. However, this latter scenario is very unlikely. The *Convention 108* of the Council of Europe also considers that biometrics linked with any information are personal data [72]. Figure 4.1 highlights some differences between biometric and non-biometric identifiers [280]. With respect to this figure, we should point out the following: 1) Point 1 depends entirely on your definition of "personal information". As mentioned in section 4.2, a convincing argument can be made that biometric data *is* in fact personal information. Additionally, some modalities like face are extremely easy to steal covertly (just use a digital camera). 2) Point 3 is correct *stricto sensu*, but no real system, save those based only on Match On Card, are likely to be used without being linked to a database of identities. To assume otherwise is naïve.

1. Unlike more common forms of identification, biometric measures contain no personal information and are more difficult to forge or steal.
2. Biometric measures can be used in place of a name or Social Security number to secure anonymous transactions.
3. Some biometric measures (face images, voice signals and "latent" fingerprints left on surfaces) can be taken without a person's knowledge, but cannot be linked to an identity without a pre-existing invertible database.
4. A Social Security or credit card number, and sometimes even a legal name, can identify a person in a large population. This capability has not been demonstrated using any single biometric measure.
5. Like telephone and credit card information, biometric databases can be searched outside of their intended purpose by court order.
6. Unlike credit card, telephone or Social Security numbers, biometric characteristics change from one measurement to the next.
7. Searching for personal data based on biometric measures is not as reliable or efficient as using better identifiers, like legal name or Social Security number.
8. Biometric measures are not always secret, but are sometimes publicly observable and cannot be revoked if compromised.

Figure 4.1: Biometric and non-biometric identifiers [280].

All the actors involved in the biometric world agree that its use should enhance the security and the efficiency in any transactions [240, 290]. As stated in Section 2.1.1, an appropriate and intelligent use of biometrics is the most secure way to prove one's identity. Regarding this enhancement of security by using biometrics, we can wonder if it has to be made to the detriment of people's liberty and if we should trade our liberty for security [40]. The use of biometric system requires a proportionality rule regarding the finality [110, 223]. Indeed, the pursued end of the use of a biometric system and the dangers generated by the constitution of databases, and thus possibilities of misuses, has to be proportional [110]. The scale of deployment of any biometric system determines the relationship between biometrics and privacy [130].

Several methodologies have been developed to gauge the impact on privacy

of computer systems deployment. A generic one that can be applied to the case of biometrics for identity documents is proposed by [65] and others under the name "privacy impact assessment". It proposes 18 categories of questions (data retention, accountability, consent...) which need to be asked when putting forward a proposal for a new system.

The International Biometric Group developed a tool to evaluate the impact of a deployment of a specific biometric system, in a specific environment [130]. Ten questions are proposed to find out the appropriate precautions and protections that are applicable in a particular situation. Each question describes the privacy risks involved.

1. Is the system deployed overtly or covertly?
2. Is the system optional or mandatory?
3. Is the system used for verification or identification?
4. Is the system deployed for a fixed period of time, or it is indefinite?
5. Is the system deployed in the private or the public sector?
6. In what capacity is the user interacting with the system, as individual/customer or as employee/citizen?
7. Who owns the biometric information, the enrollee or the institution?
8. Where is the biometric data stored, personal storage or database storage?
9. What type of biometric technology is being deployed, behavioral or physiological information?
10. Does the system utilize biometric templates, biometric images, or both?

For example, an overt match-on-card verification system has lower privacy risks than a covert identification system, with a centralized database. Even if all the risks involved are not defined with these ten questions, a privacy risk statement can be correctly postulated, for evaluating the potential of misuse of any system.

4.4 Privacy protection

The fears about the use of biometric systems are legitimate, but all excessive opinions are counterproductive. Indeed, those who claim that any use of biometrics is privacy restrictive, as well as those who claim that biometrics has to be used in any transactions, block the discussions, and thus these opinions are not appropriate [240].

The right equilibrium has to be found, thanks to the proportionality rule.

The 25th International Conference of Data Protection Commissioners 2003 [22] has adopted five resolutions for protecting people's privacy and enhancing data protection some of which apply to the biometric identity document case:

[22]The 25th International Conference of Data Protection Commissioners homepage: `http://www.privacyconference2003.org`.

1. Resolution on improving the communication of data protection and privacy information practices.
2. Resolution concerning the Transfer of Passengers' Data.
3. Resolution on Data Protection and International Organisations.
4. Proposed resolution on Automatic Software Updates.
5. Resolution on Radiofrequency Identification.

In Switzerland, the Federal Data Protection Commissioner has not yet taken position on the issue of biometric for identity documents, but is expected to do so in the coming year. Trials of biometric technologies in the Zürich County (Airport) should result in recommendations being made public from either county or federal data protection offices.

The Swiss Federal Data Protection Commissioner has however taken position on the issue of fingerprint for employees' time clocks [228]. The use of biometric data for time clocks, stored on personalised smart cards is in adequacy with the swiss legal framework on data protection. Furthermore, a centralised database with only minutiae information, related to the identity of the person, can also be in adequacy with the swiss legal framework, upon condition that security measures are applied, as specified in the *Swiss Federal Data Protection Act* [23].

In the literature, some solutions are presented to protect the privacy when biometric systems are used. Basic principles are needed to enhance both liberty and security [240]: the environment should be *overt* instead of covert; the system should use a *verification process* instead of a identification process; the system should operate with *local storage* instead of a centralize database; the system should be *"opt in"* instead of mandatory; the matching process should be based on a *template* instead of a stored image; the *pseudonymity* should be guaranteed; the system should be well *protected against misuse*; a *routine secondary review* should be conducted; and a suitable *secondary identification system* should be present if the primary does not work. Rosenzweig et al. also postulated that biometrics could not be an absolute security measure: "the system cannot be seen as the ultimate security tool, and thus the perfect solution; its simply another tool in a layered approach to security". Ratha et al. have proposed another way to protect privacy in biometric environment [230]. The biometric signal should be modified, in "*applying repeatable noninvertible distortions* to the biometric signal", for avoiding the problem of compromised biometrics. For Prabhakar et al., the solution for the enhancement of the privacy is as follow [223]: the application should use a *decentralized recognition process* and the *match-on-card* process could be an appropriate solution when fingerprint technology is used. In agreement with ethical considerations, some statements concerning privacy can be made [40]: the privacy of information entrusted should be protected by the developers of the system; some information about the systems and their uses should be transmitted to the public and the technology should be used in a socially responsible way, and thus minimize the possibility of misuse.

In adopting such protections, the enhancement of privacy and security can be guaranteed. "An accountable and responsible use of biometric systems can

[23] Section 4.1 presents more information about the Swiss legal framework and Data Protection Act.

in fact protect individual privacy" [223].

An example of a privacy protection policy can be found in the recommendation of the Ontario information and privacy commisioner for the Toronto welfare entitlement system, which uses fingerprints [54]:

- requiring the biometric, in this case, the finger scan, to be encrypted;
- restricting the use of the encrypted finger scan only to authentication of eligibility, thereby ensuring that it is not used as an instrument of social control or surveillance;
- ensuring that an identifiable fingerprint cannot be reconstructed from an encrypted finger scan stored in the database;
- ensuring that a latent fingerprint (i.e., picked up from a crime scene), cannot be matched to an encrypted finger scan stored in a database;
- ensuring that an encrypted finger scan cannot itself be used to serve as a unique identifier;
- ensuring that an encrypted finger scan alone cannot be used to identify an individual (i.e., in the same manner as a fingerprint can be used);
- ensuring that strict controls are in place as to who may access the biometric information and for what purpose;
- requiring the production of a warrant or court order prior to granting access to external agencies such as the police or government departments;
- ensuring that any benefits data (i.e., personal information such as history of payments made, etc.) are stored separately from personal identifiers such as name, date of birth, etc.

In the field of biometric identity documents, important means have to be invested by governments in order to protect the data acquired during the issuance process, especially with the biometric data. Indeed, an independent institution, such as the CNIL (the French Data Protection Board) in France, should be mandated by each government to permanently control the data collection and the access to these information.

4.5 Public perception of biometrics

The introduction of biometrics on the scale of a country, let alone internationally, is not without potential impact on society.

Face recognition is applicable both to identification and verification. Sensors (digital cameras) are readily available that can acquire high quality face images at a great distance, without the subject's knowledge or consent. This makes this modality a good choice for covert surveillance operations. Country-wide biometric enrollment for identity documents will provide the responsible agency

with a very large biometric database of faces, the use of which must be controlled with the utmost care[24].

Ideally, the criteria for being put on and off a watchlist, places of legal deployment for biometric surveillance, and other issues will be debated in Federal or County Parliaments and clearly set in law. By and large, this has not happened in Switzerland (see Section 4) and there is little public awareness of the issues at hand. A mainstream Swiss magazine (l'Hebdo) has recently deplored this state of affairs and warned about generalised surveillance [14].

In the USA, commentators from all sides of the political spectrum (from the Cato Institute [76] to the American Civil Liberties Union [261]) have warned about possible mission creep of face recognition technologies and the need for transparency in the matter. The example in Tampa, Florida [261] is particularly illustrative of what might happen when no clear policy is set on usage of face recognition, as that city's own Police Department decided to include not only wanted people on the watchlist, but also those from which "valuable intelligence" can be gathered, and people "based upon [their] prior criminal activity and record". The reader is further referred to [5] for a classic article on the societal implications of face recognition in public places.

Fingerprint sensors imply touching a surface which has been touched before by other users. Depending on their culture, some users may not feel comfortable sharing germs with other previous users. This may be a problem, for example, for Japanese people, which are accustomed to greetings involving not a handshake but bowing.

[24] In this respect, the post-9/11 blurring of provinces between intelligence and police forces in the USA can be seen as cause for concern in terms of privacy [51].

Chapter 5

Modality: Face

5.1 Introduction

The problem of face recognition can be defined as matching a scene image or sequence of scene images (video) with a stored template of the face. In this section, we focus on face recognition on single scene images. In face verification literature, training data is often called *gallery* data, and testing data is called *probe* data. Two important pre-processing tasks in automated face recognition are

face segmentation or detection which refers to the action of approximately extracting the position of the face out of the scene image, and

illumination normalization which is used to correct for differences in illumination conditions between enrollment and deployment conditions. A survey is presented in [253].

The ICAO technical report on machine readable travel documents [125] proposes that 2D face be the main modality for identity documents:

> [...] face is the biometric most suited to the practicalities of travel document issuance, with fingerprint and/or iris available for choice by States for inclusion as complementary biometric technologies.

In opposition to 2D face recognition using in most cases normal intensity images, 3D face recognition consists in using the three-dimensional shape of the face [41] as well as the texture, acquired by one or several sensors. The use of additional information, as the depth and surface curvatures, can clearly increase the performance and the accuracy of such recognition systems. Such an approach *"overcomes limitations due to viewpoint and lightning variations"* [186]. The survey of 3D face recognition in this report is largely based on 3D face recognition surveys [41, 248], and on the comments of Prof. Thomas Vetter (Graphics and Vision Research Group, University of Basel [1]).

[1] Graphics and Vision Research Group homepage at `http://gravis.cs.unibas.ch/`.

5.2 Overview of algorithmic approaches

Numerous algorithms exist for segmentation and recognition, which we briefly review below. This section is largely based on [301], to which the reader is referred for a comprehensive review of the field of face recognition.

5.2.1 Segmentation

Segmentation is critical to successful face recognition, and inaccurately located faces contribute significantly to recognition errors. Some algorithms [268] can be used both for segmentation and recognition. A method which proposes to build models of faces and non-faces, then measures the distance between the input and the distributions, and finally trains a multi-layer perceptron on these typical distances has been proposed in [263]. The correct detections ranged from 79.9% to 96.3%. Various combinations of multiple neural networks classifiers are used in [243] to classify scene regions into face or non-face, using image windows of different sizes. This achieved between 77.9% and 92.5% detection rates with varying numbers of false detections on 130 frontal face test images.

5.2.2 Recognition

Zhao [301] divides face recognition algorithms into three categories: *holistic* methods, which use the whole face image for recognition, *feature-based* methods, which use local regions such as eyes or mouth, and *hybrid* methods, which use both local regions and the whole face.

Many holistic face recognition methods, as well as image analysis methods, are based on eigenspace decomposition [256]: face images are represented as vectors by concatenating the pixels of the image line-by-line. Then, an average vector is computed that represents a mean face. Also, a difference vector is computed for each user to quantify the differences to the mean face. Then, the covariance matrix of the difference vectors is computed. Finally, principal axes can be obtained by eigendecomposition of the covariance matrix. The first N eigenvectors (mostly called *eigenfaces* in face recognition literature) presenting the highest eigenvalues will be retained and represent the most significant features of faces. Figure 5.1 shows an example of eigendecomposition of a face image. This procedure is also known as *principal component analysis (PCA) decomposition*. Finally, each user model is represented as a linear combination (weighted sum) of coefficients corresponding to each eigenface. It should be noted that, given the mean face and eigenfaces, these models are reversible.

In [268], faces are compared by projecting them into eigenface components and using an Euclidean distance measure. Results are provided for a 16-users database of 2500 images in various conditions. This technique has been the subject of many improvements, for example [196] have proposed modeling both the principal subspace containing the principal components and its orthogonal complement.

A successful feature-based method is elastic bunch graph matching [288], which tolerates deformations of the faces. This uses local features (chin, eyes, nose, etc.) represented by wavelets and computed from different face images of the same subject.

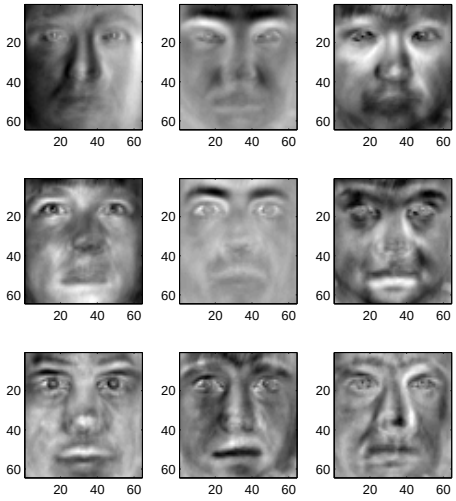


Figure 5.1: First 9 eigenfaces extracted from Yale database (see below).

Hybrid methods are currently an active area of research, and aside from standard multiple classifier methods it is not clear how and whether to combine holistic and local features [301].

5.2.3 3D recognition

For 3D facial recognition systems, the main algorithmic approaches can be classified as follows [41]. The first one is the *Principal Component Analysis*-based algorithm, where each eigenvector is a principal direction and the corresponding eigenvalue is a principal curvature [2]. In [45], PCA is applied on planar models of curved surfaces (bending-invariant canonical forms). Such an approach has better performance than 2D eigenfaces and is invariant to significant deformation of the face, as facial expressions.

With the *Extended Gaussian Images*-based algorithm, a mapping surface points onto a unit sphere, called the Gaussian sphere, can be obtained from a three dimensional object, such that all points have a corresponding surface normal direction [292]. The Extended Gaussian Image (EGI) is an alternative representation, for which a weight is associated to each point on the Gaussian sphere equal to the area of the surface having the given normal. The correlation of the EGI of the convex regions or of the curvature-based segmentation is computed from a range image for the comparison. In [26], *surface matching*- and a *central and lateral profiles* matching-based algorithms are used for 3D facial recognition. In [262], *Gaussian curvature* is used for the detection of landmarks in a 3D model, while [62] use *point signatures* to describe, more efficiency than 3D coordinates, "the structural neighborhood" of the landmarks on the 3D model. Surface-based approaches, such as EGI and profiles-based, use

[2]Section 5.2.2 presents more information about PCA.

global methods for the recognition process [248]. Surface-based approaches, as *Gaussian curvature* and *point signature*, use local methods for the recognition process [248].

Some other approaches are used for 3D facial recognition, such as *Hausdorff distance matching*, *Iterative Closest Point* (ICP) matching, *Local Feature Analysis* (LFA)-based algorithm, *Dynamic-Link-Architecture*-based paradigm, *Hidden Markovs Models*-based algorithms on depth maps and intensity images [41, 122, 248]. In [33], a *morphable face model* was created from 3D facial data by combinating linearly a large number of 3D face scans. This model is used for create a 3D face model from a 2D image and for giving the face a natural aspect (shape and texture). The commercial A4-Vision 3D facial recognition system use a *Surface Semantic Analysis*-based approach and extract local surface curvature characteristics, in order to calculate similarity scores [2].

The templates obtained in 3D face recognition systems usually range from 1000 to 3500 bytes [203] and the one obtained with the A4 Vision system is 4092 bytes [2].

5.3 Performance

The performance of face recognition systems is very dependent on the application [301], and good results in an evaluation campaign or in vendor specifications do not mean that these will be obtained in the field. A striking example of this is found in a German government report [47], which tested 4 systems in realistic deployment conditions. Quoting from the report (Phase II refers to testing in mismatched conditions):

> [...] All in all, two out of the four systems tested had a false rejection rate (FRR) of 64% and 68% respectively in Phase I and 75% and 73% in Phase II. The two other systems, with FRRs of 90% and 98% (Phase I) and 99% and 99.7% (Phase II), hardly recognised any of the subjects, and the weaker of these two systems was in fact so unreliable that it was only available for use on a few of the days. Recognition performance was not nearly as good as the promotional material of the system vendors would lead one to believe. [...]

Failure To Enroll should also be taken into consideration. In laboratory conditions, the same report tested 3 algorithms on databases of 5000 to 50000 people. The smallest database gave a FTE of 7.6% (378 persons), 7.0% (351 persons) and 0% respectively for each algorithms, while the largest database gave FTEs of 7.6% (3783 persons), 7.3% (3672 persons), and 31.5%[3] (15723 persons). A US Army Research Lab report [155] gives 51% rank 1 identification performance for a test population of 270 users over 13 weeks.

However, in laboratory conditions face recognition algorithms can display usable error rates, as will be shown in Section 5.8.

A recent study conducted in Norway demonstrated that face recognition may not obtain acceptable performance in identity verification for large-scale applications [159]. With a training data set of 1536 subjects and a test data sets

[3]This latter result was corrected after software updates but no data is available in the report.

of 1426 subjects (test data set II) and 10000 images from several thousands of national passport photos (test data set III), the authors obtained the following results. At a false acceptance rate of 1%, 97% of the subjects in the test data set II and 99.99% subjects of the subjects in the test data set III, generated one or more false acceptances. At a false acceptance rate of 0.1%, the majority of the subjects in the test test data set II did not generate any false acceptace, while 92% of the subjects in test data set III generated more than one acceptances.

An improvement of 3D face recognition systems is necessary to increase their performances, and thus to be able to use them widely in applications [41]. Indeed, this technology perform not as well as expected, while there is no reason that the performances are lower than 2D technologies, given that an additional information, the third dimension, is used. The current limitations are classified in three categories: sensor, algorithms, and methodology.

Sensor The main problem in such a technology is the bad quality of the input data used for 3D facial recognition systems. Particular efforts have to be made in reducing frequency and severity of artifacts, in increasing depth of field, spatial and depth resolution and in reducing acquisition time. Holes and spikes, the most common artifacts, are present in face regions, even under ideal illumination. Actually, the depth of field, from about 0.3 to 1 meter, is also a limitation relative to the need of cooperative subjects. The acquisition time should also be reduced, especially for structured-light systems. Furthermore, it is important to notice that such sensors were not initially developed for facial recognition and are thus not yet mature for this recognition process.

Algorithms The main difficulty appearing during the comparison process is to make reference points correspond between the samples. Indeed, this registration process is crucial for the alignment of the samples, in order to compare them accurately. Furthermore, some state-of-the-art algorithms were not able to be insensitive to size variations and to handle changes in facial expression. This latter is a "major cause of performance degradation that must be addressed in the next generation of algorithms" [41].

Methodology and Datasets A limitation to evaluate the performance of 3D face recognition systems is the lack of appropriate datasets. Using explicit, distinct training, validation and test sets could also improve the experimental methodology in this area.

In 2005, an operational evaluation of 3D and 2D facial recognition technologies was performed for the Immigration & Check points Authority (Singapore) in order to "assess the effectiveness of the 3D technology and compare it to 2D technology" [31]. 1018 subjects were enrolled for this trial: acquisition of a 2D digital photo and a structured-light image (A4Vision 3D technology). No FTE was noted for the 3D system, even if 1.7% of the subjects were enrolled manually. In the verification mode, only 7.3% (837 attempts out of 4834 from 827 subjects) of all the attempts failed to verification. In the identification mode, the 3D system achieved at a FAR of 0.0047%, a FRR of 0.103%, when the (recommended) threshold was set at 80%, while the 2D system achieved at a FAR of

0.12, a FRR of 9.79%, when the (recommended) threshold was set at 70%. The results of this trial demonstrated also that better performance can be achieved if the subjects acquire more than one attempt for the verification/identification modes and that the failures were mainly due to incorrect presentations of the subjects in front of the camera.

5.4 Sensors

Any low-cost camera ("webcam") is usable for 2D face recognition. However, best results will be obtained with cameras that have auto-focus, low-noise sensors, and optics which introduce minimal aberrations. As much as possible, cameras with similar optical characteristics should be used both for enrollment and testing [47].

To obtain a *3D image* of a face, in standarised conditions or not [4], three main approaches are available: *stereo-based*, *structured-light* and *laser scanner*. The acquisition process can be completed by several sensors placed all around the face or by a single sensor from a single view point.

Stereo-based This *passive* approach consists in using two object's images taken by separate cameras, vertically arranged in such a way that their angle of sight varies only about 8-15 degrees [186]. These cameras are calibrated and a true metric reconstruction is obtained. An image pyramid is constructed and at each level, match reliable interest are pointed, for producing a dense correspondence map, refined at every level. The final map is transposed into a 3-D mesh. Approximately 9 seconds are necessary to capture such a 3D image, from 2D images. Currently, sufficient information about the facial's shape cannot be extracted with such an approach [122]. When using range images, called *passive range* acquisition, such an approach is not able to produce in real time 3D range images [45].

Structured-light This *active* approach consists in using a projection of a known pattern to recover 3D coordinates [25], working either in monochrome lighting, or in invisible near-infrared range. The original lighting is distorted by the object and after reconstruction, the shape of the face is obtained. Range images can also be used in this approach for acquiring facial shape [3]: a sequence of stripe patterns is projected on the object and captured by a camera. Each pixel acquired is coded and the shape is obtained by triangulation, as the parameters of the projector and the camera are known. Such an approach is also called *active range* acquisition [45]. A sequential projection of a series of black and white stripes, called *coded light* can also be used and is more robust and accurate than the structured light approach [45].

Laser scanner This approach allow a cylindrical representation of the head structure [33], with parameters as surface points sampled at 512 equally-spaced angles and at 512 equally spaces vertical steps. The RGB-colour values can also

[4] Examples of standardized conditions: illumination, position and orientation of the head,...

be stored in a texture map.

The commercial *A4-Vision* 3D facial recognition system uses the structured-light approach, in invisible near-infrared range, for acquiring the data and reconstructed the 3D surface with surface reconstruction and optimization algorithms [2]. An example of 3D models from a single person, obtained by using the *A4-Vision* 3D facial recognition system, is presented in Figure 5.2.

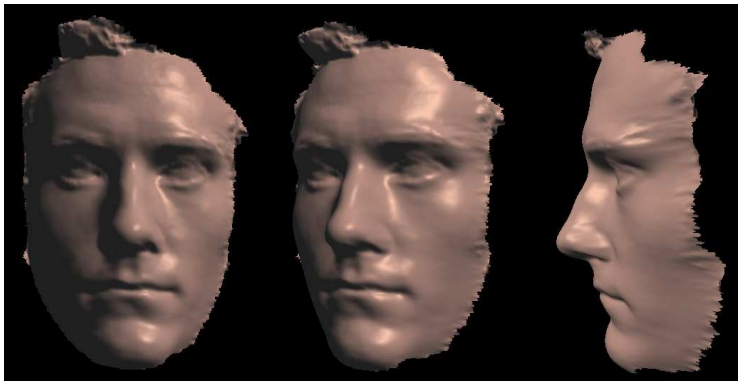


Figure 5.2: 3D Models from a single person obtained by using the *A4-Vision* 3D facial recognition system.

5.4.1 Ergonomics and acquisition environment

For best recognition performance, as many parameters should be kept constant between enrollment and field conditions. These include: distance from the camera to the head, centering of the face in the image (ideally no part of the face should be cut), yaw, pitch, and roll of the head, illumination angle and source, background colour and texture. For these reasons, outdoor face recognition is still a challenging problem [301]. Distance from the camera is also crucial and can significantly deteriorate both identification and verification performance [32]. The ISO/IEC SC37 working draft [137] has strict recommendations about acquisition control.

In 3D recognition, the ergonomics of systems are relatively demanding, as cooperative users are needed for their location in the acquisition area, and because the acquisition time lasts several seconds. The subjects should have a neutral expression and take off their glasses and hats, if these latter hide some part of the forehead. The hairstyle and the beard can also influence the results of the verification/identification process, especially if the subjects have changed it between the enrollment and the recognition process. As the sensor use in some cases near-infrared wavelengths, the ambient lightning will not disturb the acquisition process.

5.4.2 Face acquisition for identity documents

Annex A of the ICAO report [128] has a set of guideline regarding photographs for biometric identity documents. Specifically, it mentions that

- the face should cover about 70-80% of the photograph,
- the user must look directly at the camera,
- the skin tones should be "natural" (no specific details are given),
- the photograph should have "appropriate brightness and contrast" (no specific details are given),
- no hair should come across the eyes, which should be open,
- the user should be placed in front of a plain, light-coloured background (no specific details are given),
- the photographs should be taken with uniform lighting (no colour temperature or other details are provided), so that no shadow appears,
- the user should not wear glasses that cover parts of his/her eyes,
- no head coverings are permitted except for religious reasons, and in this case the face should be visible from bottom of chin to top of forehead,
- the user's expression's must be neutral.

These broad guidelines can be complemented by the already mentioned, more specific guidelines of the ISO/IEC SC37 working draft [137].

3D facial recognition is completed without any difficulties by human beings. The optical human system, a stereo-based "sensor" performs robust facial recognition. Despite that, the technologies used in automatic 3D approaches are not yet mature for a large-scale introduction in identity documents. Indeed, even if these methods are interesting for decreasing the problems of pose and illumination variations (as observed in 2D), the algorithms are not sufficiently robust when handling facial expression variations. The compatibility between 3D systems in such an application is also important. Indeed, if there are differences in resolution's quality of the sensors used, the systems will also have low performance.

5.5 Computational resources

A typical eigenfaces-based template requires between 1000 and 3500 bytes of memory for storage [203]. Depending on compression, a raw face image file can range from 100 kB to 1 kB. According to [32], compression seems not to impact identification performance up to compression ratios of 30 to 1. Compression ratios of 7:1 (70 kB to about 11 kB) have also been investigated for colour JPEGs with less than 2% relative reduction identification rate over the uncompressed image [127].

In testing and after feature extraction, a baseline eigenfaces-based system, which just uses dot products of face presentation weights with respect to an eigenface model's weights, will need approximately $2n$ floating-point operations per dot product, which means using for example 100-eigenfaces models will results in 200 floating-point operations per model compared. As a guide, support vector machine classifiers with 2000-3000 support vectors for 32x32 images

require in the order of 10 Mflops to classify one image [164]. More complex methods will require substantially more computational power, as for instance computing a Gabor wavelet transform involves computing a fast Fourier transform.

Dedicated hardware can be used to speed up computations, for example [92] reported real-time performance in a test with a 5-users database.

The storage of a 3D face template on a chip memory is possible, as the template's size is about 3000 bytes. Furthermore, an implementation of the whole system onto an identity document, using a *sensor on card* or *match on card* approach, is technically impossible, as it is necessary to use currently imposing material during the acquisition step.

5.6 Open source systems

Several open source face recognition systems exist, for example Intel's OpenCV library [42] contains face detection and recognition algorithms. A complete evaluation system is provided by the Colorado State University [36], comprising implementations of four baseline face recognition algorithms: eigenfaces, combination PCA and LDA based on the University of Maryland algorithm, Bayesian Intrapersonal/Extrapersonal Image Difference Classifier based on the MIT algorithm, elastic bunch graph matching based on the USC algorithm.

