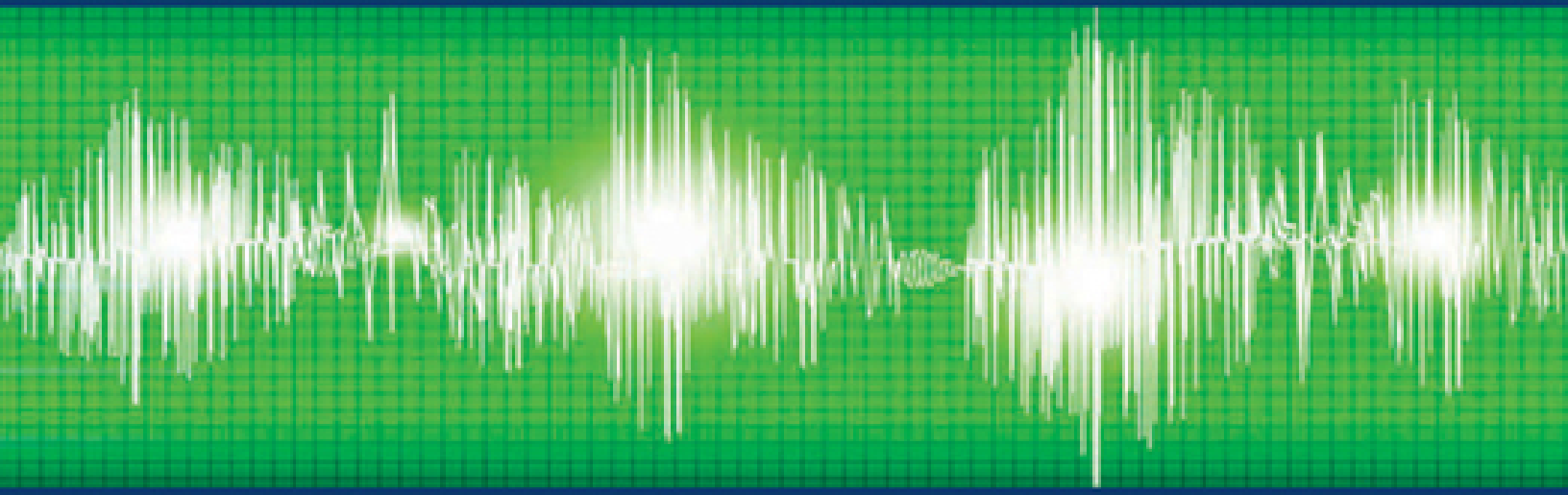
DSP

DIGITAL SIGNAL AND IMAGE PROCESSING SERIES



Signal and Image Processing for Biometrics

Edited by Amine Naït-Ali and Régis Fournier

ISTE

WILEY

Table of Contents

Signal and Image Processing for Biometrics

Edited by
Amine Naït-Ali
Régis Fournier

ISTE WILEY

First published 2012 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.iste.co.uk

www.wiley.com

Library of Congress Cataloging-in-Publication Data

Signal and image processing for biometrics / edited by Amine Na t-Ali, Régis Fournier.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-84821-385-2
1. Biometric identification. 2. Image processing. 3. Signal

processing. I. Naït-Ali, Amine. II. Fournier, Régis.
TK7882.B56S54 2012
570.1'5195--dc23

2012017918

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN: 978-1-84821-385-2

Preface

Literally, the word “biometrics” is composed of the prefix “bio”, meaning “life” in Greek, and the suffix “metrics”, meaning “measure”. Indeed, its main aim is to perform measurements on human beings. The term also refers to a discipline describing statistical and mathematical methods employed to process data related to life sciences. Even though several scientific communities “share” the word “biometrics” to deal with some specific fields such as medicine and ecology, this book is dedicated basically for security purposes. Actually, we believe that it is within this context that biometrics is best known, including the non-scientific community. This biometrics considers, in particular, the problem of identification and authentication of individuals using their characteristics. In fact, this issue goes back to the 19th Century, especially through the practice of anthropometry, but it has probably existed, under other forms, long before that time. The history of biometrics is exciting but its evolution is even more exciting. Over generations, human attitudes have changed and continued to mutate to the point where the degree of acceptability and subtlety is constantly evolving depending on the needs, constraints, and events that the world is aware of. Biometrics has changed a lot, and this term is becoming more and more common in our everyday language: the biometric passport, the biometric ID card, the biometric lock, etc. In the coming years, we expect that huge applications dealing with biometric-based systems will be developed. For example, according to the analysis of the biometrics market, published by the “International Biometric

Group (IBG)”, we can find an increasing trend for both businesses and public sectors. As an example, we may mention one of the major programs of biometric identification that no country has ever known before. It consists of enrolling all Indian citizens to build a single national database.

