Alma Mater Studiorum – Università di Bologna

Dottorato di Ricerca in Ingegneria Elettronica, Informatica
e delle Telecomunicazioni

Ciclo XXI

ING-INF/05

Biometric Fingerprint Recognition Systems

Tesi di Dottorato di:

Dott. **Matteo Ferrara**

Relatore:

Chiar.mo Prof. Ing. **Dario Maio**

Coordinatore:

Chiar.ma Prof.ssa Ing. **Paola Mello**

Esame finale anno 2009

INDEX

Index

INTRODUCTION

Biometric systems are automated methods for the identification of individuals based on their physiological (e.g. fingerprint, face, hand, retina, iris) or behavioral (e.g. voice, handwriting, keystroke style) characteristics. Biometric traits, differently from passwords and ID cards, cannot be easily altered, transferred, forgotten, lost or copied. In the past few years, academic and industrial interest in biometric systems had been considerably increased by the growing demand for reliable authentication techniques and by the availability of low-cost acquisition devices. In fact, automated identification systems can be very useful in several applications: access control, time and attendance systems, automatic surveillance, data protection, network security and secure web transactions. Among others, access control verification for computer systems and environmental surveillance are today the most promising application fields for these new technologies.

Fingerprints are a very good solution in terms of uniqueness and acceptability; for this reason, they are widely adopted in civil and government applications. Moreover, nowadays automated fingerprint recognition is very fast and well suited to real-time applications. Originally, the use of fingerprints was limited to the forensic field as evidence for identification of criminals, but in the past few years several applications grew both in the civil and government field. Thanks to the increasing interest on their potential applications, research and investments in fingerprint-recognition systems considerably grew. Although this type of recognition systems are already available in the market, the research in this field is still particularly active for the following reasons: the need for making these systems more reliable and to limit their impact on privacy, and for developing suitable methodologies to evaluate their performance and to certificate their security level.

The aim of this work is to study some of the main problems of fingerprint-based

biometric systems and to provide innovative solutions. To this purpose, firstly the evaluation and certification of the different aspects of these systems have been analyzed, from the quality of fingerprints and acquisition devices, to the accuracy of the whole fingerprint-recognition systems and the performance of its individual modules. Secondly, a new recognition algorithm specifically-designed to achieve a high performance even on light hardware (e.g. smartcards and embedded systems) has been proposed.

The materials presented in this thesis are the result of three years of research activities and experimentations, as shown by the publications cited in bibliography [1] [2] [3] [4] [5] [6] [7] [8].

The first chapter provides a general introduction to the problem, describing biometric systems and fingerprints in detail, together with their main applications and major issues.

The second chapter explains the contributions to fingerprint acquisition devices quality-certification. At first, the specifications and the standards currently at the state-of-the-art are presented in detail. Then, a well-defined testing protocol is described and, following this protocol, a set of experiments to measure the effective impact of such specifications on the performance of automatic fingerprint recognition systems is carried out. Starting from the experimental results obtained, three new sets of balanced requirements, to certify fingerprint scanners' quality, are proposed. Finally, the new specifications are compared with the state-of-the-art, showing that the new ones allow a better trade-off between the cost to produce a compliant scanner and the expected recognition performance on images acquired by that scanner. At present, the Italian National Center for ICT (CNIPA) uses these new specifications as a point of reference for the Italian biometric passport and identity card.

The third chapter presents a new fingerprint recognition algorithm based on a novel 3D minutia local structure representation. Thanks to the local structure invariance, fixed-length and bit-oriented coding, some simple but very effective metrics have been defined to compute local similarities and to consolidate them into a global score. Then the proposed algorithm is compared, on a reference benchmark, with three well-known techniques; the experimental results definitely prove its superiority and demonstrate the feasibility of obtaining a very effective (and interoperable) fingerprint recognition implementation for light platforms. The new algorithm is so promising that a patent has

been filed on it.

The fourth chapter reports the work developed in the field of the performance evaluation of fingerprint recognition systems. In particular, the chapter discusses the organization and the results of the international competition *FVC2006* and the design, development and organization of a revolutionary new approach to performance evaluation of fingerprint-based systems: *FVC-onGoing*.

Finally, the last chapter reports some concluding remarks on the work done and discusses possible future works.

1

BIOMETRIC SYSTEMS AND FINGERPRINTS

1.1 Biometric Systems

Rapid advancements in the field of communications, computer networking and transportation, coupled with heightened concerns about identity fraud and national security, has resulted in a pronounced need for reliable and efficient identity management schemes in a myriad of applications. Traditional authentication techniques based on passwords and tokens can easily be lost, shared manipulated or stolen thereby compromising the intended security. The advent of biometrics has served to address some of the shortcomings of traditional authentication methods [8].

Biometrics is the science of recognizing the identity of a person based on the physical or behavioral attributes of the individual; therefore, a biometric system is essentially a pattern recognition system able to verify or recognize the identity of a living person on the basis of some physiological characteristics, like a fingerprint or iris pattern, or some aspects of behavior, like handwriting or keystroke patterns (see Figure 1.1).

The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Question such as “Is this person authorized to enter the facility?”, “Is this individual entitled to access the privileged information?”, and “Did this person previously apply for a job?” are routinely asked in a variety of organizations in both public and private sectors.

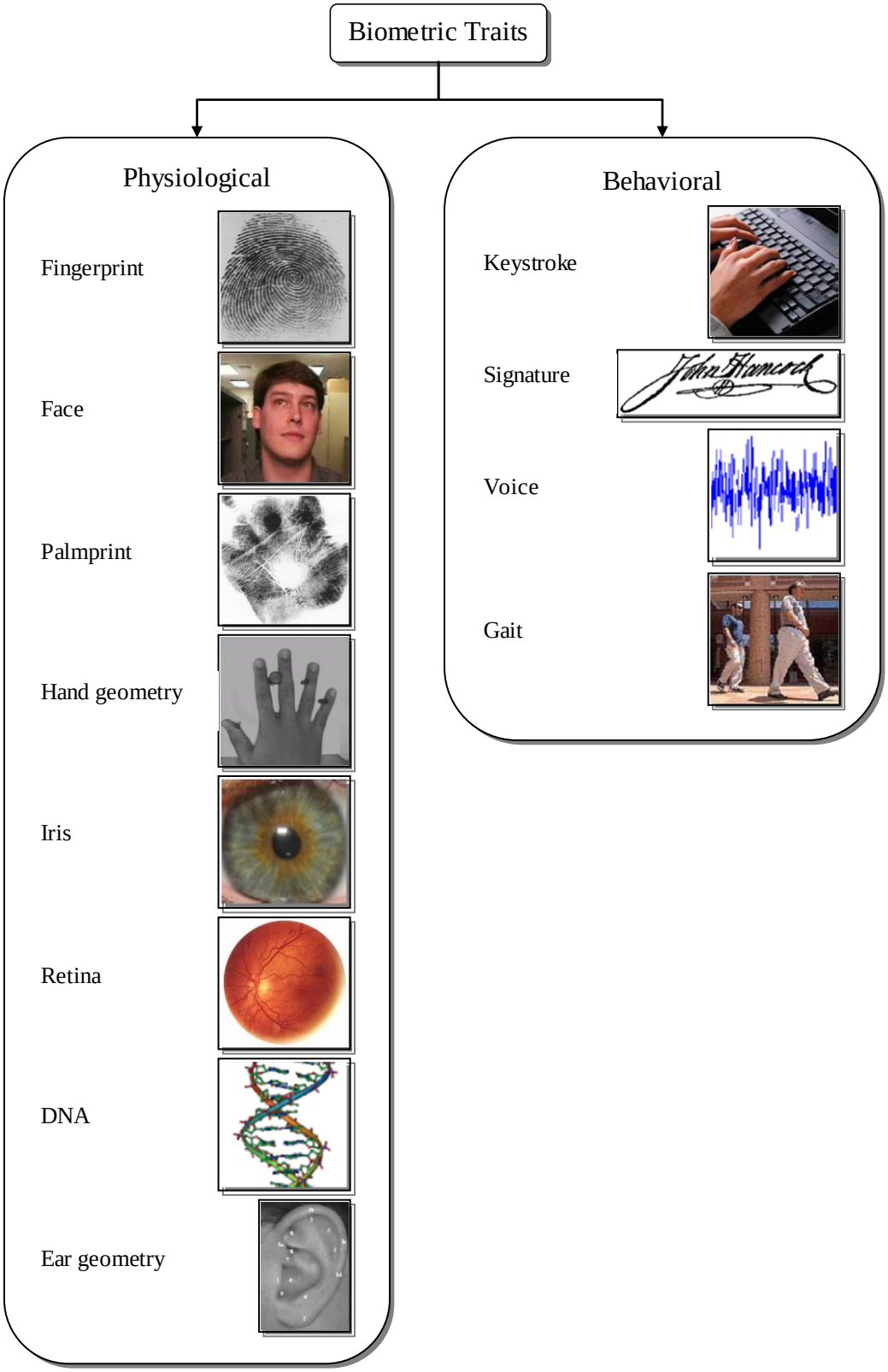


Figure 1.1 - Classification of most common biometric traits. Other biometric strategies are being developed such as those based on hand and finger veins, ear canal, facial thermogram, odor and footprints.

Chapter 1: Biometric Systems and Fingerprints

Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods based on credentials (passwords, PINs and IDs).

This is because biometrics links the event to a particular individual (based on “who you are” and not “what you know” like passwords and PINs or “what you have” such as ID card), is convenient (nothing to carry or remember), accurate and is becoming socially acceptable and inexpensive..

Although biometric technologies vary in complexity, capabilities, and performance, they all share several elements. Biometric identification systems are essentially pattern recognition systems. They use acquisition devices such as cameras and scanning devices to capture images, recordings, or measurements of an individual’s characteristics, and they use computer hardware and software to extract, encode, store, and compare these characteristics. Because the process is automated, biometric decision making is generally very fast, in most cases taking only a few seconds in real time.

1.1.1 A Historical Overview

The term "biometrics" is derived from the Greek words *bios* (life) and *metron* (to measure).

The ancient Egyptians and the Chinese played a large role in biometrics' history. Although biometric technology seems to belong in the twenty-first century, the history of biometrics goes back thousands of years. In early Egyptian history, traders were identified by their physical descriptors to differentiate between trusted traders of known reputation and previous successful transactions, and those new to the market. Possibly the first known example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that Chinese merchants used fingerprints to settle business transactions and Chinese parents also used fingerprints and footprints to differentiate children from one another.

Others date the origins of biometrics in the 1890s to Alphonse Bertillon. He was an anthropologist and police desk clerk in Paris when he sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed a method of multiple body measurements (including such measures as skull

diameter, arm and foot length, shapes of the body in relation to movements and differential markings on the surface of the body such as scars, birth marks, tattoos, etc.) used by police authorities throughout the world for identification purpose (see Figure 1.2). Bertillon's system of identification was not without fault. For example, it relied heavily on precise measurements for identification purposes, and yet two people working on measurements for the same person would record different findings.

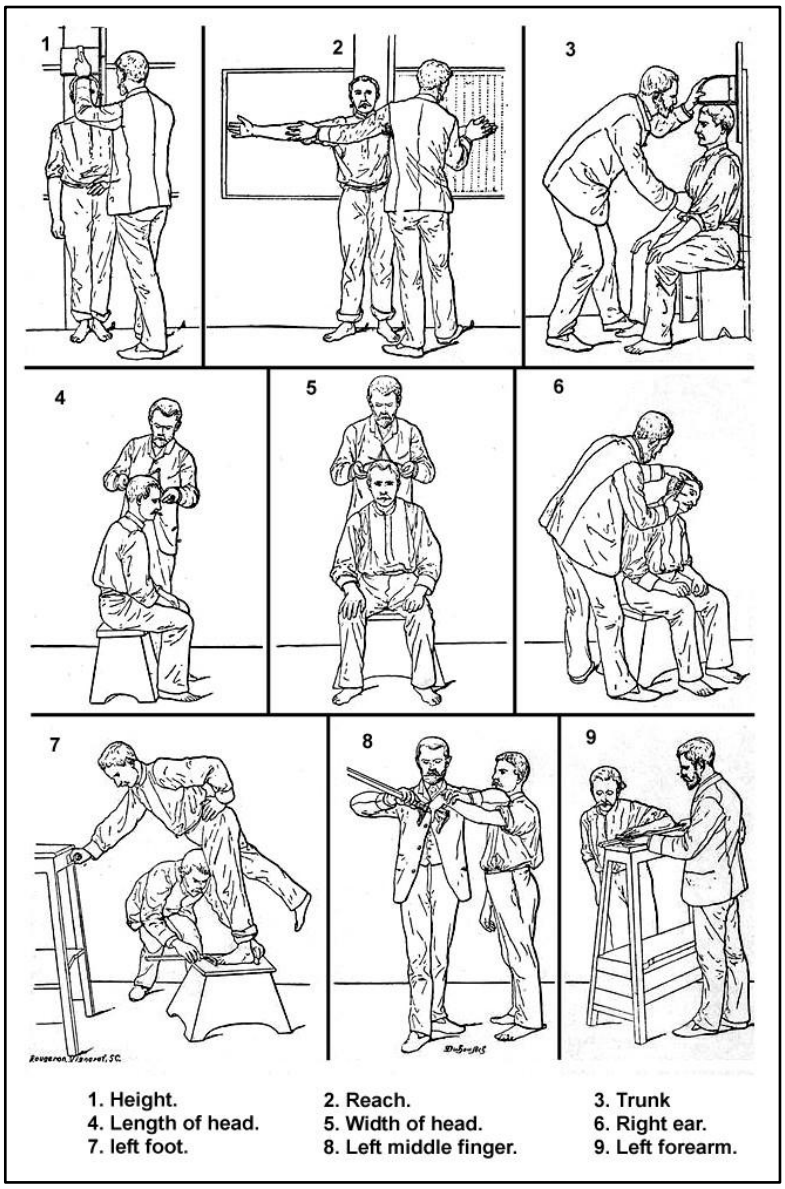


Figure 1.2 - Diagram of Bertillon Measurements.

Additionally, it turned out to be the case that the features by which Bertillon based his identification system were not unique to any one individual. This led to the possibility

of one person being convicted of another person's crimes. This possibility became abundantly clear in 1903 when a Will West was confused with a William West. Though it would later turn out to be the case that the two were identical twins, the issues posed by the Bertillon's system of identification were clear. After the failure of anthropometry, the police started using finger printing on the scene, as a more efficient and accurate means of identification, which was developed by Richard Edward Henry of Scotland Yard, essentially reverting to the same methods used by the Chinese for years.

True biometric systems began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems. In the 1960s and '70s, signature biometric authentication procedures were studied, the first semi-automatic face recognition system was developed by W. W. Bledsoe under contract to the US government, the first model of acoustic speech production was created by Gunnar Fant, and the Federal Bureau of Investigation (FBI) began its activity of developing a system to automate its fingerprint identification process.

Due to the growing demand for automatic personal recognition in our society, biometric systems have rapidly grown beyond forensic into civilian applications. Companies involved with new systems number in the hundreds and continue to improve their methods as the technology available to them advances. Prices for the hardware required continue to fall, making systems more feasible for low and mid-level budgets. As the industry grows however, so does the public concern over privacy issues. Laws and regulations continue to be drafted and standards are beginning to be developed.

Although finger printing is the most popular biometric characteristic still in use today, other biometric technologies started developing rapidly in the last quarter of the twentieth century. These techniques sought to measure human voices, hands, irises, retina, faces, etc. (see Figure 1.1).

1.1.2 A Generic Biometric System Model

Although biometric systems that use different biometric characteristics are relied on widely different technologies, in general, they are based on the same core structure. Fundamentally, a biometric system is a pattern recognition system that acquires

biometric data from an individual, extracts a salient feature set from the data, compares this feature set against the feature set(s) stored in a database, and executes an action based on the result of the comparison [8]. Therefore, a generic biometric system can be viewed as having four main modules (see Figure 1.3): i) a sensor module that defines the human machine interface, ii) a feature extraction module that extracts a set of relevant discriminatory features from the acquired data to represent the underlying trait, iii) a matching module that compares the extracted features against the stored template to generate a match score, and iv) a database module that stores biometric information.