For 3D facial recognition, several approaches are presented in the literature, but to the best of our knowledge, none are available as an open source system.

5.7 Databases

5.7.1 2D facial databases

Many databases are publicly available for 2D face recognition.

AT&T Laboratories Cambridge's Database of Faces AT&T Laboratories Cambridge's Database of Faces [5][246] contains 10 images for each of its 40 subjects, with various lighting conditions and facial expressions. The images are grayscale, 92x112 pixels.

BANCA BANCA [15] contains video and audio data for 208 users, captured with 2 different cameras (one webcam and one high-quality digital camera) and 2 different microphones in 12 sessions. It offers three lighting and acoustical conditions. In addition, 10 frontal images of 30 users are provided for world modeling. The images are 24-bits colour, 720x576 pixels.

FERET FERET [216] comprises scanned images from analogue 35 mm film. The images were taken in 15 sessions over 3 years, comprising a total of 1199 users and 14'126 images. Images have neutral and non-neutral expressions.

[5]Formerly known as the Olivetti database, this database is available online at `http://www.cl.cam.ac.uk/Research/DTG/attarchive/facedatabase.html`.

PIE PIE [254] (CMU Pose, Illumination and Expression database) contains 68 users and a total of 41368 images. Each user is simultaneously photographed by 13 high-quality cameras located at different positions, thus providing 13 different viewpoints. The person is photographed under 43 different illumination conditions, and provides 4 different facial expressions. The images are colour, 640x486 pixels. This database is not particularly suited for identity documents as conditions are likely to be less controlled than they would be in an identity verification scenario. The background, for instance, is non-uniform.

UMIST UMIST [106] contains 20 users and a total of 564 images [6]. The users are captured under a variety of poses. The images are 256-levels grayscale, 220x220 pixels. This database could be useful for experiments relating to identity documents, as the background is plain, and different poses are present. However, it has a small number of users.

XM2VTS XM2VTS [191] contains 295 users and was recorded in four sessions. Different subsets of this database are available. 8 frontal images per user (2 per session) are available, in total 2360. Furthermore, single-session image sets with different illumination conditions are available, adding 4 images per user, adding 1180 images. Lastly, an additional profile views dataset is available, adding 2360 images. All images are colour, 720x576 pixels. The background is uniform blue. Because of its controlled conditions and its relatively large user population, this database can be used for experiments with identity documents.

Yale faces database Yale faces database [7] contains 15 users and total of 165 images. 11 images per user are taken, in a variety of expressions and lighting conditions. The images are grayscale, 320x243 pixels. The lighting conditions are well controlled. While the images are of good quality and various expressions could be useful in testing face recognition for identity documents, the user population contained in the database is too small.

AR face database AR face database [8] [180] contains 126 users (70 men and 56 women). 26 images per user are taken over two sessions 2 weeks apart. Each user has a variety of expressions, illumination conditions, and partial face occlusions (scarf). The Images are 24-bits colour, 768x576 pixels. In addition, 30 sequences of 25 images each are provided.

5.7.2 3D facial database

Contrary to 2D face, only few databases are available for 3D facial recognition [107]. The *Max Planck Institute for Biological Cybernetics* [9] has created a 3D facial database, acquired with a laser scanner, and containing 200 subjects. The

[6] This database is available at `http://images.ee.umist.ac.uk/danny/database.html`.

[7] `http://cvc.yale.edu/projects/yalefaces/yalefaces.html`.

[8] `http://rvl1.ecn.purdue.edu/~aleix/aleix_face_DB.html`.

[9] Max Planck Institute (MPI) for Biological Cybernetics homepage: `http://www.kyb.tuebingen.mpg.de/`.

whole 3D data are available only for 7 subjects[10]. The XM2VTS database [191] has acquired 3D models of 293 subjects, and all these data are available [11].

5.8 International competitions

Three databases are currently the most commonly used for 2D face recognition competitions. They are FERET, XM2VTS, and BANCA.

5.8.1 Competitions on FERET

The FERET database [216] also defines a protocol for identification and verification. Three evaluations took place using this protocol, the last in 1996 and 1997 [215]. The evaluation protocol stipulates that only a development set is made available, while the real testing set remains under control of the evaluation organisers. Several testing scenarii are used, which take into account two of the main factors of recognition degradation in biometrics: environmental conditions (lighting differences) and inter-session time. It also investigates performance in fully-automated conditions (only the face image is given) and partially automatic conditions (eye coordinates are given). For the March 1997 evaluation, the best-performing partially automatic system had a correct identification at rank 1 of 96% for test images taken the same day, which dramatically dropped to about 59% for test images taken on different days. About 82% correct identification at rank 1 was obtained for test images taken on the same day but with different lighting. Images taken over 1 year apart result in a drop to 52% at rank 1. For fully automatic systems, the best result obtained is about 94% for test images taken on the same day (a 2% absolute difference with partially automatic systems). For images taken on different days, the figure drops to about 58%.

The Face Recognition Vendor Tests (FRVT) aim at independent government evaluation of commercial systems, though academic institutions are free to participate. Two evaluations took place, in 2000 and 2002 [12]. A further one is planned for 2006 [13], with the goal to measure progress since FRVT 2002. Additional facial images (high resolution and multiple-samples still facial images) will be used for the purpose of the this evaluation. The 2000 FRVT tested with a database of 1'196 users (FERET) [32], while the 2002 FRVT tested with 37'437 users [213]. The results of the FRVT 2002 will be briefly summarised here, as they are important and can be used to set expectations for the identity documents application. It is especially interesting to note the marked differences in performance between the vendors in the verification scenario. The best system had about 90% correct verification at 1% false accept (about 5% EER), while the worst system had about 25% EER. Also, verification performance markedly degrades in time, with systems loosing between 5% and 8% verification rate per year since enrollment.

[10] MPI database available online at `http://faces.kyb.tuebingen.mpg.de/`.
[11] XM2VTS database available online at `http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/`.
[12] FRVT 2002 homepage: `http://www.frvt.org/FRVT2002`.
[13] FRVT 2006 homepage: `http://www.frvt.org/frvt2006`.

5.8.2 Competitions on XM2VTS

As part of the audio and video-based personal authentication conference (AVBPA) 2003, a face verification competition was held on the XM2VTS database using the Lausanne protocol [191]. The best performing partially automatic systems had error rates between 0.97% FA at 0.5% FR and 0.25% FA at 0.5% FR depending on the train/evaluation set partition. The best performing fully automatic systems had error rates between 1.36% FA at 2.5% FR and 1.35% FA at 0.75% FR depending on the train/evaluation set partition.

As part of ICB 2006, a face verification contest has been helded on the XM2VTS database [192]. The best performing system achieved 0.26% FA at 1.57% FR, with automatic registration of the images. The worst perfroming system achieved 5.13% FA at 3.25% FR. These algorithms were also tested in order to evaluate their sensitivity to severe changes in subject illumination. In these later conditions, the best performing system with manual registration achieved 0.77% FA at 1.25% FR, while the worst performing system achieved 6.20% FA at 77.37% FR.

5.8.3 Competitions on BANCA

During the international conference on biometric authentication in 2004 (ICBA 2004), the BANCA database and evaluation protocols were used [190]. Four different institutions (academic and commercial) participated. Only data from the "controlled conditions" subset was used. In the partially-automated scenario, the best system obtained an HTER of 2.9% when equal costs are assumed for FA and FR. For the fully-automatic case, the best system obtained about 5.4% HTER.

The BANCA database was used as part of the face verification contest at the international conference on pattern recognition in 2004 (ICPR 2004), with 52 users [189]. 10 different institutions participated. Data from all 3 conditions subsets were used. For partially automatic verification, the best system had an HTER of about 2.2%, with significant differences between algorithms. The best fully automatic system obtained an HTER of about 3.1%, also at equal costs between FA and FR. Using sequestered (never seen before) test data led to a sharp decrease in performance, with the best system dropping to about 13.5%.

5.8.4 3D face verification competitions

So far, no international competition was completed for 3D facial recognition systems, aside the Face Recognition Vendor Test (FRVT) 2002 which has evaluated 3D morphable models technologies, methods increasing the performance of face recognition systems. But at the time of writing, some new competitions are in progress.

Face Recognition Vendor Test 2005 The FRVT 2006, supervised by the NIST, is planning to evaluate among others performance on 3D facial scans, what was not the case in the previous evaluations (FERET, FRVT 2000 and FRVT 2002).

Face Recognition Grand Challenge Additionally, since 2004, the FRGC [14] has been promoting face recognition technology in three main areas: high resolution images, three-dimensional face recognition and new preprocessing techniques [212]. The FRGC will assess the merits of all these three approaches simultaneously. 50'000 samples, for training and validation purposes, will be used in the FRGC. These include single still, multiple stills, outdoor/uncontrolled, 3D single view, 3D full face, and acquisition from several cameras. The goal of FRGC is to develop still and 3D algorithms in order to improve performance an order of magnitude better than FRVT 2002 (from 20% FRR in FRVT 2002 to 2% FRR at FAR=0.1%).

[14] FRGC homepage: `http://www.frvt.org/FRGC/`.

Chapter 6

Modality: Fingerprint

6.1 Introduction

Even if some archaeological vestiges allow to posit that human being knew the individuality of fingerprints 4000 years ago, the real start of the study for identification purposes was initiated by Faulds, Herschel and Galton in the late 18th century. The individuality of this modality was first formulated, almost simultaneously, by Faulds [93] and Herschel [114] for the purpose of recidivists' and recovered marks' identification. In the late 18th, Galton published upon the permanence of fingerprint all over life time [101]. He also introduced the use of minutiae features in the matching process.

Matching automation appeared since 1960 with Automatic Fingerprint Identification Systems (AFIS), for avoiding fastidious manual searches in large databases. Since then, the market did not stop developing and evolving, and a large number of criminal, non-criminal and civilian identification applications are available today. These two main applications, criminal and civilian sectors have some differences and some similarities [294]. The size of the database is larger for criminal than for civilian applications, and the image quality is more homogeneous for civilian applications as captured by the same sensor, but they follow nevertheless the same basic stages: acquisition, representation, pre-processing, feature extraction and matching.

A fingerprint can be described in three levels of features. The first level concerns the general flow of the ridges. In a fingerprint, a core and up to two deltas can be generally observed (Figure 6.1). They are also considered as level 1 features.

When the number and the position of these focal points (delta(s), core,...) change, the general ridge flow shape can differ. The general shape can thus be classified (among other methods) according to the number and positions of the deltas and the position of the core. The different shapes can be classified as: left and right loop, whorl, arch and tented arch (Figure 6.2).

The next two levels are more localized features. The second level relates to the minutiae features observed on a fingerprint. According to Galton, the individuality of this modality is related to the particular arrangement of ridge terminations and ridge bifurcations. Figure 6.3 presents examples of possible minutiae characteristics, which are all composed by ridge terminations and ridge

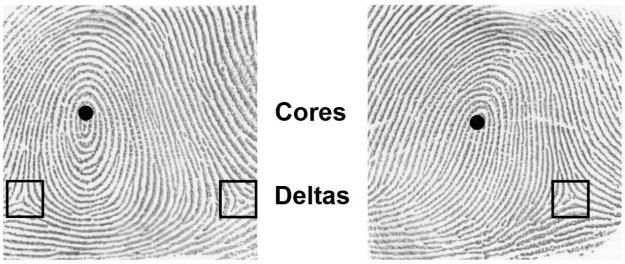


Figure 6.1: Representation of fingerprint core and delta.

Figure 6.2: Representation of general shapes of fingerprints.

bifurcations. Other characteristics, such as wrinkles, creases and warts also included in this second level are presented in Figure 6.4.

The third and last level concerns the sweat pores observed on the ridges and the ridge sides. Figure 6.5 presents examples of sweat pores presence in fingerprint representation.

6.2 Overview of algorithmic approaches

6.2.1 Human matching process

Before presenting the different algorithmic approaches used in automatic systems, we recall the ordinary process used by human experts in an off-line matching process. The Locard's tripartite rule is a good pragmatic statement [167], however the practice is more diverse (for more information on about, see [56]):

- If more than 12 concurring points are present and the fingermark is sharp, the certainty of identity is beyond debate. (The imperative requirement for the absence of significant differences is implicit).

- If 8 to 12 concurring points are involved, the case is borderline, and the certainty of identity will depend on: the sharpness of the fingermark, the rarity of its type, the presence of center of the figure (core) and the triangle (delta) in the exploitable part of the mark, the presence of pores, the perfect and obvious identity regarding the width of the papillary ridges and valleys, the direction of the lines, and the angular value of the bifurcations. In these instances, certainty can only be established following discussion of the case by at least two competent and experienced specialists.

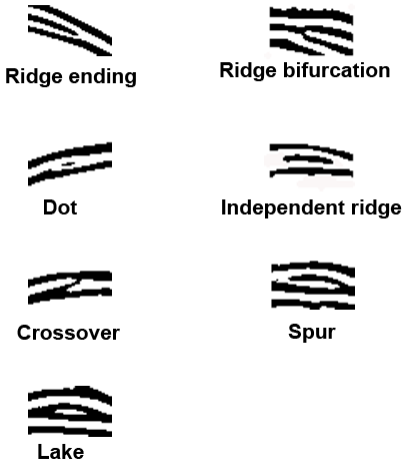


Figure 6.3: Representation of minutiae observed on fingerprints.

Figure 6.4: Representation of wrinkles, creases and warts observed on fingerprints.

- If a limited number of characteristic points are present, the fingermark cannot provide certainty for an identification, but only a presumption proportional to the number of points available and their clarity.

6.2.2 Automatic matching process

In an on-line automatic matching process, three approaches are possible [173]: the correlation-based, the minutiae-based and the ridge features-based matching.

Correlation-based matching The images are superposed and a correlation calculation is completed for different positions, obtained by translation and rotation.

Minutiae-based matching This approach, well reviewed in [294], is commonly used in most fingerprint identification systems. Methods such as local area contrast enhancement and contextual filtering are used for the enhancement procedure, a crucial step during the pre-processing stage [8]. Contextual

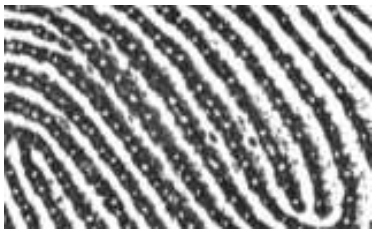


Figure 6.5: Representation of sweat pores observed on a fingerprint.

filtering or frequency analysis methods are used to enhance the fingerprint image, as the ridges have well-defined frequency and orientation in local area. The tools used in this matter are Fourier transforms, Gabor filters and wavelets. For the minutiae features extraction, this approach often use binary and skeleton images. The main stages of the whole feature extraction consist in orientation field estimation by using information about local average directions of the ridges (gradient or ridge-valley algorithm), ridge detection by using either a thresholding algorithm given a gray scale image, the ridge-valley algorithm, or gray level histogram decomposition, and thinning, by using algorithms based on mathematical morphology [294]. After feature extraction, locations and orientations of minutiae are stored as a set of points. A matching score is completed after alignment of these sets of the two fingerprint images. Figure 6.6 describes the feature extraction process of this approach.

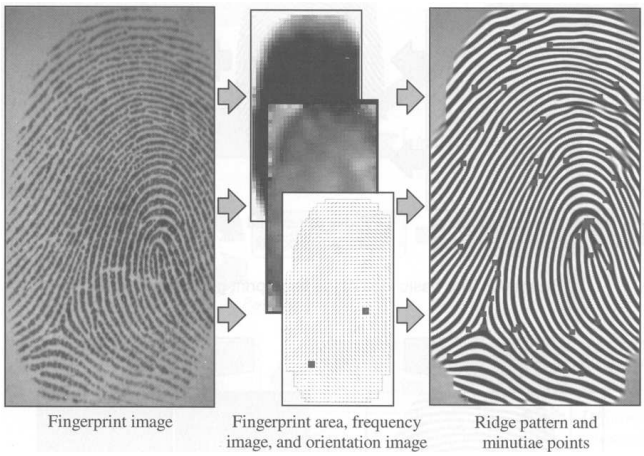


Figure 6.6: Feature extraction process [173].

Ridge features-based matching Features which are more reliably extracted from the ridge pattern in comparison to minutiae are used, such as local orientation and frequency, ridge shape, texture information. For example, the algorithm presented in [144] used this approach. The main steps are as follows: normalization and background segmentation, localization of the singular point, determination of features' extraction sectors, Gabor filterbank features extraction and statistical features, combination of the extractions to obtain a unique

feature vector from it (called FingerCode) and euclidean distance calculation. Figure 6.7 describes the process of this particular approach. This method allows obtaining a 80x8 fixed-size feature vector (FingerCode).

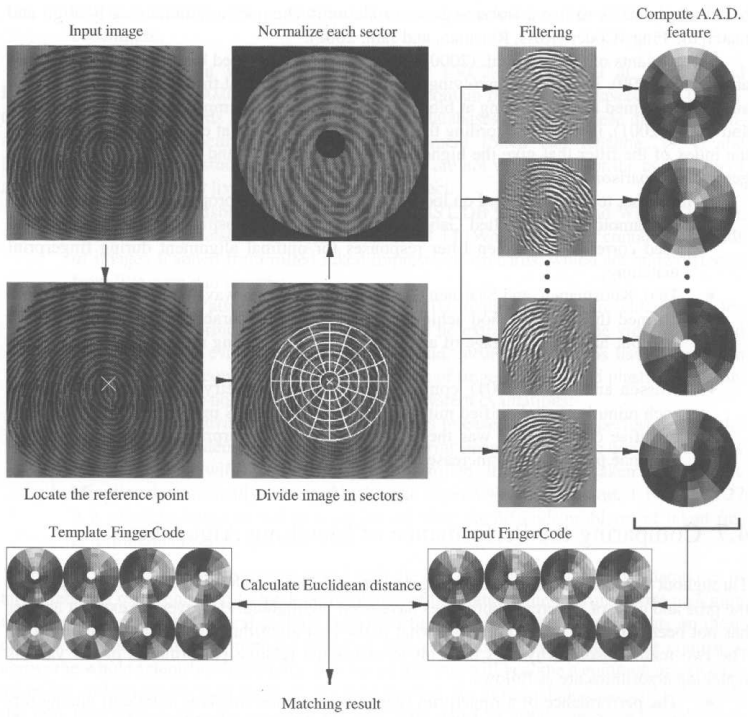


Figure 6.7: System diagram of the FingerCode approach [144].

Note that most AFIS systems just act as a filter whose candidates are then compared using the above holistic process, carried out by a fingerprint examiner trained to competency.

The templates obtained in the minutiae-based matching approach are usually of 250 to 700 bytes [203]. However, ridge features-based matching approach produces templates usually of about 900 to 1200 bytes.

According to the results of the two fingerprint verification competitions in 2000 [170] and 2002 [171], the minutiae-based methods performed better than the correlation-based methods. The reason for the superiority of minutiae-based algorithms is the stability and large signal capacity of the minutiae representation [222]. The use of minutiae information in large-scale systems will persist due to its high discrimination power, but future systems may integrate also non-minutiae features, particularly for poor quality fingerprint images [294]. For verification purposes, a ridge features-based algorithm has better performance than a minutiae-based algorithm, only if the false acceptance rate required by the specific application is not too low, or has slightly lower performance than state-of-the-art minutiae-based algorithms [144]. For forensic purposes, most of the marks recovered from crime scenes are partial and of poor quality. Minutiae-

based approaches are preferred in such situations, as the general shape is not easily recognizable automatically or amenable to manual coding using a skilled operator.

6.3 Performance

Automatic fingerprint recognition approaches are competitive systems [34, 173]. But some limitations can influence their performance [8].

At the data acquisition level, the sensor, if optical, has to be cleaned after each use, for avoiding background noise, resulting of the deposition of fingerprint secretions. This noise can distort the original image and introduce artifacts during the features extraction. Pressure and contact angle differences, displacement and rotation of the finger on the sensor, non-linear distortion and skin condition can also influence the performance of such systems in the following algorithmic stage.

During the extraction process, errors in the form of missed or wrongly detected minutiae can also appear, which can influence the performance of such a system.

Finally, the performance of such systems can also be influenced by the proportion of the population which do not have the modality or have a fingerprint of not sufficient quality to be enrolled (about 4% of the population). In the case of a large-scale use, such as it is for identity documents' purposes, this percentage corresponds to almost 300'000 persons who would be in that case in Switzerland, what is relatively important and must not be neglected. However, according to a National Institute of Standards and Technology (NIST) research report, this percentage was recently proved to be overestimated [115].

The NIST conducted several technology evaluations in order to estimate the performance of fingerprint recognition solutions.

For the joint "303A Report" to U.S. Congress from NIST, the Department of Justice and the Department of State [201] [1], the recommendations proposed in 2003 were based on previous NIST's studies presented in the Appendix A of this report [200] [2]. In its Image Quality Study, the NIST had presented the main factors that influence the flat-to-rolled matching process: the number of fingers used in the comparison process, the correspondence areas between the fingerprints compared, and the quality of the fingerprints. On a small data set of fingerprints, a correct acceptance rate of 99% was obtained for verification purposes with the thumbs, at a false acceptance rate of 1%. On a larger background data set of fingerprints (620'000 subjects), the correct identification rates at rank one were 95%, 90% and 86% when a probe set of 500, 10'000 and 100'000 subjects respectively were used for the identification process.

The NIST conducted in 2004 a technology evaluation in order to estimate the performance of the system and sensor used in the US-VISIT program [285].

[1] Section 11.2 presents more information about the recommendations of the "303A Report".

[2] The Appendix A of this joint report is available online at `http://www.itl.nist.gov/iaui/894.03/fing/fing.html`.

Verification and identification performances have been estimated in this evaluation. For the verification process, the experiments were conducted on a set of 6'000 finger pairs (right and left index) against 6'000 gallery images. The correct acceptance rates obtained at a false acceptance rate of 0.01% were 97.5% and 95.3% for the right and respectively left index. In combining these two fingers by adding the matching scores and by applying a specific threshold, the correct acceptance rate was 99.5% at a false acceptance rate of 0.1%. For the identification process, the experiments were conducted on a set of 60'000 finger pairs and on a background gallery of 6'000'000 finger pairs. The correct acceptance rate obtained at a false acceptance rate of 0.31% was 95.9%. The results showed also the influence of the background size on the performance. If the background size increased, the correct acceptance rate was constant, while the false acceptance rate increased linearly. The image quality was presenting in this report as the "most critical single factor impacting the performance of fingerprint recognition systems" and its impact is "greater than the impact of the difference in algorithms".

The NIST conducted in 2004 studies for evaluating the fingerprint matching performance by using their Verification Test Bed (VTB) [287] [3]. The evaluations were separated in small-scale studies on data sets of 20, 216, 1021 and 2700 subjects (10 seconds video sequence per finger for the first set and 2 fingerprint cards per subject for the other sets) and large-scale studies on data sets of 52'000 (and 46'000 subjects for the background), 225'000 (and 225'000 subjects for the background), 274'000 (and 6'000'000 subjects for the background) and 600'000 subjects (1 fingerprint card per subject for the two first sets, and 2 sets of left and right index per subject for the two last sets). The small-scale studies were conducted for evaluating the influence, in verification purposes, of the use of plain or rolled fingerprints and of the choice of the fingers on the performance. For rolled-to-rolled fingerprint comparisons, the correct acceptance rate was 96% at a false acceptance rate of 1%, while the correct acceptance rate of plain-to-rolled comparisons was 90% at the same false acceptance rate. When index finger and thumb are combined, the correct acceptance rate was 99% at a false acceptance rate of 1%, while the correct acceptance rate when the two index fingers were combined was 98% at the same false acceptance rate. The authors explained this difference by the fact that a larger area were available for the thumb und thus more minutiae were detected and used for the recognition process. With the large-scale studies, similar results were obtained for verification purposes, with inked and live-scan fingerprints. At a false acceptance rate of 1%, the correct acceptance rate was about 91%. With a data set of 620'000 subjects, the identification rate for right index fingers was 76% for a rank-1 thresholding, while this rate was 85% for the combination of the two index fingers.

The NIST conducted in 2004 studies for evaluating the matching performance of plain-to-rolled fingerprints using their Algorithmic Test Bed (ATB) in identification purposes [289]. With data sets of about 1'000, 48'000, 60'000, 274'000 and 300'000 subjects, the accuracy of plain-to-rolled was similar to rolled-to-rolled recognition, with a correct acceptance rate of about 98%. The use of 10 fingers in the plain-to-rolled comparison process will not provide a better accuracy than with fewer fingers.

[3] The VTB used the NIST Fingerprint Image Software (NFIS), described in Section 6.6.

The German Federal Office of Security in the Information Technology (Bundesamt für Sicherheit in der Informationstechnik) has evaluated the influence of minutiae-based matching algorithms, sensor technologies and ageing of the data available as model [48]. The evaluations, called **BioFinger1** [4], were conducted on a set of 30 persons (all the fingers, except the little fingers, were used). For each of the 11 sensors tested (6 optical, 3 capacitive, 1 thermal and 1 piezo-electric sensors), the fingers were acquired in 3 different sessions (3 samples per session and per finger). Each sensor was combinated with each of the seven minutiae-based matching algorithms tested for the evaluation of the recognition's performance. Among all the possible combinations, the half had an equal error rate lower than 5%, a third had an equal error rate lower than 3% and only 8% had an equal error rate lower than 1%. For a false acceptance rate of 0.1%, the half had a correct acceptance rate higher than 90%, while only 23% of all these combination had a correct acceptance rate higher than 97%. The best results were obtained with optical sensors, while the differences between algoritms were less relevant. Regarding the ageing and its influence on the recognition process, the autors estimated that the false rejection rate will duplicate if the age difference between the enrolled template and the template acquired during the transaction reaches 10 years. Another evaluation (**BioFinger2**) will be conducted in order to estimate the performance improvement when multiple fingerprints are used in the verification process.

"State of the art fingerprint matching algorithms are nowhere near the theoretical upper bound on their performance" [294] and thus even more efforts will be necessary to improve their performance. Several challenging evolutions have to be done in this matter:

Inconsistent and irreproducible contact The problems in inconsistent contact entail that such systems should be invariant to translations or rotations, and that they should be able to match, even if the overlap area is small.

Elastic distortions Minutiae-based algorithms should also be invariant to the nonlinear deformations introduced by the switch-over 3D-2D. If a model of these distortions could be created, which was not fully explored until now, the performance of such systems can increase in an important way.

Incomplete ridge structure The pre-processing stage should be able to work robustly with incomplete fingerprint images, especially when core or delta(s) are not visible.

6.4 Sensors

To obtain a digital image from a fingerprint, several methods are conceivable [173]. For AFIS-systems, inked-fingerprints are usually used for acquire digital images off-line. For on-line methods, two types of sensors are available using

[4] The BioFinger1 evaluation is available online at `http://www.bsi.bund.de/literat/index.htm`.

touched and sweep methods (see Table 6.1 for a quick overview of existing touched-based sensor approaches).

Optical	**Solid-state**	**Ultrasound**
FTIR	Capacitive	Ultrasound
Optical fibers	Thermal	
Electro optical	Piezoelectric	
Direct reading		

Table 6.1: Touched-based sensor approaches for fingerprint technology.

Touched methods The fingerprint is simply put in contact with a flat sensor. Touched methods use optical, solid-state and ultrasound sensor based. Such methods are easy to use and need no training. But some issues are associated: hygienic problems; unfavorable influence of dirty fingers on the image quality; remanent fingerprint residue on some sensors; critical location of the fingerprint on the sensor's area to obtain sufficient information; influence of the size of the sensed area on the cost.

Sweep methods The fingerprint is simply moved vertically on a window sensor, which is as wide as the finger. Then the slices are combined to obtain the fingerprint in its entirety. The sensor's cost is lower than previously for the touched methods, but some inconveniences have to be revealed: the period of adaptation for users is higher than other methods; sufficient number of slices have to be taken, what requires a powerful microprocessor; the reconstruction process takes time.

6.4.1 Optical sensor

For touched methods, several sensor types are available. The first sensor type presented in this chapter is the *optical sensor*.