Potentially, biometrics can be considered as an effective measure to allow an ease-of-use of technical systems or to provide some solutions to socioeconomic, management, and security issues. However, it is important to emphasize the fact that biometrics should be taught and controlled so that human identity, privacy, and freedom can be respected and that ethics is a priority or even a fundamental condition for the balance of the contemporary society.

Technically speaking, biometrics, as considered so far, would certainly not have existed without the progress reached in other disciplines, such as electronics, computer science, and signal and image processing. Within this context, many excellent books on biometrics have been published in recent years, highlighting both the software and the hardware aspects and considering more specifically acquisition systems and data processing techniques. But, this book is somehow different in the sense that the purpose is basically to provide a survey on biometrics as represented by French and some French-speaking research teams. The aim is to help postgraduate students, researchers, and engineers who need an introduction to biometrics and those who want to major in this field. In addition, we have tried to strike a balance between the chapters dedicated to research and those proposed for educational purpose by including *Matlab* code.

As the book title suggests, signal and image processing methods are presented by considering applications related to the identification and authentication of individuals. Obviously, two-dimensional/three-dimensional (2D/3D) face

recognition, iris, and hand biometrics are considered, but the contents of this book are also extended to multibiometrics as well as to the performance evaluation of biometric systems. In addition, some signal processing tools such as classification, cryptography, and data protection are also presented.

The book consists of 15 chapters and is structured as follows:

Chapter 1: entitled “Introduction to Biometrics”. The history of biometrics is briefly reviewed; then the most common biometric modalities and their evaluation are presented. The multimodality and the privacy aspects are also discussed.

Chapter 2: in this chapter, “Introduction to 2D Face Recognition”, is proposed for educational purposes. It is especially intended for beginners. Its aim is to introduce some classical techniques and algorithms of facial biometrics by considering some local, global, and hybrid approaches.

Chapter 3: in this chapter, entitled “Facial Soft Biometrics for Person Recognition”, the aim is to deal with a specific type of biometrics that deals with some traits, such as the color of the eyes and hair, to identify persons or a group of persons.

Chapter 4: entitled “Modeling, Reconstruction and Tracking for Face Recognition”, the chapter addresses issues related to the acquisition of faces “on the fly”, in particular, by the use of multiview acquisition systems. Within an authentication context, the issues related to the 3D shape and to the texture of the face are addressed.

Chapter 5: in this chapter, entitled “3D Face Recognition”, 3D acquisition for biometrics, the preprocessing, as well as the symmetric and asymmetric face recognition are discussed.

Chapter 6: biometrics cannot be presented without addressing the iris modality. This is indeed the purpose of this chapter entitled “Introduction to Iris Biometrics”. The overall architecture of an iris biometric system is presented, which is essentially helpful for beginners. Afterwards, a step-by-step reference processing technique is detailed.

Chapter 7: in this chapter, entitled “Voice Biometrics: Speaker Verification and Identification”, some signal processing tools, in particular those used for analysis, modeling, and filtering, are elaborated within the context of speech recognition.

Chapter 8: this is another chapter for beginners, entitled “Introduction to Hand Biometrics”, in which the reader can perform basic processing (e.g. minutia extraction), using *Matlab* code. Links to several helpful databases are also provided.

Chapter 9: entitled “Multibiometrics”, this chapter presents various structures of multibiometric systems and the different biometric data fusion methods. Illustrations derived from industrial systems are also presented.

Chapter 10: in this chapter, biometrics is seen from a different viewpoint, in comparison with common techniques. Specifically, it consists of extracting signatures from biosignals and medical images for the purpose of identification or authentication. This biometrics, which is particularly robust to “spoofing”, is called “hidden biometrics”. In particular, we focus on biometrics using electrocardiogram (ECG), electromyogram (EMG), and some medical imaging techniques (e.g. brain MRI images, hand X-ray images, and anatomic images).

Chapter 11: after a brief review of some common definitions related to biometric systems, this chapter, entitled “Performance Evaluation of Biometric Systems”, is dedicated to the presentation of some tools used to assess the performance of biometric systems. Furthermore,

interesting illustrations on keystroke dynamics systems are also presented.

Chapter 12: in biometric applications, it is often necessary to use classification techniques to associate a given feature with a predefined class. For this purpose, we present in this chapter, entitled “Classification Techniques for Biometrics”, numerous parametric (e.g. naive Bayesian and linear discriminant analysis (LDA)) and non-parametric (e.g. *k*-nearest neighbor (KNN), neural networks, and support vector machine (SVM)) methods. *Matlab* codes are also included.