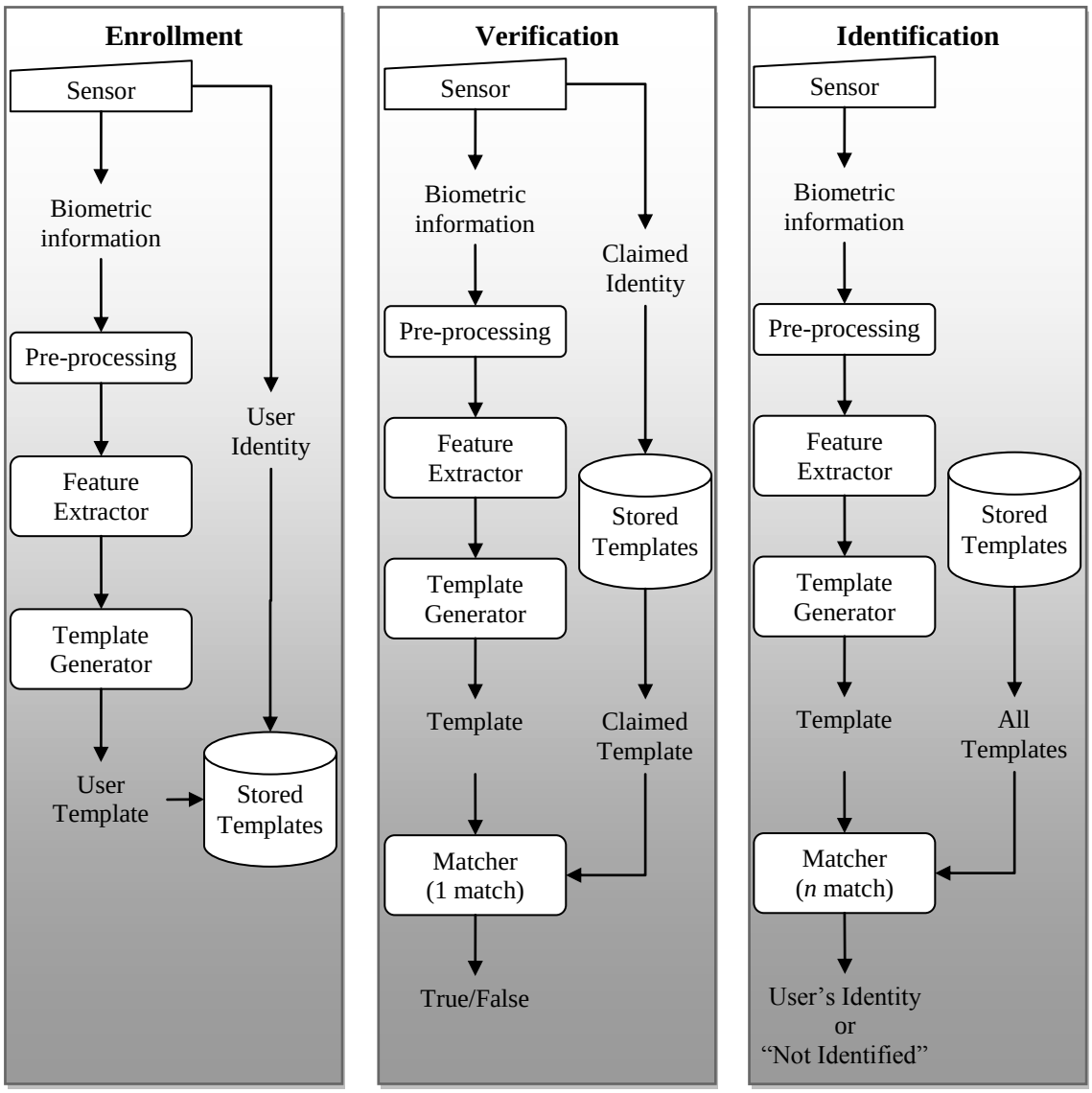


Figure 1.3 - The basic block diagrams of a generic biometric system.

An important issue in designing a biometric system is to determine how an individual is recognized. Depending on the particular application context, a biometric system may operate either in the verification or/and identification mode. In the former, the system confirms or refuses an individual's identity by comparing the acquired data with the biometric template (corresponding to the claimed identity) stored in the database. Whereas in the latter, the system performs a one-to-many comparison to recognize the person's identity or fail if the subject is not stored in the database. Figure 1.3 shows the block diagrams of a generic biometric verification and identification systems. Both recognition modes have in common the enrollment stage; in the enrollment phase, the biometric characteristic is acquired by a biometric reader, a quality check is performed to guarantee the acquired data, the digital representation of the characteristic is processed to produce a compact representation called *template*, finally the resulting template is stored in the biometric database. In the verification task, first personal identification information (user's name, PIN, etc.) is provided and a template is produced acquiring the characteristic of the individual using the biometric reader and processing it by the feature extractor. Then, the acquired template is compared against the template of a single user, retrieved from the database using the provided personal identification information. Instead, in the identification task, no personal identification information is given and the matching module compares the input template against all the templates contained in the system database. The result is either the identity of an enrolled person or the message "not identified".

1.1.3 Performance of a biometric system

A biometric system rarely encounters two samples that result in exactly the same feature set. In general, this is due imperfect sensing conditions (e.g., noisy fingerprint due to sensor malfunction), alterations in the user's biometric characteristic (e.g., respiratory ailments impacting speaker recognition), changes in ambient conditions (e.g., inconsistent illumination levels in face recognition) and variations in the user's interaction with the sensor (e.g., occluded iris). The variability observed in the biometric feature set of an individual is referred to as *intra*-class variation, and the variability between feature sets originating from two different individuals is known as

inter-class variation. A useful set exhibits small intra-class variation and large inter-class variation [8]. The response of a matcher in a generic biometric recognition system is usually a *similarity score* s that measures the similarity between two biometric feature sets. The system decision is regulated by a *threshold* t: pairs of feature sets generating similarity score higher than or equal to t are called *matching pairs*; whereas pairs producing scores lower than t are called as *non-matching pairs*. A similarity score is known as a *genuine* score if it is a result of matching two biometric samples of the same user; it is known as an *impostor* score if it involves comparing two biometric samples originating from different users.

A generic biometric verification system makes two types of errors: i) mistaking biometric measurements from two different individuals to be from the same one (called *false match* or *false acceptance*) and ii) mistaking two biometric measurements from the same person to be from two different persons (called *false non-match* or *false rejection*). In a biometric system, the *False Match Rate* (FMR) can be defined as the probability that an impostor score exceeding the threshold t; in the same way, the *False Non-Match Rate* (FNMR) may be defined as the probability that a genuine score falling below the threshold t. Generally to evaluate the accuracy of a generic biometric system one must collect scores produced from a number of genuine matching (called *genuine distribution*), and scores generated from a number of impostor matching (called *impostor distribution*). Figure 1.4 reports FMR and FNMR over genuine and impostors distributions:

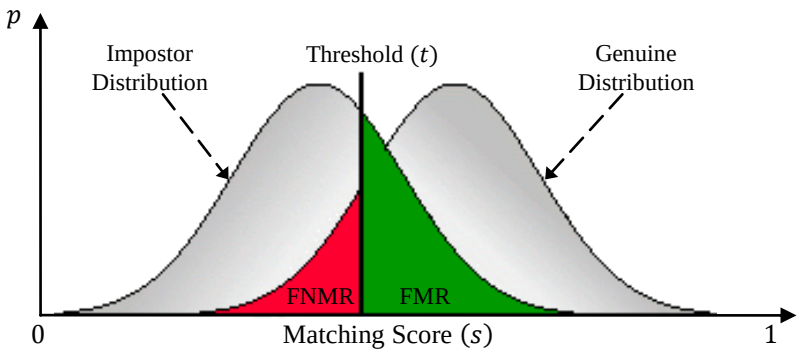


Figure 1.4 - FMR and FNMR for a given threshold t are displayed over the genuine and impostor score distributions.

As shown in Figure 1.4 FMR and FNMR are functions of the system threshold t. If t is decreased to make the system more tolerant the FMR increases and FNMR decreases; vice versa, if t is raised to make the system more secure, then FMR decreases and FNMR increases. A system designer may not know in advance the particular application for which the system may be used. So it is advisable to report system performance at all operating points (threshold, t) [9]. The FMR and FNMR at various values of t can be summarized using a *Detection-Error Tradeoff* (DET) curve that plots the FNMR against the FMR at various threshold and provides a more direct view of the error-vs-error tradeoff (see Figure 1.5).

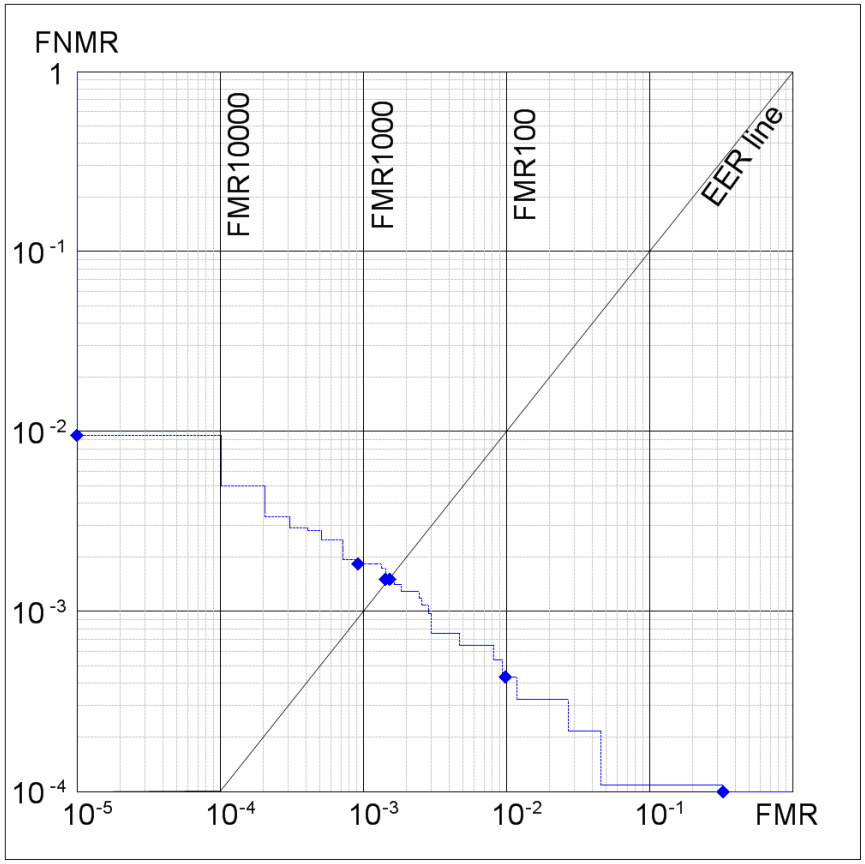


Figure 1.5 – An example of DET graph.

Additionally to the above distributions and curves, some "compact" indices are also used to summarize the accuracy of a generic biometric verification system [9] [10]:

- *Equal-Error Rate* (EER) denotes the error rate at the threshold t for which FMR and FNMR are identical (see Figure 1.6);

- *ZeroFNMR* is the lowest FMR at which no FNMR occur (see Figure 1.6);
- *ZeroFMR* is the lowest FNMR at which FMR occur (see Figure 1.6);
- $FMRx$ is the lowest FNMR for $FMR \leq \frac{1}{x}$;
- $FNMRx$ is the lowest FMR for $FNMR \leq \frac{1}{x}$;

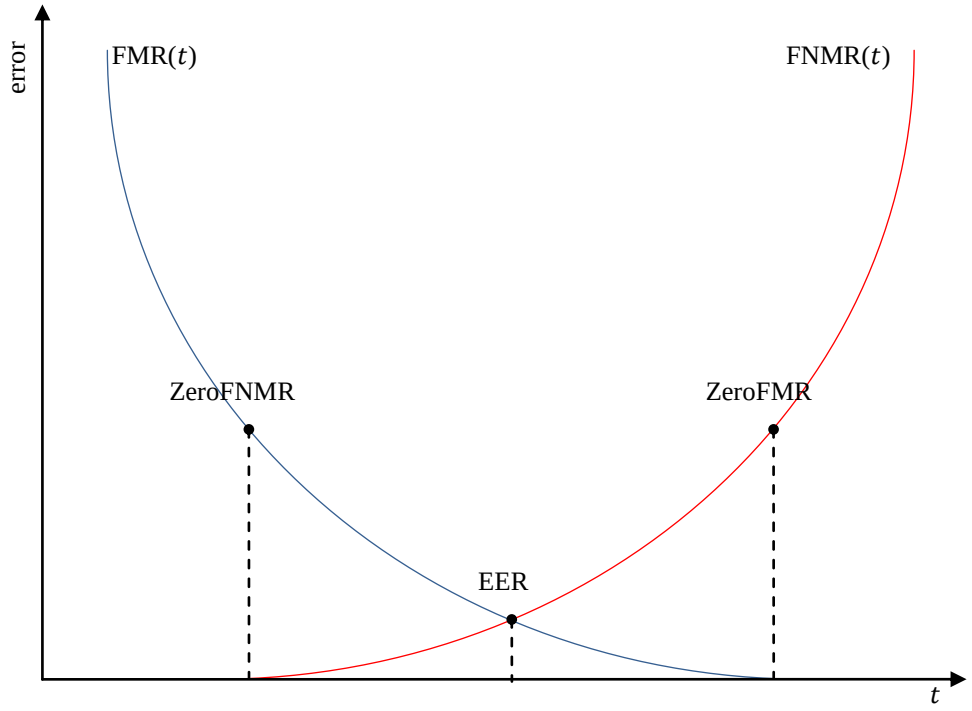


Figure 1.6 - An example of FMR and FNMR curves, where the points corresponding to EER, ZeroFNMR, and ZeroFMR are highlighted.

The real performance requirements of a biometric system are very much application related. For example, in some forensic applications such as criminal identification, it is the FNMR that is a major attention and not the FMR: that is, we do not want to ignore a criminal even at the risk of manually examining a large number of potential matches identified by the biometric system. At the other extreme, a very low FMR may be the most important factor in a highly secure access control application, where the primary objective is not to let in any impostors although we are concerned with the possible inconvenience to legitimate users due to a high FNMR [9].

In the same way, the performance estimation of a generic biometric identification system can be derived by the error estimates in the verification mode.

1.1.4 Biometric characteristics

A large number of biometric characteristics are being used in various applications (see Figure 1.1) and the choice of a biometric trait for a specific use depends on a multiplicity of issues besides its matching performance. Jain et al. [11] have detected seven factors that determine the correctness of a biometric trait to be used in a specific biometric application.

1. **Acceptability:** Peoples in the target population that will use the application should be disposed to present their biometric characteristic to the system;
2. **Circumvention:** This refers to the simplicity with which the attribute of a person can be imitated;
3. **Collectability:** It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause unjustified inconvenience to the individual;
4. **Performance:** The recognition accuracy and the resources required to achieve that accuracy should be meet the constraints imposed by the application;
5. **Permanence:** The biometric characteristic should be sufficiently invariant over a period of time with respect to the matching algorithm;
6. **Uniqueness:** The given trait should be adequately different across persons comprising the population;
7. **Universality:** Every individual accessing the application should possess the characteristic.

Table 1.1 shows a comparison of existing biometric characteristics in terms of those parameters. No single biometric trait is expected to effectively meet all the requirements imposed by all applications.

There is no overall best biometric trait, since the biometric trait most suited to a given application depends on many aspects, including the nature and requirements of the application itself [8]. On the other hand, from Table 1.1 it is clear that fingerprint recognition has a very good balance of all the desirable properties. Every human being possesses fingerprints, with the exception of any hand-related disabilities. Fingerprints are very distinctive; fingerprint details are permanent, even if they may momentarily change slightly to cuts and bruises on the skin or weather conditions. This is fingerprint recognition is one of the most largely adopted biometric technologies (see Figure 1.7).

Table 1.1 - Comparison of various biometric technologies (H=High, M=Medium, L=Low). A low ranking indicates poor performance in the evaluation criterion whereas a high ranking indicates a very good performance [12].

	Acceptability	Circumvention	Collectability	Performance	Permanence	Uniqueness	Universality
DNA	L	H	L	H	H	H	H
Ear	H	M	M	M	H	M	M
Face	H	L	H	L	M	L	H
Facial thermogram	H	H	H	M	L	H	H
Fingerprint	M	H	M	H	H	H	M
Gait	H	M	H	L	L	L	M
Hand geometry	M	M	H	M	M	M	M
Hand vein	M	H	M	M	M	M	M
Iris	L	H	M	H	H	H	H
Keystroke	M	M	M	L	L	L	L
Odor	M	H	L	L	H	H	H
Palmprint	M	M	M	H	H	H	M
Retina	L	H	L	H	M	H	H
Signature	H	L	H	L	L	L	L
Voice	H	L	M	L	L	L	M

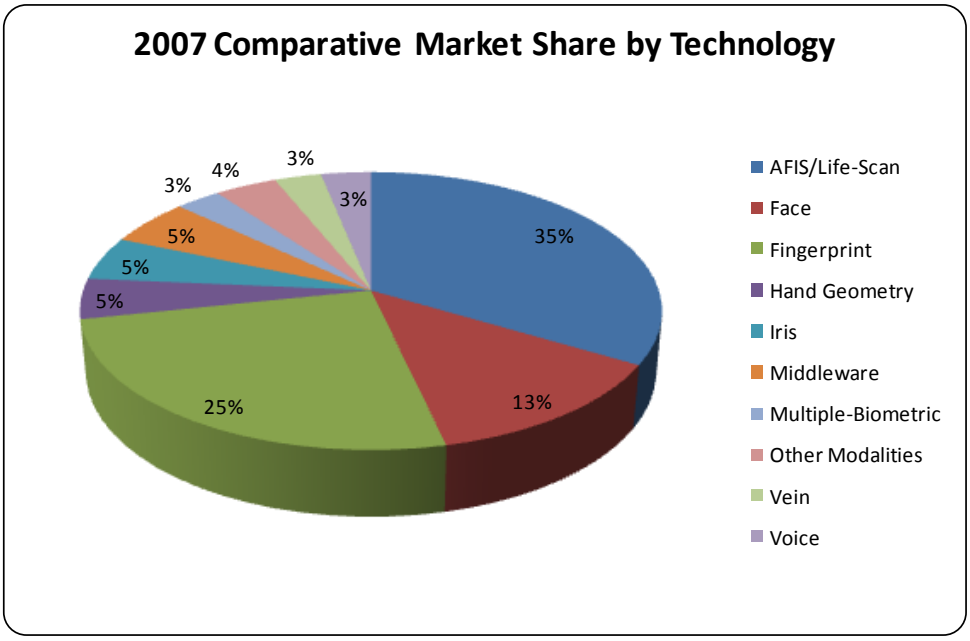


Figure 1.7 – Biometric Market Report estimated the revenue of various biometrics in the year 2007.

1.2 Fingerprints

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip (see Figure 1.8) whose formation is determined during the first seven months of fetal development [8] and ridge configurations do not change throughout the life of a person except due to accidents. By definition, identical twins cannot be distinguished based on DNA and most of the physical characteristics such as body type, voice and face are very similar. Although the minute details in the fingerprints of identical twins are different [13]. These properties make fingerprints a very attractive biometric characteristic.