Frustrated Total Internal Reflection (FTIR) The ridges of the finger are in contact with one side of a prism. From second side, light is produced and focused through a lens onto an image sensor on the third side. This glass prism can also be substituted by a sheet prism, small prisms adjacent to each other, using the same methodology.

Optical fibers The prism and the lens of the latter method is substituted by a fiber-optic platen. The ridges of the finger are directly in contact with the upper side of the platen. On the opposite side, a CCD/CMOS receives the residual light. Such methods are very expensive, as there is a large sensor's area, but the global size of the sensor is reduced, with regard to the FTIR sensors.

Electro optical This sensor is composed by two layers. A first polymer layer allows a light emission if a potential is applied, and a second photodiode array layer, converts the light emitted into a digital image. Such methods create a poor quality image, compared to the FTIR methods.

Direct reading The fingerprint is directly focused by a high-quality camera, without the need of a contact with a sensor. However well-focused and high contrasted images are difficult to obtain.

6.4.2 Solid-state sensor

The second sensor type presented in this chapter is the *solid-state sensor*, also called silicon sensor. The sensor consists of an array of pixels, in which each pixel is a tiny sensor and without any optical and CCD compound. Such systems need smaller size, and the cost are thus reduced.

Capacitive The sensor is a 2D array of micro-capacitor plate, protected by a thin coating. The other plate of the micro-capacitor is the ridges of the finger. The electrical charges are different in function of the distance between the ridges and valleys and the plate.

Thermal The sensor is made of pyro-electric material, maintained at a high temperature by electrical heating, producing current based on temperature differentials. The ridges and the valleys produce a different temperature differential, generating the creation of the image. This approach is usually used in sweep methods.

Electric field The sensor consists of a drive ring, generating a sinusoidal signal, and a matrix of active antennas, receiving a small amplitude signal transmitted by the ring and modulated by the finger skin structure. The finger has to be simultaneously in contact with both elements. For obtaining the image of the fingerprint, the sensor matrix is amplified, integrated and digitized.

Piezoelectric The sensor consists in a pressure sensitive area, composed by a non conductive di-electric material. When mechanical stress is applied to the sensor, an electrical signal, proportional to the pressure, is produced, generating the image of the fingerprint, as the pressure is different for ridges and valleys. The sensor is not sensitive enough to detect small differences in pressure. Such approaches produce poor quality images, compared to the other sensors.

6.4.3 Ultrasound sensor

The third and last sensor type presented in this chapter is the *ultrasound sensor*. This sensor consists of an acoustic signal sent through the platen, and the echo signal is captured. It works like an echography and produces good quality images. The acquisition needs a few seconds, the sensor is quite expensive and is thus not mature enough for fingerprint recognition systems.

6.4.4 Ergonomics and acquisition environment

In automatic recognition, the ergonomics of the systems are relatively pleasant. Indeed, as it is a question of putting in contact, during about 1 second, one or several fingers with one or more sensors, the system is arranged in a way that the subject can do it in a not binding position. The finger has to be placed flat

on the sensor and has to be localized in the center of the sensor. Some hygienic problems may appear. In Asian countries for example, feedback from users ranked hygienic issue at the forefront of the concerns. Some problems could also appear for people with amputated fingers. Finally, template ageing exists somehow for fingerprints. Indeed, during the life time, the quality of fingerprint pattern can decrease, especially for manual workers, and thus the features extracted during the verification/identification process will not correspond any more to the features extracted during prior enrollment.

The environment where the system is placed will also affect the quality of features extracted. Depending on the temperature or the humidity, the finger will be more or less dry, thus affecting the features acquired. The location (position, inclination,...) of the system for the verification/identification process can also influence the results, especially if it differs from the enrollment process.

6.4.5 Fingerprint acquisition for identity documents

In identity documents' applications, two possibilities are available: the acquisition device is external or internal to the document. In function of the purpose, some sensors are preferable to others. Indeed, big sensors, as FTIR optical sensor, can not be integrated in an identity document's sheet. This kind of use needs thin sensor like optical fibers or capacitive sensor. With such devices, the biometrics can be directly acquired on the identity document. Furthermore, liveness detection (the ability of a sensor to detect if the information presented to the sensor is "alive") should be integrated in all fingerprint sensors approaches used in the field of identity documents. Detection methods, based on perspiration, distortion, spectral technology, ultrasonic, pulse and electric resistance, may be used to prevent any abuse in this field.

6.5 Computational resources

A fingerprint template can be stored in several ways, as described in Section 2.7.2. The template generally consists of a matrix containing series of x, y coordinates and the orientation of the minutiae positions, approximately less than 700 bytes in most of the cases. The chip memory is then sufficient to store the fingerprint template. The possibility also exists to compute the entire process on the card, from the acquisition stage to the decision stage. Actually *match-on-card* technology using fingerprint recognition is already available from several biometric vendors (see Section 2.7). The storage and the identity verification are completed directly on the smart card. As a sensor is also integrated in the card, there would be no longer the necessity for a separate fingerprint acquisition device, reducing thus the cost of an access control system. As all the processing steps are performed on the card itself, in a closed environment, this increases thus the security and the privacy of this biometric recognition system. Indeed, the owner of the card has a complete control on his biometric information stored on it.

6.6 Open source systems

NIST Fingerprint Image Software 2 (NFIS2) This software was developed by the National Institute of Standards and Technology (NIST) [5]. Here are the main components of this software:

1. Fingerprint segmentation algorithm: the NFSEG can segment the four-finger plain impression found on a fingerprint card into individual images or can be used to remove only white space from fingerprint images;
2. Fingerprint Pattern Classification: the PCASYS can categorize the general shape of the fingerprint into six classes (arch, left or right loop, scar, tented arch, and whorl).
3. Minutiae detector: the MINDTCT can locate the ridge endings and bifurcations on a fingerprint image and assess the minutiae quality, based on local image conditions.
4. Fingerprint Image Quality Algorithm: the NFIQ can assess the image quality.
5. Fingerprint Matching Algorithm: the BOZORTH3 can proceed in verification and identification modes.

The NFIS2 Software contains also reference implementation of the ANSI/NIST-ITL 1-2000 standard and a large collection of general-purpose image utilities, such as JPEG, WSQ encoders and decoders.

FingerCode An open source software, based on the work of [144] (see Section 6.2), is available online [6]. This open source is implemented in MATLAB®.

Fingerprint Verification System An easy to use library that allows programmers to integrate fingerprint technology into their software is available online [7].

6.7 Databases

Some fingerprint databases are publicly available [34]. First, the National Institute of Standards and Technology (NIST) has a large number of fingerprint databases, with rolled fingerprint (NIST-9, NIST-10 and NIST-29), livescan video fingerprint (NIST-24), latent crime scene fingerprint (NIST-27), fingerprint of different resolutions (NIST-30), and some other databases (NIST-4 and NIST-14). The University of Bologna (Italy) organized Fingerprint Verification Competition (FVC) in 2000 [170], 2002 [171] and 2004 [172] using three different live-scan devices, for each competition, to acquire the images of the databases. These databases contain also for each competition new synthetic generated fingerprints sets [8]. These twelve databases are all available in [173].

[5] NFIS2 open source system available online at `http://fingerprint.nist.gov/NFIS/`.

[6] FingerCode source code implemented in MATLAB® available at `http://utenti.lycos.it/matlab/speed.htm`.

[7] Fingerprint Verification System source code available at `http://fvs.sourceforge.net/`.

[8] More information about the Synthetic Fingerprint Generator (SFinGe) program, developed by the Biometric Systems Lab (University of Bologna), can be found in [173] and online at `http://biolabs.csr.unibo.it`.

6.8 International competitions

The National Institute of Standards and Technology (NIST) is at the origin of some international competitions, so is the University of Bologna. It is necessary to clarify that, because every evaluation uses different databases, the results are not comparable between competitions. Indeed, every result is related to the database on which the evaluation was completed, as the performances can vary dramatically based on the characteristics, or type of the data [170, 286].

6.8.1 Fingerprint Vendor Technology Evaluation 2003

This evaluation is the FpVTE 2003 [286] [9], performed by the NIST. It was conducted to evaluate the accuracy of the state-of-the-art fingerprint matching, identification and verification systems. 34 systems from 18 different companies, were evaluated. The tests were conducted on three separated datasets: large-scale, medium-scale and small-scale tests. The large-scale test used 64'000 fingerprint sets, containing 1 to 10 fingerprint images each, and these sets were partitioned in 31 subgroups (varying the number of fingers contaning in the sets). The correct acceptance rates, when multiple fingers were used, were about 100% at a false acceptance rate of 0.01%. The three best matchers had on all the subtests of this large-scale evaluation, correct acceptance rates higher than 95% at a false acceptance rate of 0.01%. The medium-scale test used a set of 10'000 fingerprint images, containing only right index fingers. For the two best algorithms, the correct acceptance rates were higher than 99.3% at a false acceptance rate of 0.031%. Finally, the small-scale test used a set of 1'000 fingerprint images, containing also only right index fingers. The three best algorithms had correct acceptance rates of about 100% at a false acceptance rate of 0.1%. In conclusion, the most accurate system at a false acceptance rate of 0.01% had correct acceptance rates higher than 98.6%, 99.6% and 99.9% for every single-finger subtests, two-finger subtests, and 4, 8 or 10-finger subtests respectively. The variable which had the largest effect on system's accuracy, exept the number of fingers used, was the fingerprint quality.

6.8.2 Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers

This evaluation is the Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers [279] [10], performed by the NIST in 2003. It was conducted to evaluate the accuracy of one-to-one matching used in the US-VISIT program. Additionally, 8 fingerprint matching vendor systems were also evaluated. These systems were tested on 12 different single finger data sets of varying difficulties. A random sample of 5800 subjects were selected from some live-scans databases and inked impressions databases. In this study, only fingers from same type are compared between them (right middle fingers between them and so on). Each SDK evaluated had performed 614'638'238 comparisons. According to the results of this evaluation, the two most accurate systems had a correct

[9] The FpVTE 2003 Summary of Results and Analysis Report are available online at `http://www.itl.nist.gov/iaui/894.03/fing/fing.html`.

[10] These one-to-one studies of vendor SDK matchers are available online at `http://www.itl.nist.gov/iaui/894.03/fing/fing.html`.

identification rate of more than 98%, at a false acceptance rate of 0.01%, and the worst more than 94%, at a similar false acceptance rate. This evaluation revealed also that in general, better performance was obtained with thumbs, rather with index. Furthermore, with right fingers, the performances were also better than with left fingers. However, thumbs and index fingers had similar performance when high quality images were used for the matching process.

6.8.3 Fingerprint Verification Competition

This evaluation is the Fingerprint Verification Competition (FVC) performed by the University of Bologna in 2000 [11] [170]. The four databases created for this evaluation used the state-of-the-art sensor technologies for three of them and the synthetic fingerprint generation program SFinGe for one of them. Each database contained 880 impressions from 110 different fingers. The first two were acquired in two different sessions from 25 people. 4 fingers per person and per session were acquired. The third database were acquired from 19 people with age variations. In four sessions, 6 fingers per person were acquired twice. The impressions of the 10 last fingers were used as a training set for the participants. 11 algorithms had been submitted for testing. According to the results of this evaluation, the two most accurate systems had an average equal error rate lower than 2.28%, with an average equal error rate (for all participants and all databases) around 14%. This evaluation revealed also that the synthetically generated database was adequate to evaluation purposes, such as the FVC2000.

6.8.4 Second Fingerprint Verification Competition

This evaluation is the second Fingerprint Verification Competition (FVC) performed by the University of Bologna in 2002 [12] [171]. Four new databases were created, with three state-of-the-art sensors technologies and one synthetically generated database (generated by the SFinGe program). The evaluation was conducted on three groups, one for each non virtual fingerprint database, of 30 people each. The 4 fingers per person were acquired in three different sessions, making vary some acquisition's conditions, such as distortion, rotation, dry and moist. 4 impressions per finger and per session were acquired. For each database, only a subset of 110 fingers, with 8 impressions per finger were taken into account in this evaluation. The impressions of the 10 last fingers were used as a training set for the participants. 33 algorithms had been submitted for testing. According to the results of this evaluation, the six most accurate systems had an average equal error rate lower than 1.00%, and false non-match rates lower than 1.46% and 1.87%, at a false match rates of 0.01% and 0.001% respectively, with an average equal error rate for all participants and all databases of about 7%.

6.8.5 Third Fingerprint Verification Competition

This evaluation is the third Fingerprint Verification Competition (FVC) performed by the University of Bologna in 2004 [13] [172]. Four new databases were

[11] FVC 2000 homepage at `http://bias.csr.unibo.it/fvc2000/`.
[12] FVC 2002 homepage at `http://bias.csr.unibo.it/fvc2002/`.
[13] FVC 2004 homepage at `http://bias.csr.unibo.it/fvc2004/`.

created, with three state of the art sensors technologies and one synthetically generated database (generated by the SFinGe program). The evaluation was conducted on three groups, one for each non virtual fingerprint database, of 30 people each. The 4 fingers per person were acquired in three different sessions, making vary some acquisition's conditions, such as distortion, rotation, dry and moist. 4 impressions per finger and per session were acquired. For each database, only a subset of 110 fingers, with 8 impressions per finger were taken into account in this evaluation. 67 algorithms, classified in open and light categories, had been submitted for testing. According to the results of this evaluation, the five most accurate systems had an average equal error rate lower than 2.90%, and false non-match rates lower than 4.57% and 7.44% at false match rates of 0.01% and 0.001% respectively.

6.8.6 Fourth Fingerprint Verification Competition

A fourth fingerprint verification evaluation will be performed by the University of Bologna, the Michigan-State University, the San Jose State University and the Universidad Autonoma de Madrid in 2006. The results will be available on the FVC 2006 homepage on January 2007 [14].

[14] FVC 2006 homepage at `http://bias.csr.unibo.it/fvc2006/`.

Chapter 7

Modality: Iris

7.1 Introduction

In 1965, Adler, cited in [282], claimed that the human iris, which has a very complex layered structure unique to an individual, is an extremely valuable source of biometric information. The general structure of the iris is genetically determined, but the particular characteristics are "critically dependent on circumstances (e.g. the initial conditions in the embryonic precursor to the iris)" and stable with age: iris recognition is thus considered as a promising biometric approach [281]. At the time of the use of the anthropometrical system of Bertillon [24], such an individuality was not yet presupposed, even if it was necessary to introduce the colour of the iris.

Some people believe that the iris patterns are reflecting, amongst other things, the state of health of each of the organs in the human body, calling this science iridology. But several scientific tests declared the iridology a medical fraud [22] and discredited its claims [281].

The number of features in the human iris is large [284]. It contains many collagenous fibers, contraction furrows, coronas, crypts, colour, serpentine vasculature, striations, freckles, rifts and pits. The iris is stable, as it is an internal organ and thus protected by the eyelid, cornea and aqueous humour. This modality does not vary with age starting from the first year after birth until death. No foreign material usually contaminates the iris.

The uniqueness of the iris is due to the chaotic morphogenesis of that organ [78]: the statistical probability that two irises would be exactly the same is estimated at 1 in 10e72 [284]. Two different irises are extremely unlike to be equal, even in the case of genetically identical twins [80].

7.2 Overview of algorithmic approaches

Several iris recognition systems have been developed, which exploit the complexity and stability over time of iris patterns and claim to be highly accurate [169, 181, 281]. The most well-known algorithm, on which the principle state-of-the-art iris recognition systems are based, is the algorithms developed by Prof. Daugman [1] (Computer Laboratory, Cambridge University UK). This approach

[1] Personal homepage of Prof. Daugman at `http://www.cl.cam.ac.uk/users/jgd1000/`.

comprises the following steps [79]:

Position localization of the iris After located the position of the eye on the image, before the image capture, the first step is to locate the region of the image corresponding to the iris. Indeed, it is necessary to localize precisely the inner and outer boundaries of the iris, and to detect and exclude eyelids if they intrude. This preprocessing step is completed by the application of pseudo-polar coordinates, taking into account that the inner and outer circular boundaries may not be completely concentric.

Normalization The portion of the image corresponding to the iris is translated to a normalized form, with a radius from 0 to 1, so that possible dilation of the pupil does not affect the system.

Features Extraction The features extraction process is completed by the use of 2D Gabor wavelets to perform a multiscale analysis of the iris. The regions of the image are analyzed at different scales by frequency-selective filters. Thus the information about local phase, coded with two bits corresponding to the signs of the real and imaginary parts, is obtained. The result is a 256-byte code, which represents a specific iris and is called IrisCode.

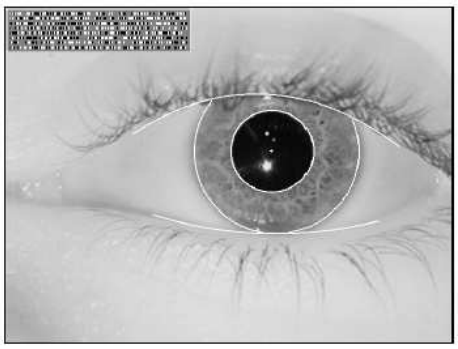


Figure 7.1: Localization of the iris patterns and the correspondent IrisCode [79].

Matching step Similarity scores are obtained by computing a Hamming Distance, with exclusive -or operations, to detect the fraction of the bits of the two IrisCode that disagree. The computation speed is very high, as it uses Boolean logic approach.

Here is a short description of three other iris recognition approaches. The first approach, described in [281, 282, 283], localizes the iris using a histogram based model fitting method. For representation and matching, it registers a captured image to a stored model, filters with isotropic 2D bandpass decomposition (Pyramid Laplacian), followed by a correlation matching based on Fischer's Linear Discriminant. The second approach, described in [266], uses a combination of gradient decomposed Hough transform and integro-differential operators for localize the iris, a 2D Hilbert transform to extract the features, and a Hamming

distance calculation for the matching process. The last approach, described in [181], uses circular and linear Hough transforms for localizing the regions of interest and occluding eyelids, a convolution of the normalized regions of interest with 1D Log-Gabor filters and phase quantising for encoding the features, and a Hamming distance calculation for the matching process.

The template obtained by iris recognition systems is approximately 500 bytes [203].

7.3 Performance

The performance of iris recognition systems is impressive. Even if these approaches have high accuracies, some difficulties appear with iris recognition technology, and thus influence the performance of such systems [281]:

While some **iris features** are yet in lace at birth, some features are only mature around the second year of birth. Furthermore, the pigmentation pattering continues until adolescence and a depigmentation appears with advanced age. Additionally, some drug treatments and intensive exposure to contaminants can alter the iris pigmentation. Even if these problems do not really affect the performance of state-of-the-art systems at the moment, it will certainly do in the future, in a large scale application of such a technology due to template ageing.

During the **acquisition process**, some difficulties may appear. The iris is a target which has a small size and which is in movement. The iris is also located behind a curved, wet and reflecting surface. It can be obscured by lashes, lenses and reflecting eyeglasses. The iris can also be partially occluded by eyelids. According to the properties of the eye, the illumination light influences the form and the full-presence of the iris.

During the **preprocessing steps**, the shape of the iris can influence the IrisCode. Indeed, pupils are often not very round.

The performance of iris recognition systems remain however impressive. Some laboratory-based experiments allow to evaluate the overall performance of state-of-the-art iris technology solution [281]. No false match was observed in all these experiments, only few false non-match errors were observed. Indeed, in one case, for a false match rate of 0%, the false non-match rate was about 2%.

In [266], the system developed obtains a false rejection rate of 8.2%, with a false acceptance rate of 0% and the verification time lasts about 600ms. In [181], the system developed obtains a false acceptance rate of 0.005%, with a false rejection rate of 0.238%. A US Army Research Lab deployment test [155] reports about 6% false reject and 0.00001% false accept on a sample population of 258 users.

The International Biometric Group has conducted from July 2004 to April 2005 the "Independent Testing of Iris Recognition Technology" [131], where three iris recognition acquisition devices, using the software and the SDK provided by Iridian, were tested with 1224 subjects. The samples were acquired in two separate sessions (only 458 subjects participated in the second session). For

the two enrollment transactions, two to four samples per eye and per device for each subject were acquired, while three samples per eye and per device for each subject were acquired for the three different recognition transactions. The matching process was completed off-line, after the acquisition process. The best result obtained was a FNMR of 0.583% at a FMR of 0.00129% in the transaction level and a FNMR of 0.759% at a FMR of 0.00013% in the enrollment level.

7.4 Sensors

The acquisition device of such systems, used to capture the details of the iris patterns, is well described in [281]. The image should resolve a minimum of 100 pixels of along the iris radius, from the pupil boundary to the white boundary. Some approaches capture the image from a distance of 15 to 46 cm with a resolution of 100 to 200 pixels for the diameter of the iris, and some other capture the iris from 20 cm with a resolution of about 256 pixels. A new acquisition device captures the iris pattern from a distance of 3 meters, with a similar resolution as traditional systems, while the subject is on the move [149], but no real performance evaluation was conducted with this prototype device. Originally, visible range illumination was used during the acquisition stage. Recently, the near infrared (NIR) illumination, in the 700nm-900nm region was proposed to cope with de variability of ambient illumination. A monochrome CCD camera is used to acquire high-resolution images. Due to the use of NIR illumination, even darkly pigmented irises reveal rich and complex features. The capture device has also to be able to localize first the eyes in the face, and has thus to be a wide-angle camera. It is why, most of the iris recognition systems usually use two different cameras, for this two different purposes.

The "Independent Testing of Iris Recognition Technology", conducted by the International Biometric Group, has evaluated three iris recognition acquisition devices [131]: LG IrisAccess 3000 Enrollment Optical unit, the OKI IRISPASS-WG and the Panasonic BM-ET300. The lower failure to enroll rate obtained with one of the devices was 1.61% for both eyes, and 8.50% for a single eye, while the worst failure to enroll rate obtained with one of the devices was 7.05% for both eyes, and 9.63% for a single eye. The failure to acquire rate when no samples were acquired on the transaction level was between 0.32% and 0.69%, while the failure to acquire rate when at least one sample of the right eye or at least one sample of the left eye were not acquired on the transaction level was between 0.91% and 0.1.77%. The enrollment duration is about 35 seconds for two of the devices and about 50 seconds for the third device, while the acquisition duration of a successful transaction's sample was between 1.92 and 5.05 seconds.

7.4.1 Ergonomics and acquisition environment

The recognition process with iris pattern needs a good positioning of the eyes in front of the sensor. Some systems inform if the subject is too close or too far from the sensor. The subjects have also to take off the glasses and contact lenses. Some problems could also appear with blind people, or with individuals with some eye diseases. As some sensors use near-infrared wavelengths, the

ambient lightning will disturb the acquisition process only if it is not too dark. Indeed, darkness can dilate the pupil and hide most of the iris pattern.

7.4.2 Iris acquisition for identity documents

The iris-based recognition technology uses sensor approaches which involve an imposing technology and thus is not appropriate for sensor on card-based architecture solutions. But the high computational speed, the non-complexity of the algorithm approaches and the low memory needed for storing templates allow the use of such a technology for match on card and data on card architecture solutions.

7.5 Computational resources

The storage of an iris template, like the IrisCode, is possible, as the template's size is very low (about 500 bytes). Furthermore, as the matching algorithm used in such systems is very fast, it seems to be possible to complete the matching process on the card itself, but not the complete recognition process as the sensor-on-card approach with fingerprint. Recently, PreciseBiometrics [2] has proposed a multimodal match-on-card solution incorporating iris, face and fingerprint [23].

7.6 Open source systems

An open source iris recognition system, implemented in MATLAB ® and derived from [181], is available online [3].

7.7 Databases

Some databases were created for commercial use, and thus the data on the statistical properties and singularity of iris patterns, presented in [79], is based on 9.1 million comparisons. Unfortunately, these databases are not available. But recently, Four iris databases were collected and are available for research purposes. The National Laboratory of Pattern Recognition, Institute of Automation from the Chinese Academy of Sciences made available to all interested researchers, iris databases : the **CASIA Iris Image Databases** (ver 1.0 and ver 2.0) [4]. The version 1.0 includes 756 iris images from 108 eyes, captured in two different sessions, three samples collected in the first and four in the second session. The version 2.0 includes 2400 iris images from 120 eyes, captured by two different devices, each device collecting 20 samples per eye. The Department of Informatics from the University of Beira Interior (Portugal) made available for biometric purposes, an iris database containing images with noise: the **UBIRIS database** [5]. This database is composed of 1877 iris images, captured in two different sessions, five samples collected on a set of 241 subjects for the first session and five samples collected on a set of 231 subjects for the second session

[2]Precise Biometrics homepage at `http://www.precisebiometrics.com/`.
[3]Source code available at `http://www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html`.
[4]CASIA Iris Image Databases available at `http://nlpr-web.ia.ac.cn/english/irds/irisdatabase.htm`.
[5]UBIRIS database available online at `http://iris.di.ubi.pt/`.

[226]. The images contain different kinds of noise, simulate a minimal collaboration from de subjects. The Department of Automation & Computer-Aided Engr., Computer Vision Laboratory, from the Chinese University of Hong Kong is making available for biometric purposes, an iris database: the **CUHK** [6]. This database is composed of 252 iris images, captured in a single session on 36 subjects, 7 samples collected for one eye. The Department of Computer Science from the Palacky Univeristy in Olomouc (Czech republic) is making available for biometric purposes, an iris database: the **UPOL iris database** [7]. This database is composed of 384 iris images, captured in a single session on 64 subjects, 3 samples collected for each eye.

7.8 International competitions

The first competition of iris recognition, borrowing the main ideas from the FVC2004, has been organized by the Institute of Automation of the Chinese Academy of Sciences (CASIA), using two databases including 13200 iris images (20 samples of the eyes of 330 volunteer, under two different illumination settings). As the other international biometric competition, each participant had to submit executable algorithms. The results were firstly presented at the Fifth Chinese National Conference on Biometrics Recognition, in December 2004 in China, but no proceedings paper was published on this topic. To the best of our knowledge, only four iris recognition systems have participated to this competition. The first two best iris recognition systems have obtained an average equal error rate for both databases of 4.25% and of 12.48%, while the worst two systems have obtained an average equal error rate of 19.88% and of 21.07% [8].

To avoid this lack of international evaluation and to assess the performance of state-of-the-art iris recognition solutions, the NIST will conduct the *Iris Challenge Evaluation* [9]. The first phase of this evaluation consists in a distribution of an iris recognition challenge problem from August 2005 until June 2006. The second phase consists in a large-scale iris technology evaluation, measured on sequestered data and will take place in the first quarter of 2006.

From January until August 2006, the NIJ-TSA Iris Recognition Study 2006 (IRIS06) focused on "standards-based performance and user cooperation studies of commercial iris recognition products" [10]. The aim of thsi study are:

- evaluation of the performance and interoperability of iris recognition products using international and US iris image data interchange format standards;

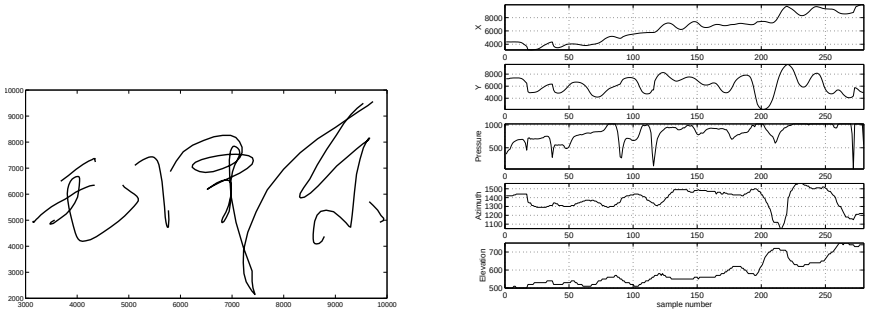
- investigation of hte influence of test subject presentation parameters, such as pose and eye-gaze angles, and of the ability of iris recognition technology to acquire and recognize non ideal iris images.

[6] CUHK iris database available online at `http://www2.acae.cuhk.edu.hk/%7Ecvl/main_database.htm`.
[7] UPOL iris database available online at `http://phoenix.inf.upol.cz/iris/`.
[8] These average results were sended to us courteously by Mr. Qiu Xianchao, from the National Laboratory of Pattern Recognition - Institute of Automation, of the China Academy of Sciences.
[9] ICE homepage at `http://iris.nist.gov/ICE/`.
[10] IRIS06 homepage: `http://www.authenti-corp.com/iris06`.