Chapter 13: the main purpose of this chapter entitled “Data Cryptography” is to understand the basics of cryptography, including modern cryptography. It is obvious that the reader can use such a tool to encrypt biometric data.

Chapter 14: this chapter, entitled “Visual Data Protection”, is complementary to the previous chapter. It is dedicated to the protection of visual data through some specific methods, including digital watermarking and fingerprinting.

Chapter 15: in this chapter, entitled “Biometrics in Forensics”, the issues of facial comparison and voice comparison are discussed within the forensic context. The inference of the identity in forensics is also considered.

Finally, it is important to point out that this book would not have been possible without the active contribution of researchers from the French and French-speaking biometric community as well as some non-French-speaking researchers. This book is also the result of the participation of some members representing major industries and institutions active in the fields of biometrics and security. It is to all these participants that we wish to express our gratitude.

Amine NAIT-ALI and Régis FOURNIER
June 2012

Chapter 1

Introduction to Biometrics [1]

Nowadays, biometrics is an emerging technique that allows us to verify the identity of an individual by using one or more of his or her personal characteristics. Its advantage is to increase the level of security by using as an identifier data that cannot be lost, stolen, or tampered with unlike passwords or personal identification number (PIN) codes, since they are directly related to the body or the behavior of the individual. A resurgence of interest in these techniques has been observed since the 2000s, a period when security policies were implemented in the G8 countries following the attacks of 9/11, among others. Recently several big deployments of biometrics systems have taken place. Let us quote the biometric passport, national identity cards and the new census of the Indian population. The purpose of this chapter is to give a brief introduction to biometric systems and to the various challenges that remain to be tackled by researchers of the field, in particular to cope with these large-scale deployments.

1.1. Background: from anthropometry to biometrics

Biometrics first emerged in the late 19th Century for police usage only. The taking of fingerprints, which is the oldest of biometric technologies, ultimately prevailed in the 19th Century for the identification of individuals, including

criminals, after the work of various anthropologists, notably the English anthropologist Francis Galton in 1892.

In France, around 1880, Alphonse Bertillon developed forensic science through the implementation of anthropometric data sheets for each arrested person. The data sheets were used to identify detainees using the metric survey of their anatomical characteristics. This method gave him worldwide success but hid from him the global progress of dactyloscopy. At last, he agreed to add fingerprints to his data sheets. Then, in 1902, he identified the perpetrator of a crime through his fingerprints (Scheffer case) after failing with an anthropometry test [SCI 10].

1.2. Biometrics today

Different biometric modalities have been published. We distinguish between physiological modalities (iris, fingerprints, hand veins, etc.) that are more stable over time, *a priori*, and can be acquired with much difficulty, and behavioral modalities (handwriting, gait, keystroke dynamics, etc.) that are not only more variable but also more natural and can be acquired through simple and user-friendly means. Biological modalities can also be used (cardiac signal, see Chapter 10, DNA). They are more difficult to process for an immediate identification.

Nowadays, it is possible to process biometric data using a computer because we can digitize, store, and retrieve them from databases. This may thus lead to large-scale deployments, which are only made possible because of this "digitization" of personal and corporal information.

Let us take the example of identity documents. Traditionally, our passport contains personal information such as name, filiation, address, height, and eye color (this type of information is nowadays called "soft biometrics" — see Chapter 3). Apart from these textual data, a printed

photograph of the face is also included in this passport (the face image is frontal and more or less recent).

The verification of our identity using this passport was “manually” done by a person who confirmed the identity from the document and printed photograph.

In the new biometric passport, which since late June 2009, is gradually replacing the traditional passport, the personal textual information is contained in the machine readable zone (MRZ) band (at the bottom of the passport) (Figure 1.1). The facial image is digitized and stored in a chip embedded in the passport, as well as the scanned images of two fingerprints. This operation is combined with an encryption process (see Chapter 13) that ensures the safety of data. The identity verification can thus be done fully automatically as follows: the reading and the automatic identification of textual data allow for generating a key giving access to biometric data stored in the chip. The verification itself is then based on an algorithm that measures the similarity between the fingerprints collected during the identity test and those stored in the card.

Figure 1.1. *The new biometric passport*

The advantage of allowing an automatic check is threefold: automate the controls with the aim of introducing less subjectivity, accelerate the flow to increase the number

of travelers, and reduce frauds, especially to detect false documents or multiple documentation for a single person.