Figure 1.8 – Example of a portion of the fingertip's surface.

1.2.1 History

Fingerprints have been found on ancient Babylonian clay tablets, seals, and pottery. They have also been found on the walls of Egyptian tombs and on Minoan, Greek, and Chinese pottery — as well as on bricks and tiles in Babylon and Rome. Some of these fingerprints were deposited unintentionally by workers during fabrication; sometimes the fingerprints served as decoration. However, on some pottery, fingerprints were impressed so deeply that they were likely intended to serve as the equivalent of a brand label.

Fingerprints were also used as substitutes for signatures. In Babylon (from 1885-1913 B.C.E.), in order to protect against forgery, parties to a legal contract impressed their

fingerprints into the clay tablet on which the contract had been written. By 246 B.C.E., Chinese officials impressed their fingerprints in clay seals, which were used to seal documents. With the advent of silk and paper in China, parties to a legal contract impressed their handprints on the document. Sometime before 851 C.E., an Arab merchant in China, Abu Zayd Hasan, witnessed Chinese merchants using fingerprints to authenticate loans. By 702 C.E., Japan had adopted the Chinese practice of sealing contracts with fingerprints. Supposedly, in 14th century Persia, government documents were authenticated with thumbprints.

Although the ancient peoples probably did not realize that fingerprints could identify individuals, references from the age of the Babylonian king Hammurabi (1792-1750 B.C.E.) indicate that law officials fingerprinted people who had been arrested. In China around 300 C.E. handprints were used as evidence in a trial for theft. In 650 C.E., the Chinese historian Kia Kung-Yen remarked that fingerprints could be used as a means of authentication. In his Jami al-Tawarikh, Persian official and physician Rashid-al-Din Hamadani (1247-1318) comments on the Chinese practice of identifying people via their fingerprints: "Experience shows that no two individuals have fingers exactly alike."

It was not until the late sixteenth century that the modern scientific fingerprint technique was first initiated; in 1684, the English, Nehemiah Grew, published the first scientific paper reporting his study on the ridge, valley, and pore structure in fingerprints.

Since then, a large number of researcher have invested huge amounts of effort on fingerprint studies.

An important advance in fingerprint recognition was made in 1899 by Edward Henry, who established the “Henry system” of fingerprint classification.

In the early twentieth century, fingerprint recognition was formally accepted as a valid personal identification method and became a standard routine in forensics.

With the rapid expansion of fingerprint recognition in forensics, operational fingerprint databases became so huge that manual identification became infeasible (in 1924 the FBI databases contained over 800.000 fingerprint cards; today stands well over 200 million cards and the number is continuously growing). In 1969, the FBI (Federal Bureau of Investigation) and NIST (National Institute of Standards and Technology) began to invest a large amount of effort to develop a system to automate its fingerprint identification process [9]. Their efforts were so successful that today, almost every law

enforcement agency worldwide uses a commercial IAFIS (Integrated Automated Fingerprint Identification System).

Automatic fingerprint recognition technology has now rapidly grown beyond forensic applications into civilian applications. In fact, fingerprint-based biometric systems are so popular that they have almost become the synonym for biometric systems [9].

1.2.2 Analysis and Representation

The term fingerprint normally refers to an impression of the friction ridge of the last joint of fingers and thumbs. Fingerprints may be deposited in natural secretions, made by ink transferred from the peaks of friction skin ridges to a relatively smooth surface such as a fingerprint card or acquired by directly sensing the finger surface with an electronic fingerprint scanner [9].

The most evident structural characteristic of a fingerprint is a pattern of interleaved *ridges* and *valleys* often run in parallel (see Figure 1.9).

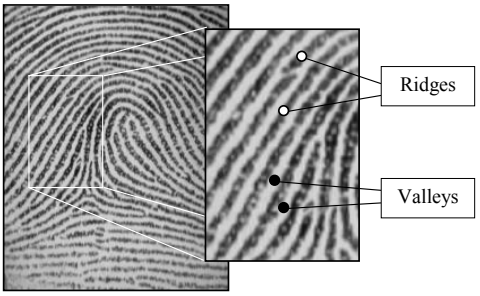


Figure 1.9 - Ridges and valleys in a fingerprint image.

When analyzed at the global level, the fingerprint pattern exhibits one or more zones where the ridge lines assume distinctive shapes. These zones, called *singularities*, may be classified into three categories: *loop*, *delta*, and *whorl* (see Figure 1.10) [9].

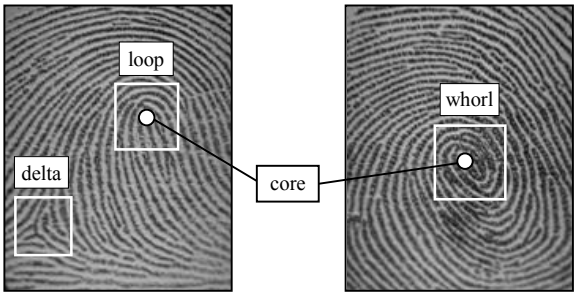


Figure 1.10 - Singular regions (white boxes) and core points (small circles) in fingerprint images.

At the local level, important features, called *minutiae* can be found in the fingerprint pattern. The term *minutia* refers to various ways that the ridges can be discontinuous (see Figure 1.11) [9]. Each minutia is denoted by its type, the *x*- and *y*-coordinates and the angle between the tangent to the ridge line at the minutia position and the horizontal axis (see Figure 1.12).

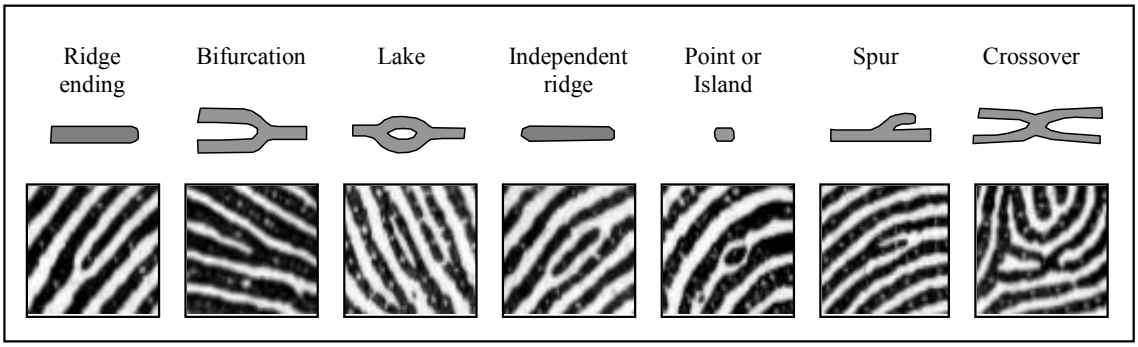


Figure 1.11 - Seven most common minutiae types.

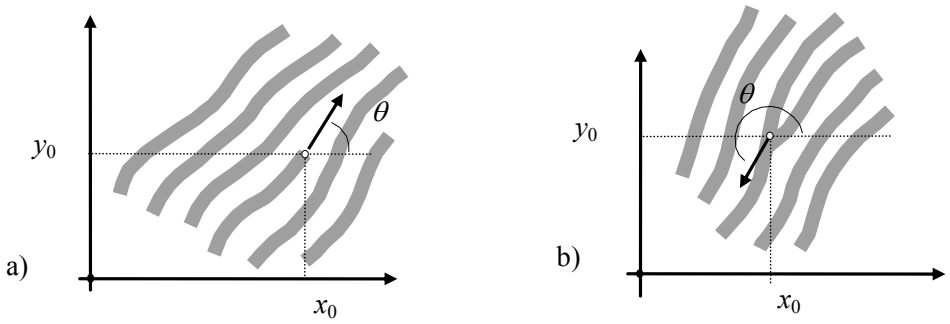


Figure 1.12 - a) a ridge ending minutia: [x_0,y_0] are the minutia coordinates; θ is the angle that the minutia tangent forms with the horizontal axis; b) a bifurcation minutia: θ is now defined by means of the ridge ending minutia corresponding to the original bifurcation that exists in the negative image.

Moreover, if a fingerprint image is acquired at a high resolution (at least 1000dpi), it is possible to identify the *sweat pores* (see Figure 1.13) [9]. Although pore information is highly distinctive, few automatic matching techniques use pores since their reliable detection requires very high resolution and good quality fingerprint images [9].

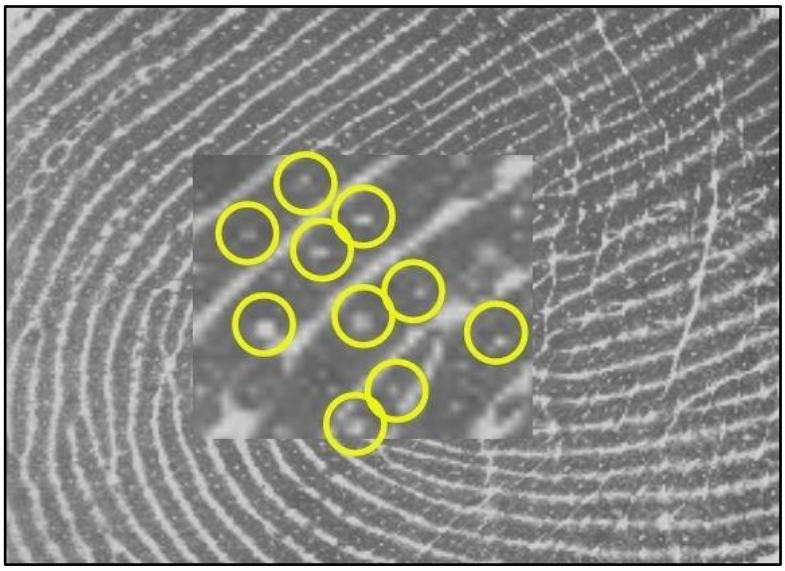


Figure 1.13 – A fingerprint where pores are highlighted.

1.2.3 Applications

Fingerprint recognition is rapidly evolving technology that has been widely used in forensics and has a very strong potential to be widely adopted in a broad range of civilian applications [9].

In forensics they are used not only to link suspects to crime scenes, but also to link persons arrested under another name to previous arrests, identify deceased persons, and associate persons with questioned documents. The cumbersome and time-consuming nature of filing, searching and matching fingerprints manually led to efforts in automating parts of the process as computer technology became more readily available to law enforcement agencies [14].

Recently, in civilian applications, fingerprints have been applied to application/registration forms in an attempt to associate applicants with certain benefits (welfare, voting, banking). In many countries, it has been, and still is, a common practice to capture fingerprints for all individuals when they reach a certain age in order to issue a national identity card [14]. Figure 1.14 summarizes the main application fields in the civilian market.

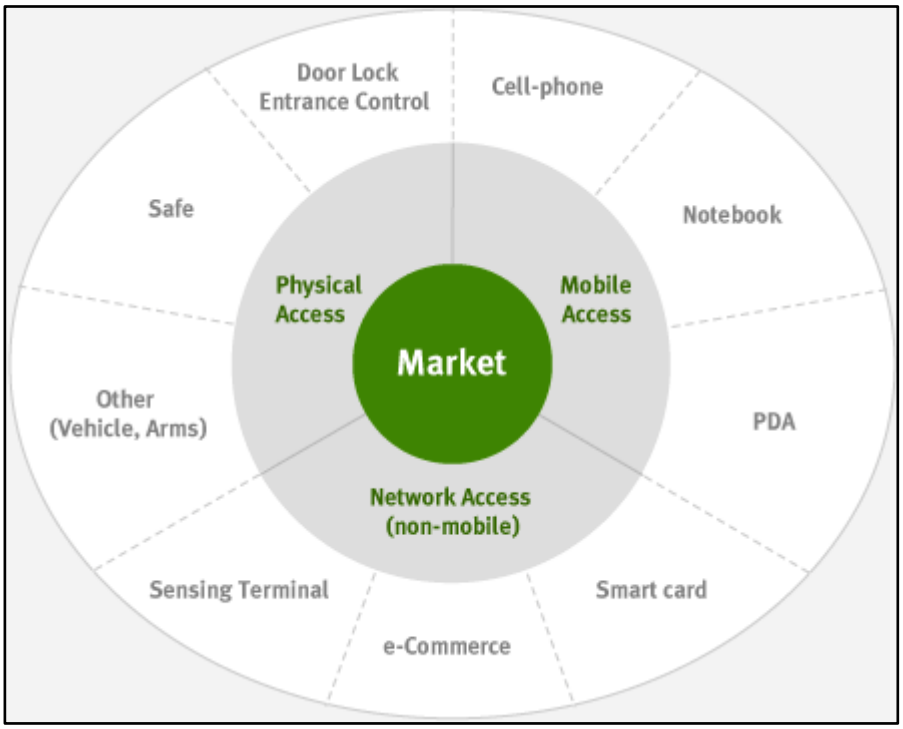


Figure 1.14 – Graph of the main application fields of fingerprint recognition systems in the civilian market.

2

FINGERPRINT ACQUISITION SENSORS AND THEIR QUALITY

2.1 Introduction

One of the most important elements needed for fingerprint automation was a method for scanning inked fingerprint cards that would provide images of sufficient quality for subsequent enhancement, feature extraction and matching (see Figure 2.1).

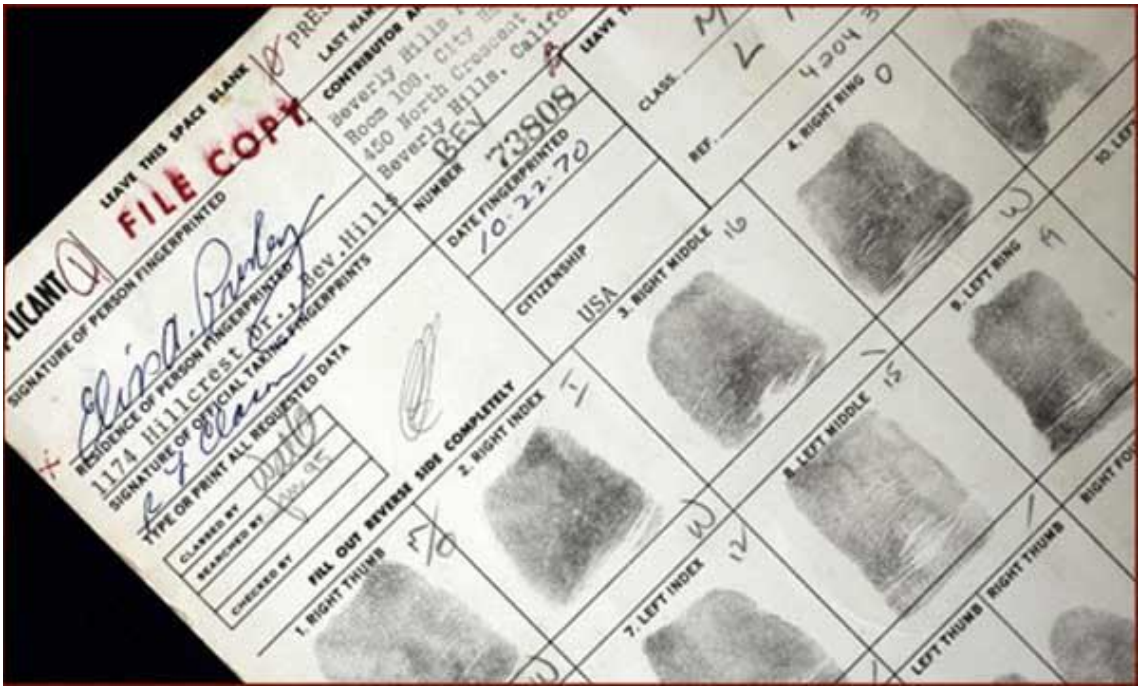


Figure 2.1 – An example of inked fingerprint card.

However, these days there is a trend to move away from capturing fingerprints on paper using ink; most of the fingerprint input devices now used in both forensic and civil fingerprint systems directly scan the fingerprint from the finger (Figure 2.2). These scanners are called “live-scan” fingerprint devices. The most common types of live-scan fingerprint devices either directly digitize the fingerprint image or digitize the

fingerprint image created through optical means. For many civil and commercial applications, there is no mandate for a set of ten fingerprints for each individual to be recorded by the system. Often, it is sufficient for the scanning device to capture a fingerprint from a single finger [14].

Figure 2.2 – Different types of fingerprint scanners.

The most important part of a fingerprint scanner is the sensor, which is the component where the fingerprint image is formed. Almost all the existing sensors belong to one of the three families: optical, solid-state and ultrasound (see [9] for a throughout treatment of this topic).

The quality of a fingerprint scanner, the size of its sensing area and the resolution can heavily influence the performance of a fingerprint recognition algorithm (as shown in Figure 2.3) (for more details see [3] [2] [1]).

Figure 2.3 – Fingerprint images of the same finger as acquired by different commercial scanners. Images are reported with right proportions: a) Biometrika FX2000, b) Digital Persona UareU2000, c) Identix DFR200, d) Ethentica TactilSense T-FPM, e) ST-Microelectronics TouchChip TCS1AD, f) Veridicom FPS110, g) Atmel FingerChip AT77C101B, h) Authentec AES4000 [9].

Particularly in large-scale biometric applications (such as the US-VISIT [16] and PIV [17] programs in the United States, the Biometric Passport in Europe [17], the Malaysian government multipurpose card [18] and the Singapore biometric passport [19] in Asia), the choice of the acquisition devices is one of the most critical issues since many, often conflicting, requirements have to be taken into account, such as the need for high-quality images, interoperability requisites and budget.

Typically, in large-scale projects a set of specifications is given for the input devices, in order to guarantee a minimum quality level for some relevant parameters.