Chapter 8

Modality: On-line signature

8.1 Introduction



(a) x-y plane representation.

(b) x, y, pressure, azimuth and elevation signals.

Figure 8.1: Example of a signature realisation from the SVC 2004 corpus.

On-line handwritten signatures are those for which the pen trajectory and dynamics are recorded during the signing. Recorded information typically contains pressure, pen azimuth and pen elevation in addition to the trajectory on the pen tablet. The raw signature data is typically preprocessed by translation, rotation and/or scaling [100] to afford some degree of invariance to changes with each realisation. Some algorithms also require segmentation, for instance into "components" that are perceptually significant according to a motor model [43].

Features can be extracted from the pre-processed signature, which can then be represented according to two broad paradigms [218]. In the function-oriented paradigm, signals extracted from signature data (such as pressure or velocities) are considered as functions of time, the values of which directly constitute the feature vectors. In the parametric paradigm, local or global parameters are computed from the measured signals and used as features. Local parameters represent properties of sampling points, pen strokes, or components and can be extracted from local segments of the signature; examples of local parameters are the starting angle at initial pen-down, a segment's local radius of curvature, and so on. Global parameters concern some property of the complete observed

signature; for instance the total signing time, pen-up to pen-down ratio, bounding box aspect ratio and so on. A list of commonly-used global features and an algorithm to perform feature selection can be found in [151, 154]

Most works on on-line signature verification propose to use exactly the same set of features for every user, but some studies have reported gains in performance from using user-dependent feature sets, arguing that this accounts for signer intra-variability [165].

8.2 Overview of algorithmic approaches

Over the past 30 years, numerous algorithms and models have been developed to verify on-line signatures. While many algorithms rely on a temporal representation of the signature, some authors (notably Nalwa [199]) suggest that on-line signatures should be parameterized spatially. Currently, the lowest error rates are achieved by hidden Markov models using mixture of Gaussians output distribution, and Gaussian mixture models.

8.2.1 Dynamic Time Warping

The most widely studied on-line signature verification method is elastic matching (string matching) using dynamic time warping (DTW), also called dynamic programming (DP). Originally used in on-line signature verification by Sato and Kogure in 1982 [247], DTW has been gradually refined over the years. Two main approaches are seen in published literature: in the first the data points are used directly for matching after preprocessing (typically including subsampling), while in the second the signature is segmented according to perceived importance of boundary points.

Sakamoto et al. [245] have used position, pressure, and pen inclination to achieve 3% EER using three signature realisations templates per user with a 8-users corpus comprising a total of 1066 authentic signatures and 1921 forgeries. Jain et al. [140] have used a mixture of global features such as the number of strokes and local features, both spatial (e.g. x and y coordinate differences with respect to the previous point) and temporal (e.g. relative speed between points). They achieve about 2.2% EER using between three and five signature realisations templates per user with a 102-users corpus comprising a total of 1232 authentic signatures and 60 forgeries, thus probably underestimating the FAR.

Yanikoglu and Kholmatov [296], the winners of the signature verification competition 2004 (see Section 8.8), have used a Dynamic Time Warping to align signatures based on two local features (Δx and Δy), after which they compute three distances with respect to that user's training set, perform PCA to decorrelate the three distances and classify on this last measure. They report 1.65% FRR and 1.28% FAR on a 94-users database, using 8 signatures per user for the user models and holding out 2 and 7 signatures for testing, thus testing with 182 authentic signatures. 313 skilled forgeries are used for testing.

Recently, DTW has been used as one of the classifier in a multi-classifier scheme [198]. It has also been used as the main classifier in a multi-stage verification system which was tested on 121 users with 726 authentic signatures and 89 forgeries, obtaining about 0.23% FAR at 3.63% FRR [229].

8.2.2 Hidden Markov models

Inspired by the successful application of Hidden Markov models (HMMs) to on-line character recognition [162], HMMs have now become the best-performing models for on-line signature verification. The most commonly used similarity measure for HMMs is the log-likelihood ratio of the test signature given the user model to the test signature given the background model.

Yang et al. [295] have used quantised angle sequences as features, trying several HMM topologies and number of states. The best results, 3.8% EER, are obtained with a 6-states, left-to-right with skips topology, using 8 training signature realisations per model with a 31-users corpus comprising a total of 496 authentic signatures. The results are given for random forgeries.

Kashi et al. [151] have used a mixed-model approach, where global features such as average horizontal speed are combined with a variable duration discrete output HMM using inclination angles (with respect to the horizontal axis) and the difference between adjacent inclination angles as feature vectors. The reported error rate for a 20-states, left-to-right with no skips topology is 2.5% EER, using 6 training signature realisations per model with a 59-users corpus comprising a total of 542 authentic signatures and 325 forgeries.

Yoon et al. [299] transform the data into polar space with speed information, and further use vector quantisation to generate the feature vectors. A 5-states, left-to-right with skips HMM is used for verification, resulting in 2.2% EER using 15 training signature realisations per model, with a 100-users corpus comprising 2000 signatures. The results are given for random forgeries.

Richiardi and Drygajlo [236] have used a GMM (1-state HMM) with 64 diagonal-covariance mixture components to model local features and their time derivatives, and have obtained 1.7% EER on a 50-user subcorpus of the MCYT database, which provides 25 authentic signatures and 25 skilled forgeries for each user, training with 5 signatures per user and thus testing with a total 1000 authentic and 1250 forgeries.

Fierrez-Aguilar et al. [95] have used a 2-states, 32-mixtures per state, left-to-right HMM to model local features, and used score normalisation to obtain 5.79% EER on the SVC2004 development set (40 users, 20 authentic and 20 forged signatures per user, training with 5 signatures).

These results show that signature verification algorithms based on HMMs have the potential to perform as well or better than those based on DTW or a variant thereof.

8.2.3 Neural networks

Neural networks have been explored for on-line signature verification but the performance reported in published literature is inferior to other methods such as DTW, HMMs or GMMs. Chang et al. [58] have used a Bayesian neural network trained with incremental learning vector quantisation. The EER achieved on chinese signatures is about 2.3%, using 4 signatures per user model . The 80-user corpus comprises a total of 800 authentic signatures and 200 skilled forgeries. Wu et al. [293] have used linear predictive cepstral coefficient derived from the x, y trajectory of the pen to train single-output multi-layer perceptrons (MLPs). Each "word" (chinese character) of a user's signature is modeled independently by an MLP. The EER achieved on chinese signatures is 4.3%, using

an average of 12 authentic signature realisations and 12 forgeries to train each user's MLPs. The 27-users corpus comprises a total of 810 authentic signatures and 638 forgeries. It is not clear how this system would be applied to roman character-based signatures, where the relationship between the real letter and the signature-style letter is more ambiguous.

8.2.4 Euclidean distance

Euclidean distances or other distance measures have been used for on-line signature verification, generally achieving performance inferior to DTW, HMMs or GMMs. Rhee et al [235] use a model-based segmentation step prior to computing an Euclidean distance to a reference signature for each user. This results in an EER of 3.4%, using 10 signature realisations to build a reference signature with a 50-users corpus comprising a total of 1000 authentic signatures and 1000 very skilled forgeries.

Kashi et al. [152] have also used Euclidean distance with global and local features.

8.2.5 Regional correlation

The regional correlation approach has many proponents [210]. Nalwa [199] uses a function-based approach where the signature is parameterised using functions of arc-length, then cross-correlating these functions with each user's function prototype in her signature model. This achieves 3.6% EER on average over 3 different databases, amounting to a total of 204 users, 2676 authentic signatures and 1150 forgeries. Each user model was built using six signature realisations. While the corpus size is larger than what is used in most research papers, some pruning occurred which caused some inconsistent genuine signatures to be rejected.

Lau, Yuen and Tang [163] have used a correlation-based approach and achieved about 1.7 % EER on a database of 100 persons, where each person contributes 5 authentic signatures and is forged 3 times. Each user is modelled using 2 signatures, thus resulting in testing with 300 authentic and 300 forged signatures.

8.3 Performance

The current state of the art EER for medium-to-large databases (above 50 users) lies between 0.5% and 5%. A problem in comparing performances is that little work has been published on standard databases (with the notable exception of the SVC effort), thus some databases may be easier than others, for example because forgers are not as talented, or have more or less information about their targets. Environmental noise is absent from signature data, and performance drops will occur mostly due to ergonomical issues (tablet position, writing space) and inter-session time.

Health-related issues can affect handwriting, for example most patients that are not responsive to treatment with neuroleptics will exhibit symptoms of micrographia, whereby the writing size is significantly reduced [50].

Some percentage of the population will also exhibit dyspraxia (difficulty in planning and carrying out complex movements), meaning more variability can

be expected in signature realisations. These factures contribute to decreasing signature modality performance and are likely underestimated by the bias in population sampling present in most academic databases.

8.4 Sensors

Sensors for on-line signature acquisition typically divide the acquisition part in two components: the pen itself and the surface on which the pen writes. The electronics can be contained entirely within the writing surface (as in the case of PDAs), entirely within the pen (as in some research prototypes), or divided between the pen and the writing surface (as in the case of pen tablets commonly used by digital artists).

8.4.1 Electronics in the writing surface

Most modern PDAs (3COM/PalmOne's Palm, Sony's Clié, HP/Compaq's Ipaq, and numerous others as well as a recent portable game machine by Nintendo (Nintendo DS)) propose pen-input as a modality, generally coupled with more-or-less natural handwriting recognition. Some laptop computers (Toshiba Satellite 5200 series) also propose that the touchpad double as signature input hardware. These sensors typically report only (x, y) coordinates, and a binary pressure value. Pen orientation (azimuth and elevation) are not reported. With current processor speeds routinely in the MHz range for these devices, embedded signature verification becomes an attractive prospect.

"Dumb pens" offer the advantage that pen replacement in case of loss is very simple, and could be key to a more widespread acceptance of signature verification technologies in fields such as banking.

However, the lack of pressure information (and for some algorithms, of pen orientation information) is a serious drawback for on-line signature verification, which performs better if that signal is provided.

8.4.2 Electronics in the pen

While this approach is not the most commonly seen in recent research, the benefits of having a single device to acquire signature (portability, no need for special surface, possibly lower costs in volume production) have pushed several groups to investigate the feasibility of a standalone pen that does not need a specific surface to acquire dynamic handwriting signals.

In 1983, Plamondon *et al.* have proposed a self-contained pen, fitted with two pairs of orthogonal accelerometers and a pressure switch [217], based on a mathematical model of handwriting.

The SmartPen developped by Reynaerts and others [231] acquires x, y and z forces as well as elevation and azimuth.

More recently, Hook et al. have proposed the Biometrical Smart Pen[1] [120], which exists in several variants. The mechanical pen acquires forces in the x, y, and z (pressure) direction, as well as elevation and azimuth. Furthermore, it is fitted with a fingerprint sensor. Another version is a microphone-based pen,

[1] More details at `http://www.bisp-regensburg.de`.

which can be used to perform handwriting analysis from the writing sounds. The data transfer from the pen to a computer can be wired or wireless (bluetooth).

8.4.3 Electronics both in the pen and the surface

General-purpose sensors suitable for on-line signature acquisition are called *pen tablets* or *graphic tablets*. A research prototype has been used for signature verification in 1977 by Herbst and Liu [113], providing x, y positions and binary pressure information. Nowadays, many manufacturers supply tablets, for instance Wacom, Aiptek, AceCad, Genius, GTCO CalComp, and others.

In the Wacom implementation (Graphire, Intuos, Volito, and other tablets), the surface of the pen tablet sends electro-magnetic signals which power the pen, thus avoiding the use of batteries in the pen (other vendors, such as AceCad or Aiptek, require batteries to be inserted in the pen). A capacitive pressure gauge in the pen tip as well as two additional sensors provide pressure and azimuth/elevation data. The tablet also determines the x, y position of the pen. Wacom tablets have a resolution of 2540 or 5080 lines per inch, 1024 pressure levels, and can sample at up to 200 Hz.

The AceCad AceCat range tablets have 2540 lines per inch resolution, 1024 levels of pressure, and sample the pen data at 125 Hz.

The HyperPen series of Aiptek offers 3048 lines per inch resolution, and 512 pressure levels.

The prices for general-purpose pen tablets suitable for on-line signature verification starts at about CHF 90.

Dedicated signature pads also exist, some of them showing immediate feedback through a LCD placed directly on the writing surface. One of the most widely used is Interlink/Integrisign's ePad[2], offering a resolution of 300 lines per inch, 128 levels of pressure and a sampling frequency of 100 Hz. It is shown on Figure 8.2. An interesting model in the ePad series is the ePad-ID which combines a fingerprint sensor and a pen tablet. None of the ePad series can acquire azimuth and elevation data.

Figure 8.2: Dedicated signature sensor (Interlink's ePad).

MotionTouch provides a range of dedicated signature-capture sensors (with or without LCD feedback), having 500 or 1000 lines per inch resolution, 512

[2] `http://www.integrisign.com/products/epad.html`.

levels of pressure, and 100 to 200 Hz sampling. The Legapad model was adopted by the UK bank Nationwide Building Society.

8.4.4 Ergonomics and acquisition environment

The angle of the signature should be kept constant with respect to the acquisition surface, or rotation normalisation should be performed as a pre-processing task, which unfortunately can result in slightly decreased verification performance.

The size of the signing area should be kept constant, to avoid resampling of the signature which can also be detrimental to verification rates.

There seems to be no significant difference between signatures acquired with the user sitting and those acquired with the user standing [87].

Visual feedback is important for signature tasks. Thus, the user should be able to see the signature appear under the tip of the pen as she signs. To this end, a sheet of paper can be placed between the tip of the inking pen and the tablet surface, to provide more friction and a natural feel to the writing. Furthermore, this enables researchers to also investigate off-line signature at a later stage should they wish to do so and leaves a (legally binding) written proof of the transaction, which could be useful in applications such as e-voting.

8.4.5 Online signature acquisition for identity documents

To summarise, a general-purpose pen tablet device should be used as they are widely available and the price is fairly low; an A6 tablet is sufficient for acquisition. Feedback should be provided, either in the form of an immediate LCD response or a simple sheet of paper. The writing area should be constrained by a box, which will fix both maximum size and orientation of the signature. Provision should be made for left-handed users to fix the tablet at an appropriate angle. Similarly, vertical-style signatures (for example chinese or japanese) should be accommodated for by providing a second set of box sizes on a sheet of paper.

8.5 Computational resources

One signature datafile comprising x, y, pressure, azimuth and elevation data is typically between 5 kB and 10 kB. More efficient file formats can be used, and compression ratios of about 3:1 can be obtained by using a general-purpose compression such as Lempel-Ziv. Depending on the classifier type and model parameters, parametric models can typically be stored in 1 kB-2 kB.

Feature extraction is fairly simple in most parameterisations, and can involves regression computations (for velocity, acceleration, and other derivative computations). The feature vector will typically comprise between 1 and 15 dimensions. Once the features are extracted, modeling for instance with mixtures of Gaussians will involve several iterations of the EM algorithm. Scoring a pattern will involve evaluating likelihoods on each point of n-dimensional data and summing the results.

Thus, because of the small size of the features extracted from a signature and the possibility to achieve low error rates with simple classifiers, it seems

match-on-card would be feasible for the signature modality.

8.6 Open source systems

Although no open source on-line signature verification reference systems are available to the best of our knowledge, numerous statistical and other modeling toolkits are freely available and can be used to implement published algorithms.

8.7 Databases

Not many databases are publicly available to on-line signature verification researchers. Most research groups develop their own database.

MCYT MCYT [207] contains signature and fingerprint data for 330 users. A 100-users subset of this database is available to the members of the European BioSecure network of excellence. Each user provides 25 authentic signature samples (x, y, pressure, azimuth and elevation), and is forged 5 times by 5 different users. The forgers are given time to practice on their target and are shown a static image of the target's signature.

SVC2004 SVC2004 [298] is divided in two parts: an evaluation set of 40 users which is freely available, and a sequestered set used in the competition, which is not distributed. Each user contributes 20 signatures, and is forged 20 times. The data is acquired in two sessions at least a week apart. The forgeries are performed by at least 4 different forgers, which are allowed to practice by watching a dynamic replay of the signing sequence. The data contains (x, y, pressure, azimuth, elevation, pen down status, time stamp) signals. A noteworthy information is that this for privacy reasons, users were advised not to contribute their real signatures so this database contains alias signatures. This means the intra-user variability is probably overimportant. Also, this database contains both chinese-style (ideograms) and latin-style (left-to right latin alphabet) signatures.

Philips Laboratories Philips Laboratories [86] contains 51 users, and each user provides 30 signatures. There are also 3000 amateur forgeries (practiced based on static image and over-the-shoulder), and 240 professional forgeries (contributed by forensic document examiners). This database is not generally available.

8.8 International competitions

The only international competition so far is the Signature Verification Competition 2004 [298]. It defined two tasks, task 1 with only (x, y, pen down status) information and task 2 with additional pen pressure and orientation signals. Task 1 is suitable for PDA-type devices which report only coordinates and binary pressure (see section 8.4), while task 2 is suitable for higher-end devices. It is interesting to note that contrary to most previously published results, the results for task 1 were marginally worse than the results for task 2.

The testing protocol for task 2 is suitable for testing inclusion of on-line signatures in biometric identity documents, but the database itself, acquisition methodology, and forgery methodology are not appropriate to this application.

Chapter 9

Modality: Speech

9.1 Introduction

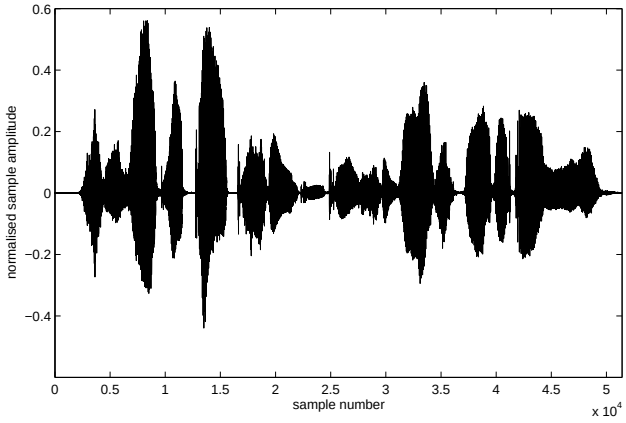


Figure 9.1: Speech waveform for the TIMIT sentence "she had your dark suit in greasy washwater all year".

Automatic speaker recognition was pioneered in 1970 by Doddington [85], and subsequently became a very active research area. Today, speaker recognition systems and algorithms can be subdivided into two broad classes:

Text-dependent systems rely on the user pronouncing certain fixed utterances, which can be a combination of digits, a password, or any other phrase. Thus, the user will prove her knowledge of the passphrase in addition to providing her biometrics. *Text-prompted* systems are a special kind of text-dependent systems which ask the user to pronounce a certain utterance which may not be known in advance, to deter recording and replaying of the user's passphrase.

Text-independent systems allow the user to pronounce any utterance of their choosing.

9.2 Overview of algorithmic approaches

An article that compares the hidden Markov model, dynamic time warping and vector quantisation approaches is [300]. Another comparing vector quantisation and dynamic time warping is [13].

9.2.1 Dynamic time warping

Taking into account the dynamics of speech parameters has been proposed in the eighties and seen many subsequent refinements. A useful technique in this context is Dynamic Time Warping (DTW), which allows for compensation of the variability of speaking rate inherent to human speakers. Dynamic Time Warping has relatively low computational requirements, and is mostly used for text-dependent verification. Nowadays, DTW is less frequently used as a stand-alone speaker recognition algorithm [209], but rather as a way to supplement the decision process with auxiliary information. Recently, DTW has been used to model pitch contours as auxiliary information, providing improved recognition rates [4], and as part of a multi-model speaker recognition system [91].

9.2.2 Vector quantisation

Vector quantisation (VQ) for speaker recognition has been proposed and tested for a digit-based system over a 100-users database in 1985 [258], and has seen little use recently [193]. This approach is not commonly used anymore for speaker verification because it is consistently outperformed by statistical methods, which do take into account feature overlap and correlations by incorporating covariance information. However, VQ can outperform statistical methods when little data is available. [183]

9.2.3 Statistical methods: HMM

Probabilistic methods rely on a parametric modeling of the speech signal. The modeling can be time-dependent (hidden Markov models) or not (Gaussian mixture model (GMM)). The value of model parameters have to be learned from training data, which is a critical point in probabilistic methods: sufficient training data has to be obtained. HMMs are very commonly used for text-dependent systems, where scores are typically obtained by finding the best path through the states. Ergodic (fully connected) HMMs have also been used for speaker recognition [183].

Poritz proposed using HMMs (5 states) to model speakers in 1982 [220], and performed identification on 10 speakers which resulted in no error. In 1991 Rosenberg et al. [239] used speaker-dependent whole word (digits) models, and tested on a 10-users population.

9.2.4 Statistical methods: GMM

Schwartz, Roucos and Berouti first proposed probabilistic modeling for speaker recognition in 1982 [252]. In 1995, Reynolds [232] proposed using a mixture of Gaussian models (termed MoG or more commonly GMM) for modeling speech

features belonging to a particular user. This approach has proved very successful and GMMs are now the dominant model for speaker recognition, often in combination with higher-level information provided for instance by DTW. A further refinement on the GMM method comes in the form of the universal background model (UBM) [234]: a large amount of data from many speakers is bundled together and a high-order GMM (typically 512 to 2048 mixture components [28]) is trained on that data. Then, a limited amount of speaker-specific data is used to adapt the UBM to each speaker. Essentially, the idea is to use a well-trained model (the UBM) as a good basis for initialisation of the user models. The vast majority of speaker recognition systems today are based on GMMs.

9.2.5 Neural networks

Neural networks have sometimes been used for text-independent speaker recognition, trained by providing both client and impostor data. Oglesby and Mason first proposed a multi-layer perceptron (MLP) neural network with LPC-cepstral coefficients in 1988 and 1989 [204, 205], then expanded their work to a radial basis function network in 1991 [206] with better results than both VQ and MLP approaches. In [98], a radial basis function neural network is used for speaker identification on the TIMIT and NTIMIT databases. More recently, an auto-associative neural network has been tested on part of the NIST 2002 SRE database [111].

9.2.6 Support vector machines

Support vector machines (SVM), an approach that has successfully been applied to many pattern recognition problems, has also been used in speaker recognition.

Schmidt and Gish proposed in 1996 to use support vector machines to perform speaker identification [249]. They tested their approach on a 26-users subset of the switchboard corpus and reported better results than with Gaussian Mixture models. In 2001, Gu and Thomas [109] reported improvements over GMMs by using SVMs for a 250-speakers phone-quality database. More recently, Wan and Renals [277] have also reported better results for SVMs than for GMMs.

9.3 Performance

As for the case of face verification, error rates of speaker recognition systems are very dependent on the application, and good results in an evaluation campaign or in vendor specifications do not mean that these will be obtained in the field.

While speaker recognition research has been going on for some time and speech processing is a mature field, many problems remain unsolved. We will list below some of the problems inherent to this modality, which are in addition to the inter-session variability shared with other biometric modalities.

Channel (convolutional) noise will distort speech signals as soon as they leave the speaker's mouth. All microphones have their specific transfer functions, most of the time non-linear, and reverberation in a room will also alter

speech. It is known that speaker recognition performance degrades significantly when the enrollment and deployment conditions are not matched. Noise robustness techniques used in speech processing for speech recognition (such as cepstral mean normalisation) can often be applied to speaker recognition. Compensation techniques derived from forensic speaker recognition [39] can also be applied to the biometric case.

Environmental (additive) noise is added to the speech signal by other audio sources surrounding the speaker, for example car noise, interfering speech, background music, etc. In general, at low signal-to-noise ratios the error rates of speaker recognition systems drop significantly. Again, experience in other fields of speech processing can be drawn upon and applied to speaker recognition. A recent approach [237] is to ignore classifier decisions when they are deemed too unreliable and to acquire a new presentation in this situation.

Emotional state and health factors come into play because speech is a partly behavioural, partly physiological modality. The emotional state of users is known to alter the characteristics of the vocal tract. Many diseases, including the common cold, can change the voice of a person so much as to make it unrecognisable even by human listeners. Alcohol ingestion can also lead to significant changes in speech for some users, notably in fundamental frequency [117].

Since speaker recognition performance depends so much on acquisition and testing conditions, it is nearly pointless to provide approximative error rate ranges and the latter are not directly comparable to other modalities. International competitions enable more accurate comparisons.

9.4 Sensors

Numerous transducers exist to transform the acoustic pressure wave produced by the speech aparatus into electrical waves. The most common types are:

Moving-coil (dynamic) Moving-coil microphones have a light diaphragm attached to a conductive coil which is placed in the gap of a magnet. When the sound pressure waves hit the diaphragm, it moves accordingly and displaces the coil, which in turn induces current. Many dynamic microphones have a peak in the frequency response around 5 kHz, and a fall-off from around 8 kHz due to the mass of the coil-diaphragm assembly, though some higher-quality dynamic microphones have a flatter frequency response [244].

Ribbon Ribbon microphones have a strip of metal placed between the two poles of a magnet. When sound pressure waves hit the ribbon, it moves in the magnetic field and a current is induced through it. This type of microphone has a flatter frequency response than moving-coils, with a roll-off below about 40 Hz and above about 14 kHz.

Capacitor (condenser) The capacitor microphone has a fixed backplate, which is charged (permanently in the case of electret microphones), and a moving diaphragm constituting the other plate. When sound pressure waves hit the diaphragm, the capacitance of the assembly varies, meaning that the voltage across the capacitor varies in proportion. The main advantage of capacitor microphones is that the mass of the diaphragm is very small, thus allowing its good frequency response throughout, with a small peak in resonance between 12 kHz and 20 kHz.

Bauer [21] wrote a review of many types of microphone (including carbon microphones!) and their historical development.

Three important characteristics of a microphone are the directional response, frequency response, and sensitivity. The *directional response* quantifies the output level of the microphone at different incidence angles of the sound pressure wave with respect to the capsule's front. An omnidirectional response means sounds are picked up from all directions with equal sensitivity. It is important to know that the directional response of a microphone changes with the frequency, for instance omnidirectional microphones tend to become more directional with higher frequencies.

The *frequency response* quantifies the gain of the microphone over a range of frequencies. Ideally, the response would be perfectly flat meaning that all frequencies would be transduced into current in the same way. Practically, microphones will deviate from that and typically quote the frequency response over a range of frequencies with a maximum deviation from the response at 1kHz, for example "40Hz-14kHz ($\pm 3dB$)".

The *sensitivity* of a microphone indicates how much voltage will ensue from a given sound pressure level (with a reference to 1 V at 94 dB SPL).

9.4.1 Ergonomics and acquisition environment

To avoid picking up environmental noise both in enrollment and in deployment, a directional microphone should be used (cardioid or hyper-cardioid), and ideally a sound-proof booth would be used (which is unfortunately unpractical).

The position and distance of the mouth with respect to the microphone should be kept constant.

9.4.2 Voice acquisition for identity documents

About 30 seconds to 1 minute of speech should be collected from the user. This should ideally be phonetically-rich sentences in the native language of the user.

9.5 Computational resources

Raw speech data takes an amount of space depending on the sampling rate, quantisation levels, and number of channels (mono most of the time). Thus, a 16-bits, 16 kHz sampled speech signal will take about 31 kB per second of speech. Speech parameters (for example MFCCs) will compress the signal by a factor depending on the output frame rate and the number of features selected.

For example, a 39-coefficients parameterisation with a 10 ms frame rate results in about a 2:1 compression for the above example.

The memory needed for template storage depends on the template type. For GMM-based models, the size of the model will depend on the number of Gaussian components and the type of covariance matrices, as well as parameter tying. A typical size for a small (32-64 components) model would be between 5 kB and 10 kB without Lempel-Ziv compression.

Depending on the implementation of the matching algorithm (an idea is not to load the speech features for the whole utterance at once, but "stream" them to the chip), match-on-card could be feasible for the speech modality.