1.3. Different modes of use of a biometric system and associated uses

There are several distinct modes of use of a biometric system [JAI 04, DOR 04, DOR 11]. On a large scale, we may want to identify a person among a group of a large number of individuals (e.g. many millions). This is the case of applications such as national identity cards, border controls, electronic voting, judicial police investigations, postmortem identification, and the search for relatives of an abandoned child. This is achieved with the use of a database containing data for characterizing each person and the system will then search for the person who best fits the observed data. The individual is usually aware of this research and the fact that we are acquiring and exploiting their biometric data. Furthermore, the use of biometrics is done in interaction with the inspection or corresponding monitoring services.

The same type of research can be done on a more limited scale. This is called screening. In this case, we want to know whether the observed individual is part of a suspect list (composed of a small number of individuals, usually several hundred). Most of the time in this kind of usage, the research is surreptitiously and discreetly performed. This is the context for airport surveillance and public place surveillance such as at football stadiums. In this case, people are not necessarily aware of being observed and the quality and reliability of the data used (video recording most often) are questionable because the acquisition is made without any “control”.

It may happen, for example, that the camera is placed so far away from the individuals that the size of the face in a shot is very small or even that more faces simultaneously appear in a single shot, thereby increasing the risk of misinterpretation. Despite these limitations, the use of biometric identifiers provides a relatively easy solution to implement for this large-scale identification and screening security need.

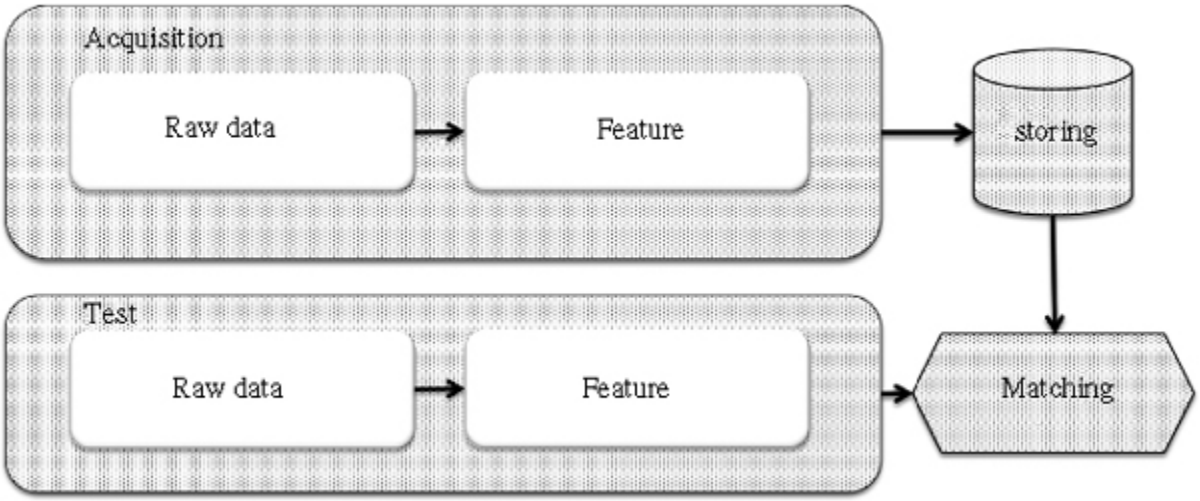
Verifying the identity (authentication) of a single person is an easier task. Thus, in front of an individual coming to a bank counter or at the entrance of a building and claiming to be a known customer, the system will simply make a decision of acceptance or rejection of such person from his or her biometric identifier. In this case, it may not be necessary to store the information about the individual in a database. It can be stored on a smart card held by the customer, allowing a greater confidentiality. The possible uses in this area include the authentication on a personal computer, on a Universal Serial Bus (USB) flash drive, on a cell phone, or even increasing the reliability of electronic banking or legal transactions and the access controls to some places. The success of the implementation of such applications largely depends on the cost involved and the ease of use.

1.4. Biometrics as a pattern recognition problem

The construction of a biometric system passes through the implementation of various modules that are those typically foun in any pattern recognition system. This is, indeed, to process a signal emitted from fairly simple physical sensors (such as cameras and microphones) to determine a higher-level information (Who is the person in front of me? Do

these patterns match that of person X or not?). We thus find processing modules as described in Figure 1.2.