To maximize compatibility between digital fingerprint images and ensure good quality of the acquired fingerprint impressions, the Federal Bureau of Investigation (FBI) established an IAFIS image-quality specification (IQS) in order to define the quantitative image-quality requirements for IAFIS fingerprint scanners. The FBI IAFIS IQS was defined in Appendix F of the *Electronic Fingerprint Transmission Specification* (EFTS) [20]. More recently, to support the *Personal Identity Verification* (PIV) program [17], whose goal is to improve the identification and authentication for access to U.S. Federal facilities and information systems, the FBI established a PIV IQS [22], which defines the quantitative image-quality requirements for single-fingerprint capture devices suitable for application in the PIV program; these requirements are similar to (but less stringent than) the IAFIS ones. Finally, the PassDEÜV requirements, targeted to single-finger scanners, were established by the German Federal Office for Information Technology Security (BSI) for the capture and quality assurance of fingerprints by the passport authorities and the transmission of passport application data to the passport manufacturers [23]. In these specifications, the "quality" is defined as "fidelity" of the scanner in reproducing the original fingerprint pattern, and it is hence quantified by measures traditionally used for vision, acquisition, and printing systems: geometric accuracy, gray-level dynamic range, Signal-to-Noise Ratio (SNR), Spatial Frequency Response (SFR), etc.. This definition of quality is clearly appropriate to IAFIS and other applications where the images may be examined by forensic experts. In fact human experts' comparison techniques heavily rely on very fine details such as pores, incipient ridges, etc., for which the fidelity to the original signal is fundamental.

On the other hand, the situation is different in totally-automated biometric systems, where: i) the images are stored but used only for automated comparisons, or ii) only fingerprint templates are stored. As shown in the following, in these cases it may be more appropriate to define the fingerprint scanner quality as the ability of a fingerprint scanner to acquire images that maximize the accuracy of automated recognition algorithms (in the following called *operational quality*) (for more details see [3] [2] [1]). A first advantage of the operational quality is that it allows to estimate the loss of performance of a scanner compliant to a given IQS with respect to an "ideal scanner".

2.2 Image Quality Specifications

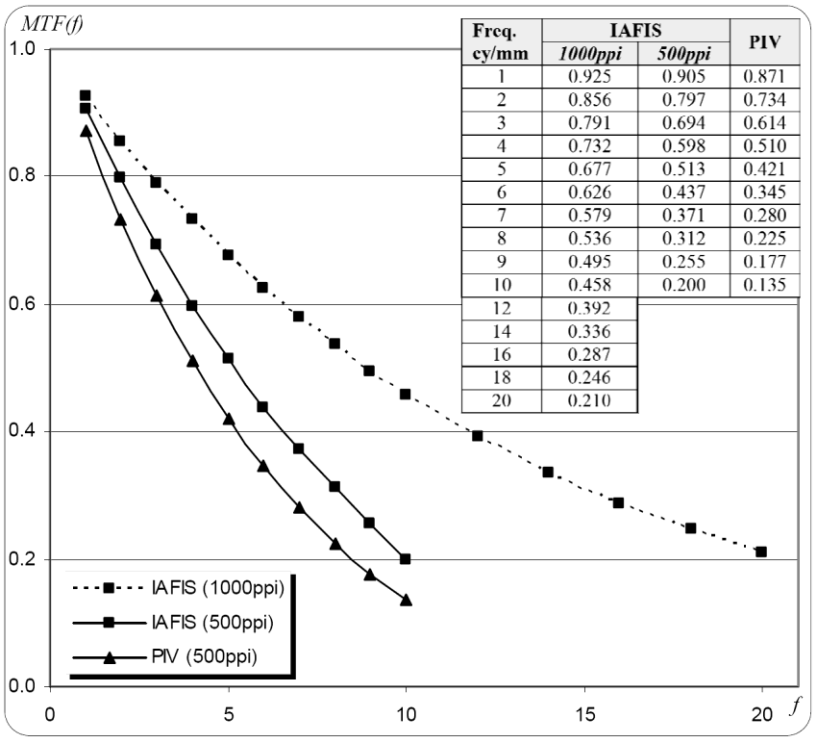
The IAFIS IQS was defined in Appendix F of the EFTS [20]; test procedures to verify compliance of fingerprint scanners to the specification were delineated in [23], which has been recently revised and updated in [24]. At the moment, the most updated PIV IQS are available in [22], with the corresponding test procedures described in [25]. The PassDEÜV IQS [23] are identical to the FBI IAFIS requirements except for the acquisition area. These specifications consider the following quality parameters:

- *Acquisition area*: Capture area of the scanner ($w \times h$).
- *Native resolution*: The scanner's true internal resolution (R_N) in pixels per inch (ppi).
- *Output resolution*: The resolution of the scanner's final output fingerprint image (R_O) in ppi.
- *Gray-level quantization*: Number of gray levels in the final output fingerprint image.
- *Geometric accuracy*: Geometric fidelity of the scanner, measured as the absolute value of the difference D, between the actual distance X between two points on a target and the distance Y between those same two points as measured on the output scanned image of that target; this parameter is measured in two different modalities: across bar (D_{AC}) and along bar (D_{AL}), see [24] for more details.
- *Input/output linearity*: The degree of linearity is measured as the maximum deviation D_{Lin} of the output gray levels from a linear least -squares regression line fitted between input signal and output gray levels scanning an appropriate target (see [24]).
- *Spatial frequency response*: The device modulation transfer function (MTF) measured at nominal test frequencies using a continuous-tone sine-wave target.
- *Gray-level uniformity*: Defined as the gray-level differences found in the image obtained by scanning a uniform dark (or light) gray target. This parameter is evaluated by dividing the acquisition area in 0.25×0.25-in regions and measuring the differences between: 1) the average gray levels of adjacent rows/columns (D_{RC}^{dark}, D_{RC}^{light}); 2) the average gray level of any region and the gray level of each pixel (D_{PP}^{dark}, D_{PP}^{light}); and 3) the average gray levels of any

two regions (D_{SA}^{dark} , D_{SA}^{light}).

- *Signal-to-noise ratio*: The signal is defined as the difference between the average output gray levels obtained from acquisition of a uniform light gray and a uniform dark gray target, measuring the average values over independent 0.25×0.25-in areas; the noise is defined as the standard deviation of the gray levels in those areas, leading to two values SNR_{dark} and SNR_{light}.
- *Fingerprint gray range*: Given a set of scanned fingerprint images, the dynamic range (DR) of each image is defined as the total number of gray levels that are present in more than four pixels.
- *Fingerprint artifacts and anomalies, fingerprint sharpness and detail rendition*: scanned fingerprint images are visually examined to determine whether any significant artifacts, anomalies, or false details are present.

Table 2.1 reports, for each aforementioned quality parameter, the requirements that a scanner has to meet in order to comply with the three IQS; note that the IAFIS IQS targets 500- and 1000-ppi scanners; hence, some requirements depend on the scanner resolution. The PIV and PassDEÜV IQS target only 500-ppi scanners.



Freq. cy/mm	IAFIS 1000ppi	IAFIS 500ppi	PIV
1	0.925	0.905	0.871
2	0.856	0.797	0.734
3	0.791	0.694	0.614
4	0.732	0.598	0.510
5	0.677	0.513	0.421
6	0.626	0.437	0.345
7	0.579	0.371	0.280
8	0.536	0.312	0.225
9	0.495	0.255	0.177
10	0.458	0.200	0.135
12	0.392		
14	0.336		
16	0.287		
18	0.246		
20	0.210		

Figure 2.4 - Minimum values $MTF_{min}(f)$ at nominal frequencies f (expressed in cycles per mm) for the IAFIS (1000ppi and 500ppi) and PIV (500ppi) IQS. Values for PassDEÜV IQS are equal to IAFIS (500ppi) IQS.

Table 2.1 - A comparison of IAFIS, PIV and PassDEÜV IQS requirements for the main quality parameters; the differences in the PIV and PassDEÜV requirements respect to the IAFIS requirements are highlighted using bold font.

Parameter	**Requirement**		
	IAFIS IQS (see [20][24]***)***	***PIV IQS (see*** [22][25]***)***	***PassDEÜV IQS (see*** [23]***)***
Acquisition area	Depending on the scanner type; for a plain 4-fingers scanner: $w \geq 73.2mm$ (2.88″) and $h \geq 45.7mm$ (1.8″)	$w \geq \mathbf{12.8mm}$ $(\mathbf{0.504}$″) and $h \geq \mathbf{16.5mm}$ $(\mathbf{0.650}$″)	w $\geq$ **16.0mm** (**0.630**) and h $\geq$ **20.0mm** (**0.787**)
Native resolution	$R_N \geq 500ppi$ *(500ppi scanners)* $R_N \geq 1000ppi$ *(1000ppi scanners)*	$R_N \geq 500ppi$	
Output resolution	$R_O = 500ppi \pm 1\%$ *(500ppi scanners)* $R_O = 1000ppi \pm 1\%$ *(1000ppi scanners)*	$R_O = 500ppi \pm \mathbf{2}\%$	$R_O = 500ppi \pm 1\%$
Gray-level quantization	256 gray-levels (8 bpp)		
Geometric accuracy	At least in 99% of the test measurements: $D_{AC} \leq max\{0.0007'', 0.01 \cdot X\}, X \leq 1.50''$ *(500ppi)* $D_{AC} \leq max\{0.0005'', 0.0071 \cdot X\}, X \leq 1.50''$ *(1000ppi)* $D_{AL} \leq 0.016''$	At least in 99% of the test measurements: $D_{AC} \leq max\{\mathbf{0.0013}'', \mathbf{0.018 \cdot X}\}, X \leq 1.50''$ $D_{AL} \leq \mathbf{0.027}''$	At least in 99% of the test measurements: $D_{AC} \leq max\{0.0007'', 0.01 \cdot X\}, X \leq 1.50''$ $D_{AL} \leq 0.016''$
Input/output linearity	$D_{Lin} \leq 7.65$	No requirements	$D_{Lin} \leq 7.65$
Spatial frequency response	For each spatial frequency *f* considered: $MTF_{min}(f) \leq MTF(f) \leq 1.05$ (see Figure 2.4 for $MTF_{min}(f)$ values)	For each spatial frequency *f* considered: $\boldsymbol{MTF_{min}(f)} \leq MTF(f) \leq \mathbf{1.12}$ (see Figure 2.4 for $MTF_{min}(f)$ values)	For each spatial frequency f considered: $MTF_{min}(f) \leq MTF(f) \leq 1.05$ (see Figure 2.4 for $MTF_{min}(f)$ values)
Gray level uniformity	At least in 99% of the cases: $D_{RC}^{dark} \leq 1$; $D_{RC}^{light} \leq 2$ At least for 99.9% of the pixels: $D_{PP}^{dark} \leq 8$; $D_{PP}^{light} \leq 22$ For every two small areas: $D_{SA}^{dark} \leq 3$; $D_{SA}^{light} \leq 12$	At least in 99% of the cases: $D_{RC}^{dark} \leq \mathbf{1.5}$; $D_{RC}^{light} \leq \mathbf{3}$ At least for **99%** of the pixels: $D_{PP}^{dark} \leq 8$; $D_{PP}^{light} \leq 22$ For every two small areas: $D_{SA}^{dark} \leq 3$; $D_{SA}^{light} \leq 12$	At least in 99% of the cases: $D_{RC}^{dark} \leq 1$; $D_{RC}^{light} \leq 2$ At least for 99.9% of the pixels: $D_{PP}^{dark} \leq 8$; $D_{PP}^{light} \leq 22$ For every two small areas: $D_{SA}^{dark} \leq 3$; $D_{SA}^{light} \leq 12$
Signal-to-noise ratio[1]	$SNR_{dark} \geq 125$; $SNR_{light} \geq 125$	$SNR_{dark} \geq \mathbf{70.6}$; $SNR_{light} \geq \mathbf{70.6}$	$SNR_{dark} \geq 125$; $SNR_{light} \geq 125$
Fingerprint gray range	At least for 80% of the fingerprint images: $DR \geq 200$ At least for 99% of the fingerprint images: $DR \geq 128$	At least for 80% of the fingerprint images: $DR \geq \mathbf{150}$	At least for 80% of the fingerprint images: $DR \geq 200$ At least for 99% of the fingerprint images: $DR \geq 128$
Fingerprint artifacts and anomalies	Artifacts or anomalies […] shall not be significant enough to adversely impact support to […] Automated Fingerprint Identification System (AFIS) search reliability. [24]	Artifacts, anomalies, […] shall not significantly adversely impact supporting the intended applications. [25]	Artifacts or anomalies […] shall not be significant enough to adversely impact support to […] Automated Fingerprint Identification System (AFIS) search reliability. [24]
Fingerprint sharpness and detail rendition	The sharpness and detail rendition […] shall be high enough to support the […] Automated Fingerprint Identification System (AFIS) search reliability. [24]	The sharpness and detail rendition […] shall be high enough to support the intended applications. [25]	The sharpness and detail rendition […] shall be high enough to support the […] Automated Fingerprint Identification System (AFIS) search reliability. [24]

[1] Actually in PIV IQS this requirement is given by setting the maximum noise standard deviation to 3.5. To make it comparable with the corresponding IAFIS IQS, here this value has been provided as a SNR under the hypothesis of a 247 gray-level range (see [24]): $SNR = {}^{247}/_{3.5} = 70.6$.

2.3 Test Approach

In order to evaluate the effects of the various quality parameters on fingerprint recognition accuracy, a systematic experimentation has been carried out. Starting from a fingerprint database, for each quality parameter, the output of scanners compliant with gradually-relaxed requirements has been simulated by modifying the images with appropriate transformations. This section describes the test approach and introduces the notation that will be used in the rest of the chapter.

Off-line performance evaluation of fingerprint recognition algorithms is based on a set of *genuine* and *impostor* recognition attempts [10]. In a genuine recognition attempt, two fingerprints of the same finger are compared, while in an impostor recognition attempt, two fingerprints of different fingers are compared. From the errors made by an algorithm in these recognition attempts, it is possible to calculate performance indicators that quantify its accuracy, such as the Equal Error Rate (EER) [26].

In each genuine/impostor attempt, the first image is supposed to have been acquired during an "enrollment" stage and the second during a "verification" stage. In general, the scanner used during enrollment may be different from the one used during verification; for this reason, in the following definitions, any test database DB is considered as made of two sets of images: DB_e (acquired during enrollment) and DB_v (acquired during verification). For the original database $DB^0 = \{(DB_e)^0, (DB_v)^0\}$, which is supposed to have been acquired using an "ideal" scanner, $(DB_e)^0$ and $(DB_v)^0$ simply contain the original images without any modification.

For a given quality parameter Q, let $DB_Q^j = \{(DB_e)_Q^j, (DB_v)_Q^j\}$ be a database that simulates enrollment and verification images acquired by two fingerprint scanners compliant with a given requirement R_Q^i on Q. Each image $(F_e)_Q^j \in (DB_e)_Q^j$ is obtained from the corresponding original image $(F_e)^0 \in (DB_e)^0$ by applying a transformation Te_Q to $(F_e)^0$ that simulates its acquisition through the scanner used for enrollment: $(F_e)_Q^j = Te_Q((F_e)^0, j)$; similarly, for each $(F_v)_Q^j \in (DB_v)_Q^j$, $(F_v)_Q^j = Tv_Q((F_v)^0, j)$, with $(F_v)^0 \in (DB_v)^0$.

For each quality parameter Q considered, an ordered set of gradually-relaxed requirements $\{R_Q^j, j = 1, \dots, M_Q\}$ has been established and a pair of transformations

(Te_Q, Tv_Q) has been defined according to a medium or large-scale application scenario where the scanners used for enrollment and verification are not the same physical device.

Given a set of recognition algorithms $\{A_i, i = 1, \dots, n\}$, let $EER_i(DB^0)$ be the EER of algorithm i on the original database, and $EER_i(DB_Q^j)$ the EER of algorithm A_i on DB_Q^j.

The dependency between the requirements on a given quality parameter Q and the recognition accuracy has been measured by considering, for each algorithm i and for each requirement R_Q^j, the relative EER difference:

$$(\rho_i)_Q^j = \frac{EER_i(DB_Q^j) - EER_i(DB^0)}{EER_i(DB^0)} \tag{2.1}$$

A positive value for $(\rho_i)_Q^j$ denotes a performance drop, whereas a negative value denotes a performance improvement. Although in this work the performance variations are based on the EER, similar results have been observed using other operating points, such as FMR1000.

In the following, experimental results are reported by using box-plots, where descriptive statistics of the $(\rho_i)_Q^j$ values (i.e., how the different algorithms in the set behave for a given j) are shown for each R_Q^j; see Figure 2.5 for a general example.

2.4 Experiments on a Single Parameter

The FVC2006 DB2 [28] has been selected as DB^0; it consists of 1680 fingerprints from 140 fingers (12 impressions per finger) of 50 subjects, acquired through a scanner with the following characteristics:

- acquisition area: $w = 17.8mm, h = 25.0mm$;
- output resolution: $R_{ORIG} = 569ppi$.