9.6 Open source systems

The LIA_RAL package [1], by the Université d'Avignon in France, is an open source speaker verification software implemented in C++ and based on the Alize toolkit [37]. It can read several feature types (HTK, SPRO, raw), runs reasonably fast, and has been used in NIST evaluations. Thus, it can be a good basis with which to compare other systems.

9.7 Databases

Many databases are available freely or at low cost for speaker recognition tasks [53, 104, 187]. However, many are geared towards telephone-quality speech and thus of not practical interest to identity documents, where it is anticipated acquisition will only occur through microphones and not telephone channels. Thus, we do not present PolyCost, SIVA, HTIMIT, LLHDB, Switchboard, OGI Speaker Recognition Corpus, YOHO, etc. Below, we focus only on those that may be relevant to our application.

AHUMADA AHUMADA [208] contains speech for 104 male users and 80 females users, captured with 4 different microphones and more than 10 different telephone handsets, sampled on DAT tape. The data consists of isolated digits, strings of digits, phonetically balanced sentences, read text at various speaking rates, and spontaneous speech. The data was recorded in 6 different sessions days or weeks apart. A subset of this data (electret microphone) can be used for initial testing of identity documents, but more users are needed.

BANCA BANCA [15] contains speech data for 208 users, captured with 2 different microphones (one high-quality and one low-quality) in 12 sessions (three acoustical conditions). The data, about 40 seconds per session, consists of isolated digits and spontaneous speech, and is sampled at 32 kHz, quantised at 16 bits per sample, and recorded in mono. This database offers a sufficient amount of users for perform initial testing for identity documents, but the acoustic conditions of the recording may not match the identity documents application.

[1] Available at `http://www.lia.univ-avignon.fr/heberges/ALIZE/LIA_RAL/index.html`.

EUROM1 EUROM1 (the multilingual European speech database) [57] contains speech data in 7 languages (Danish, Dutch, English, French, German, Norwegian, and Swedish), with 60 users per language. Most users were only recorded once, but some were recorded on different days; this is not consistent from country to country The data contains numbers and read speech, with emphasis on phonetic balancing. The data is sampled at 20 kHz and quantised at 16 bits, and recordings take place in an anechoic room. Laryngograph data is also available for some subset of the data. While the total population is large, language effects may prevent this database from being used for speaker verification evaluation; furthermore, the inter-session time is not strictly controlled as this database was not originally meant for speaker verification tasks.

King-92 King Speaker Verification (King-92) [116] contains speech data from 51 male users, recorded over 10 30-to-60 seconds sessions acquired weeks or months apart. The data is acquired with both telephone handsets (the recording quality varies depending on the location of the recording due to equipment differences) and a wideband microphone in a sound booth. The data is sampled at 8 kHz (originally 10 kHz in 1987 but resampled) and 16-bits quantised. This is not suitable for our identity documents purposes because the gender balance has to be representative of that found in the Swiss population, and the number of users is too limited.

STC STC Russian Speech Database [260] contains speech data from 89 users (54 males and 35 females), recorded over 15 or less 25-seconds sessions acquired within 1 to 3 months. The data is acquired using a high-quality, omnidirectional microphone in an office setting. The data contains 5 read sentences per session, is sampled at 11 kHz and quantised to 16 bits by a low-quality PC sound card. This can also be used as an initial development set for our application, though language effects may be a problem as the data is in Russian.

TIMIT TIMIT Acoustic-Phonetic Continuous Speech Corpus [103] contains speech data for 630 users (438 males and 192 females), recorded over a single 30-to-40 seconds session. The data is acquired in a sound booth, sampled at 16 kHz and quantised to 16 bits. The data contains phonetically-balanced read sentences in american English. The main problem with this data is that it has been recorded in one session and thus inter-session effects can not be evaluated. Furthermore, the amount of data per user is fairly limited. Campbell and Reynolds [53] advise against use of this database for speaker verification evaluation.

TSID TSID Tactical Speaker Identification Speech Corpus contains 40 users (39 males, 1 female) recorded in a single session. The data is acquired in open air, using military radio handsets and an wideband electret microphone. The data contains phonetically-balanced read sentences, digit strings, and spontaneous speech. This database is not suitable for our application because it is mono-session and gender-imbalanced. Furthermore, the open air environment does not correspond to the anticipated deployment environment.

Verivox Verivox [150] contains 50 male users recorded in a single 30-minutes session. The data is acquired in a sound booth, using a high-quality microphone. The data consists of digit sequences in Swedish. The data is sampled at 22 kHz, then downsampled to 8 kHz and quantised using 8 bits A-law companding. While a large amount of data is available per speaker, the gender-imbalance, Swedish language and narrowband sampling mean this database is not suitable for our purposes.

XM2VTS XM2VTS [191] contains 295 users and was recorded in 4 sessions about a month apart. It contains about 24 seconds of speech per user, read material (2 digits sequences and one sentence), for a total of total 7080 files. The files are sampled at 32 KHz and 16-bits quantised. While the amount of data per user is not very large and could lead to under-trained models, this database represents a good start for verification tests in our application.

9.8 International competitions

The main competition in speaker recognition is the USA's National Institute of Standards (NIST) speaker recognition evaluations series.

The NIST speaker recognition evaluations (SREs) [84] have been going on since 1996, where the test started with 20 males and 20 females. The 2003 evaluation focused on the Switchboard corpus (cellular or PSTN parts), and recognition of a single speaker with about 2 minutes of training, a single speaker with about an hour of training data, and a single speaker when the training data has 2 speakers. NIST SRE's are strongly focused on telephone speech, and thus not appropriate for our purpose, though some evaluation methodology can be borrowed.

Chapter 10

Multimodality

10.1 Multimodality and Identity Documents

As presented in Sections 2.3.2 and 2.10, the use of multiple biometrics is useful for increasing the security of biometric systems against spoof attacks and for minimizing the limitations of single biometric, as non-universality and intra- and inter-class variation. In a large scale introduction of biometric information in identity documents, the use of at least two modalities is recommended, in order to allow a more robust and more secure verification process between the information on the travel document and the supposed owner, as proposed in the NIST's joint report to the U.S. Congress and the European Commission's Proposals [201, 88] [1]. This multimodal approach is also recommended in order to avoid penalizing people who do not possess the required biometric.

The use of multiple biometrics, instead of a single modality, in identity documents will not be only beneficial, but will also create some constraints. First, the information size to be stored on the identity document will be increased, whether it is the raw data (as recommended by the ICAO) or the biometric templates. A combination into a single template of the biometric features or models from different modalities of a single person should be also a way to protect people's privacy. An example of a template combination of multiple units of a single modality (fingerprint) is presented in [297] [2]. For multiple modalities, a single template from partial biometric features or models will also provide an additional security measure for privacy protection, as the information available for each modality taken separately are not enough for an identification / verification process and thus can not be used for other purposes. Then, the use of multiple biometrics in identity documents will increase the number of sensor devices and recognition systems required at borders control and in enrollment centers, in comparison to the use of a single modality. This also means the training of additional people, in order to be able to use in a suitable way these systems. The increase of qualified staff and technical components will thus increase the overall costs of such an introduction.

[1] Chapter 11 presents more information about the NIST's recommendations and the European Commission's proposals.

[2] Section 10.2.3 presents more details on this approach.

10.2 Multimodal biometric systems and databases

The Section 2.10 presents several scenarios and strategies for combining biometrics. Some examples will be presented here, according to these categories, with indication, if mentioned, about the modalities, the acquisition protocol, the fusion levels and the fusion approaches used. This review is partially based on [146, 169, 241, 242].

10.2.1 Single biometric, multiple sensors

In [267], a multimodal Embedded Hidden Markoy Model-based (EHMM) approach was proposed for 2D and 3D face recognition, with a fusion method, a weighted-sum rule after score normalisation, at the match level. The experiments were conducted on 3000 images of 50 subjects, acquired in 5 different sessions. For each session, 12 views per subject were captured, varying lighting and facial expressions. The images consist of grayscale images and the corresponding depth map. The fusion of the data is obtained by normalising the scores in order to map them to a same domain and by giving a relative weight, chosen experimentally for each kind of data. By using the combined approach, the authors obtained an improvement of the EER of about 2-5% after fusion, comparing to the monomodal approaches.

In [59], a multimodal PCA-based approach was proposed for 2D and 3D face recognition, with a fusion method, a weighted-sum rule after score normalisation, at the match level. The experiments were conducted on the images of 278 subjects, acquired in two different sessions. The range camera captured simultaneously colour images and range data images, thanks the projection of striped light. The fusion of the data is obtained by normalising the scores in order to map them to a same domain and by giving a confidence accordingly to the distances which separated the top rank and the two follows ranks. By using a PCA-based approach for the two kind of data, the authors obtained a rank-one recognition rate of 92,8% after fusion, while these rates were only about 83,1% for 2D and 83,7% for 3D before the combination. The data used in this study is a part of the Human ID databases and is available for research purposes [3].

In [60], a multimodal approach was proposed for a PCA-based 2D face recognition (for visible-light and infrared light), with fusion methods at the decision and the score level. The experiments were conducted on the images of 240 subjects. For each session, four views per subject were captured, varying lighting and facial expressions. Two cameras were used to acquire the images, a long-wavelenght IR camera and a visible-light digital camera. The three fusion approaches used were an unweighted rank based strategy, a logarithmically rank transformation strategy and a score based strategy. All these combinations methods outperforms the monomodal approaches, and the score based strategy outperforms the other fusion methods.

[3] Computer Vision Research Laboratory of the Univesity of Notre Dame homepage at `http://www.nd.edu/~cvrl/`.

10.2.2 Multiple biometrics

In [142], a multimodal approach was proposed for face, fingerprint and hand-geometry, with fusion methods at the score level. The experiments were conducted on the traits of 100 subjects. For 50 subjects, five facial and five fingerprint images were acquired by a CCD camera and a fingerprint sensor respectively. For 50 other subjects (even if some of them were also present in the previous set), five hand-geometry images were obtained by a commercial camera. All the traits of this first set of subjects were randomly paired. Another database of 50 subjects was created for the three traits, captured by a video for face images, by another commercial sensor for fingerprint, and by the same camera for hand-geometry. It results in a database of 100 subjects, with 1000 genuine and 24'500 impostor score vectors, each vector containing the scores of these three modalities. The matching approaches for these modalities are as follows: minutiae-based matcher for fingerprint, which has as output similarity scores, PCA-based algorithm for face recognition, which has as output an Euclidean distance, and a 14-dimensional features vector for hand-geometry, which has for output an Euclidean distance. Seven score normalisation techniques (simple distance-t-similarity transformation with no change in scale, min-max normalisation, z-score normalisation, median-MAD normalisation, double sigmoid normalisation, tanh normalisation and Parzen normalisation) and three fusion techniques on the normalized scores (simple-sum-rule, max-rule and min-rule) were tested in this study. Excepted for one normalisation technique (the median-MAD), all fusion approaches outperform the monomodal approaches. For example, the fingerprint system, which is the best monomodal system in this study, obtained a genuine acceptance rate of 83.6% at a FAR of 0.1%, while the multimodal approach obtained a genuine acceptance rate of 98.6% at a FAR of 0.1% when the z-score normalisation and the sum-rule were used. At low FARs, the tanh and min-max normalisation techniques outperforms the other techniques, while at higher FARs, the z-score normalisation performs better than the other techniques. By using user-specific weights in the min-max and tanh normalisation, a significant performance improvement can also be obtained.

In [257], a multimodal approach was proposed for face and fingerprint, with fusion methods at the score level. The experiments were conducted on the traits of 972 subjects. For face recognition, the FERET image database was used in order to obtain 2 face images of 972 subjects, while for fingerprint recognition, a proprietary database was used. This later database contains two fingerprint images, captured by a live-scan, of 972 subjects. All the traits of these subjects were randomly paired. Three fingerprint recognition commercial systems and one face recognition commercial system were used in this study. Seven score normalisation techniques (min-max, z-score, tanh, adaptive, two-quadrics, logistic and quadric-line-quadric) and five fusion techniques on the normalized scores (simple-sum, min-score, max-score, matcher weighting and user weighting) were tested in this study. The EER of the best fingerprint system and of the face recognition system was respectively 2.16% and 3.76%, while the max-score fusion approach on quadric-line-quadric normalized scores obtained an EER of 0.63%. Excepted for the min-score fusion approach, all the normalization-fusion combinations outperform any monomodal systems tested in this study.

The **BIOMET** database [102] includes five different modalities, face, voice, fingerprint, hand and signature, and was acquired in three different sessions: 130 people in the first, 106 in the second and 91 in the last session. An audio-video camera has acquired frontal and sideways shots, using a list of sentences to pronounce. Furthermore, an infrared camera (1, 5 and 10 images per person in the respective sessions) and a 3D acquisition system based on structured light (only 5 acquisitions of 91 people were done) were also used in order to be invariant of the background lightening. For acquiring 2 dimensional images of the hand (with a resolution of 130 to 200 dpi in the fist two session and 300 dpi in the last one), a scanner was used (1 image per person in the first two sessions and 3 in the last one). The on-line signature modality was acquired on a graphical tablet with a grip pen during the first session and an ink pen (signing on a sheet of paper, on the tablet) during the two last sessions, capturing five parameters, the x, y coordinates, pressure, azimuth and altitude of the pen. Genuine signatures and impostor signatures were acquired during the sessions (15 genuine signatures and 17 impostor signatures per person were acquired, realized by five different impostors. Two different sensors, an optical and a capacitive, were used to capture the middle and index fingers of the right hand (1 image per person in the first session using only the optical sensor, 2 images per person in the second one and 3 images with the optical sensor and 4 images with the capacitive sensor per person in the last one). Validation of the collected data and evaluation of the difficulty of the database were also accomplished (for each modality separately), in performing the same algorithms used in the project on other biometric databases. More information about this database is available online [4], but the biometric data collected is not yet available.

The **BANCA** database [15] includes two different modalities, face and voice and was acquired in four European languages. Two different quality acquisition levels (high and low) and three different recording conditions (controlled, degraded and adverse) were used to capture the modalities of 208 people. A cheap analogue web cam (for the degraded condition) and a high quality digital camera (for the adverse and controlled conditions) were used for acquiring the face modality. Two microphones, a poor and a good quality one, were used simultaneously for recoding the voice modality. For each of the 12 sessions (4 sessions per condition) per person, every people have recorded 1 true client access and 1 informed impostor attack. This database is available online for research purposes [5].

MCYT database [207] includes two different modalities, fingerprint and signature, of 330 individuals in 4 different places (35, 75, 75 and 145 in the respective places). Two different sensors, an optical and a capacitive, were used to capture for each sensor 12 samples of all the fingers of each person under three different control levels, which are low, medium and high (3 samples in the first two control levels, and 6 samples in the last control level). The on-line signature modality was acquired on a pen tablet, capturing five parameters, the x, y coordinates, pressure, azimuth and altitude of the pen. Genuine signatures and skilled forgeries, produced by the five subsequent users of the concerning person,

[4] `http://www.int-evry.fr/biometrics/english/index.php?item=1&menu=projects`.
[5] `http://www.ee.surrey.ac.uk/Research/VSSP/banca`.

were acquired (25 genuine signatures and 25 skilled forgeries per person). This database is available for research purposes from the Biometrics Research Lab of the University of Madrid [6].

In [94], a multimodal approach was proposed including a face verification system based on a global appearance representation scheme, a minutiae-based fingerprint verification system and an on-line signature verification system based on HMM modeling of temporal functions, with fusion methods, sum-rule and support vector machine (SVM) user-independent and user-dependent, at the score level. The experiments were conducted on 50 subjects of the MCYT database for fingerprint and signature and on 50 subjects of the XM2VTS face database. All the traits of these subjects were randomly paired. The EERs of the face, the on-line signature and the fingerprint verification systems were 10%, 4% and 3%, respectively, while the sum-rule, the SVM user-independent and the SVM user-dependent fusion approaches obtained EERs of 0.5%, 0.3%, and 0.05% respectively.

In [161], a multimodal approach was proposed for palmprint and hand geometry, with fusion methods at the features level by combinating the feature vectors by concatenation, and the matching score level by using max-rule. The experiments were conducted on hand images of 100 subjects, 10 images for each subject, captured by a digital camera (500 images for training and 500 images for testing). The two modalities were derived from the same image. Only the fusion approach at the matching score level outperforms the monomodal systems. For a FRR of 1.41%, the multimodal approach obtained a FAR of 0%, while the palmprint-based verification system, the best monomodal approach in this study, obtained at a FRR of 2.04% a FAR of 4.49%.

In [241], multimodal approach was proposed for face, fingerprint and hand-geometry, with three fusion methods at the matching score level, sum-rule, decision trees and linear discriminant function, after a score normalisation (the scores are mapped to the range [0-100]). The experiments were conducted on a set of 50 subjects, 5 face images and 5 fingerprint images of the same finger were captured. Hand geometry images were captured on a second set of 50 subjects. Each trait were randomly paired to obtain a virtual multimodal database. The multimodal approach with the sum-rule fusion method outperforms the other fusion strategies, as well as the monomodal systems. At a FAR of 0.03%, the combination approach obtained a FRR of 1.78%, while the best monomodal system, fingerprint approach, obtained at a FAR of 0.01%, a FRR of 25%.

In [278], a multimodal approach was proposed for a PCA-based face verification system and a key local variation-based iris verification system, with fusion methods at the matching score level by using unweighted and weighted sum-rules, Fischer Discriminant Analysis and Neural Networks. The experiments were conducted on two different databases, the first of very high quality and the second of lower quality. 5 face images for each of 90 subjects of the first database were collected partially from public available face databases, such as

[6] Biometrics Research Lab homepage at `http://atvs.ii.uam.es`.

ORL, MIT and Yale, while for the second database, 10 face images for each 40 subjects were collected from the ORL database. The authors collected also for the first database 5 iris images per subject of another set of 90 subjects, while 10 iris images were acquired per subject from another set of 40 subjects for the second database. For each database, the biometric traits were randomly paired to obtain a virtual bimodal database. With the first database, only the weighted sum-rule and the neural network fusion methods outperform the best monomodal verification system, the iris-based approach, while all the fusion strategies outperform the monomodal approaches with the second database. Furthermore, with a neural network training for every subject, this fusion approach obtained the highest verification accuracy with the two databases. With the second database, the enrollment failure, due to the poor quality of the iris images, can also be decreased by fusion approaches.

A review of bimodal approaches for acoustic speech and visual speech can be found in [61]. The authors have presented the principal components and the gain in accuracy and robustness of such approaches, compared to single modalities.

BioID is a commercial multimodal approach for a model-based face classifier, a VQ-based voice classifier and an optical-flow-based lip movement classifier [99] for verifying persons. Lip motion and face images were extracted from a video sequence and the voice from an audio signal. Accordingly to the security level, experiments on 150 persons demonstrated a decrease below 1% of the FAR.

In [118], a bimodal approach was proposed for a PCA-based face and a minutiae-based fingerprint identification system with a fusion method at the decision level. The experiments were conducted on 1500 fingerprint images from a set of 150 subjects, captured with an optical sensor, and on 1132 images from a set of 86 subjects. To obtain a virtual bimodal database, 86 subjects of the fingerprint subset were randomly paired with the 86 subjects of the face subset. At a FAR of 0.01%, the monomodal systems obtained a FRR of 61.2% and 10.6% for face and fingerprint respectively. For the same FRR, the fusion approach obtained a FRR of 6.6%.

In [27], a bimodal approach for face and speech recognition was proposed, with a fusion method at the decision level by using Bayesian statistics. This fusion method takes into account the estimated biases of individual expert opinions, in order to obtain a single decision from the bimodal system. This single decision approach reached a success rate of 99.5%.

In [46], a bimodal approach for a pixel level-based face recognition and a VQ-based text-independent speaker recognition system was proposed with a fusion method at the matching score level by using a weighted geometric average after a normalisation step. The bimodal approach obtained a correct identification rate of 98%, while the monomodal approaches obtained a correct identification rate of 88% and 91% for the voice and the face based systems respectively.

10.2.3 Single biometric, multiple matchers, units and/or representations

In [297], a monomodal approach was proposed for minutiae-based fingerprint recognition, with a combination method at the features level. The experiments were conducted on two fingerprints of 100 subjects, each finger acquired two times. After the extraction process, the minutiae points of both fingers were overlayed, regarding their center of masses. For the matching process, two fingerprints of a same person are compared to the combined templates. The corresponding points between the first fingerprint and the template are removed and the remaining points are compared to the second fingerprint. The match is accepted if the ratio ot the matched points between this second fingerprint and the remaining minutiae is above a certain threshold. The FAR was about 1.8% and the EER was about 1.9%. The authors have also demonstrated that a single fingerprint was not sufficient to regain the combined template in the template database, as the identification rate at top-5 ranking was about 39%.

In [168], a monomodal approach was proposed for a PCA-based, an ICA-based and LDA-based face recognition systems with a fusion method at the matching score level by using a sum-rule and a RBF Network-based strategies. The experiments were conducted on 2060 face images, collected from a set of 206 subjects derived partially from public available face databases, such as ORL, Yale, AR. The recognition accuracy of the combined approaches was significantly higher, 90.0% and 90.2% for the sum-rule and the RBF-based respectively, than those of the single classifiers, 79.1%, 88.1% an 81.0% for the PCA-based, ICA-based and LDA-based respectively.

In [221], the authors proposed the combination at the decision level using the confidence level of each classifier, of 4 different fingerprint matching algorithms, 3 minutiae-based (Hough transform, string distance and 2D dynamic based) and 1 ridge features-based (filterbank-based). The experiments were conducted on 167 subjects, for which 2 impressions of 4 different fingers were acquired two times (after an interval of six weeks) by an optical sensor. The experiments showed that the combination of all the matchers improved the performance more than 3%, without increasing the *time to match*. When such an approach is used, the authors also proposed to apply a classifier selection scheme, the class separation statistic, before the decision combination, in order to reject matchers which give no performance improvement after combination. Some other experiments showed also that the combination of multiple representations or multiple units of a same modality also improve the performance of such a system.

In [143], the authors proposed the combination, at the score level with logistic transform, of 3 different fingerprint minutiae-based matching algorithms (Hough transform, string distance and 2D dynamic based). The experiments were conducted on 167 subjects, for which 2 impressions of 4 different fingers were acquired two times (after an interval of six weeks) by an optical sensor. The experiments performed the combination of all three different pairwise algorithms. With one matcher, the performance improvement is not significant,

while when the two other algorithms are combined, a significant performance improvement was noticed.

Chapter 11

Integration to identity documents

This section first describes technical requirements of the International Civil Aviation Organization (ICAO) and the National Institute of Standards and Technology (NIST), following by some Regulations and Proposals of the European Council, as these recommendations will be followed by the Swiss government in its choice of biometric solutions for Swiss identity documents. Finally, the main projects of biometric identity documents in some European countries will be presented, as Switzerland, France, Belgium, Italy, Spain, the Netherlands, Great-Britain, Germany and the United States of America [67].

11.1 ICAO technical specifications

The recommendations about the deployment of biometrics in machine readable travel documents of the ICAO were presented previously in Section 3.5, while the most important technical components of such a deployment will be presented below [125]:

- Inclusion of a contactless IC ISO compliant chip, readable up to 10 cm. This chip should possess an ISO compliant operating system, a high speed of data retrieval, a high storage capacity.

- Encryption and protection of the data according to the ICAO's *PKI technical report* [157] [1].

- Indication about the positioning of the storage medium (on the data page, in the centre of booklet, between front-end paper and front cover or between rear-end paper and rear cover) and the standardized organization of the data stored on the chip, according to the ICAO's *PKI technical report* [157] and *LDS technical report* [126] [2].

[1] Section 2.8.1 presents more information about the PKI technical report.

[2] Sections 2.8 and 2.7.2 present more information about the ICAO's PKI and LDS technical reports.

- Modification of the durability of the contactless IC chip (from 10 to 5 years) [129] [3].

11.2 NIST recommendations

In a joint report to U.S. Congress from National Institute of Standards and Technology (NIST), the Department of Justice and the Department of State, some recommendations were proposed after evaluations of the accuracy of both face and fingerprint modalities for the U.S. border checking [201]. This report, usually referred to as the "303A Report", has the following recommendations:

- For the verification process, a bi-modal approach, with two fingerprints and face, is needed for achieving the required accuracy for the border control. Each biometric image, of 10kB or less, should be stored on a chip of 32kB capacity [4]. These two modalities are the only biometric modalities which have studied by NIST for accuracy certification.
- For the identification process, the use of ten plain image impressions to perform the background check is recommended.

In the Appendix A of this report [200], the NIST specifies some additional requirements:

- For certifying the accuracy of any biometric, large-scale databases are needed. The evaluations can only be conducted on databases of at least 100'000 subjects, in order to properly determine the performances of biometric recognition systems.
- The enrollment images, as well as the images acquired during the verification / identification process should have similar quality standards, and thus international standards, as ANSI, WSQ and JPEG standards, have to be used for a large interoperability between systems.
- The storage medium should be adequally protected with a Public Key Infrastructure (PKI), in order to authenticate that the travel document was provided from a legitimate source, to ensure that the data has not been altered or modified since the issuance, and to protect the data's privacy.

11.3 European Community - European Council, legal specifications

Since 2003, six proposals and decisions, concerning the use of biometric information in travel documents at European level, were submitted or adopted to the European Commission and Council [147] [5].

[3] Section 2.7.2 presents more information about the Annex I of the ICAO's MRTD report.

[4] In a later report, the NIST recommended rather the use of face recognition "only for cases where fingerprints of adequate quality cannot be obtained" [285].

[5] The report of the Joint Research Center is available online at `ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf`.

In September 2003, the *Proposal for a Council Regulation amending Regulations (EC) 1683/95 laying down a uniform format for visas and (EC) 1030/02 laying down a uniform format for residence permits for third-country nationals* [88] [6], proposed to move forward the implementation date for photograph (2005 instead of 2007) and to integrate biometric information in the visa and residence permits. Furthermore, this proposal specified that a robust security level can only be achieved by the use of a minimum of two modalites. The modalities chosen for this purpose are: a facial image designed as the primary biometric identifier and a fingerprint image designed as the secondary biometric identifier, which is more able to work with large databases. These biometric identifiers will only be used for verification purposes, and in no case searches will be performed in the Visa Information System database.

In June 2004, the *Council Decision No 2004/512/EC establishing the Visa Information System (VIS)* [7], decided to establish a common identification system for visa data, in order to exchange these data between Member States [74]. A centralised architecture, the Central Visa Information System (CS-VIS) and an interface in each Member State, the National Interface (NI-VIS), should be developed by the Commission, respectively by the Member States.

In December 2004, the *Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States* [8] specifies the minimum security standards required for biometric Identity Documents, accordingly to the ICAO requirements, in order to have a harmonisation at an European level [75]. The use of biometrics shall establish a more reliable link than previously between the genuine holder and the document. The medium storage of the identity document shall contain a facial image [9] and fingerprints [10]. These data shall be secured and the medium storage "shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data". This regulation requires that additional technical specifications, on security features for enhancing anti-forgery, counterfeiting and anti-falsification standards, on the storage medium and on requirements for the biometric format, shall be established. The personal data stored on the identity documents can be available by the concerned person, who has a rectification or erasure right. This regulation specifies also that the biometric information stored shall only be used for verifying the authenticity of the document and the identity of the holder.

In December 2004, the *Proposal for a Regulation of the European parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas* [89] [11] has for main objective to define the purpose, the functionalities and responsabilities for the implementation of the VIS.

In February 2005, the *Council Regulation No C(2005)409 on standards for*

[6] Available at `http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0558en01.pdf`.

[7] The Council Decision No 2004/512/EC is available online at `http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_213/l_21320040615en00050007.pdf`.

[8] Council Regulation No 2252/2004 available online at `http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf`.

[9] At the latest 18 months after the adoption of the requirements of this regulation (end of August 2006 at the latest).

[10] At the latest 36 months after the adoption by the European Union of additional requirements concerning fingerprints.

[11] `http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004PC0835:EN:HTML`.

security features and biometrics in passports and travel documents issued by Member States [12] presented technical specifications which are not yet described in the *Council Regulation No 2252/2004* [68]. This regulation is based on international standards such as the ISO's and ICAO's requirements and presents the specifications for the biometric information used in travel documents, the storage medium, the logical data structure on the chip, the security specifications of the data stored on the chip, the conformity assessment of chip and applications and the RF compatibility with other travel documents.