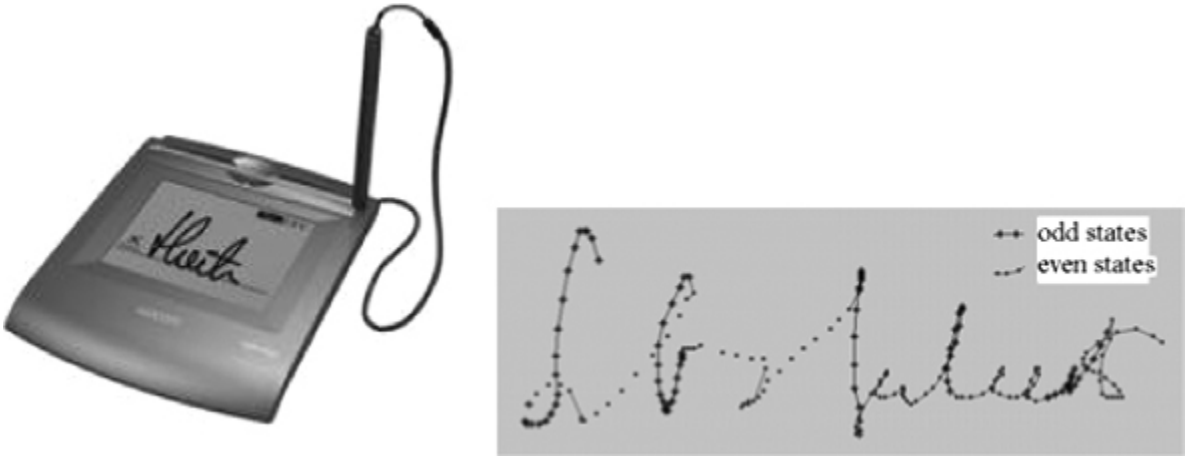
Figure 1.2. *The different modules of a biometric system*



1.4.1. *Capture module: from the sensor to the image*

Each biometric modality is associated with a capture mode. So if we want to process a dynamic signature, we will use a digitizing tablet or a touchscreen interface for retrieving a sequence of points associated with the drawing when we write or sign. A signature will then be associated with a sequence of points in the plane (see Figure 1.3).

Figure 1.3. *Acquisition of dynamic signatures*



An image of the eye can be scanned in order to perform a verification using the iris through infrared sensors that should be placed relatively close to the eye and at a fixed distance, making the acquisition device highly restrictive. The infrared acquisition has the advantage of limiting reflections and making the texture of the iris clearly visible. On the other hand, the field depth of this type of capture is very low. Hence, there is the need to carefully choose the distance between the shooting and the person in order to have a clear image (see Figure 1.4).

Figure 1.4. *Iris sensor and resulting images*

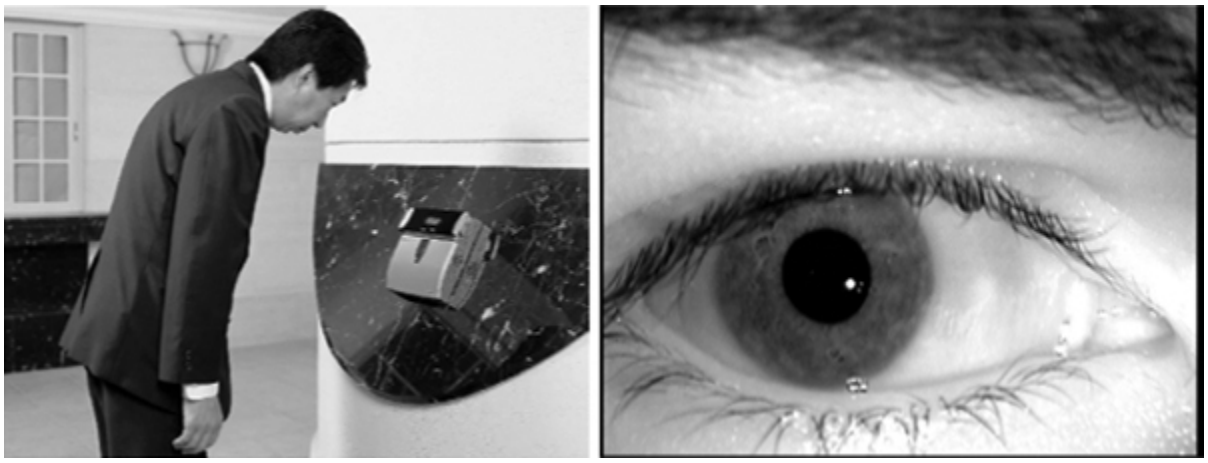


Figure 1.5. *Fingerprint sensors and corresponding signal*

Different types of fingerprint sensors are available on the market. They differ in size and technology (optical, capacitive). Each type of sensor induces fingerprint images that, although they are from the same person and the same

finger, may appear different (more or less contrasted, more or less resolved).