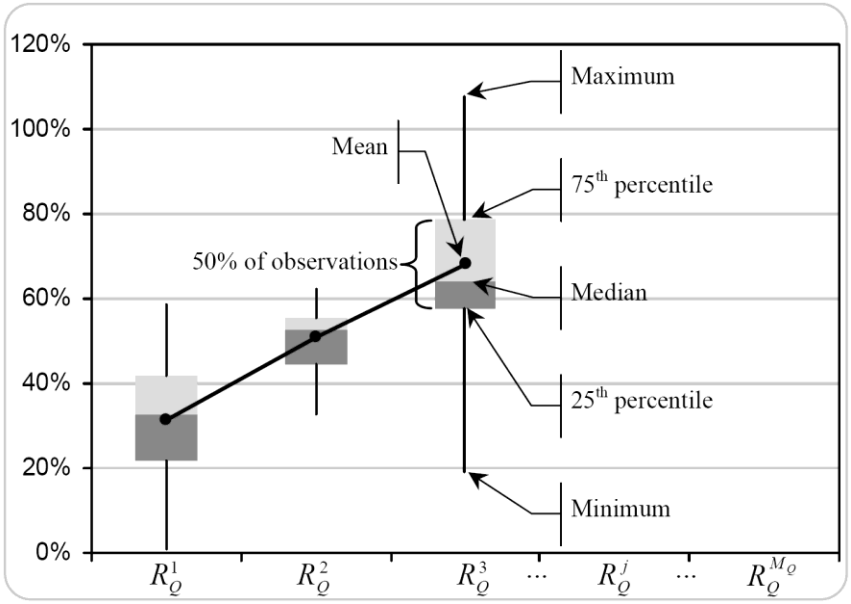


Figure 2.5 - An example of how the results are presented in the following section. The horizontal axis reports the various requirements $\{R_Q^j, j = 1, \ldots, M_Q\}$ and the vertical axis the relative EER difference (expressed as a percentage value). The box corresponding to each R_Q^j shows descriptive statistics of the $\{(\rho_i)_Q^j, i = 1..n\}$ values. The median value is denoted by the line separating the two halves of the box; the mean values are marked with black points, which are connected by a line to better highlight their trend.

The choice of using this database is motivated by the following reasons:

- a sufficiently-large database acquired in a real-life scenario using an IAFIS IQS compliant scanner was not available;
- even if a database had been collected with such a scanner, a sufficient number of state-of-the-art algorithms tuned to work on the images produced by that device would have not been available;
- the FVC2006 DB2 was collected within the European project BioSec [28] in three different European countries, following a well-defined acquisition protocol [29] and is being made available to the scientific community;
- although the scanner used to acquire that database (Biometrika Fx3000) is not IAFIS IQS certified, the performance of the best algorithms on FVC2006 DB2 are extremely good (the best EER is just 0.021%): this means that the perturbations introduced by the scanner do not cause (or cause to a very limited extent) “matchability” problems.

The FVC2006 protocol [28], defines the following recognition attempts on the database:

- *genuine recognition attempts*: each fingerprint is compared against the remaining impressions of the same finger, but avoiding symmetric comparisons, thus totaling $\frac{140\times12\times11}{2} = 9240$ genuine comparisons;
- *impostor recognition attempts*: the first impression of each finger is compared against the first one of the remaining fingers, but avoiding symmetric comparisons, thus totaling $\frac{140\times139}{2} = 9730$ impostor comparisons.

The following subsections describe the experiments performed for each quality parameter considered and report the results. In all the cases, the pair of transformations (Te_Q, Tv_Q) has been defined considering a worst-case scenario for a medium or large-scale application. For instance, for the Output Resolution parameter (see Subsection 2.4.2), given a requirement of $R_O \pm 2\%$ for the resolution, the worst case is identified by a scanner with $R_O - 2\%$ resolution used for enrollment and one with $R_O + 2\%$ resolution for verification (or vice versa).

2.4.1 Acquisition Area (Q = Area)

To evaluate this quality parameter, an experiment has been carried out under the following hypotheses:

- each requirement R^j_{Area} is given as a minimum acquisition area (in square millimeters);
- the acquisition area of the scanners simulated has the same aspect ratio of that used to acquire the original images (about ¾, which is also similar to the aspect ratio between the minimum w and h in the PIV IQS);
- for each requirement R^j_{Area}, a scanner with the minimum-allowed area is used for both enrollment and verification.

The transformations are defined as follows:

$$Te_{Area}(F^0, j) = Tv_{Area}(F^0, j) = Crop\left(F^0, w\sqrt{\frac{R^j_{Area}}{w \cdot h}}, h\sqrt{\frac{R^j_{Area}}{w \cdot h}}\right) \qquad (2.2)$$

where $Crop(F^0, w', h')$ crops a $w' \times h'$ image from the center of image F^0 (Figure 2.14.b).

The set of requirements $\{R^j_{Area}\}$ used in the experimentation is {352, 332, 291, 271, 251, 231, 211, 191, 171, 151}; note that R^7_{Area} is analogous to the PIV IQS requirement for the acquisition area: in fact $12.8\,mm \times 16.5\,mm = 211.2\,mm^2 \approx 211\,mm^2$.
The experimental results are reported in Figure 2.6. It can be observed that, on the average, there is no significant performance change for R^1_{Area}, a certain loss of accuracy from R^2_{Area} to R^4_{Area}, and a clear worsening trend starting from R^5_{Area} ($251\,mm^2$). The average performance drop for R^2_{Area} (corresponding to the PassDEÜV IQS requirement) is 12% while, the average performance drop for R^7_{Area} (corresponding to the PIV IQS requirement) is 73%.

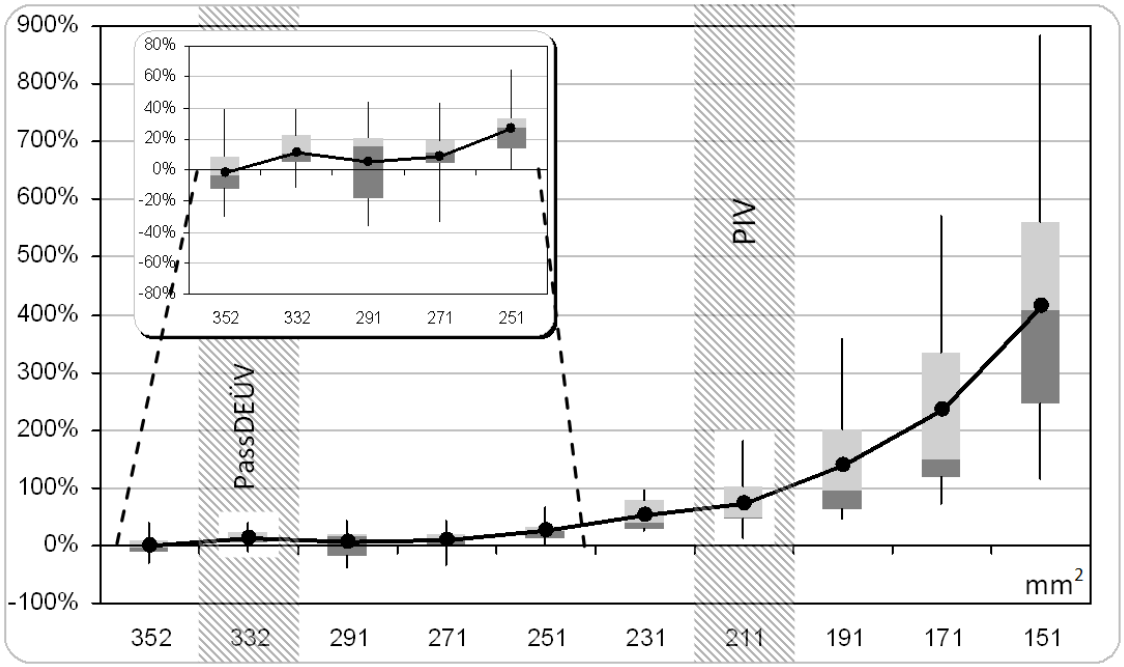


Figure 2.6 - Box-plot of the Acquisition area experiment; the first five boxes are expanded in the inner graph to better show their statistics. The horizontal axis reports the minimum acquisition area requirements (in square millimeters) and the vertical axis the relative EER difference (expressed as a percentage value). The requirement analogous to the PassDEÜV and PIV IQS are highlighted.

2.4.2 Output Resolution ($Q = Res$)

The experiment to evaluate the effect of imposing requirements on the scanner's output resolution has been carried out under the following hypotheses:

- each requirement R^j_{Res} is given as a maximum percentage variation from R_{ORIG};

- for each requirement R_{Res}^{j}, a scanner with the minimum-allowed resolution ($R_{ORIG} - R_{Res}^{j}\%$) is used for enrollment, and one with the maximum-allowed resolution ($R_{ORIG} + R_{Res}^{j}\%$) for verification.

The transformations are defined as follows:

$$Te_{Res}(F^0, j) = Resample\left(F^0, -R_{Res}^{j}\right) \tag{2.3}$$

$$Tv_{Res}(F^0, j) = Resample\left(F^0, +R_{Res}^{j}\right) \tag{2.4}$$

where $Resample(F^0, \Delta_r)$ resamples F^0 through bilinear interpolation, to simulate an image acquired at resolution $R_{ORIG} + \Delta_r\%$ (Figure 2.14.c).

The set of requirements $\{R_{Res}^{j}\}$ used in the experimentation is {0.5%, 1.0%, 1.5%, 2.0%, 2.5%, 3.0%, 3.5%, 4.0%, 4.5%, 5.0%}; note that R_{Res}^{2} and R_{Res}^{4} are the IAFIS/PassDEÜV and PIV IQS requirements for the output resolution, respectively.

The experimental results are reported in Figure 2.7. On the average there is no significant loss of accuracy for the first three requirements; then the average performance drop noticeably increases from 20% for R_{Res}^{4} (PIV IQS) to 258% for R_{Res}^{10}.

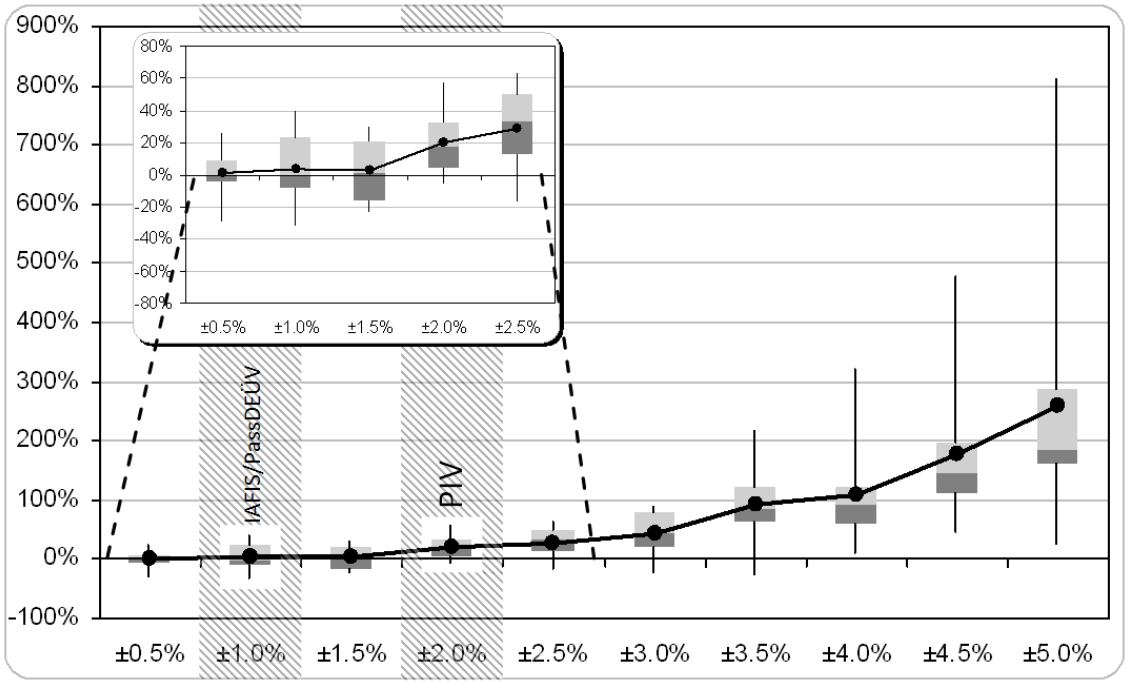


Figure 2.7 - Box-plot of the Output resolution experiment; the first five boxes are expanded in the inner graph to better show their statistics. The horizontal axis reports the requirements on the maximum percentage variation from the nominal output resolution (R_{ORIG}); the vertical axis reports the relative EER difference (expressed as a percentage value). The requirements of the IAFIS/PassDEÜV (±1%) and PIV (±2%) IQS are highlighted.

2.4.3 Geometric Accuracy ($Q = GAcc$)

This experiment has been carried out under the following hypotheses:

- each requirement R_{GAcc}^{j} is given as the maximum relative difference between the actual distance X between two points and the distance Y between those same two points as measured on the output scanned image;
- for each requirement R_{GAcc}^{j}, an "ideal" scanner (with negligible geometric distortion) is used for enrollment, and a scanner with the maximum allowed geometric distortion R_{GAcc}^{j} is used for verification;
- the scanners used for verification are characterized by a barrel distortion [30] (which is one of the most common types of lens distortions).

The transformations are defined as follows:

$$Te_{GAcc}(F^0, j) = F^0 \tag{2.5}$$

$$Tv_{GAcc}(F^0, j) = BarrelDist\left(F^0, R_{GAcc}^{j}\right) \tag{2.6}$$

where $BarrelDist(F^0, d)$ applies to F^0 a barrel distortion whose parameters are adjusted to impose a maximum relative distortion d while preserving the image size (see Figure 2.8 and Figure 2.14.d). The approach described in [31] has been adopted to implement this transformation function.

The set of requirements $\{R_{GAcc}^{j}\}$ used in the experimentation is {1.0%, 1.5%, 2.0%, 2.5%, 3.0%, 4.5%, 6.0%, 7.5%, 9.0%, 12.0%}. It is worth noting that for a scanner characterized by this type of barrel distortion:

- meeting requirement R_{GAcc}^{2} is necessary and sufficient to be compliant to the geometric accuracy requirements of the IAFIS 500ppi and PassDEÜV IQS (while R_{GAcc}^{3} is not enough);
- meeting requirement R_{GAcc}^{4} is necessary and sufficient to be compliant to the geometric accuracy requirements of the PIV IQS (while R_{GAcc}^{5} is not enough).

The two conditions above can be empirically verified by applying the corresponding transformations to digital images of the bar targets adopted in [24].

The experimental results are reported in Figure 2.9. It can be observed that, on the average, there is no significant performance change for the first four requirements (which include the three R^{j}_{GAcc} corresponding to the IAFIS, PassDEÜV and PIV IQS). Starting from R^{5}_{GAcc}, the performance drop shows a clear increasing trend.

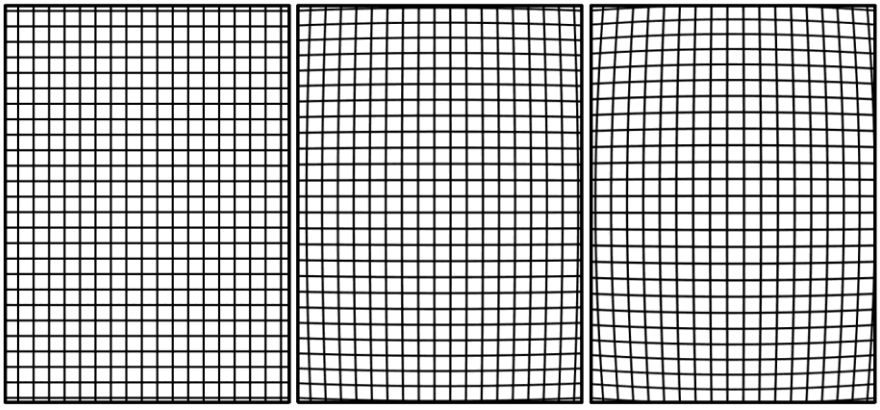


Figure 2.8 - Examples of the $BarrelDist(T, d)$ transformation applied to a square mesh grid T. From left to right: original image (T), result with $d = 5\%$, and result with $d = 10\%$.

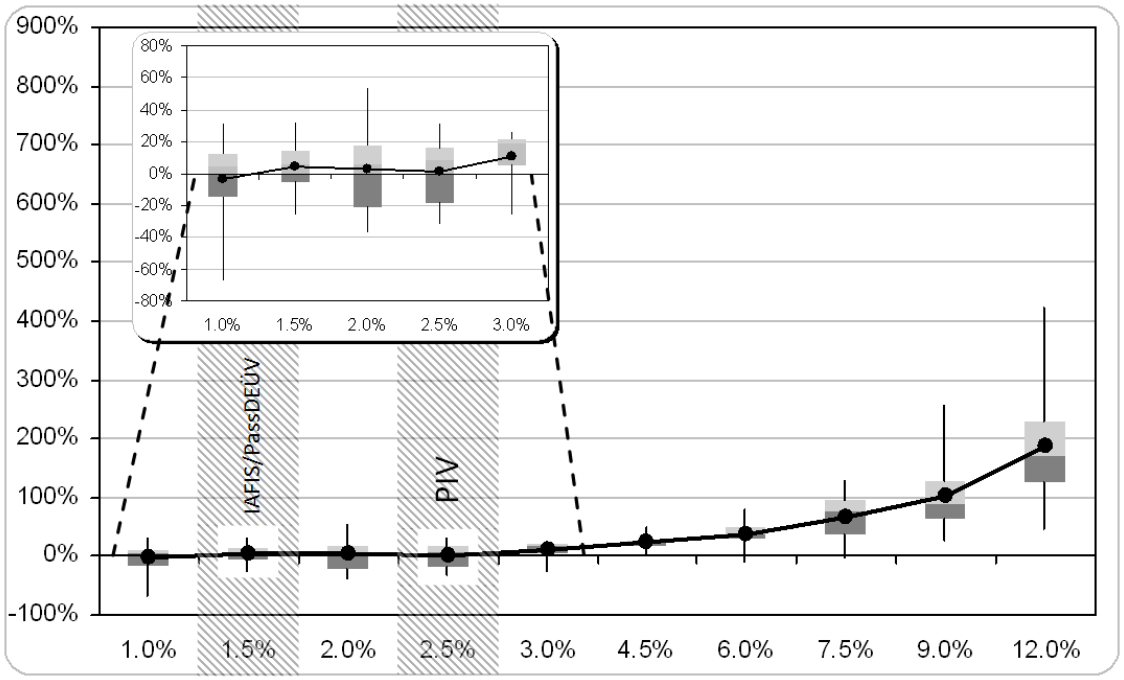


Figure 2.9 - Box-plot of the Geometric accuracy experiment; the first five boxes are expanded in the inner graph to better show their statistics. The horizontal axis reports the requirements on the maximum allowed relative distortion; the vertical axis reports the relative EER difference (expressed as a percentage value). The requirements corresponding to the IAFIS/ PassDEÜV and PIV IQS are highlighted.