Recently, the European Commission has officially asked the United States Congress to accept another extension of the deadline for introducing biometric information in all European travel documents until August 2006, instead of October 2005, as only six European Countries will satisfy the US requirements at the initial deadline [13]. This request was finally accepted by the United States [14] and thus the EU members have until September 2006 to fulfill the US requirements for biometric passports. Indeed, the USA require that the biometric passports of each state should be submitted by the beginning of September 2006, in order to be validated by the end of October 2006. In addition, the USA require that lost and stolen passports have to be reported by the issuance state to the US Department of Homeland Security (DHS) and to the Interpol, that intercepted lost and stolen passports have to be reported to the DHS's Fraudulent Document Analysis Unit, and that the trends and analysis of these lost and stolen passports, as well as the other security features of the travel documents, have to be shared with the DHS.

The actual Presidency of the European Union, the United Kingdom, has invited the Council, the European Commission and the Member States to "draft common security standards for national identity cards taking into account the achievements in relation to the EU passport and the ICAO framework" [224]. Some further discussions should be started about the security of enrollment and issuing processes, digital signatures and anti-fraud measures.

Finally, in November 2005, the *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offenses and of other serious criminal offenses* has for main objectives "to allow for and to lay down the conditions under which Member States authorities responsible for internal security and the European Police Office (Europol) may access the Visa Information System (VIS)" for the purpose of "prevention, detection and investigation of terrorist offences" and other type of crime and offenses for which Europol are competent [90] [15]. The European Data Protection Supervisor has put forward an opinion about this proposal [123] [16], and proposes some improvements which ca be made for example about the VIS accessibility conditions, the level of data protection and the supervision that should be ensured.

[12] Commission decision No C(2005)409 available online in French at `http://europa.eu.int/comm/justice_home/doc_centre/freetravel/documents/doc/c_2005_409_fr.pdf`.

[13] Press release available online at `http://europa.eu.int/idabc/en/document/4068/194`.

[14] Press release available online at `http://europa.eu.int/idabc/en/document/4380`.

[15] Proposal available online at `http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0600en01.pdf`.

[16] Opinion available online at `http://www.edps.eu.int/12_en_opinions.htm`.

11.4 Biometric identity documents projects

As mentioned in [153], 11 Visa Waiver Program countries (out of 27) have introduced a biometric passport before the end of 2005, while 8 VWP countries have extended their deadline introduction to the end of 2006. For the remaining VWP countries, the introduction date of their biometric identity document is not decided yet.

11.4.1 Switzerland

The introduction of biometric information in Swiss identity documents will follow the ICAO Doc 9303 [124] and the European regulations (Section 11.3 presents more information about the Council Regulations and Proposals). Currently, the Swiss prescription and law on identity documents [69, 70] will be modified [17] in order to allow the introduction of biometric information in Swiss identity documents, at first as a pilot project of a duration of 5 years, and then in a permanent way. During this pilot project, a limited number of biometric passports will be issued on a voluntary base, in parallel with the current machine-readable passport (2003 model) from September 2006. The current Swiss passport contains the following informations: the name, the first name, the date of birth, place of origin, nationality, the height, the signature, the photography, the information concerning the prefecture which has issued the card, the issuance and expiration date and the card number. The new biometric passport will contain on a chip, besides all the information already present on the current passport, the facial image in a digital form. The biometric information will be stored on the chip and in the information system relative to the Swiss identitiy document called *ISA*, which is the database containing already the personal information present on the current passport since 2003. This database allows the correct management of Swiss identity documents, avoids the issuance of several identity document for the same person, prevents any abuses and verifies the person's identities and the authenticity of the documents. The biometric data on the chip will be authenticated and protected with a electronical signature, while the data contained in the *ISA* will be secured with protection means proper to the information system. As specified in the Swiss prescription and law on identity documents [69, 70], restrictives measures are applied to the access to the data contained in the ISA. Indeed, these data are only accessible to authorized people, and can not be used for any police investigation. This new identity document will be valid during 5 years and will cost 250 CHF. For the pilot project, enrollment centers will be put in place in eight Swiss Cantons (AG, BE, BS, GR, SG, TI, ZH and VD) and in eight Swiss representations outward (Paris, Francfort, London, Mexiko, Toronto, Sao Paulo, Hong Kong and Sydney). The budget assigned to this five year pilot project is estimated of about 14 millions CHF.

The Swiss Federal Department of Justice and Police is also investigating in the purpose of a digital identity card. The electronic signature and certificate present on the chip will be used for the access to public and private authentication processes and for signing electronically authentic documents. The current

[17] The draft versions of the Swiss prescription and law on identity documents are available at `http://www.schweizerpass.admin.ch`.

Swiss identity card has a format of a credit card and contains the same information as the Swiss passport [18].

11.4.2 France

The *INES* program [19] has for main objectives to enhance the security of the French issuance process, to improve the management of identity documents, to issue highly secure documents, and to allow citizens to authenticate on the Internet. The new Identity Card called *CNIE* [20] will have a format of a credit card and will include a contactless chip. The informations printed on the card are as follows: the name, the first name, the date and place of birth, the gender, the address, the signature, the information concerning the prefecture which has issued the card, and the card number. The information contained on the contactless chip will be subdivided in five distinctive blocks. The *Identity block*, which will only be accessible to authorized people and will be secured with cryptographic approaches, will include the biometric information, as the photography and two fingerprints, and all the information present on the card. The *Card authentication block* will allow an automatic and anonymous authentication of the card itself. The *Certified identification block*, secured with a PIN code, will allow the access to public and private authentication processes. The *Electronic signature block* will allow, by mean of a PIN code, to sign electronically authentic documents. The *Personal "portfolio" block* will allow people to store complementary personal information. Each person in possession of such a card will receive a document with all the information included in the card, and will have a rectification right. The access to the biometric information by authorized people will be contactless and its traceability guaranteed, while the other functionalities will be used with contact. This new identity document will be valid during 5 years. Before its introduction, the French government has mandated the *Internet Rights Forum* [21] for an online debate, as well as public debates in several regions, about this new identity card. The summary and the conclusion about this latter was recently submitted to the French Home Secretary and made publicly available [97] [22]. This debate has produced interesting results. While three-fourths of the population support the introduction of a new identity card for security reasons, some fears and reluctances appeared. The main recommendations of this organisation are as follows:

- A rigorous study has to be conducted in order to evaluate the real extent of the identity fraud in France.
- The new identity card should not be introduced at the same time as the new biometric passport.
- The citizens should have a free and permanent online access to their administrative folders and to the state of progress of their administrative procedures.

[18] Complete description of the Swiss identity card available on the Swiss Federal Office of Police's homepage at `http://www.schweizerpass.admin.ch`.

[19] Complete description of the French INES program available at `http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050201.pdf`.

[20] *CNIE*: Carte Nationale d'Identité Electronique.

[21] *Internet Rights Forum*'s homepage at `http://www.foruminternet.org`.

[22] This report is available on the *Internet Rights Forum*'s homepage.

- A coherence between the unique and centralised identification used with the INES project and the plurality of the identifiers used currently in the electronic administration.
- A global and permanent control of the system should be conducted by the CNIL.
- The use of contactless chip should only be admitted when studies demonstrate that no covert access to the data will be possible.
- The CNIE should only be introduced when the computerization of the registry office is achieved.
- An explanation campaign should be conducted in order to inform people about the use of the CNIE in administrative e-procedures.
- The CNIE should be costless for the first issuance, but payable in the case of loss and renewal.
- The mandatory nature of the CNIE should be evaluated with care, as it will be a considerable modification.
- The issuance in municipalities should first be debated with regional politicians.
- Some harmonisation works about norms, standards and interoperability should be conducted with other countries.

After the publication of these recommendations, the French Government would have decided to move back to 2008 the introduction of the CNIE, in order to focus their efforts on the development of the new biometric passports and to eliminate the mandatory nature of the CNIE in the INES project.

The French biometric passport, fulfilling the ICAO Doc 9303 [124] and the European regulations, will be issued in autumn, 2006. The chip will contain, besides all the information already present on the current passport, at first a digital photography and then fingerprints. The CNIL has given its approval about the introduction of such identity documents [23].

11.4.3 Belgium

The *eID* [24], the new electronic identity card, is introduced since 2003. Until the 31th of December 2009, all non-electronic identity cards will be replaced. This new card has a format of a credit card and includes a chip, readable by contact, but containing no biometric information. The information printed on the card are as follows: the photography, the name, the first name, the gender, the signature, the date and place of birth, the nationality, the national identification number, and the issuance and expiration date. All these information are contained in the chip (except the photography), as well as the address of the subject. The electronic signature and certificate present on the chip can be used for the access to public and private authentication processes. As a centralized database of the national population already exists, the same framework is used

[23] CNIL's approval available at `http://www.cnil.fr/index.php?id=1773`.

[24] Complete description of the new Belgian electronic identity card program available at `http://eid.belgium.be/fr/navigation/12000/index.html`.

with this new identity card. Every people has an access and modification right of all the information included in the card and also an access to the people who has consulted it, and for which reason. The consent of the concerned person will be necessary for accessing the information present on the card. This new identity document is valid during 5 years.

The new Belgian biometric passport [25] will follow the ICAO Doc 9303 [124] and the European regulations (see also Section 4.1 for more information about the Council Regulations and Proposals). This new passport, with a contactless readable chip, is issued since November 2004. The information contained on page 2 of the document are also contained on the chip: the name, the first name, the nationality, the gender, the date and place of birth, the issuance and expiration date and the signature and photography. The fingerprints will be introduced later. This new identity document is valid during 5 years.

11.4.4 Italy

The new Italian identity smart card [26] use two kinds of technology, a chip with a capacity of 34kB, and a laser readable band. The information stored on the chip will only be used for the access to public authentication and identification processes, by means of symmetric and asymmetric keys, for electronic signature purposes, and for online voting. The laser band will be used as an identity card. The information printed on the card are as follows: the photography, the name, the first name, the gender, the height, the nationality, the date and place of birth, the identification number, the address and the validity period of the card. While the laser band will contain the personal information, the chip will contain a digitized signature and a fingerprint. All these informations will only be stored on the card, and not in a centralized database. The access to the information contained on this card will only be possible with consent of the concerned person. This new identity document will be valid during 5 years.

11.4.5 Spain

The new Spanish identity card contains the same data as the old one. The informations printed on the card are as follows: the name, the first name, a colour photography, the signature, the identification number, the issuance date and the validity period. The readable part contains the gender, the residence place, the date and place of birth, the name of his/her parents and the information concerning the administrative service which has issued the card. The chip will include, in addition to all these informations, an electronic attestation of authentication, a certificate for electronic signature, biometric information (a fingerprint and the photography), the digitized signature. An asymmetric cryptographic approach will be used to enhance the security of the identity card, a public key known by the police and the private key stored on the chip, activated by a PIN code. This new identity document will have an estimated life time of 10 years.

[25] Complete description of the new Belgian biometric passport available at `http://www.diplomatie.be/fr/travel/passports.asp`.

[26] Complete description of the Italian Identity Card available at `http://www.cartaidentita.it`.

11.4.6 Netherlands

A biometric passport has being tested on a six-month period in the Netherlands since August 2004, until the end of February 2005. [17, 19, 20, 18] [27]. This pilot test, named "2b or not 2b" and conducted by the Dutch Ministry of the Interior and Kingdom Relations, evaluated the impact of the new generation of Dutch passports and identity cards, in the request process, the biometric acquisition process and in its day-to-day use. 14'700 volunteers, from 6 different municipalities have taken part in this pilot evaluation. The chip contains amongst other things a photography and two fingerprints. During the issuance process of this pilot project, additional information about physical characteristics which can influence the biometric recognition process, such as beard, glasses, dark skin, hobby or jobs that can damage the fingerprints, are also collected. This pilot project acquired these two modalities and will store them in the biometric passport and in a "test document", which was in possession of the authorities. This latter was only used for the performance evaluation of the biometric technologies and the quality evaluation of the biometric information, in a anonymous way, and was destroyed at the end of the evaluation. When the biometric passport is delivered to the bearer, a verification procedure (identical to a border checking control) is completed in order to determine if the biometric data recorded on the chip corresponds to the data acquired during this process. The first results of this large-scale evaluation will be presented later. This new identity document will have a validity period of 5 years.

11.4.7 Great-Britain

Since the beginning of 2005, UK has adopted the *Identity Cards Bill* [28], which has for main objective to introduce a national identity card [271]. The Bill is composed of eight components. The *National Identification Register*, a centralised register, which will contain information from all UK residents aged over 16. The *National Identity Registration Number* will give a unique number for every individual. The *biometric information*, such as face, fingerprint and iris, which have to be collected for every individual. The *Identity Card* will be generated from this register and contain a chip, protecte by cryptographic methods. The informations printed on the card are the photography, the name, the address, the gender, the date of birth and the identification number. The information stored on the chip are the name, the first name, the date and place of birth, the photography of the face (and the shoulders), the fingerprints, the irises, the digitalized signature, residence places, the nationality, the national identity register number, and all other information that the concerned person will store on it. *Legal obligations* will require this identity card for obtaining some public services and *administrative convergence* will allow the centralization of all registration numbers used by a single person. *Cross notification* will allow all agencies to reach the data of a person, without its consent, through the Secretary of State. *New crimes and penalties* will be established, in order to comply with the requirements of the program. The *National Identity Scheme*

[27] The promotion document of the "2b or not 2b" project, as well as the Biometrie In-Zicht journal, are available online at `www.bprbzk.nl`.

[28] The UK Identity Cards Bill and the explanatory notes to the Bill are available online at `http://www.publications.parliament.uk/pa/cm200405/cmbills/008/2005008.htm`.

Commissioner will have for objective the supervision of this program. As previously mentioned, the access to the information contained on this card will only be possible with consent of the concerned person. However, these information will be available for some public authorities, under some conditions and rules.

The choice of the UK Government is questioned by a recent report of the London School of Economics & Political Science [265][29]. For the Advisory Group and the Research Group (38 persons in all), authors of this report, the Identity Cards Bill proposals are "too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence" and "do not represent the most appropriate, secure, cost effective or practical identity system for the United Kingdom". Indeed, other methods, more appropriate for the purpose, should be used to achieve the main objectives of the Bill. The technology which is planned to be used at large scale is "untested and unreliable". Furthermore, the costs of such an identity system has been underestimated by the UK government, and the legal framework proposed will create conflicts with national and international laws. Add another oversight body in the UK will increase the complexity and inefficiency of the the current oversight process. The LSE report concludes also that the Government has "failed to correctly interpret international standards, generating unnecessary costs, using untested technologies and going well beyond the measures adopted in any other country that seeks to meet international obligations".

An enrollment trial was performed by the UK Passport Service from April to December 2004, with more than 10'000 persons [270]. The main goals of this trial was to "test the processes and record customer experience and attitude during the recording and verification of facial, iris and fingerprint biometrics". The enrollment procedure had not taken place in laboratory conditions, but in six fixed and one mobile enrollment centers, placed in the United Kingdom. A booth was specially designed for the enrollment procedure of this trial. During the enrollment, the subjects were placed on a standard office chair within the booth, with an operator outside the booth which has a visual contact. The trial had the following stages: registration, photograph participant (head and shoulders), record facial biometric, record iris biometric, record fingerprint biometric, record electronic signature, print card, post-enrollment questionnaire, verification and post-verification questionnaire. The subjects were separated in three groups: the *quota sample* with 2'000 subjects (representative to the UK population), the *opportunistic sample* with 7'266 subjects (recruited from the area around the enrollment centers, without any other criteria) and the *disabled participant sample* with 750 subjects. The enrollment times for all three biometrics was about 8 minutes for the quota sample and about 10 minutes for the disabled participants. The verification times for the quota sample were 39 seconds, 58 seconds and 1 minute 13 seconds for facial, iris and respectively fingerprint verification. The verification times for the disabled participants were 1 minute 3 seconds, 1 minute 18 seconds and 1 minute 20 seconds for facial, iris and respectively fingerprint verification. For all three biometrics, the enrollment success rates were higher for the quota sample than the disabled participants: nearly 100% and 98% for face, 90% and 61% for iris and nearly 100% and 96% for fingerprint. The verification success rates were also higher for the quota sample

[29]The Interim Report of the LSE is available online at `http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf`.

than the disabled participants: nearly 69% and 48% for face, 96% and 91% for iris and nearly 81% and 80% for fingerprint. Whilst the participant experience of positioning for the iris modality was considered as more or less difficult, the participants have yet chosen this modality as their preferred. Furthermore, the majority of participants concidered that the use of biometric data in identity documents will increase the passport security, prevent the identity fraud and illegal immigration, and will not be an infringement of their liberties. Whilst a majority of the participants are not very or not at all concerned before the enrollment trial about having their biometrics recorded, the number of those who were very concerned about it before decreased after enrollment. The main recommendations of this report are as follows:

- The camera should be maneuverable enough in the enrollment booth.
- Any headwear may be removed by applicants, or arranged so that the face or forehead is not obscured.
- Considerations should be given when a biometric modality is not available on a temporary basis.
- Trained operators should be specially present when disabled persons are enrolled.
- Further investigations should be performed with persons who had enrollment difficulties, without being disabled.
- The enrollment of the fingerprint modality should be successful, even if some fingers do not satisfy some quality measurements.
- If the first verification procedure fails, some further attempts should be allowed.
- The use of fingerprint sensors with a large acquisition area should be preferred, in order to acquire sufficient information.
- The biometric devices used for UK passports should be chosen on the basis of a test ring.
- Some education initiatives have to be conducted, on the basis of the results from the customer experience and attitude questions obtained during the trial.

Since the beginning of this year, Great-Britain is delivering the Biometric British Passport which will contain the holder's facial image on a chip [30]. According to the UK Passport Service, the biometric information will be used to link a person to a passport in order to help the detection of counterfeit or manipulated documents and to confirm the identity of the individual.

[30] Complete description of the Biometric British Passport at `http://www.passport.gov.uk/general_biometrics.asp`.

11.4.8 Germany

All new German biometric passport (the *ePass*) will include from November 2005 a contactless readable RF-chip and a digital photography stored on it. The *ePass* [31] issued from the beginning of 2007 will also include two fingerprints. The access to the information contained on the card will only be possible after a previous optical lecture of the machine readable zone and a cryptographical protocol between the reader and the identity document. The biometric information will only be stored on the chip. Indeed, no centralised biometric database will be created for the new passport. This identity document will be used for authentication purposes and will allow signing electronically authentic documents. The new German biometric identity document will follow the ICAO and European Union requirements.

Furthermore, some studies have already been conducted by the "Bundesamt fuer Sicherheit in der Informationstechnik" for evaluating facial recognition technologies, such as BioFace 1 & 2 and BioP I (see Section 5.3) and fingerprint recognition technologies such as BioFinger 1 (see Section 6.3) for Identity Document purposes. Another study, based on BioP, has been conducted on a larger population set and with additional biometric modalities (fingerprint and iris) in order to evaluate more in details the influence and the feasibility of the introduction of biometric information in travel documents [49] [32]. This evaluation was conducted during four month on 2000 subjects. The biometric systems used were: two fingerprint verification systems, one face recognition verification system and one iris recognition verification system. Biometric images (as specified in the ICAO specifications) and biometric templates were used separately in order to compare these two approaches. The main results of this evaluation can be summarized as follows. First, the performances of each system were dependent on the frequency of use of the subjects, particularly for the iris recognition system (false rejection rates for the iris system have reached in this evaluation about 20% with low frequency users). Then, the use of biometric template for the reference data performs better than the biometric images. Finally, this evaluation proposed a ranking of the three modalities, accordingly to the results obtained in these tests: fingerprint, face and iris.

The BioPII results, especially those about the iris modality, was questioned by Prof. John Daugman after this modality ranking and the high FRR and FAR for iris recognition reported by this evaluation [81]. So, all the comparisons with the iris data will be computed again with the algorithm of Prof. Daugman.

11.4.9 United States of America

The Biometric U.S. passports, which will follow the ICAO requirements, will include on the chip a digital image of the face and the biographic information printed on the data page, such as the name, the date and place of birth, the passport number, the dates of issuance and expiration, the issuing authority, the document type, the passport application reference number and a unique chip

[31] Complete description of the new German electronic identity document *ePass* available on the `http://www.bmi.bund.de/` server and at `http://www.bsi.bund.de/fachthem/epass/index.htm`.

[32] The BioP II evaluation is available online at `http://www.bsi.bund.de/literat/index.htm`.

identification number [82] [33]. All the information contained on the chip will be digitally signed (but not encrypted), in order to protect their integrity, as well as that of the identity document. The contactless chip will have a memory of 64 kB of EEPROM storage and will be written only once, without that a modification can me made. This identity document will be valid during 5 years for persons under 16 years old and 10 years for other persons and will be first issued in mid-2005.

11.4.10 International Labour Organisation (ILO)

The Seafarers' Identity Documents Convention No 185 (2003) [34] was adopted by the ILO for introducing security elements in their identity cards, which are conform in all respects to the ICAO and ISO specifications and requirements [132]. The information include on the card will not be stored on a chip, but printed directly on the card. These information shall be restricted to the full name, the gender, the date and place of birth, the nationality, physical characteristics, a digital photography, the signature, and two fingerprint templates. These latter, non-reversible minutia-based templates, will be visible on the document and printed as numbers in a bar code, which will contain up to 686 Bytes of data. Up to 52 minutiae features per finger will be extracted and stored in the barcode. The verification procedure will be completed in a serial mode: if the first finger is unavailable, failed to acquired or does not match with the corresponding template, the second finger is

[33] The proposed rule of the Department of State is available online at `http://www.access.gpo.gov/su_docs/fedreg/a050218c.html`.

[34] Complete version of the ILO Convention 185 available online at `http://www.ilo.org/ilolex/cgi-lex/convde.pl?C185`.

Chapter 12

Summary and future work

In this chapter, despite Wayman's pronouncement [280]:

> *"It is impossible to state that a single biometrics is better than the others for any applications, populations, technologies, and administration policies ",*

we summarise the state-of-the-art and make recommendations concerning the introduction of biometrics in Swiss identity documents.

12.1 Usage of biometrics

The Swiss public, parliaments and government will need to debate about the use of biometric identity documents they would like allow/implement. Should a biometric identification system be put in place, incorporating a centralised database and a potentially a watchlist, or should it be a verification system to confirm the identity of the identity holder, which is the primary objective of identity documents.

The locations of biometric identification or verification points should be discussed.

Additionally, the enrollment and issuance processes for different identity documents may need to be revised to avoid problems with source documents.

12.2 Performance

The Swiss public, parliaments and government will need to debate about performance requirements for a biometric identity documents scheme. This choice will dictate in large part the choice of a given modality and the technical requirements of the system.

We should point out that some modalities can be expected to achieve close to (but not exactly) 0% false accept rate on large populations, with 2% to 8% false reject (iris), while other modalities can provide about 5% false reject with a false accept rate of 0.01% on much smaller populations (fingerprint). However, if every Swiss citizen is enrolled in the system, the population size jumps to more than 7 millions, and even small error rates on paper can become significant.

In any case, what should be taken into account is that no biometric modality will give 0% error for both false accepts and false rejects. Furthermore, for all modalities presented in this report some users will be non-enrollable, and thus a non-biometric option of identity verification should be provided (as in current secure passports).

Some modalities such as face and speech are very sensitive to changes in acquisition conditions and thus their use in a large-scale system for identity documents seems difficult at best, as noted in many medium-scale evaluation campaigns.

12.3 Systems architecture and information security

For this section and this report in general, we should emphasize that we assume a secure issuance process is in place, as is in principle the case today. That is, we do not deal with issuance issues such as fake source documents (birth certificates and others) and we suppose clerical staff are skilled in establishing the authenticity of the latter.

Also, it should be noted that some of our recommendations may be at odds with the ICAO standard on some points (notably storage medium for biometric data).

As much of the processing steps as possible should take place in a distributed fashion, that is within one smartcard or PC host, without resorting to a centralised storage where information would need to travel over networks. This is mainly because a centralised database containing biometric templates of citizens can lead to compromise through technical or other means, in turn entailing private data loss and identity theft problems.

For several security reasons, the *match on card* approach is preferred to a simple *template on card* system: The identity document holder does not need to trust the computer and network to which the card is connected, or the human operator. Cracking or *trojanization* of the matching terminal is not an issue, as the template never leaves the secure identity document.

Table 2.7.3 summarises the options available for locations of the processing steps. Based on this table, the above, and typical performances, two modalities can be recommended: fingerprint or iris, together with a sensor-on-card approach for fingerprint. Also, we recommend that only templates should be stored on the smartcard, not raw data.

12.4 Privacy and public perception

As part of the feasibility study and before deployment, a full privacy impact assessment should be carried out, under the leadership of the federal data protection commissioner.

Standard privacy guidelines (access rights, consent, ...) can be used as a starting point, and augmented with the guidelines exposed in Section 4.3. An important issue to address is whether biometrics in identity documents should serve for verification, or their scope be extended to incorporate identification with a central database. The proportionality rule can be applied in this case.

Where a user is non-enrollable (for instance, it is estimated that about 4% of any population does not possess suitable fingerprints), he/she should not become subject to more intensive scrutiny (failure of the system comes through no fault of their own).

12.5 Choice of modality

Here, we summarise the state of the art in the different modalities presented so far, according to the following criteria: error rates, inter-session variability, universality, noise sensitivity, architectural features such as feasibility of distributed template storage, sensor cost, choice of vendors, pre-existing smartcard match-on-card implementations, susceptibility to covert acquisition. We roughly classify each attribute into low (L), medium (M), or high (H) and present the results in Table 12.1 to the best of our knowledge.

It should be strongly emphasised that, at least in terms of biometric performance metrics such as error rates or inter-session variability, these results are comparing evaluations made using very different populations and protocols. Therefore, Table 12.1 and the following ranking are at best broad approximations and will need to be confirmed through rigorous experiments using a controlled population and corresponding protocols.

Criterion	**2D face**	**FP**	**Iris**	**Sig.**	**Sp.**
error rates	M-H	L	very L	L	M-H
inter-session var.	M	L	very L	M	M-H
universality	H	H	H	M-H	M-H
risk of FTE	L	M-L	L	L	L
noise sensitivity	H	M-L	M-L	L	H
TTE	L	L	L	M	M
distributed templates	H	H	H	H	H
sensor cost	M-L	L	H	M	L
choice of vendors	H	H	very L	M	H
MOC implementation	L	H	L	none	none
covert acquisition risk	H	M-H	L	M-L	H

Table 12.1: Broad summary of modalities according to several criteria.

Taking into account the biometric identity document application, we propose the following ranking based on the literature survey for this state-of-the-art. All the criteria presented in Table 12.1 were used to establish this ranking.

1. Fingerprints offer the advantage of low error rates, small inter-session variability, low noise sensitivity (assuming residual fingerprints are removed every few users), fast enrollment, a wide choice of vendors, low-cost sensors (less than CHF 100), numerous match-on card and/or sensor-on-card implementations, difficulty of covert acquisition and corresponding reduction in "identity theft" probability.

2. Irises offer very low false accept rates for large size populations with reasonable false rejection rates (which is the main advantage of this modality), fast enrollment, small inter-session variability, and difficulty of covert

acquisition. Unfortunately, currently the monopoly of iris recognition systems is holded principally by one major vendor [1], but several commercial vendors for iris cameras can be found on the market. Furthermore, the sensors and recognition systems are very expensive (about USD 5000 for the camera and more for the recognition system). Failure to Enroll rate may also be an issue.

3. Signatures have been shown to have relatively low error rates on populations size in the low hundreds. It suffers mainly from inter-session variability, but is immune to environmental noise. An advantage is that it is the only truly "revocable" modality: a signature can be changed if compromised. Different vendors propose signature verification algorithms, and low-cost sensors can be obtained in volume. Covert acquisition is a moderate risk as the user must explicitly sign for her signature to be acquired (but could be tricked into doing so by social engineering).