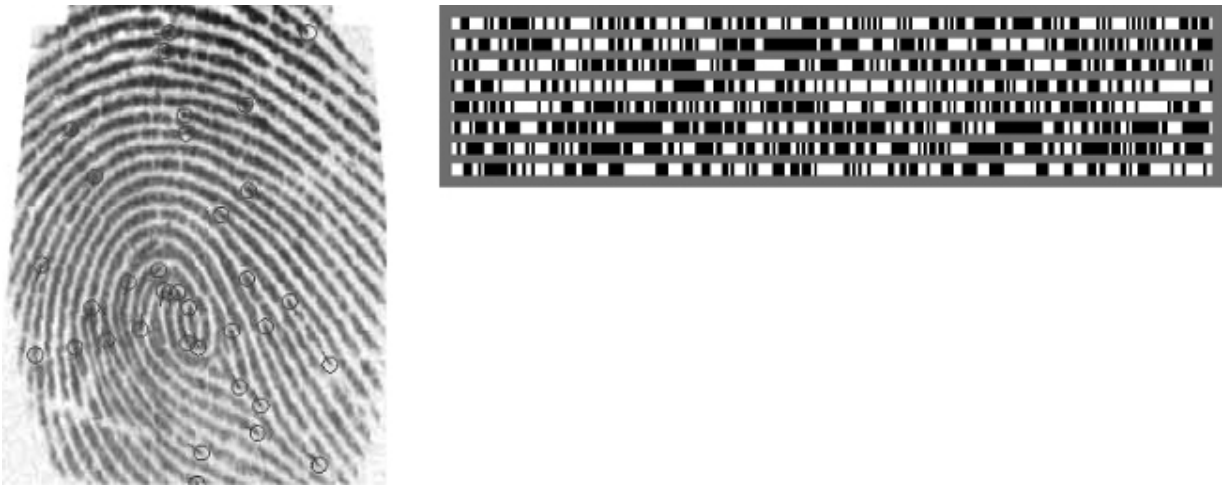
This short overview makes it possible to realize that whatever the modality considered, even if we measure the same corporal data (finger, eye), we have a different digital image at each capture because the acquisition process itself introduces “noise” (finger or eye rotations). Moreover, two different sensors of the same object will yield different images. Finally, the change between two shots also comes from the person himself/herself. This is especially true for behavioral modalities because the way persons walk, the way they write, and the way they type on the keyboard largely depend on their mood and tiredness. But even the iris of the eye, which does not vary much over time *a priori*, may be more or less visible in different images of the eye of a person because it is partially covered by eyelids and eyelashes and is sensitive to pupil dilation (see Chapter 6).

1.4.2. *From the image to the features*

The second phase of the processing is to extract from each image a set of feature vectors. The aim is to obtain a compressed representation of the considered pattern that also increases the distance between two patterns that do not correspond to the same person. The nature of these representations varies considerably according to the biometrics considered. We can obtain vectors associated with well-chosen points in the image (the fingerprints minutiae for instance (see Chapter 8)), vector sequences (as in dynamic speech or signatures). The components of these vectors can be discrete or continuous. For instance, the representation can correspond to a simple sequence of 0s and 1s in the case of the iris.

Examples of such representations are given in Figure 1.6 for fingerprints and the iris.

Figure 1.6. *Minutiae extracted from a fingerprint image (on the left) and binary code of the iris (on the right)*



1.4.3. *The matching*

The decision of the biometric system is based on the result of a comparison between a reference and a test pattern. For this, a similarity measure related to the distance between two feature vectors associated with the patterns to be compared is used.

If an identification is performed, there are two sets of data called “gallery” and “test”. In fact, there is at least one pattern per person in the gallery but there may also be several. The purpose is to determine for each test pattern the most similar pattern in the gallery. A threshold can be used if we want to have the possibility of rejection, i.e., the fact that the test pattern is paired with no data (open identification) when it is sufficiently distant from all the patterns present in the gallery. A classification is then carried out (with rejection) of the test patterns into N classes, where N is the number of patterns in the gallery. The performances of the biometric system are assessed by calculating the correct classification rate in the first position, in the second position, in the first five positions, etc., on labeled databases.