2.4.4 Spatial Frequency Response ($Q = SFR$)

A simple technique to simulate the acquisition of images through a scanner with a given SFR is to apply a low-pass filter $H(f)$ in the Fourier domain, whose input parameter f is the frequency (measured in cycles per millimeter). This operation attenuates the amplitude at each frequency f by a factor of $H(f)$: if it were applied to an image acquired through an "ideal" scanner (i.e. $MTF = 1$ at every frequency), the resulting image would correspond to that obtained from a scanner with $MTF(f) = H(f)$ for each f.

A Butterworth-like function [32] has been selected for the low-pass filtering:

$$H_{f_0}^{\gamma}(f) = \frac{1}{1 + \left(\frac{f}{f_0}\right)^{\gamma}} \tag{2.7}$$

where parameter γ has been fixed to the value 1.65, which minimizing the mean-square-error of the difference between $H_{f_0}^{\gamma}(f)$ and $MTF_{min}(f)$ for the IAFIS (500ppi) and PIV IQS (see Figure 2.4).

The experiment has been carried out under the following hypotheses:

- each requirement R_{SFR}^{j} is given as a value for parameter f_0, hence, the minimum MTF value for each frequency f is simply $H_{R_{SFR}^{j}}^{1.65}(f)$;
- for each requirement R_{SFR}^{j}, a scanner with exactly the minimum-allowed MTF at each frequency is used for both enrollment and verification.

The transformations are defined as follows:

$$Te_{SFR}(F^0, j) = Tv_{SFR}(F^0, j) = FilterFFT\left(F^0, H_{R_{SFR}^{j}}^{1.65}\right) \tag{2.8}$$

where $FilterFFT(F^0, H)$ performs the low-pass filtering of image F^0 with filter H in the Fourier domain (Figure 2.14.e).

The set of requirements $\{R_{SFR}^{j}\}$ used in the experimentation is {15, 10, 7, 5, 4, 3, 2.5, 2, 1.5}; Figure 2.10 shows the minimum MTF curves corresponding to each R_{SFR}^{j}

requirement and the curves corresponding to the IAFIS (500ppi), PassDEÜV and PIV IQS (see also Figure 2.4).

The experimental results are reported in Figure 2.11. It can be observed that, on the average, there is a small performance improvement for the first five requirements; then the average performance drop noticeably increases from 16% for R^6_{SFR} to 548% for R^9_{SFR}. The very high performance drop for R^9_{SFR} is mainly due to an outlier (a single algorithm with an exceptionally large loss of performance), anyway the increasing trend is confirmed by the median value (172%). The small performance improvement for the first requirements is probably due to the low-pass filtering, which, by removing high frequencies (and therefore cleaning small noise artifacts), makes the fingerprint images easier to be processed by automated algorithms (although they appear less focused to the human eye).

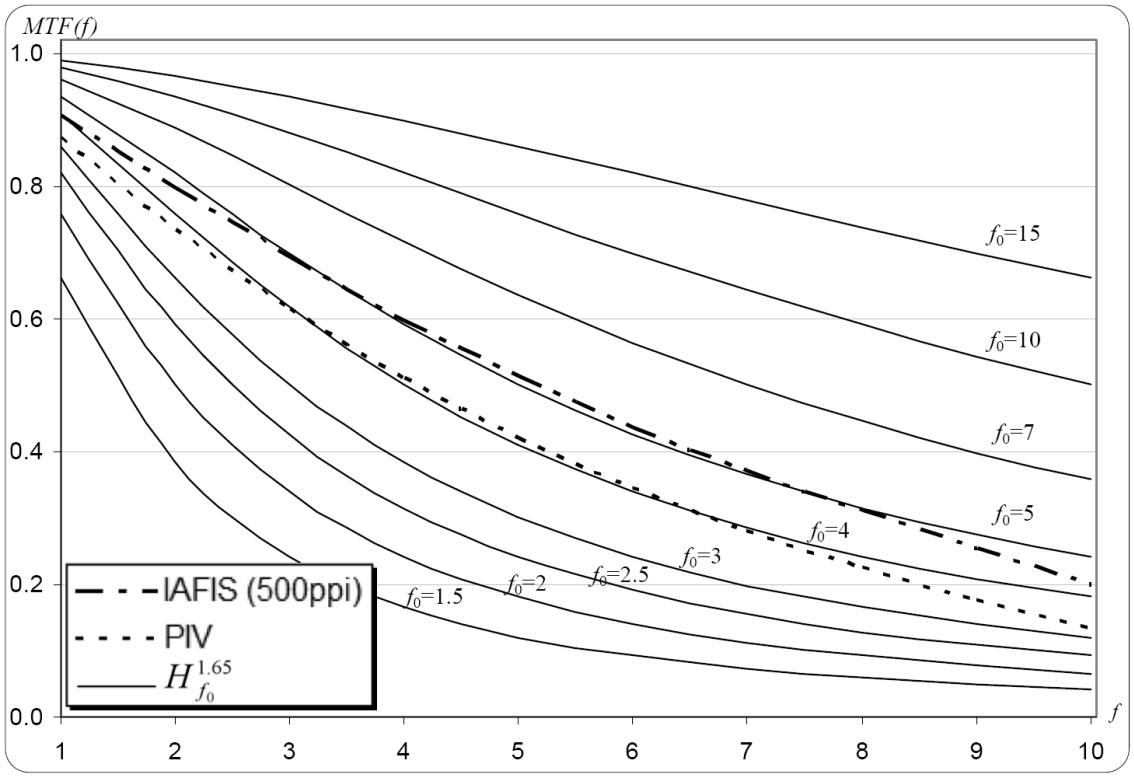


Figure 2.10 - Solid curves: minimum MTF values for the various R^j_{SFR} requirements; dashed curves: minimum MTF values for the IAFIS (500ppi) and PIV IQS. PassDEÜV IQS curve is the same of IAFIS (500ppi) IQS.

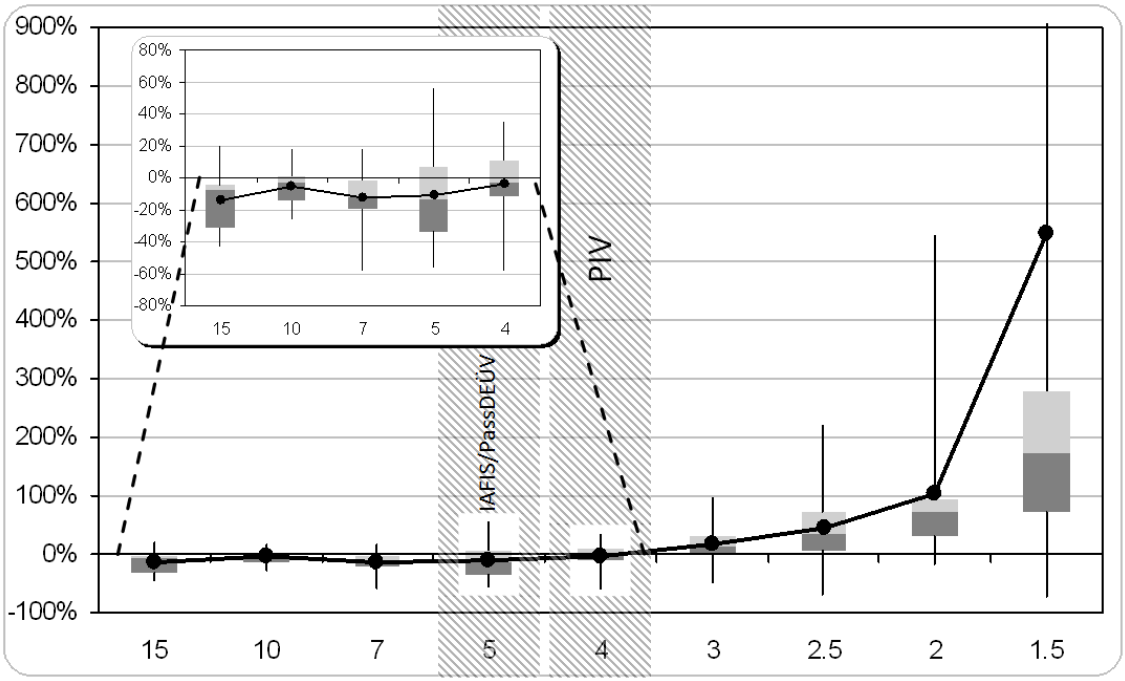


Figure 2.11 - Box-plot of the SFR experiment; the first five boxes are expanded in the inner graph to better show their statistics. The horizontal axis reports the requirements, given as values for the f_0 parameter and the vertical axis reports the relative EER difference (expressed as a percentage value). The requirements corresponding to the IAFIS/PassDEÜV and PIV IQS are highlighted.

2.4.5 Signal-to-Noise Ratio ($Q = SNR$)

Let $\bar{g}_{light}$ and $\bar{g}_{dark}$ be the average gray level for the light and dark target, respectively (see [24]); the SNR can be expressed as:

$$SNR = \frac{\left|\bar{g}_{light} - \bar{g}_{dark}\right|}{\sigma} = \frac{\Delta_g}{\sigma} \tag{2.9}$$

where σ is the standard deviation of the gray-levels in the image.

Assuming an image acquired through an "ideal" scanner with negligible noise, a practical way to simulate acquisition by a device with $SNR = K$ is to modify the gray level g of each pixel as follows:

$$g' = max\left\{min\left\{g + N\left(0, \frac{\Delta_g}{K}\right), 255\right\}, 0\right\} \tag{2.10}$$

where the function $N(\bar{x}, \sigma)$ generates an integer random number according to a normal distribution with mean $\bar{x}$ and standard deviation σ.

The SNR experiment has been carried out under the following hypotheses:

- each requirement R_{SNR}^{j} is given as a minimum SNR for the scanner;
- the scanner has a full 256 range of gray levels, hence, assuming a 4 gray-level offset at each side (see [24]), $\Delta_g = 247$;
- for each requirement R_{SNR}^{j}, a scanner with the minimum-allowed SNR is used for both enrollment and verification.

The transformations are defined as follows:

$$Te_{SNR}(F^0, j) = Tv_{SNR}(F^0, j) = AddNoise\left(F^0, R_{SNR}^{j}\right) \tag{2.11}$$

where $AddNoise(F^0, K)$ modifies each pixel in F^0 according to equation (2.10), see Figure 2.14.f.

The set of requirements $\{R_{SNR}^{j}\}$ used in the experimentation is {150, 125, 115, 100, 85, 70, 55, 40, 25, 15}; note that R_{SNR}^{2} is the IAFIS/PassDEÜV IQS requirement and R_{SNR}^{6} is close to the PIV IQS requirement.

The experimental results are reported in Figure 2.12. It can be observed that, on the average, there is no significant performance change for all the requirements except R_{SNR}^{10}, where the average performance drop is 52%. Actually, a small performance improvement can be noted for the second, third and fourth degradations. To explain this strange behavior (i.e., adding a small amount of noise seems to improve the overall accuracy) genuine and impostors distributions and some cases of genuine and impostor matches had been analyzed. Although a precise study is beyond the scope of this work, from this examination it is clear that adding a limited amount of random noise tends to leave almost all the genuine matching scores unaltered, while reduces some high impostor matching scores that were probably due to chance.

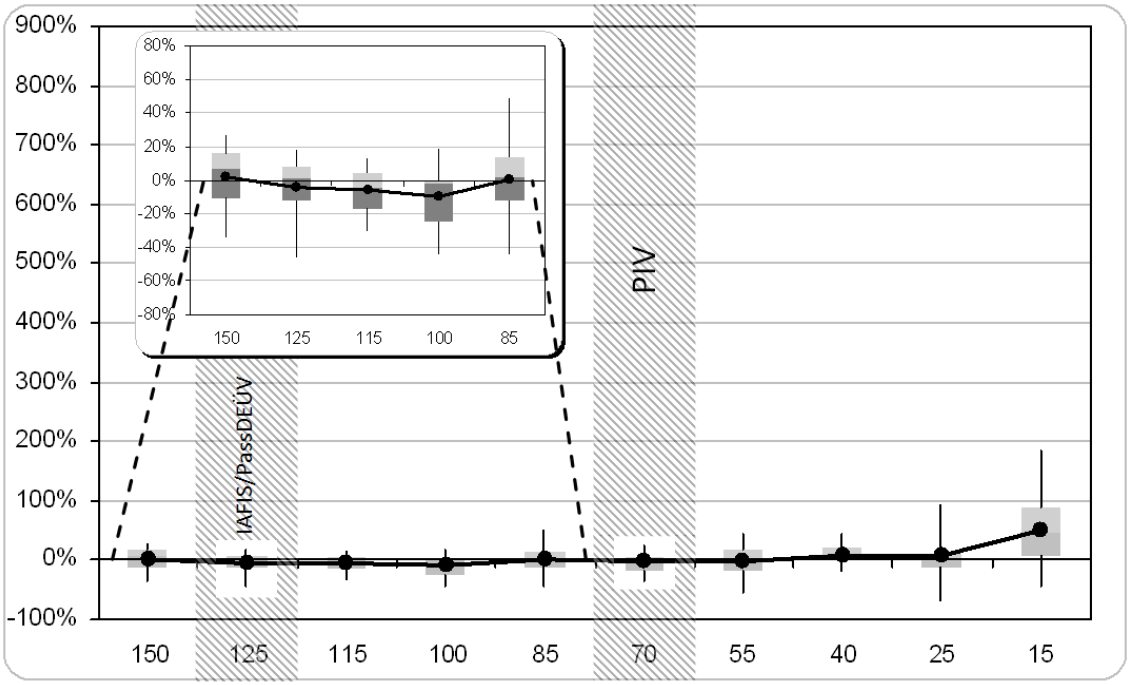


Figure 2.12 - Box-plot of the SNR experiment; the first five boxes are expanded in the inner graph to better show their statistics. The horizontal axis reports the requirements on the minimum SNR and the vertical axis reports the relative EER difference (expressed as a percentage value). The requirements corresponding to the IAFIS/PassDEÜV ($SNR \geq 125$) and PIV ($SNR \geq 70$) IQS are highlighted.

2.4.6 Fingerprint Gray Range ($Q = GRange$)

The experiment to evaluate the effect of imposing requirements on the scanner's gray range has been carried out under the following hypotheses:

- each requirement R^j_{GRange} is given as a minimum DR (see Section 2.2) for the fingerprints acquired by the scanner;
- for each requirement R^j_{GRange}, a scanner with the minimum-allowed DR is used for both enrollment and verification.

The transformations are defined as follows:

$$Te_{GRange}(F^0, j) = Tv_{GRange}(F^0, j) = DecGLevels\left(F^0, R^j_{GRange}\right) \qquad (2.12)$$

where $DecGLevels(F^0, m)$ applies the Median Cut algorithm [33] to decrease the

number of gray levels in F^0 to m (Figure 2.14.g).

The set of requirements $\{R^j_{GRange}\}$ used in the experimentation is {200, 175, 150, 128, 64, 32, 16, 8, 4, 2}; note that R^1_{GRange} is the DR that the IAFIS/PassDEÜV IQS requires for at least 80% of the fingerprints, R^3_{GRange} is the DR that the PIV IQS requires for at least 80% of the fingerprints, and R^4_{GRange} is the DR that the IAFIS/PassDEÜV IQS requires for at least 99% of the fingerprints.

The experimental results are reported in Figure 2.13. On the average there is no significant loss of accuracy for the first six requirements; then the average performance drop noticeably increases from 23% for R^7_{GRange} to 524% for R^{10}_{GRange}.