4. The 2D face modality suffers from environmental noise and inter-session time effects, but in controlled/laboratory conditions error rates can be quite low. A large array of vendor solutions are on the market and the technology is maturing rapidly. Sensors vary largely in cost according to image quality specification. It is very prone to covert acquisition. 3D face modality was not taken into account because of the relative immaturity of the technology.

5. Speech is affected by noise and speaker verification performance drops significantly with channel or environmental noise. Another problem is the long enrollment and verification time, as with current algorithms a user would be required to speak for about 10-15 seconds for the verification to happen. Inter-session variability and easy covert acquisition seem to make this modality a poor choice for identity documents.

12.6 Multimodality for identity documents

For the identity documents application, multimodality may be an effective tool to reduce the FTE rate. The sequential use of multiple modalities guarantees that the non-enrollable population is reduced drastically. Furthermore, sequential use of modalities permits fair treatment of persons that do not possess a certain biometric trait.

We also need to investigate multimodal fusion with partial templates, at the score and decision levels, to provide better privacy protection to the users enrolled, as partial templates by themselves (i.e. not in combination) would yield very low identification power.

12.7 Acquisition and evaluation protocols

An ill-managed introduction of biometrics in identity documents can decrease the security and go against the initial end of such a use. Thus, given the very

[1] This monopoly situation is going to change, as the patents are expected to expire this year and next year.

large target population size (millions of people)) only a wide-ranging test with a strict evaluation protocol on a large number of users will provide us with the confidence needed to deploy a large-scale system.

We need to establish an acquisition and evaluation protocol, drawing from both international competitions, vendor tests, established practices, and our expertise in the field. This will propose application scenarios suitable for identity documents, such as border-crossing and airport registration settings.

We need to collect a large database of more than 100 users for all 5 modalities presented in this report (2D and 3D face, fingerprints, iris, on-line signature speech), so that vendor technologies can be evaluated using strictly the same scenarios and population for all modalities. No such large multi-modal database currently exist.

Bibliography

[1] *Oxford English Dictionary.* Oxford Edition, 2004.

[2] A4 Vision, *Vision Access Technology White Paper.* A4 Vision, 2003.

[3] B. Achermann, X. Jiang, and H. Bunke, "Face recognition using range images," in *Proceedings of the International Conference on Virtual Systems and Multimedia*, 1997, pp. 126–136.

[4] A. Adami, R. Mihaescu, D. Reynolds, and J. Godfrey, "Modeling prosodic dynamics for speaker recognition," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'03)*, vol. 4, 2003, pp. 788–791.

[5] P. Agre, "Your face is not a bar code: arguments against automatic face recognition in public places," *Whole Earth Magazine*, no. 106, pp. 74–77, 2001, also available at http://polaris.gseis.ucla.edu/pagre/bar-code.html.

[6] A. Albrecht, "Privacy best practices in deployment of biometric systems," BIOVISION: Roadmap to Successful Deployments from the User and System Integrator Perspsective, Final report IST-2001-38236, 28th of August 2003.

[7] A. Albrecht, 2005, personal communication.

[8] R. Allen, P. Sankar, and S. Prabhakar, "Fingerprint identification technology," in *Biometric Systems: Technology, Design and Performance Evaluation*, J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds. London: Springer-Verlag, 2005, ch. 2, pp. 21–61.

[9] A. Alterman, ""A piece of yourself": Ethical issues in biometric identification," *Ethics and Information Technology*, vol. 5, pp. 139–150, 2003.

[10] American National Standards Institute, *Information technology - BioAPI Specification (Version 1.1) (formerly ANSI INCITS 358-2002).* New York, USA: American National Standards Institute, 2002.

[11] American National Standards Institute, *Biometric Information Management and Security for the Financial Services Industry: ANSI X9.84-2003.* New York, USA: American National Standards Institute, 2003.

[12] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "A new approach to fake finger detection based on skin distortion," in *Proceedings of International Conference on Biometrics 2006 (ICB)*, D. Zhang and A. Jain, Eds., vol. LNCS 3832, 2005, pp. 221–228.

[13] A. Ariyaeeinia and P. Sivakumaran, "Comparison of VQ and DTW classifiers for speaker verification," in *Proceedings European Conference on Security and Detection (ECOS'97)*, 1997, pp. 142–146.

[14] M. Audétat, A. Rebetez, and Y. Cornu, "Comment on grignote nos libertés," *l'Hebdo*, no. 8/2005, pp. 15–18, 2005.

[15] E. Bailly-Bailliére, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariéthoz, J. Matas, K. Messer, V. Popovici, F. Porée, B. Ruiz, and J.-P. Thiran, "The BANCA database and evaluation protocol," in *Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, J. Kittler and M. Nixon, Eds., vol. LNCS 2688, 2003, pp. 625–638.

[16] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Proceedings of International Conference on Biometrics 2006(ICB)*, D. Zhang and A. Jain, Eds., vol. LNCS 3832, 2005, pp. 265–272.

[17] Basisadministratie Persoonsgegevens en Reisdocumenten, *2b or not 2b: Doe mee aan de praktijkproef biometrie en ontvang 10 euro korting!* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2004.

[18] Basisadministratie Persoonsgegevens en Reisdocumenten, "Biometrie In-Zicht, April 2005 - Extra Editie," *Biometrie In-Zicht*, vol. 1, no. 3, p. 1, 2005.

[19] Basisadministratie Persoonsgegevens en Reisdocumenten, "Biometrie In-Zicht, Januari 2005," *Biometrie In-Zicht*, vol. 1, no. 1, pp. 1–2, 2005.

[20] Basisadministratie Persoonsgegevens en Reisdocumenten, "Biometrie In-Zicht, Maart 2005," *Biometrie In-Zicht*, vol. 1, no. 2, pp. 1–2, 2005.

[21] B. Bauer, "A century of microphones," *Journal of the AES (Audio Engineering Society)*, vol. 35, no. 4, pp. 246–258, April 1987.

[22] L. Berggren, "Iridology: A critical review," *Acta Ophthalmologica*, vol. 63, no. 1, pp. 1–8, 1993.

[23] C. Bergman, "Multi-biometric match-on-card alliance formed," *Biometric Technology Today*, vol. 13, no. 5, p. 6, 2005.

[24] A. Bertillon, *Identification Anthropométrique et Instructions Signalétiques*. Melun: Imprimerie administrative, 1893.

[25] C. Beumier and M. Acheroy, "3D facial surface acquisition by structured light," in *Proceedings of the International Workshop on Synthetic-Natural Hybrid Coding and Three Dimensional Imaging*, 1999, pp. 103–106.

[26] C. Beumier and M. Acheroy, "Automatic 3D face authentication," *Image and Vision Computing*, vol. 18, no. 4, pp. 315–321, 2000.

[27] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multimodal person authentication systems using bayesian statistics," in *Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, vol. LNCS 1206, 1997, pp. 291–300.

[28] F. Bimbot, G. Gravier, J.-F. Bonastre, C. Fredouille, S. Meignier, T. Merlin, I. Magrin-Chagnolleau, J. Ortega-García, D. Petrovska-Delacrétaz, and D. Reynolds, "A tutorial on text-independent speaker verification," *Eurasip Journal on Applied Signal Processing*, vol. 2004, no. 4, pp. 430–451, 2004.

[29] Biometric Technology Today, "Part 1: Biometrics and ePassports," *Biometric Technology Today*, vol. 13, no. 6, pp. 10–11, 2005.

[30] Biometric Technology Today, "Biometric standards - an update," *Biometric Technology Today*, vol. 14, no. 1, pp. 10–11, 2006.

[31] Biometric Technology Today, "Biometric standards - an update," *Biometric Technology Today*, vol. 14, no. 1, pp. 7–9, 2006.

[32] D. Blackburn, M. Bone, and P. Phillips, "Facial recognition vendor test 2000, Evaluation report," February 2001, available online at http://www.frvt.org/.

[33] V. Blanz and T. Vetter, "A morphable model for the synthesis of 3D faces," in *Proceedings of the 26th International Conference on Computer Graphics and Interactive Techniques*, 1999, pp. 187–194.

[34] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. New-York: Springer-Verlag, 2003.

[35] J. Bolling, "A window to your health," *Jacksonville Medicine (special issue on retinal diseases)*, vol. 51, no. 9, 2000.

[36] D. Bolme, R. Beveridge, M. Teixeira, and B. Draper, "The CSU face identification evaluation system: Its purpose, features and structure," in *Proceedings International Conference on Vision Systems 2003*, Graz, Austria, April 2003, pp. 304–311.

[37] J.-F. Bonastre, F. Wils, and S. Meignier, "ALIZE, a free toolkit for speaker recognition," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005)*, Philadelphia, USA, March 2005, pp. 737–740.

[38] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," 2005, draft version, available at http://rfidanalysis.org/.

[39] F. Botti, A. Alexander, and A. Drygajlo, "On compensation of mismatched recording conditions in the bayesian approach for forensic automatic speaker recognition," *Forensic Science International*, vol. 146, no. S1, pp. S101–S106, December 2004.

[40] K. W. Bowyer, "Face recognition technology: Security versus privacy," *IEEE Technology and Society Magazine*, vol. 23, no. 1, pp. 9–20, 2004.

[41] K. W. Bowyer, K. Chang, and P. J. Flynn, "A survey of 3D and multi-modal 3D and 2D face recognition," Departement of Computer Science and Engineering of the University of Notre Dame, Tech. Rep., 2004.

[42] G. Bradski, "Programmer's tool chest: The OpenCV library," *Dr. Dobbs Journal*, Nov. 2000.

[43] J.-J. Brault and R. Plamondon, "Segmenting handwritten signatures at their perceptually important points," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 15, no. 9, pp. 953–957, Sept. 1993.

[44] C. M. Brislawn, J. N. Bradley, R. J. Onyshczak, and T. Hopper, "The FBI compression standard for digitized fingerprint images," in *Proceedings of the SPIE*, vol. 2847, 1996, pp. 344–355.

[45] A. M. Bronstein, M. M. Bronstein, and R. Kimmel, "Expression-invariant 3D face recognition," in *Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, J. Kittler and M. Nixon, Eds., vol. LNCS 2688, 2003, pp. 62–70.

[46] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI)*, vol. 17, no. 10, pp. 955–966, 1995.

[47] Bundesamt fuer Sicherheit in der Informationstechnik, "BioFace comparative study of facial recognition systems - public final report," Bundesamt fuer Sicherheit in der Informationstechnik, Godesberger Allee 185–189, 53175 Bonn, Germany, Tech. Rep., June 2003.

[48] Bundesamt fuer Sicherheit in der Informationstechnik, "Evaluierung biometrischer Systeme Fingerabdrucktechnologien - BioFinger," Bundesamt fuer Sicherheit in der Informationstechnik, Tech. Rep. Version 1.1, 2004.

[49] Bundesamt fuer Sicherheit in der Informationstechnik, "Untersuchung der leistungfähigkeiten von biometrischen verificationssystemen - biop ii," Bundesamt fuer Sicherheit in der Informationstechnik, Tech. Rep. Version 12.0, August 2005.

[50] M. Caligiuri, H.-L. Teulings, J. Filoteo, D. Song, and J. B. Lohr, "Quantitative measurement of handwriting in the assessment of drug-induced parkinsonism," in *Proc. 12th Biennial Conference of the International Graphonomics Society*, Salerno, Italy, June 2005, pp. 300–304.

[51] M. Caloyannides, "Does privacy really constrain security? or does it enhance security in a paper-free world?" *Keesing's Journal of Documents & identity*, no. 9, pp. 7–9, 2004.

[52] J. W. M. Campbell, "The role of biometrics in ID document issuance," *Keesing's Journal of Documents & Identity*, no. 4, pp. 6–8, 2004.

[53] J. Campbell and D. Reynolds, "Corpora for the evaluation of speaker recognition systems," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'99)*, vol. 2, March 1999, pp. 829–832.

[54] A. Cavoukian, "Privacy and biometrics: An oxymoron or time to take a 2nd look?" in *Proceedings Computers, Freedom and Privacy 98*, Austin, Texas, 1998, available online at http://www.ipc.on.ca/.

[55] Chairman of the Committee created by Article 6 of Regulation 1683/95 laying down a uniform format for visas, "Note - technical feasibility of the integration of biometric identifiers into the uniform format..." Council of the European Union, Note 14534/04, November 2004, available at http://www.statewatch.org/news/2004/dec/bio-visas.pdf.

[56] C. Champod, C. Lennard, P. Margot, and M. Stoilovic, *Fingerprints and Other Ridge Impressions*. Boca Raton: CRC Press, 2004.

[57] D. Chan, A. Fourcin, B. Gibbon, D.and Granstrom, M. Huckvale, G. Kokkinakis, K. Kvale, L. Lamel, B. Lindberg, A. Moreno, J. Mouropoulos, F. Senia, I. Trancoso, C. Veld, and J. Zeiliger, "EUROM - a spoken language resource for the EU," in *Proceedings 4th European Conference on Speech Communication and Speech Technology (Eurospeech'95)*, vol. 1, Madrid, Spain, September 1995, pp. 867–870.

[58] H.-D. Chang, J.-F. Wang, and H.-M. Suen, "Dynamic handwritten chinese signature verification," in *Proceedings second IEEE International Conference on Document Analysis and Recognition*, 1993, pp. 258–261.

[59] K. I. Chang, K. W. Bowyer, and P. J. Flynn, "Multi-modal 2D and 3D biometrics for face recognition," in *Proceedings of the IEEE International Workshop on Analysis and Modeling of Faces and Gestures (AMFG'03)*, 2003, pp. 187–194.

[60] X. Chen, P. J. Flynn, and K. W. Bowyer, "Visible-light and infrared face recognition," in *Proceedings of Workshop on Multimodal User Authentication*, 2003, pp. 48–55.

[61] C. C. Chibelushi, F. Deravi, and J. S. D. Mason, "A review of speech-based bimodal recognition," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 23–37, 2002.

[62] C. S. Chua and R. Jarvis, "Point signatures: A new representation for 3D object recognition," *International Journal of Computer Vision*, vol. 271, pp. 63–85, 1997.

[63] T. Clancy, N. Kiyavash, and D. Lin, "Secure smartcard-based fingerprint authentication," in *Proceedings ACM Multimedia 2003 Workshop on Biometric Methods and Applications*, Berkeley, USA, Nov. 2003.

[64] R. Clarke, "Human identification in information systems: Management challenges and public policy issues," *Information Technology and People*, vol. 7, no. 4, pp. 6–37, 1994.

[65] R. Clarke, "Privacy impact assessments," 2003, available online at http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html.

[66] R. Clarke, "Identification and authentication fundamentals," 2004, available online at http://www.anu.edu.au/people/Roger.Clarke/DV/IdAuthFundas.html.

[67] CNIL, "La carte d'identité électronique en Europe: Belgique, Italie, Espagne, Pays-Bas, Grande-Bretagne," Commission Nationale de l'Informatique et des Libertés, Tech. Rep., 2005.

[68] Commission des Communautés Européennes, "Décision de la Commission du 28/II/2005 établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres," *Official Journal of the European Union*, 2005.

[69] Confédération helvétique, "Loi fédérale sur les documents d'identité des ressortissants suisses," *Recueil Systématique*, 2001.

[70] Confédération helvétique, "Ordonnance fédérale sur les documents d'identité des ressortissants suisses," *Recueil Systématique*, 2002.

[71] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1–5, 2005.

[72] Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Council of Europe, 1981, no. 108, European Treaty Series.

[73] Council of Europe, *Draft Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*. Council of Europe, 2004.

[74] Council of the European Union, "Council Decision No 2004/512/EC establishing the Visa Information System (VIS)," *Official Journal of the European Union*, no. L 213, pp. 15–7, 2004.

[75] Council of the European Union, "Council regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States," *Official Journal of the European Union*, no. L 385, pp. 1–6, 2004.

[76] C. Crews, "Human bar code - monitoring biometric technologies in a free society," Cato Institute, Policy Analysis 452, September 2002.

[77] J. Darch, B. Milner, X. Shao, S. Vaseghi, and Q. Yan, "Predicting formant frequencies from MFCC vectors," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005)*, Philadelphia, USA, March 2005, pp. 941–944.

[78] J. G. Daugman, "High confidence visual recognition of persons by test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148 – 1161, 1993.

[79] J. G. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[80] J. G. Daugman and C. Downing, "Epigenetic randomness, complexity, and singularity of human iris patterns," *Proceedings of the Royal Society Lond. B*, vol. 268, pp. 1737–1740, 2001.

[81] J. Daugman, "Biop ii contreversy to be tackled," *Biometric Technology Today*, vol. 13, no. 10, pp. 1–2, 2005.

[82] Department of State, United States of America, "Electronic passport, Proposed Rule," *Federal Register*, vol. 70, no. 33, pp. 8305–8309, 2005.

[83] R. Derakhshani, S. A. Schuckers, L. A. Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fngerprint scanners," *Pattern Recognition*, vol. 36, no. 2, p. 383 Ű 396, 2005.

[84] G. R. Doddington, M. A. Przybocki, A. F. Martin, and D. A. Reynolds, "The nist speaker recognition evaluation - overview, methodology, systems, results, perspective," *Speech Communication*, vol. 31, no. 2-3, pp. 225–254, June 2000.

[85] G. Doddington, "A method of speaker verification," Ph.D thesis, University of Wisconsin, Madison, USA, 1970.

[86] J. Dolfing, E. Aarts, and J. van Oosterhout, "On-line signature verification with Hidden Markov Models," in *Proceedings International Conference on Pattern Recognition 1998*, vol. 2, Aug. 1998, pp. 1309–1312.

[87] S. Elliott, "Differentiation of signature traits vis-à-vis mobile- and table-based digitizers," *ETRI Journal*, vol. 26, no. 6, pp. 641–646, December 2004.

[88] European Commission, *Proposal for a Council Regulation amending Regulations (EC) 1683/95 laying down a uniform format for visas and (EC) 1030/02 laying down a uniform format for residence permits for third-country nationals*. EUR-OP, 2003, no. COM(2003) 558 final.

[89] European Commission, *Proposal for a Regulation of the European parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas*. EUR-OP, 2004, no. COM(2004) 835 final.

[90] European Commission, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*. EUR-OP, 2005, no. COM(2005) 600 final.

[91] K. Farrell, "Adaptation of data fusion-based speaker verification models," in *Proceedings IEEE International Symposium on Circuits and Systems (ISCAS'02)*, vol. 2, 2002, pp. 851–854.

[92] H. Fatemi, R. Kleihorst, H. Corporaal, and P. Jonker, "Real-time face recognition on a smart camera," in *Proceedings of Acivs 2003 (Advanced Concepts for Intelligent Vision Systems)*, Ghent, Belgium, Sept. 2003.

[93] H. Faulds, "On the skin-furrows on the hands," *Nature*, vol. 22, p. 605, 1880.

[94] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification," in *Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, J. Kittler and M. Nixon, Eds., vol. LNCS 2688, 2003, pp. 830–837.

[95] J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Target dependent score normalization techniques and their application to signature verification," in *Proceedings Biometric Authentication: First International Conference (ICBA 2004)*, vol. LNCS 3072, Hong Kong, China, July 2004, pp. 498–504.

[96] J. Fontana, "A national identity card for canada?" Standing Committee on Citizenship and Immigration, House Of Commons Canada, Tech. Rep., 2003.

[97] Forum des Droits sur l'Internet, "Projet de carte nationale d'identité électronique," Forum des Droits sur l'Internet," Rapport, 16 Juin 2005.

[98] S. Fredrickson and L. Tarassenko, "Text-independent speaker recognition using neural network techniques," in *Proceedings Fourth International Conference on Artificial Neural Networks*, June 1995, pp. 13–18.

[99] R. W. Frischholz and U. Dieckmann, "BioID: A multimodal biometric identification system," *IEEE Computer*, vol. 33, no. 2, p. 1998.

[100] D. Fuentes, D. Mostefa, J. Kharroubi, S. Garcia-Salicetti, B. Dorizzi, and G. Chollet, "Identity verification by fusion of biometric data: on-line signatures and speech," in *Proceedings COST 275 Workshop on the Advent of Biometrics on the Internet*, Nov. 2002, pp. 83–86.

[101] F. Galton, *Finger Prints*. London: Macmillian and Co., 1892.

[102] S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J. Leroux les Jardins, J. Lunter, Y. Ni, and D. Petrovska-Delacrétaz, "BIOMET: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities," in *Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, J. Kittler and M. Nixon, Eds., vol. LNCS 2688, 2003, pp. 845–853.

[103] J. Garofolo, L. Lamel, W. Fisher, J. Fiscus, D. Pallett, N. Dahlgren, and V. Zue, "Timit acoustic-phonetic continuous speech corpus," lDC catalog number LDC93S1.

[104] J. Godfrey, D. Graff, and A. Martin, "Public databases for speaker recognition and verification," in *Proceedings ESCA Workshop on Automatic Speaker Recognition, Identification and Verification*, Martigny, Switzerland, April 1994, pp. 39–42.

[105] A. Goh and C. Ngo, "Computation of cryptographic keys from face biometrics," *Lecture Notes in Computer Science*, vol. 2828, pp. 1–13, 2003.

[106] D. Graham and N. Allinson, *Characterizing Virtual Eigensignatures for General Purpose Face Recognition*, ser. NATO ASI Series F, Computer and Systems Sciences, 1998, pp. 446–456.

[107] R. Gross, "Face databases," in *Handbook of Face Recognition*, A. K. Jain and S. Z. Li, Eds. New-York: Springer-Verlag, 2005, ch. 13, pp. 301–327, to appear.

[108] Groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel (G29), *Avis No 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS).* Union Européenne, 11 août 2004.

[109] Y. Gu and T. Thomas, "A text-independent speaker verification system using support vector machines classifier," in *Proceedings 7th European Conference on Speech Communication and Technology (EUROSPEECH 2001 Scandinavia)*, Aalborg, Denmark, September 2001, pp. 1765–1768.

[110] C. Guerrier and L.-A. Cornelie, "Les aspects juridiques de la biométrie," Institut national des télécommunications (INT), Tech. Rep., 2003.

[111] S. Guruprasad, N. Dhananjaya, and B. Yegnanarayana, "AANN models for speaker recognition based on difference cepstrals," in *Proceedings International Joint Conference on Neural Networks*, vol. 1, July 2003, pp. 692–697.

[112] F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," University of Cambridge Computer Laboratory, Tech. Rep., 2005.

[113] N. Herbst and L. C.N., "Automatic signature verification based on accelerometry," *IBM Journal of Research and Development*, vol. 21, no. 3, pp. 245–253, 1977.

[114] W. Herschel, "Skin furrows on the hand," *Nature*, vol. 23, p. 76, 1880.

[115] A. Hickling, C. Watson, and B. Ulery, "The myth of goats: How many people have fingerprints that are hard to match?" National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 7271, 2005.

[116] A. Higgins and D. Vermilyea, "King speaker verification," lDC catalog number LDC95S22.

[117] H. Hollien, G. Dejong, C. Martin, R. Schwartz, and K. Liljegren, "Effects of ethanol intoxication on speech suprasegmentals," *Acoustical Society of America Journal*, vol. 110, no. 6, pp. 3198–3206, 2001.

[118] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 12, pp. 1295–1307, 1998.

[119] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?" *Proceedings AutoID'99*, pp. 59–64, 1999.

[120] C. Hook, J. Kempf, and G. Scharfenberg, "New pen device for biometrical 3d pressure analysis of handwritten characters, words and signatures," in *Proceedings 2003 ACM SIGMM workshop on Biometrics methods and applications*, Berkeley, USA, November 2003, pp. 38–44.

[121] T. Hopper, "Compression of gray-scale fingerprint images," in *Proceedings of the SPIE*, vol. 2242, 1994, pp. 180–185.

[122] R.-L. Hsu and A. K. Jain, "Face modeling for recognition," in *Proceedings International Conference on Image Processing (ICIP)*, 2001, pp. 693–696.

[123] P. HUSTINX, "Opinion of the european data protection supervisor on the proposal for a council decision concerning access for consultation of the visa information system (vis) by the authorities of member states responsible for internal security and by europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (com (2005) 600 final)." European Data Protection Supervisor" Opinion, 20th of January 2006.

[124] ICAO, *Document 9303 on Machine Readable Travel Document*. International Civil Aviation Organisation, 2003.

[125] ICAO, "Biometrics deployment of machine readable travel documents, technical report v. 2.0," International Civil Aviation Organisation, Tech. Rep., 2004.

[126] ICAO, "Developpment of a logical data structure - LDS - for optional capacity expansion technologies," International Civil Aviation Organisation, Tech. Rep. Machine Readable Travel Documents, Revision - 1.7, 2004.

[127] ICAO, "Document 9303 on Machine Readable Travel Document, annex a - facial image size study 1," International Civil Aviation Organisation, Tech. Rep., 2004.

[128] ICAO, "Document 9303 on Machine Readable Travel Document, annex a - photograph guidelines," International Civil Aviation Organisation, Tech. Rep., 2004.

[129] ICAO, "Use of contactless integrated circuits in machine readable travel documents," International Civil Aviation Organisation," Biometrics Deployment of Machine Readable Travel Documents, Annex I, 2004.

[130] International Biometric Group, "The bioprivacy initiative: A framework for evaluating the privacy impact of biometric deployment and technologies," International Biometric Group (IBG), Tech. Rep. M1/03-0227, 2002.

[131] International Biometric Group, "Independent testing of iris recognition technology," International Biometric Group, Final Report NBCHC030114/0002, May 2005.

[132] International Labour Organization, *Seafarers' Identity Documents Convention: The standard for the biometric template required by the Convention*. International Labour Office, Geneva, Switzerland, 2004, no. 185, Revised.

[133] International Standards Organisation, *ISO/IEC 7816*. Geneva, Switzerland: International Standards Organisation, 1998.

[134] International Standards Organisation, *ISO/IEC JRC 1/SC 37 Working Draft, Biometric Data Interchange Formats - Part 2: Fingerprint Minutiae Data*. Geneva, Switzerland: International Standards Organisation, 2004.

[135] International Standards Organisation, *ISO/IEC JRC 1/SC 37 Working Draft, Biometric Data Interchange Formats - Part 3: Fingerprint Pattern Spectral Data*. Geneva, Switzerland: International Standards Organisation, 2004.

[136] International Standards Organisation, *ISO/IEC JRC 1/SC 37 Working Draft, Biometric Data Interchange Formats - Part 4: Finger Image Data*. Geneva, Switzerland: International Standards Organisation, 2004.

[137] International Standards Organisation, *ISO/IEC JRC 1/SC 37 Working Draft, Biometric Data Interchange Formats - Part 5: Face iImage data*. Geneva, Switzerland: International Standards Organisation, 2004.

[138] International Standards Organisation, *ISO/IEC JRC 1/SC 37 Working Draft, Biometric Data Interchange Formats - Part 6: Iris Image Data*. Geneva, Switzerland: International Standards Organisation, 2004.

[139] International Standards Organisation, *ISO/IEC 19794-1:2005 (BioAPI 2.0)*. Geneva, Switzerland: International Standards Organisation, 2005.

[140] A. Jain, F. Griess, and S. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, pp. 2963–2972, 2002.

[141] A. K. Jain, R. P. W. Duin, and J. Mao, "Statistical pattern recognition: A review," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 4–37, 2000.

[142] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, 2005, to appear.

[143] A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple matchers for high security fingerprint verification system," *Pattern Recognition Letters*, vol. 20, no. 11-13, pp. 1371–1379, 1999.

[144] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transaction on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[145] A. K. Jain and A. Ross, "Learning user-specific parameters in a multibiometric system," in *Proceedings International Conference on Image Processing (ICIP)*, vol. 1, 2002, pp. 57–60.

[146] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, vol. 14, no. 1, pp. 4–20, 2004.

[147] Joint Research Center, "Biometrics at the frontiers: Assessing the impact on society," Joint Research Center, Institute for Prospective Technological Studies, European Commission, Technical Report Series EUR 21585 EN, 2005.

[148] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," Cryptology ePrint Archive, Report 2005/095, 2005, available online at http://eprint.iacr.org/2005/095.

[149] L. Kanda, "Iris recognition on the move," *Biometric Technology Today*, vol. 13, no. 10, p. 1, 2005.