In verification mode, reference data are available for each person. These data are used to build a model of the person after a learning phase or they are just independently stored. In testing phase, an identity is proclaimed and we want to know if the tested data correspond to the reference data of the person whose identity was proclaimed. The aforementioned similarity measure can be used for this purpose. The acceptance or rejection decision is related to a threshold according to which the similarity measure is compared (if the similarity is greater than the threshold, we accept the tested pattern as true; otherwise we reject it). To evaluate the performance of a biometric system in verification mode, we must define for each person in the test set a number of “genuine” patterns and a number of “impostor” patterns. Therefore, a false acceptance rate (FAR — person wrongly recognized as genuine) and false rejection rate (FRR — person wrongly considered as an impostor) can be measured for each value of the decision threshold.

Distances between vectors of identical size (such as the Euclidean, Mahalanobis, and Hamming distances) or elastic distances if the vectors to be compared do not have the same size as is the case for dynamic signatures or speech signals can be used as dissimilarity measures. A statistical model of a person can also be built using several reference samples. In this case, part of the reference samples are used to learn the model parameters for each person. Once the model is learned, the similarity of a test pattern to different people is calculated as the likelihood that the test pattern to be generated by the model of the person in question.

Regardless of the modality, linear or nonlinear projection methods (principal component analysis and the variants) are frequently used to decrease the size of feature vectors before the similarity calculation phase.

1.5. Evaluation of different modalities

Performance evaluation of biometric systems is a difficult problem (see Chapter 11). It requires the availability of large databases representative of the problem addressed and appropriate protocols to compare different systems. Recently, various databases and comparative evaluations have been proposed for speech, facial, and iris biometrics, provided in particular by the US National Institute of Standards and Technology (NIST), allowing us to benchmark the competitors and stimulate research on the residual difficulties of each biometric modality. We can also cite the environmental evaluation released by BioSecure [PET 09].

The comparison of these biometrics among each other is an issue whose interest lies within an applicative context and notably to explain the technological limitations of different modalities with respect to desired error rates in a given application [DOR 11]. Therefore, the sole evaluation of error rate is too restricted. We should also compare the costs, acceptability, and security levels (the ease of being imitated).

Generally, it is considered that the iris, studied in highly constrained conditions, yields a very low FRR rate (of the order of 10^{-3} for a FAR of 10^{-3}). This is a very accurate biometrics but with a high failure attached due to very stringent acquisition conditions. Fingerprints also show very good performances that allow performing identification on a large scale. On the other hand, the quality of the image has a great influence on the performances. Performances in face recognition, a very well-accepted biometrics, vary greatly according to the bases used. These reflect the different degradations and variabilities that may be encountered.

1.6. Quality

The evaluation of the quality of biometric signals is a very important factor at the operational level but it is still relatively unexplored, perhaps because measuring a signal or image quality is not an easy task. In fact, this measure may reflect three factors: first, does the signal correspond to what we want to measure? Thus, we will consider as bad the image of an eye with most of the iris occluded by the eyelids or a fingerprint largely damaged by a scar.

Secondly, we seek to measure the fidelity of the signal measured at the source. We then have to measure the noise associated with the acquisition of the biometric data (blur on the images, background noise on a voice signal, etc.). Finally, we may also want to qualify a biometric pattern as good if it allows us to achieve good performance during the verification. In other words, we want to qualify it on the basis of its impact on the system performance. In the latter case, the quality measure provided will be directly linked to the classifier used.

These quality measures have several uses: first, a signal of poor quality may be simply removed and can justify asking the user for a new acquisition. This is, for instance, the case at the outset for identity papers requests or during the verification phase, if there are several test samples, to be able to choose which one to use. This quality criterion can also be used during the identification phase to determine if a person deliberately provides a poor-quality sample to escape the system.

In some cases, it is not possible to ask the user for a new acquisition. Measuring the quality of the signal thus allows us to know whether it is necessary to introduce a preprocessing before the extraction phase of the parameters itself. For instance, a measure of the illumination on a facial image could lead to propose an

algorithmic processing in order to overcome the floodlight effects.

The question “how to use quality measures to forecast the performances of the matching?” is a matter of discussion and is responsible, among others, for the evaluation [IRE 10] organized by NIST and aims to identify the most important defects (occlusion, lack of focus, blur, etc.) on images of eyes that can degrade the performances of iris systems. In fact, a matching is performed between two images, a reference and a test. We can therefore consider the two associated quality measures. All the experiments show that when the reference sample is of good quality and better than the test sample, the quality of the test sample is sufficient to forecast the performance. On the contrary, if the quality of the reference sample is not good, the performance during the test phase is degraded regardless of the quality of the test samples. In fact, it is mostly the false rejections that are being reduced by the choice of good-quality images. For this reason, quality control during the registration is very important and embedded in most of the biometric trait capture devices in fingerprints [TAB 05]. Similarly, iris sensors that acquire an image sequence of the eye also feature an embedded quality control. The image is only captured when it is of a really good quality (eye at the correct distance from the sensor, iris sufficiently visible, clear image). Recently, quality criteria of dynamic signatures (acquired on a digitizing tablet) have also been proposed on the basis of calculation of an entropy measure of the signal [GAR 09]. The quality can be measured by an integer or a real number, or even by the fusion of several indicators. This quality value can then be integrated into the classifier itself in several ways that are still a subject of scientific exploration [POH 11] for improving the classifier performance.