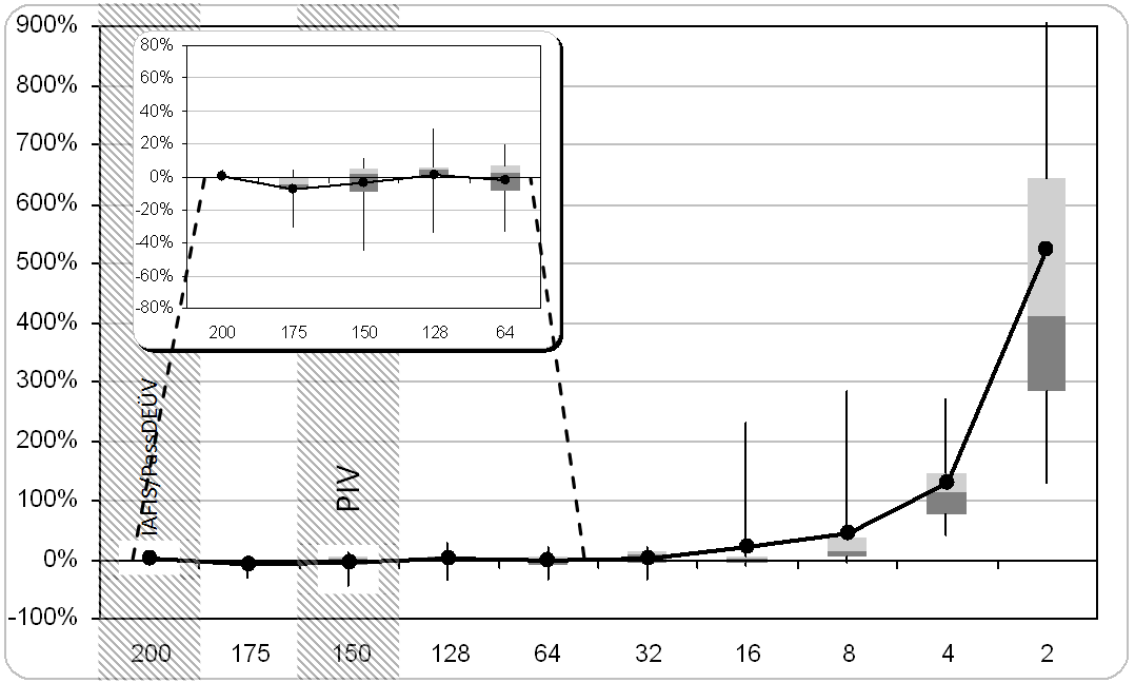


Figure 2.13 - Box-plot of the Fingerprint gray range experiment; the first five boxes are expanded in the inner graph to better show their statistics. The horizontal axis reports the requirements on the minimum number of different gray levels (DR) and the vertical axis reports the relative EER difference (expressed as a percentage value). The requirements corresponding to the IAFIS/PassDEÜV ($DR \geq 200$) and PIV ($DR \geq 150$) IQS are highlighted.

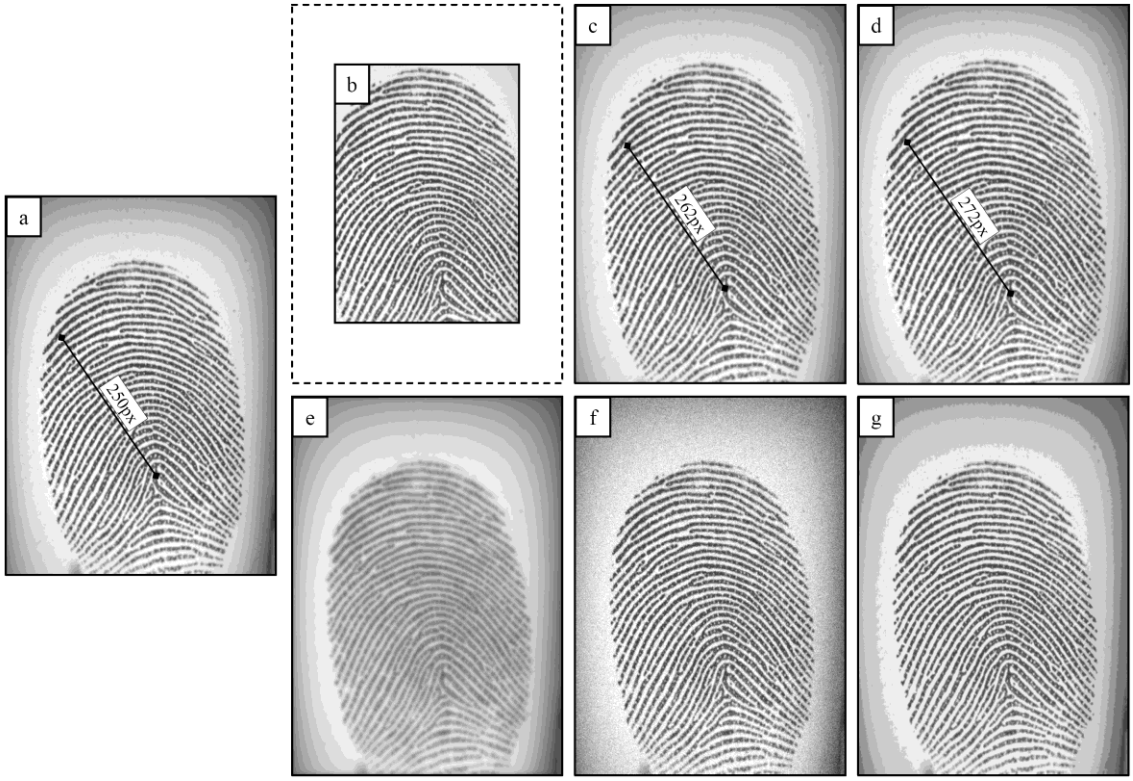


Figure 2.14 - An example of application of each transformation. a) Original image; b) Image cropped to simulate the minimum acquisition area for R^{7}_{Area} (PIV IQS); c) Image resampled to simulate the maximum allowed resolution for R^{10}_{Res} (the 250 pixel segment highlighted in the original image is here 262 pixel); d) Maximum barrel distortion allowed by R^{10}_{GAcc} (the 250 pixel segment highlighted in the original image is here 272 pixel); e) Image obtained by applying the Butterworth-like filter to simulate the minimum MTF values for R^{9}_{SFR}; f) Noise added to simulate the minimum SNR for R^{10}_{SNR}; g) Number of gray levels reduced to the minimum number required by R^{8}_{GRange} .

2.4.7 Result Analysis

From the analysis of the previous graphs, the following observations can be made.

- All the box-plots show almost no changes in the average and median performance variation for the first three/four requirements; this means that a small degradation of the database images does not cause significant performance drops: a substantial degradation is needed to observe significant changes. The initial flatness of all the trends confirms that the FVC2006 DB2 used in our experiments is not biasing the results; in fact, even if the results partially depend on the specific scanner used, similar results would be obtained with other scanners. In any case, the proposed methodology does not depend on the

particular scanner choice and it will be possible to repeat these experiments with other scanners in the future, including 1000ppi optical devices.

- The quality parameter that mostly affects the fingerprint matching performance is the acquisition area (Subsection 2.4.1): in fact, the same performance drop caused by a slight reduction of the area can be obtained only with a strong worsening of any of the other quality parameters. For instance, simulating a scanner with a $231\,mm^2$ area (larger than most single-finger commercial scanners and than the PIV IQS minimum requirement), an average performance drop of 52% has been observed; to obtain a similar result by modifying the Geometric accuracy parameter (Subsection 2.4.3), it would be necessary to allow a maximum distortion of 7.5% (about three times that allowed by the PIV IQS).
- The SNR and Fingerprint gray range quality parameters (Subsections 2.4.5 and 2.4.6) do not seem to affect much the performance: only starting from very strong degradations ($SNR < 25$, $DR < 32$) it is possible to observe a significant performance decrease. According to our experience, these results can be explained by considering that the type of perturbations that negatively affect the matching accuracy are those that modify the ridge pattern topology (e.g. merging, splitting or deforming ridge lines and valleys). The scanner noise quantified by the SNR parameter typically does not alter the ridge line structure and can be easily removed by smoothing filters in spite of a small degradation of the SFR (which does not seem to be a critical parameter as well, see Subsection 2.4.4). Similarly, the DR does not affect the accuracy since most matching algorithms tend to quantize (or even binarize) the image, hence only a drastic reduction of the gray range (able to change the pattern topology) may have a negative impact on the performance.

How should the results presented in these sections be related to the IAFIS, PassDEÜV and PIV IQS specifications and requirements? How may these results be exploited in practice to help choosing fingerprint scanners for a given application? The fundamental issue is whether the application might require human examination of fingerprint images or not (i.e., all the fingerprint processing and comparison steps are automated):

- the former case is typical of IAFIS and other large scale systems where the

images may be examined by forensic experts. In such situations, it is clearly very important to define the scanner quality as fidelity to the original signal and follow the IAFIS IQS requirements. In fact, differently from state-of-the-art matching algorithms, human experts' fingerprint comparison heavily relies on very fine details such as pores, incipient ridges, etc. for which the fidelity to the original signal is very important [35];

- the latter case is typical of totally-automated biometric systems, where: i) the images are stored but used only for automated comparisons, or ii) only fingerprint templates are stored. Here the definition of "operational quality" appears to be more important than the absolute fidelity to the original signal because the choice of a particular scanner should be driven by the desired performance.

Figure 2.15 compares the results obtained at the minimum IAFIS, PassDEÜV and PIV IQS requirements for each quality parameter. The performance variation for the Area parameter at the minimum IAFIS requirement is not available, but it can be assumed to be negligible (IAFIS compliant scanners are always able to acquire a full fingerprint). From the two graphs it can be observed that, at the IAFIS IQS minimum requirements, no quality parameter caused a sensible performance drop: this means that, for scanners compliant with the IAFIS IQS, the two definitions of quality ("fidelity to the signal" and "operational") are not in contrast and such devices are able to guarantee optimal results under both points of view; the PassDEÜV IQS differs from the IAFIS IQS only for the acquisition area where the performance drop is small (about 12%). Different is the case of the PIV IQS, where the requirements have been relaxed to deal with applications for which the cost and size of IAFIS IQS compliant scanners would not be feasible. The two graphs in Figure 2.15 highlight how the PIV requirement on the acquisition area may cause a large performance drop in automated systems with respect to scanners of larger area. A significant (but smaller) loss of performance may also be caused by the requirements on the output resolution, while the requirements imposed on other quality parameters (see the corresponding graphs in Section 2.4) do not seem to bring real advantages in spite of a potentially higher device manufacturing cost.

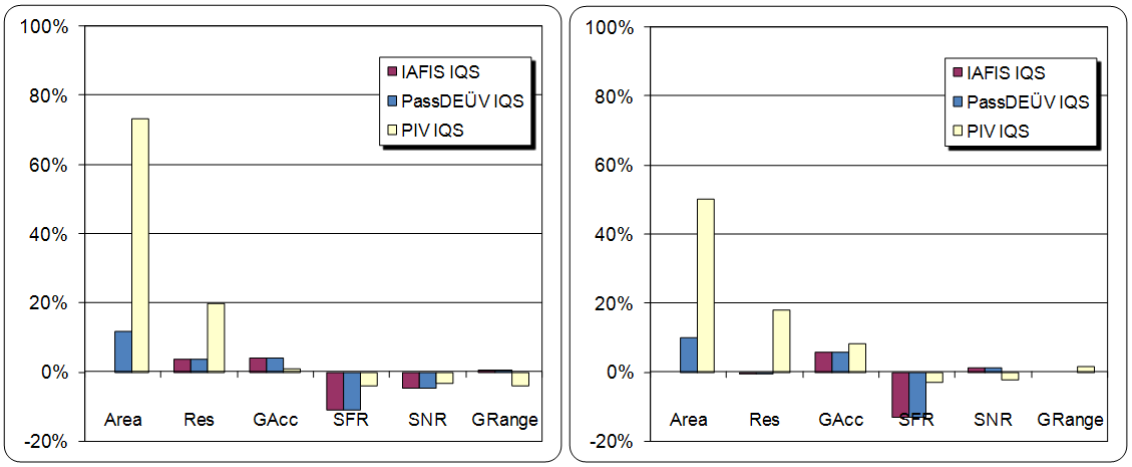


Figure 2.15 - Average (left graph) and median (right graph) performance variation for each quality parameter Q at the requirement R_Q^j corresponding to the IAFIS, PassDEÜV and PIV requirements.

2.5 New Image Quality Specifications for Single Finger Scanners

In this section, three new specifications, for single-finger scanners targeted to different types of applications, are presented and their potential effects on fingerprint recognition accuracy are compared and analyzed with PIV [22] and PassDEÜV [23] image quality specifications for single-finger scanners. The three new set of specifications are currently being evaluated by the Italian National Center for ICT in the Public Administration [36] (CNIPA) for inclusion within the guidelines for the Italian public administrations involved in biometric projects.

2.5.1 Proposed IQS

Starting from the obtained results reported in Section 2.4, in cooperation with CNIPA, three new set of IQS, for single-finger scanners to be used in different applications, are presented. In particular:

- CNIPA-A is conceived for: i) enrolment in large-scale applications where device interoperability is crucial (e.g. passports, national identity card); ii) identity verification in large-scale applications where the enrolment has been performed with an IAFIS IQS or CNIPA-A complaint scanners (e.g. passport or visa verification);

- CNIPA-B is conceived for: i) enrolment and verification in medium-scale projects (e.g. intra-organization projects); ii) identity verification in large-scale applications where the enrolment has been performed with CNIPA-A scanners (e.g. national identity card verification);
- CNIPA-C is conceived for enrolment and verification in small-scale applications, where typically users are authenticated on the same device (e.g. logical and physical security in small organizations).

The three new IQS are mainly based on the following quality parameters:

- *Acquisition area*: capture area of the scanner ($w \times h$).
- *Native resolution*: the scanner's true internal resolution (R_N) in pixels per inch (ppi).
- *Output resolution*: the resolution of the scanner's final output fingerprint image in ppi.
- *Gray-level quantization*: number of gray-levels in the final output fingerprint image.
- *Geometric accuracy*: geometric fidelity of the scanner, measured as the absolute value of the difference D, between the actual distance X between two points on a target and the distance Y between those same two points as measured on the output scanned image of that target; this parameter is evaluated by measuring the *Relative difference* ($D_{Rel} = \frac{D}{X}$).
- *Spatial frequency response*: the new specifications assess this factor by dividing the acquisition area in $0.25'' \times 0.25''$ regions and measuring, for each region, the *Top Sharpening Index* (TSI), see Section 2.6 for more details.
- *Signal-to-noise ratio*: the signal is defined as the difference between the average output gray-levels obtained from acquisition of a uniform light gray and a uniform dark gray target, measuring the average values over independent $0.25'' \times 0.25''$ areas; the noise is defined as the standard deviation of the gray-levels in those areas.
- *Fingerprint gray range*: given a set of scanned fingerprint images, the dynamic range (DR) of each image is defined as the total number of gray levels that are present in the image.

Table 2.2 reports, for each of the above quality parameters, the requirements that a

scanner has to meet in order to be compliant with the three proposed specifications.

Table 2.2 - A comparison of CNIPA-A/B/C requirements for the main quality parameters

Parameter	**Requirement**		
	IQS A	**IQS B**	**IQS C**
Acquisition area	$w \geq 25.4mm\ h \geq 25.4mm$	$w \geq 15.0mm\ h \geq 20.0mm$	$w \geq 12.8mm\ h \geq 16.5mm$
Native resolution	$R_N \geq 500ppi$		
Output resolution	$R_N \pm 1\%$	$R_N \pm 1.5\%$	$R_N \pm 2\%$
Gray-level quantization	256 gray-levels (8 bpp)		
Geometric accuracy	In all the tests: $D_{Rel} \leq 1.5\%$	In all the tests: $D_{Rel} \leq 2.0\%$	In all the tests: $D_{Rel} \leq 2.5\%$
Spatial frequency response	For each region: $TSI \geq 0.20$	For each region: $TSI \geq 0.15$	For each region: $TSI \geq 0.12$
Signal-to-noise[1]	$SNR \geq 70.6$	$SNR \geq 49.4$	$SNR \geq 30.9$
Fingerprint gray range	For 10% of the images: $DR \geq 150$	For 10% of the images: $DR \geq 140$	For 10% of the images: $DR \geq 130$

[1] Actually in CNIPA this requirement is given by setting the maximum noise standard deviation. To make it comparable with the corresponding PassDEÜV IQS, here this value has been provided as a SNR under the hypothesis of a 247 gray-level range (see [23] [20]): $SNR = {}^{247}/_{\sigma}$.

2.5.2 Impact of the IQS on the Recognition Accuracy

In order to evaluate the impact on fingerprint recognition accuracy of the IQS described in the previous subsection, a systematic experimentation has been carried out. Following the testing methodology introduced in Section 2.3 and using the same test database, fingerprint images acquired by hypothetical scanners compliant with each IQS have been simulated. To this purpose, the transformations described in Section 2.4 have been sequentially applied to the original fingerprint images according to the worst-case scenario hypothesized in Table 2.3 (see Figure 2.16).

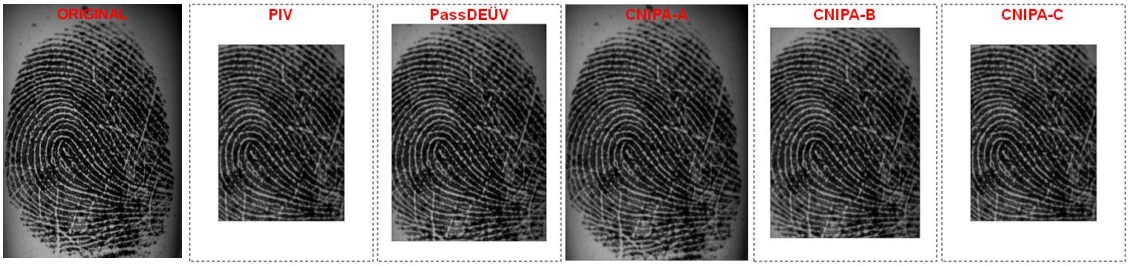


Figure 2.16 – Fingerprint image acquired by simulating scanners compliant with each IQS.

Table 2.3 - The table reports, for each quality parameter, the characteristic of the scanners hypothesized for enrolment and verification. In fact, in a typical large-scale application, the scanner used during enrolment may be different from those used during verification. Note that "different" does not necessarily imply a distinct model/vendor: in fact, two scanners of the same model may produce different output images. For instance if a certain scanner model is compliant to a 500ppi±1% output resolution specification, one of such devices may work at 505ppi and another at 495ppi.