[150] I. Karlsson, T. Banziger, T. Dankovicová, J.and Johnstone, J. Lindberg, H. Melin, F. Nolan, and K. Scherer, "Speaker verification with elicited speaking styles in the verivox project," *Speech Communication*, vol. 31, no. 2-3, pp. 121–129, June 2000.

[151] R. Kashi, J. Hu, W. Nelson, and W. Turin, "A Hidden Markov Model approach to online handwritten signature recognition," *International Journal on Document Analysis and Recognition*, vol. 1, no. 2, pp. 102–109, 1998.

[152] R. S. Kashi, W. T. Turin, and W. L. N. Nelson, "On-line handwritten signature verification using stroke direction coding," *Optical Engineering*, vol. 35, no. 9, pp. 2526–2533, September 1996.

[153] Keesing's Journal of Documents & Identity, "e-Passports 2005-2006 - The State of the e-passport industry, institution = Keesing's Journal of Documents & Identity, type = Annual Report, month=, number=, year = 2006," Tech. Rep.

[154] H. Ketabdar, J. Richiardi, and A. Drygajlo, "Global feature selection for on-line signature verification," in *Proceedings International Graphonomics Society 2005 Conference*, Salerno, Italy, June 2005.

[155] S. King, H. Harrelson, and G. Tran, "Testing iris and face recognition in a personnel identification application," 2002, available online at http://www.aclu.org/Privacy/Privacy.cfm?ID=13556&c=130.

[156] T. Kinneging, "The ICAO PKI scheme: what's in it for me?" *Keesing's Journal of documents and identity*, no. 9, pp. 3–6, 2004.

[157] T. A. F. Kinneging, "PKI for machine readable travel documents offering ICC read-only access," International Civil Aviation Organisation, Tech. Rep. Machine Readable Travel Documents, PKI Task Force, 2004.

[158] P. L. Kirk, "The ontogeny of criminalistics," *Journal of Criminal Law, Criminology and Police Science*, vol. 54, pp. 235–238, 1963.

[159] M. Kosmerli, T. Fladsrud, E. Hjelmas, and E. Snekkenes, "Face recognition issues in a border controll environment," in *Proceedings of International Conference on Biometrics 2006(ICB)*, D. Zhang and A. Jain, Eds., vol. LNCS 3832, 2005, pp. 33–39.

[160] K. Kryszczuk and A. Drygajlo, "Adressing vulnerabilities of likelihood-ratio-based face verification," in *Proceedings of 6th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, T. Kanade and N. R. (A.K.) Jain, Eds., vol. LNCS 3546, 2005, pp. 426–435.

[161] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometrybiometric," in *Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, J. Kittler and M. Nixon, Eds., vol. LNCS 2688, 2003, pp. 668 – 678.

[162] A. Kundu, Y. He, and P. Bahl, "Recognition of handwritten word: First and second order hidden markov model based approach," *Pattern Recognition*, vol. 22, no. 3, pp. 283–297, 1989.

[163] K. K. Lau, P. C. Yuen, and Y. Y. Tang, *Advances in Handwriting Recognition*. World Scientific, 1999, ch. An efficient Function-based On-line Signature Recognition System, pp. 559–568.

[164] Y. LeCun, F.-J. Huang, and L. Bottou, "Learning methods for generic object recognition with invariance to pose and lighting," in *Proceedings of IEEE CVPR'04 (Computer Vision and Pattern Recognition)*. IEEE Press, 2004.

[165] L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 18, no. 6, pp. 643–647, June 1996.

[166] E. Locard, *L'identification des récidivistes*. Paris: A. Maloine, 1909.

[167] E. Locard, *La preuve judiciaire par les empreintes digitales*. Paris: Archives d'anthropologie criminelle de médecine légale et de psychologie normale et pathologique, 1914.

[168] X. Lu, Y. Wang, and A. K. Jain, "Combining classifiers for face recognition," in *Proceedings International Conference on Multimedia and Expo (ICME)*, vol. 3, 2003, pp. 13–16.

[169] R. Luis-Garcia, C. Alberola-Lopez, O. Aghzout, and J. Ruiz-Alzola, "Biometric identification systems," *Signal Processing*, vol. 83, pp. 2539–2557, 2003.

[170] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 2, pp. 402–412, 2000.

[171] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second fingerprint verification competition," in *Proceedings of the 16th International Conference on Pattern Recognition*, vol. 3, 2002, pp. 811– 814.

[172] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third fingerprint verification competition," in *Proceedings of the First International Conference on Biometric Authentication*, vol. 3072, 2004, pp. 1–7.

[173] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New-York: Springer-Verlag, 2003.

[174] G. Manoranjan, "JPEG 2000 - a versatile image compression standard," *Keesing's Journal of Documents & Identity*, no. 9, pp. 26–29, 2004.

[175] A. J. Mansfield, G. Kelly, D. Chandler, and J. Kane, "Biometric product testing: Final report," National Physical Laboratory, Center fo Mathematics and Scientific Computing, Tech. Rep. Issue 1.0, 2002.

[176] A. J. Mansfield and J. L. Waymann, "Best practices in testing and reporting performance of biometric devices," National Physical Laboratory, Center fo Mathematics and Scientific Computing, Tech. Rep. Version 2.01, 2002.

[177] MAOSCO Limited, *MULTOS Standard C API, MAO-DOC-REF-016*. London, United Kingdom: MAOSCO Limited, 2004, available from http://www.multos.com.

[178] M. W. Marcellin, M. J. Gormish, A. Bilgin, and M. P. Boliek, "An overview of JPEG-2000," in *Proceedings of IEEE Data Compression Conference*, 2000, pp. 523–541.

[179] A. Martin, G. Doddington, T. Kamm, M. Ordowsk, and M. Przybock, "The DET curve in assessment of detection task performance," in *Proceedings of EuroSpeech*, vol. 4, 1997, pp. 1895–1898.

[180] A. Martinez and R. Benavente, "The ar face database," Computer Vision Center, CVC Technical Report 24, June 1998.

[181] L. Masek, "Recognition of human iris patterns for biometric identification," Bachelor of Engineering degree, School of Computer Science and Software Engineering, University of Wester Austrialia, 2003.

[182] J. Mathyer, "Quelques remarques sur le problèmes de la sécurité des pièces d'identité et des pièces de légitimation: une solution intéressante," *Revue Internationale de Police Criminelle*, vol. 35, no. 336, pp. 66–79, 1980.

[183] T. Matsui and S. Furui, "Comparison of text-independent speaker recognition methods using vq-distortion and discrete/continuous hmm's," *Speech and Audio Processing, IEEE Transactions on*, vol. 2, no. 3, pp. 456–459, July 1994.

[184] T. Matsumoto, "Gummy finger and paper iris: An update," in *Proceedings of the 2004 Workshop on Information Security Research*, 2004.

[185] T. Matsumoto, K. Matsumto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Proceedings of SPIE*, vol. 4677, 2002, pp. 275–289.

[186] G. Medioni and R. Waupotitsch, "Face modeling and recognition in 3-D," in *Proceedings of the IEEE International Workshop on Analysis and Modeling of Faces and Gestures (AMFG'03)*, 2003, pp. 232–233.

[187] H. Melin, "Databases for speaker recognition: Activities in COST250 working group 2," in *Proceedings COST250 Workshop on Speaker Recognition in Telephony*, Rome, Italy, Nov 1999.

[188] J. Menn, "Fraud rings taps into credit data," *Los Angeles Times*, 2005.

[189] K. Messer, J. Kittler, M. Sadeghi, M. Hamouz, A. Kostin, F. Cardinaux, S. Marcel, S. Bengio, C. Sanderson, N. Poh, Y. Rodriguez, J. Czyz, L. Vandendorpe, C. McCool, S. Lowther, S. Sridharan, V. Chandran, R. P. Palacios, E. Vidal, L. Bai, L. Shen, Y. Wang, C. Yueh-Hsuan, L. Hsien-Chang, H. Yi-Ping, A. Heinrichs, M. Muller, A. Tewes, C. von der Malsburg, R. Wurtz, Z. Wang, F. Xue, Y. Ma, Q. Yang, C. Fang, X. Ding, S. Lucey, R. Goss, and H. Schneiderman, "Face authentication test on the BANCA database," in *Proceedings 17th International Conference on Pattern Recognition (ICPR)*, vol. 4, Cambridge, United Kingdom, August 2004, pp. 523–532.

[190] K. Messer, J. Kittler, M. Sadeghi, M. Hamouz, A. Kostyn, S. Marcel, S. Bengio, F. Cardinaux, C. Sanderson, N. Poh, Y. Rodriguez, K. Kryszczuk, J. Czyz, L. Vandendorpe, J. Ng, H. Cheung, and B. Tang, "Face authentication competition on the BANCA database," in *Proceedings first International Conference on Biometric Authentication (ICBA)*, Hong Kong, July 2004, pp. 8–15.

[191] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB: The extended M2VTS database," in *Proceedings of 2nd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, 1999, pp. 72–77.

[192] K. Messer, J. Kittler, J. Short, G. Heusch, F. Cardinaux, S. Marcel, Y. Rodriguez, S. Shan, Y. Su, W. Gao, and X. Chen, "Performance characterisation of face recognition algorithms and their sensitivity to severe illumination changes," in *Proceedings of International Conference on Biometrics 2006(ICB)*, D. Zhang and A. Jain, Eds., vol. LNCS 3832, 2005, pp. 1–11.

[193] W. Mikhael and P. Premakanthan, "Speaker recognition employing waveform based signal representation in nonorthogonal multiple transform domains," in *Proceedings IEEE International Symposium on Circuits and Systems (ISCAS'02)*, vol. 2, May 2002, pp. 608–611.

[194] B. Miller, "Vital signs of identity," *IEEE Spectrum*, vol. 31, no. 2, pp. 22–30, 1994.

[195] J. Miller, "Dermatoglyphics," *Journal of Investigative Dermatology*, vol. 60, no. 6, pp. 435–442, 1973.

[196] B. Moghaddam and A. Pentland, "Probabilistic visual learning for object representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 696–710, July 1997.

[197] C. Mund and P.-Y. Baumann, "Legal and societal aspects of exchange and storage of biometric data," in *Biometrics 2005 - Technology and Societal Impacts*, September 2005.

[198] I. Nakanishi, H. Sakamoto, Y. Itoh, and Y. Fukui, "Multi-matcher online signature verification system in DWT domain," in *Proceedings 2005 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Philadelphia, USA, March 2005, pp. 965–968.

[199] V. Nalwa, "Automatic on-line signature verification," *Proceedings of the IEEE*, vol. 82, no. 2, pp. 215–239, February 1997.

[200] NIST, "NIST standards for biometric accuracy, tamper resistance, and interoperability," National Institute of Standards and Technology (NIST), Tech. Rep. 303A Report, Appendix A, 2003.

[201] NIST, "Use of technology standards and interoperable databases with machine-readable tamper-resistant travel document," National Institute of Standards and Technology (NIST), Tech. Rep., 2003.

[202] R. Norton, "The evolving biometric marketplace to 2006," *Biometric Technology Today*, vol. 10, no. 9, pp. 7–8, 2002.

[203] OECD, "Biometric-based technologies," Organisation for Economic Cooperation and Development (OECD), Tech. Rep., 2004.

[204] J. Oglesby, J. Mason, "Speaker recognition with a neural classifier," in *Speech 88: Proceedings of the 7th Federation of Acoustical. Societies of Europe (FASE) Symposium*, Edinburgh, UK, 1988, pp. 1357–1363.

[205] J. Oglesby, J. Mason, "Speaker recognition with a neural classifier," in *Proceedings First IEE International Conference on artificial Neural Networks*, vol. 313, October 1989, pp. 306–309.

[206] J. Oglesby, J. Mason, "Radial basis function networks for speaker recognition," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'91)*, vol. 1, April 1991, pp. 393–396.

[207] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro, "MCYT baseline corpus: A bimodal biometric database," in *IEE Proceedings - Vision, Image and Signal Processing*, vol. 150, no. 6, 2003, pp. 395–401.

[208] J. Ortega-Garcia, J. Gonzalez-Rodriguez, and V. Marrero-Aguiar, "AHUMADA: A large speech corpus in spanish for speaker characterization and identification," *Speech Communication*, vol. 31, pp. 255–264, 2000.

[209] M. Pandit and J. Kittler, "Feature selection for a DTW-based speaker verification system," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'98)*, vol. 2, 1998, pp. 769–772.

[210] M. Parizeau and R. Plamondon, "A comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 7, pp. 710–717, July 1990.

[211] J. Peters, "Enhanced security for chip-based ID cards," *Keesing's Journal of Documents & Identity*, no. 7, pp. 9–11, 2004.

[212] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the Face Recognition Grand Challenge," in *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, 2005, to appear.

[213] P. Phillips, P. Grother, R. Micheals, D. BoneBlackburn, E. Tabassi, and M. Bone, "Facial recognition vendor test 2002, Evaluation report," March 2003, available online at http://www.frvt.org/.

[214] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction to evaluation biometric systems," *IEEE Computer*, pp. 56–63, 2000.

[215] P. Phillips, H. Moon, S. Rizvi, and P. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090–1104, 2000.

[216] P. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image and Vision Computing Journal*, vol. 16, no. 5, pp. 295–306, 1998.

[217] R. Plamondon, J. Brault, and P. Robillard, "Optimizing the design of an accelerometer pen for signature verification," in *Proceedings 1983 Conference on Crime Countermeasures and Security*, Lexington, USA, May 1983, pp. 35–40.

[218] R. Plamondon and G. Lorette, "On-line signature verification: how many countries are in the race?" in *Proceedings IEEE International Carnahan Conference on Security Technology*, Zuerich, Switzerland, 1989, pp. 183–191.

[219] F. L. Podio, J. S. Dunn, L. Reinert, C. J. Tilton, L. O'Gorman, M. P. Collier, M. Jerde, and B. Wirtz, *Common Biometric Exchange File Format (CBEFF) - NISTIR 6529*. USA: The National Institute of Standards and Technology (NIST), 2001.

[220] A. Poritz, "Linear predictive hidden markov models and the speech signal," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'82)*, vol. 7, May 1982, pp. 1291–1294.

[221] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognition*, vol. 35, no. 4, pp. 861–874, 2002.

[222] S. Prabhakar and A. K. Jain, "Fingerprint matching," in *Automatic Fingerprint Recognition Systems*, N. Ratha and B. Ruud, Eds. London: Springer-Verlag, 2004, ch. 11, pp. 229–248.

[223] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security and Privacy*, vol. 1, no. 2, pp. 33–42, 2003.

[224] Presidency of the European Union, "Note - minimum common standards for national identity cards," Council of the European Union, Note 11092/05, 11th of July 2005.

[225] Privacy International et al., "An open letter to the ICAO," March 2004, available at http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf.

[226] H. Proença and L. A. Alexandre, "Ubiris: A noisy iris image database," Tech. Rep., 2005, iSBN 972-99548-0-1.

[227] Préposé Fédéral à la Protection des Données, *11ème Rapport d'activités 2003/2004 du PFPD*. Confédération Helvétique, 2004.

[228] Préposé Fédéral à la Protection des Données, *12ème Rapport d'activités 2004/2005 du PFPD*. Confédération Helvétique, 2005.

[229] J. Putz-Leszczynska and A. Pacut, "Dynamic time warping in subspaces for on-line signature verification," in *Proc. 12th Biennial Conference of the International Graphonomics Society*, Salerno, Italy, June 2005, pp. 108–112.

[230] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[231] D. Reynaert and H. Van Brussel, "Design of an advanced computer writing tool," in *Proceedings sixth International Symposium on Micro Machine and Human Science (MHS '95)*, October 1995, pp. 229–234.

[232] D. Reynolds, "Speaker identification and verification using gaussian mixture speaker models," *Speech Communication*, vol. 17, pp. 91–108, 1995.

[233] D. Reynolds, W. Campbell, T. Gleason, C. Quillen, D. Sturim, P. Torres-Carrasquillo, and A. Adami, "The 2004 MIT Lincoln laboratory speaker recognition system," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005)*, Philadelphia, USA, March 2004, pp. 177–180.

[234] D. Reynolds, T. Quatieri, and R. Dunn, "Speaker verification using adapted Gaussian mixture models," *Digital Signal Processing*, vol. 10, no. 1–3, pp. 19–41, 2000.

[235] T. Rhee, S. Cho, and J. Kim, "On-line signature verification using model-guided segmentation and discriminative feature selection for skilled forgeries," in *Proceedings Sixth International Conference on Document Analysis and Recognition*, September 2001, pp. 645–649.

[236] J. Richiardi and A. Drygajlo, "Gaussian mixture models for on-line signature verification," in *International Multimedia Conference, Proceedings 2003 ACM SIGMM workshop on Biometrics methods and applications*, Berkeley, USA, Nov. 2003, pp. 115–122.

[237] J. Richiardi, P. Prodanov, and A. Drygajlo, "A probabilistic measure of modality reliability in speaker verification," in *Proceedings IEEE International Conference on Acoustics, Speech and Signal Processing 2005*, Philadelphia, USA, March 2005.

[238] F. Roli, J. Kittler, G. Fumera, and D. Muntoni, "An experimental comparison of classifier fusion rules for multimodal personal identity verification systems," in *Proceedings of the Third International Workshop on Multiple Classifier Systems*, 2002, pp. 325–335.

[239] A. Rosenberg, C. Lee, and S. Gokcen, "Connected word talker verification using whole word hidden markov models," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'91)*, vol. 1, April 1991, pp. 381–384.

[240] P. Rosenzweig, A. Kochems, and A. Schwartz, "Biometric technologies: Security, legal, and policy implications," *Legal Memorandum*, vol. 12, pp. 1–10, 2004.

[241] A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, pp. 2215–2125, 2003.

[242] A. Ross and A. K. Jain, "Multimodal biometrics: An overview," in *Proceedings of 12th European Signal Processing Conference*, 2004, pp. 1221–1224.

[243] H. Rowley, S. Baluja, and T. Kanade, "Neural network-based face detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 1, pp. 23–38, January 1998.

[244] F. Rumsey and T. McCormick, *Sound and recording: an introduction*, 3rd ed. Oxford, UK: Focal press, 1997.

[245] D. Sakamoto, H. Morita, T. Ohishi, Y. Komiya, and T. Matsumoto, "On-line signature verification incorporating pen position, pen pressure and pen inclination trajectories," in *Proceedings 2001 IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2001, pp. 7–11, dynamic Time Warping.

[246] F. Samaria and A. Harter, "Parameterisation of a stochastic model for human face identification," in *Proceedings of 2nd IEEE Workshop on Applications of Computer Vision*, Sarasota, United States of America, December 1994.

[247] Y. Sato and K. Kogure, "Online signature verification based on shape, motion, and writing pressure," in *Proceedings 6th International Conference on Pattern Recognition*, 1982, pp. 823–826.

[248] A. Scheenstra, A. Ruifrok, and R. C. Veltkamp, "A survey of 3D face recognition methods," in *Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, 2005, to be published.

[249] M. Schmidt and H. Gish, "Speaker identification via support vector classifiers," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'96)*, vol. 1, May 1996, pp. 105–108.

[250] B. Schneier, *Applied Cryptography*, 2nd ed. John Wiley and Sons Inc., 1996.

[251] S. A. C. Schuckers, "Spoofing and anti-spoofing measures," *Information Security technical report*, vol. 7, no. 4, pp. 56–62, 2002.

[252] R. Schwartz, S. Roucos, and M. Berouti, "The application of probability density estimation to text-idenpendent speaker identification," in *Proceedings IEEE International Conference on Speech, Acoustics, and Signal Processing*, 1982, pp. 1649–1652.

[253] J. Short, J. Kittler, and K. Messer, "Comparison of photometric normalisation algorithms for face verification," in *Proceedings 6th IEEE International Conference on Automatic Face and Gesture Recognition (FGR 2004)*, 2004, pp. 254– 259.

[254] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression database," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 12, pp. 1615–1618, December 2003.

[255] J. Simitian, "SB 682, Identity Information Protection Act of 2005," California State Senate, March 2005, available at http://www.sen.ca.gov/.

[256] L. Sirovich and M. Kirby, "Low-dimensional procedure for the characterization of human faces," *Journal of the Optical Society of America*, vol. 4, no. 3, pp. 519–524, 1987.

[257] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. K. Jain, "Large scale evaluation of multimodal biometric authentication using state-of-the-art systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 450–455, 2005.

[258] F. Soong, A. Rosemberg, L. Rabiner, and B. Juang, "A vector quantization approach to speaker recognition," in *Proceedings IEEE International Conference on Speech, Acoustics, and Signal Processing*, 1985, pp. 387–390.

[259] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar, "Biometric encryption using image processing," in *Proc. SPIE Optical Security and Counterfeit Deterrence Techniques II*, R. L. van Renesse, Ed., vol. 3314, no. 1. SPIE, 1998, pp. 178–188. [Online]. Available: http://link.aip.org/link/?PSI/3314/178/1

[260] S. T. C. (St.-Petersburg), "STC russian speech database," eLDA catalogue number S0050.

[261] J. Stanley and B. Steinhardt, "Drawing a blank: The failure of facial recognition technology in Tampa, Florida," American Civil Liberties Union," ACLU special report, January 2002.

[262] R. Suikerbuik, H. Tangelder, H. Daanen, and A. Oudenhuijzen, "Automatic feature detection in 3D human body scans," in *Proceedings of the Conference SAE Digital Human Modelling for Design and Engineering*, 2004.

[263] K. Sung and T. Poggio, "Example-based learning for view-based human face detection," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 20, pp. 39–51, 1997.

[264] G. Swain, "A smart alternative: an introduction to high-density two-dimensional barcodes," *Keesing's Journal of Documents & Identity*, no. 8, pp. 9–11, 2004.

[265] The London School of Economics & Political Science, "The identity project: An assessment of the UK Identity Cards Bill & its implications," The London School of Economics & Political Science, Tech. Rep. Interim Report, March 2005.

[266] C.-L. Tisse, "Contribution à la vérification biométrique de personnes par reconnaissance de l'iris," Ph.D, Université de Monpellier II, 2003.

[267] F. Tsalakanidou, S. Malassiotis, and M. G. Strintzis, "Integration of 2D and 3D images for enhanced face authentication," in *Proceedings of 6th IEEE International Conference on Automatic Face and Gesture Recognition (FGR'04)*, 2004, pp. 266– 271.

[268] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[269] P. Tuyls and J. Goseling, "Capacity and examples of template protecting biometric authentication systems," in *Proceedings Biometric Authentication Workshop*, Prague, 2004, pp. 158–170, lNCS 4677.

[270] UK Passport Service, "Biometrics enrolment trial," United Kingdom Passport Service," Report, May 2005.

[271] United Kingdom, *Identity Cards Bill*. U.K. Home Office, 2004.

[272] C. Van Oel, W. Baare, H. Hulshoff Pol, J. Haag, J. Balazs, A. Dingemans, R. Kahn, and M. Sitskoorn, "Differentiating between low and high susceptibility to schizophrenia in twins: The significance of dermatoglyphic indices in relation to other determinants of brain development," *Schizophrenia Research*, vol. 52, no. 3, pp. 181–193, 2001.

[273] R. L. van Renesse, "Implications of applying biometrics to travel-documents," in *Proceedings of SPIE*, vol. 4677, 2002, pp. 290–298.

[274] J. Verbov, "Clinical significance and genetics of epidermal ridges - a review of dermatoglyphics," *Journal of Investigative Dermatology*, vol. 54, no. 4, pp. 261–271, 1970.

[275] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures," in *Proc. 16th International Conference on Pattern Recognition (ICPR)*, vol. 1, 2002.

[276] J.-P. Walter, "Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé," in *26th international conference of the data protection and privacy commissioners*, Wroclaw, Poland, September 2004, available at http://26konferencja.giodo.gov.pl/program/j/en.

[277] V. Wan and S. Renals, "Speaker verification using sequence discriminant support vector machines," *IEEE Transactions on Speech and Audio Processing*, vol. 13, no. 2, pp. 203–210, March 2005.

[278] Y. Wang, T. Tan, and A. K. Jain, "Combining face and iris biometrics for identity verification," in *Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, J. Kittler and M. Nixon, Eds., vol. LNCS 2688, 2003, pp. 805–813.

[279] C. Watson, C. Wilson, K. Marshall, M. Indovina, and R. Snelick, "Studies of one-to-one fingerprint matching with vendor sdk matchers," National Institute of Standards and Technology (NIST), Tech. Rep., 2003.

[280] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, "An introduction to biometric authentication systems," in *Biometric Systems: Technology, Design and Performance Evaluation*, J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds. London: Springer-Verlag, 2005, ch. 1, pp. 1–20.

[281] R. Wildes, "Iris recognition," in *Biometric Systems: Technology, Design and Performance Evaluation*, J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds. London: Springer-Verlag, 2005, ch. 3, pp. 63–95.

[282] R. P. Wildes, "Iris recognition: An emerging biometric technology," in *Proceedings of the IEEE*, vol. 85, no. 9, 1997, pp. 1348–1363.

[283] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, "A system for automated iris recognition," in *Proceedings of the Second IEEE Workshop on Applications of Computer Vision*, 1994, pp. 121–128.

[284] G. O. Williams, "Iris recognition technology," Iridian technologies, Tech. Rep., 2001.

[285] C. L. Wilson, M. D. Garris, and C. I. Watson, "Matching performance for the US-VISIT system using flat fingerprints," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 7110, 2004.

[286] C. Wilson, R. A. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. Micheals, S. Otto, and C. Watson, "Fingerprint vendor technology evaluation 2003: Summary of results and analysis report," National Institute of Standards and Technology (NIST), Tech. Rep., 2004.

[287] C. L. Wilson, C. I. Watson, M. D. Garris, and A. Hicklin, "Studies of fingerprint matching using the NIST verification test bed (VTB)," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 7020, 2004.

[288] L. Wiskott, J.-M. Fellous, N. Kuiger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 775–779, July 1997.

[289] S. S. Wood and C. L. Wilson, "Studies of plain-to-rolled fingerprint matching using the NIST algorithmic test bed (ATB)," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 7112, 2004.

[290] J. D. Woodward, "Biometrics: Privacy's foe or privacy's friend?" in *Proceedings of the IEEE*, vol. 85, no. 9, 1997, pp. 1480–1492.

[291] J. D. Woodward, C. Horn, J. Gatune, and A. Thomas, "Biometrics : A look at facial recognition," RAND Documented Briefing, Tech. Rep., 2003.

[292] J. Wu, "Rotation invariant classification of 3d surface texture using photometric stereo," Ph.D, Departement of Computer Science, School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh, UK, 2003.

[293] Q.-Z. Wu, I.-C. Jou, and S.-Y. Lee, "On-line signature verification using LPC cepstrum and neural networks," *IEEE Trans. on systems, man and cybernetics, Part B*, vol. 27, no. 1, pp. 148–153, Feb. 1997.

[294] N. Yager and A. Amin, "Fingerprint verification based on minutiae features: a review," *Pattern Analysis and Application*, vol. 17, pp. 94–113, 2004.

[295] L. Yang, B. Widjaja, and R. Prasad, "Application of hidden Markov models for signature verification," *Pattern Recognition*, vol. 28, no. 2, pp. 161–170, 1995.

[296] B. Yanikoglu and A. Kholmatov, "An improved decision criterion for genuine/forgery classification in on-line signature verification," in *Proceedings ICANN/ICONIP 2003*, June 2003.

[297] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *Proceedings of ICPR-BCTP Workshop*, 2004.

[298] D.-Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "SVC2004: First international signature verification competition," in *Proceedings 2004 Biometric Authentication: First International Conference, (ICBA 2004)*, Hong Kong, China, July 2004, pp. 16–22.

[299] H. Yoon, J. Lee, and H. Yang, "An on-line signature verification system using Hidden Markov Model in polar space," in *Proceedings Eigth International Workshop on Frontiers in Handwriting Recognition*, Aug. 2002, pp. 329–333.

[300] K. Yu, J. Mason, and J. Oglesby, "Speaker recognition using hidden Markov models, dynamic time warping and vector quantisation," *IEE Proceedings - Vision, Image and Signal Processing*, vol. 142, pp. 313–318, October 1995.

[301] W. Zhao, R. Chellappa, J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, December 2003.