1.7. Multimodality

As we often rely on several modalities (voice, gait, face) to recognize a person, multimodality is presented as a means to overcome the difficulties that result from the use of a single biometric trait (see Chapter 9). Thus, we first hope to increase the recognition performances by reducing the errors, especially when one of the modalities is tainted by noise (for instance, voice coarsened by a cold, face altered by glasses or beard), or is missed. The fusion of information can be performed sequentially (the best classifier is first used and then the others, ordered by decreasing quality) [ALL 10] or at the same time (all the classifiers are used simultaneously and their results are merged). In this case, there are several types of fusion, depending on the level of abstraction where this fusion is performed. If each system corresponds to a black box, which is the case of commercialized systems, we can only merge decisions or scores. The contribution of the fusion will be even more important in that the modalities are independent and therefore complementary [ALL 11]. If we have access to the different modules, we can perform a fusion of images or features that will bring even more improvement than the fusion at the score or decision level.

A multimodal system is also more difficult to forge. We can imagine easily deceiving a face recognition system with a photograph or a voice system with a recording. However, it will be more difficult to forge a system that recognizes within a video a speaking face by explicitly using the synchronization of lip motion with the uttered sentence because it is more complicated to artificially fabricate such videos.

However, it should be noted that the implementation of a multimodal biometric system imposes a significant cost because it generally introduces the need for different sensors and increases the number of necessary processings

and especially because obtaining improved performance is only possible through a fine-tuning of the fusion parameters that should be performed in a configuration phase of the system.

1.8. Biometrics and preservation of privacy

If it turns out to be technically possible, then the large-scale deployment of biometrics will require finding some solutions, which allow us to address the demands of citizens in terms of security and preservation of privacy.

This is first to ensure the security of biometric systems against possible attacks. These attacks can occur at different levels of the processing chain. Thus, an impostor might want to impersonate another person by submitting fingerprints of that person to the system input, printed on a fake finger or a latex glove, prints that the impostor would have left on a glass or another surface. In fact, our fingerprints are not secret; we leave traces of them that can be recovered without our knowledge. This, may seem like science fiction, but is actually not that difficult to do as shown by [MAT 02]. Nowadays, many studies are devoted to developing counterattacks to this type of forgery, notably by adding sensors to detect the living nature of a finger [GAL 12].

The biometric data (or features) that are stored in a smart card or on a database are usually encrypted, but one of the characteristics of biometric data is that, unlike a PIN code or a password, they are not revocable. We cannot change our fingerprints or iris in case of theft or loss of our biometric passport. That is why the concept of revocable biometrics has recently emerged [RAT 06], which proposes the addition of a key that will be revocable when needed.

A number of fears about the centralized storage of biometric data limits the use of biometrics in developed countries and particularly in France. The risk of profiling, data misappropriation, and database crossing (state and commercial) thus encourage the French legal regulation agency “Commission Nationale Informatique et Liberté” (CNIL) to prefer biometric systems where the data are stored on a smart card and to only issue an authorization to implement a biometric system using databases according to a proportionality principle (using biometrics only if the security needs justify it). Biometrics without traces (signature, veins of the hand) is also appreciated because it is more difficult for a possible impostor to recover them.

When the use of a centralized database cannot be avoided, we have to propose data security techniques such as anonymization, encryption, and revocation of biometric data.

1.9. Conclusion

It is now widely accepted that biometrics is an interesting tool to verify the identity of individuals, identify or reidentify them. In fact, this technique allows us to automatically process large amounts of information (with little or no human intervention) and, similarly, to reduce the subjectivity of manual processings. Moreover, it allows us to find someone whose other identifying information has been lost (postmortem identification for example). The use of biometrics should make it harder for fraud, and therefore helps to reduce it.

However, biometrics presents a number of disadvantages. In fact, there is a variability of digital data related to single personal data that introduces errors in the recognition system. Therefore, it is important to consider this factor in the use of these “automatic” systems.