Parameter	Enrolment scanner	Verification scanner
Acquisition area	The minimum-allowed	The minimum-allowed
Output resolution	The minimum-allowed ($Res_{OR} - R_{Res}\%$)	The maximum-allowed ($Res_{OR} + R_{Res}\%$)
Geometric accuracy	Negligible	The maximum-allowed
Spatial frequency response	The minimum-allowed	The minimum-allowed
Signal-to-noise ratio	The minimum-allowed	The minimum-allowed
Fingerprint gray range	The minimum-allowed	The minimum-allowed

The outcome of this analysis is an estimation of the loss of accuracy that scanners compliant with each specification may cause with respect to the performance that would be obtained using "ideal" scanners (i.e. devices with negligible perturbations). The loss of accuracy is quantified by the relative EER difference between the two cases, expressed as a percentage value (see Section 2.3); for instance, if the relative EER difference is 100%, it means that the EER obtained by the simulated scanners is twice the EER obtained by the ideal scanners. All the experiments have been carried out using ten state-of-the-art fingerprint recognition algorithms. Figure 2.17 reports a box-plot for each specification: each box-plot shows descriptive statistics about the relative EER difference of the ten algorithms.

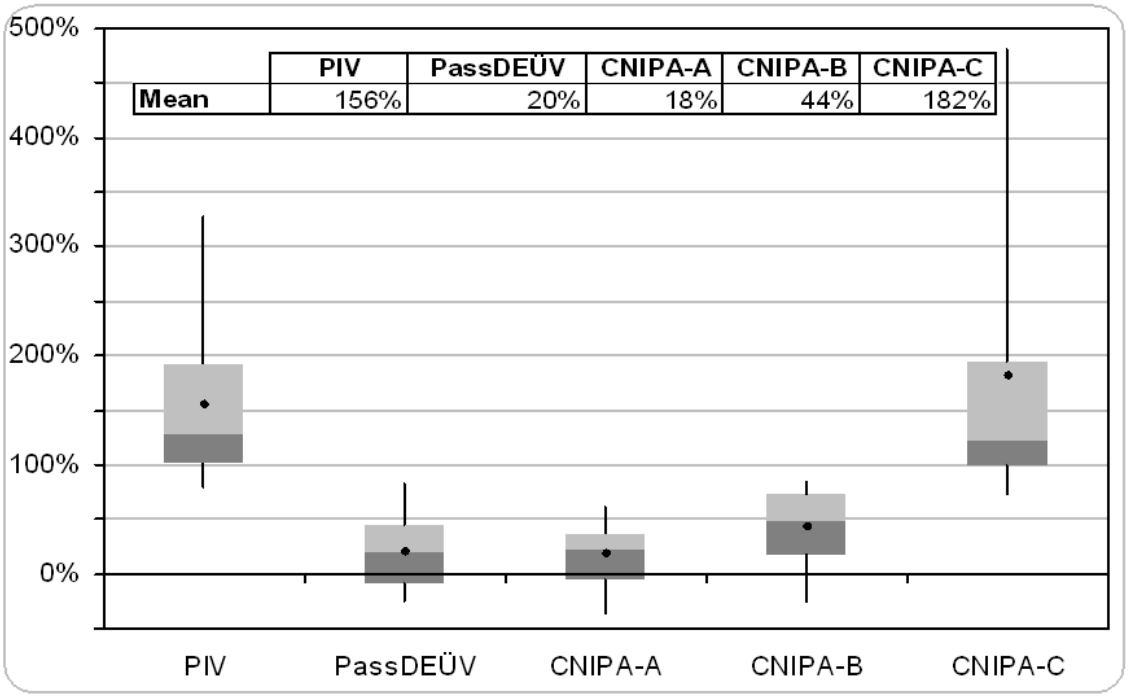


Figure 2.17 - A box-plot for each specification. Each box-plot graphically shows descriptive statistics of a set of data: the top and bottom of the vertical line denotes the largest and smallest observation, respectively; the rectangle contains 50% of the observations (from the first to the third quartile) and highlights the median (second quartile); finally the mean of all the observations is marked with a black circle.

In order to better understand the results summarized in Figure 2.17, it is useful to compare the five IQS as shown in Table 2.4, where the "strictness" of the various quality parameters with respect to the FBI IAFIS IQS [20] is highlighted. The most "tolerant" specification is CNIPA-C, which has the least demanding requirements for all the parameters: as it was reasonable to expect, this specification can cause the largest performance drop (182% on the average). Less tolerant but still not very strict are PIV and CNIPA-B (both with three "L" and three "M" requirements); however the loss of performance that can be caused by them is definitely different: on the average 156% and 44%, respectively. This means that the impact of the various quality parameters on the recognition accuracy is not uniform: the first three parameters in Table 2.4 are more critical than the last three ones. The two most demanding specifications (PassDEÜV and CNIPA-A) cause definitely smaller performance drops (on the average 20% and 18%, respectively); Table 2.4 shows that CNIPA-A has the most strict requirement for the acquisition area, while PassDEÜV for spatial frequency response, signal-to-noise ratio and fingerprint gray range. CNIPA-A IQS produces the smallest loss of

performance, mainly due to the larger acquisition area that is the most critical parameter, as proved in Subsection 2.4.7.

Table 2.4 - For each of the quality parameters a label in {"L: Low", "M: Medium", "H: High"} is used to characterize the level of "strictness" of the requirement in the specifications. "H" is used when the constraint is as "strict" as in the FBI IAFIS-IQS [20]; "M" and "L" are used when the specification is moderately or significantly relaxed, respectively, with respect to the corresponding FBI IAFIS-IQS.

Parameter	Level of "strictness" of the requirements				
	PIV IQS	**PassDEÜV**	**CNIPA-A**	**CNIPA-B**	**CNIPA-C**
Acquisition area	L	M	H	M	L
Output resolution accuracy	L	H	H	M	L
Geometric accuracy[1]	L	H	H	M	L
Spatial frequency response[2]	M	H	M	L	L
Signal-to-noise ratio	M	H	M	L	L
Fingerprint gray range	M	H	M	L	L

[1] CNIPA-A/B/C IQS set requirements on a slightly different measurement of geometric accuracy; however it can shown that PIV IQS is comparable to CNIPA-C requirement and PassDEÜV requirement (the same of the IAFIS IQS) is comparable to CNIPA-A requirement (see Subsection 2.4.3).

[2] Although CNIPA-A/B/C IQS on spatial frequency response are based on a different measure (see Section 2.6), according to our internal tests, PIV-IQS requirement is close to CNIPA-A.

2.6 Estimating Image Focusing in Fingerprint Scanners

The IQS [20], [22] and [23] provide clear specifications for the certification of fingerprint scanners for forensic and civil applications; unfortunately, the related testing procedures ([24] [25]) to certify these devices are rather complex and requires specific expensive targets.

The need for simple and practical techniques to evaluate the quality of fingerprint scanners is the main motivation of the work described in this section. Several factors have to be considered for a comprehensive evaluation, such as the deviation with respect to the nominal resolution, the geometric accuracy, the signal to noise ratio, etc. This section addresses the problem of how to efficiently evaluate the ability of the scanners to clearly focus the fingerprint.

A fingerprint image could be out of focus for two main reasons: i) the device internal sampling resolution is not sufficient to transfer the fine details of the pattern (i.e.

Nyquist sampling theorem); ii) some components of the device (e.g. a lens) produce a certain amount of blurring because of technology-specific reasons.

According to the testing procedures described in [24] and [25] the image focusing can be indirectly estimated through the MTF or CTF (as described in Subsection 2.6.1), but these require expensive calibrated targets and complex testing procedures (e.g. it is sometime necessary to open the device or remove some parts to properly image the target).

An alternative to MTF/CTF is using the Image Quality Measure (IQM) proposed in [36]. IQM is a good quality measure and demonstrated to be highly correlated to the MTF. On the other hand it has been developed for the evaluation of generic digital images and therefore it takes into account several factors, some of which are not directly applicable to the analysis of fingerprint images (e.g. the directional scale factor).

In this section a novel index (named TSI) [6] [7], to simply evaluate fingerprint image focusing, is proposed. The method is based on the measurement of the steepness of the ridge/valley transitions of the fingerprint impressions and does not require any specific setup.

2.6.1 MTF and CTF Measures

The modulation transfer function (MTF) denotes the ability of an imaging system to transfer the object contrast (i.e. the signal difference between dark and light areas) to the captured image.

The system MTF can be computed from an impulse function input such as a point source of light, a narrow line, or a sharp edge. It can also be computed from non-impulse inputs such as a sine wave, square wave, or even from a random pattern. The evaluation of the spatial frequency response (SFR) for fingerprint scanners, according to the FBI/NIST recommendations, requires the use of continuous tone sine wave targets. A typical target, including sine waves of increasing frequencies is shown in Figure 2.18.

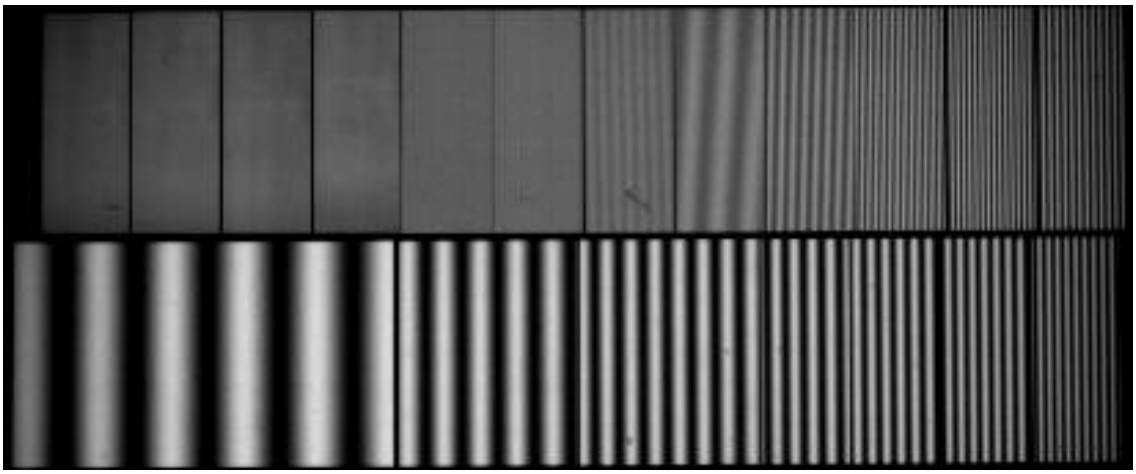


Figure 2.18 - Example of a sine wave target used to calculate MTF.

The MTF for a given frequency is defined as:

$$MTF = \frac{peak\ image\ modulation}{target\ modulation} \tag{2.13}$$

The *target modulation* is a value provided by the target manufacturer, while the image modulation is computed as:

$$peak\ image\ modulation = \frac{maximum - minimum}{maximum + minimum} \tag{2.14}$$

where the maximum and minimum values correspond respectively to the gray level value of the peak and adjacent valley in each sine wave period.

If the scanner cannot obtain adequate tonal response from this kind of target, a bi-tonal bar target shall be used to measure the SFR, denoted as Contrast Transfer Function (CTF) measurement. In this case the modulations are determined in image space, normalized by the image modulation at zero frequency . The scanner CTF at each frequency is then defined as:

$$CTF = \frac{peak\ image\ modulation}{zero\ frequency\ image\ modulation} \tag{2.15}$$

2.6.2 IQM

Image Quality Measure (IQM) has been proposed in [36], based on the digital image power spectrum of arbitrary scenes. This measure, differently from MTF, does not require imaging specific targets. IQM is derived from the normalized 2D image power spectrum, based on the assumption that the equational form of the imaging system input scene power spectrum is invariant from scene to scene [36]. This invariance is a necessary assumption for the technique to work when only the output image is available for measurement. The analysis of power spectrum allows to identify image degradation.

Given a 2D image of size $M \times M$ pixels, where a pixel gray level is given by $h(x, y)$, with spatial coordinates x and y ranging from 0 to $M - 1$, the image power spectrum is defined as $|H(u, v)|^2$ where $H(u, v)$ is the discrete Fourier transform of the image:

$$H(u,v) = \sum\sum e^{\left(-2\pi \cdot i \cdot y \cdot \frac{v}{M}\right)} \cdot e^{\left(-2\pi \cdot i \cdot x \cdot \frac{u}{M}\right)} \cdot h(x,y) \tag{2.16}$$

with $u, v = -\frac{M}{2}, \dots, \frac{M}{2}$.

IQM is derived from the analysis of the image power spectrum and incorporates several factors. It can be derived as follows:

$$IQM = \frac{1}{M^2} \sum_{\theta=-\pi}^{\pi} \sum_{\rho=0.01}^{0.5} S(\theta_1) \cdot W(\rho) \cdot A^2(T \cdot \rho) \cdot P(\rho, \theta) \tag{2.17}$$

where ρ, θ are the polar coordinates of the spatial frequency and M^2 is the image size in pixel. The term $P(\rho, \theta)$ represents the normalized power spectrum, and it is used in place of the power spectrum to account for the image size and the possible image-to-image brightness variations:

$$P(u,v) = \frac{|H(u,v)|^2}{\mu^2 \cdot M^2} \tag{2.18}$$

where μ^2 is the square of the average gray level of the image. The term $S(\theta_1)$ represents

a weighting factor related to the scale at which the scene is acquired (directional scale factor). This term is needed in particular for aerial images for which the image quality is strictly related to the object-image scale. The factor $W(\rho)$ is derived by applying a modified version of the Wiener filter, and allows to evaluate the presence of noise in the image power spectrum. Finally the term $A^2(T \cdot \rho)$ introduces into IQM a model of the human visual system to obtain a measure highly correlated to visual quality assessments.

2.6.3 Top Sharpening Index

The proposed technique is based on the consideration that if a fingerprint image is well focused, then its ridge/valley transitions are sharp. Hence focusing can be evaluated by measuring the response of the image to a sharpening filter. This is not a novel idea, and is often used for the development of auto-focusing systems (e.g. [37]). On the other hand, a specific implementation of sharpening in order to achieve invariance with respect to the particular pattern sensed is necessary. In other words, the measured focusing level must be related only to the scanner characteristics and not to the specific fingerprint acquired. In particular it must be invariant to:

- the frequency of a ridge/valley cycle . In fact the frequency can vary from finger to finger and also from zone to zone in the same finger [9];
- the gray level range in the image. The aim is to estimate the steepness of the ridge/valley transitions and not its amplitude.

Top Sharpening Index (TSI) has been studied to fulfil the above requirements which are not satisfied by the MTF, CTF and IQM measures.

Let I be an image of size $u \times v$ pixels, totally covered by a fingerprint pattern. The proposed index is calculated as follows:

1. *Gray level normalization.*

   This step is needed to make TSI independent on the gray level range of the image. The normalized image I_n is obtained by applying a contrast stretching function to the gray level value g_i of each pixel of the original image I:

$$f(g_i) = 255 \cdot \frac{g_i - \min(I)}{\max(I) - \min(I)} \tag{2.19}$$

where $min(I)$ and $max(I)$ represent respectively the minimum and maximum gray level value of the image I determined by discarding the 1% of the lowest and highest values (to prevent outliers affecting the normalization too much).

2. *Image convolution with a sharpening filter.*

   The normalized image I_n is convolved with a sharpening filter F thus obtaining a new image $I_c = |I_n * F|$:

$$F = \frac{1}{9} \cdot \begin{bmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{bmatrix} \tag{2.20}$$

   where $*$ denotes the image convolution operation and the operator $|\cdot|$ replaces each element of the convolved image with its absolute value. Taking the absolute value of the filter response is necessary since both high (positive) and low (negative) responses denote high steepness. From the example shown in Figure 2.19 it is evident that I_c pixels assume high values in correspondence of I edges.

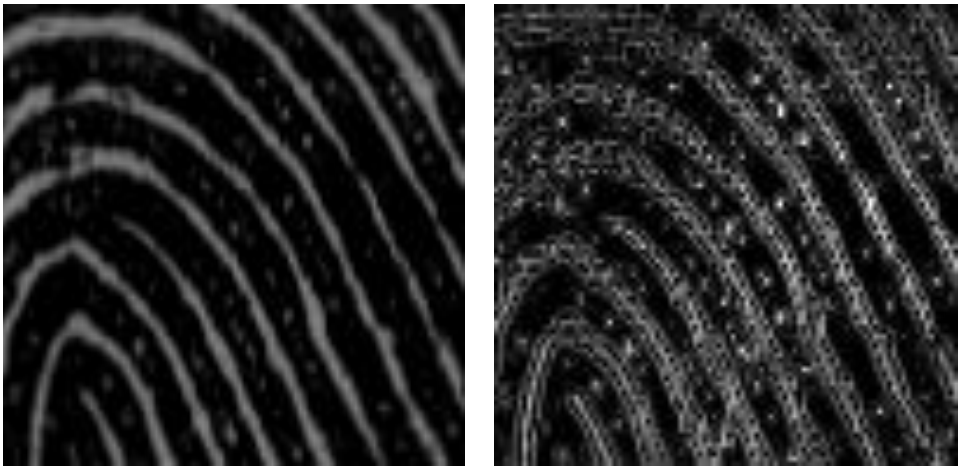


Figure 2.19 - A fingerprint image and the result of the convolution I_c.

3. *TSI computation.*

   TSI is calculated by accumulating the values of the top p% pixels of I_c (i.e., those with highest intensity). Considering only the top percentage of sharpening responses allows to achieve invariance with respect to the ridge/valley

frequency: in fact, provided that a sufficient number of edges are present in the image, further increasing the number of edges does not increase the TSI value. On the other, the value of p must be tuned according to the scanner nominal output resolution. The invariance has been experimentally verified by fixing the percentage as follows: 10% at $500dpi$ resolution and 5% at $1000dpi$. For different resolutions the percentage p can be derived by linear interpolation. The resulting value is normalized in the range $[0;1]$ by dividing it by a factor f representing the theoretical maximum sharpening value:

$$f = \frac{8}{9} \cdot 255 \cdot p \cdot u \cdot v \tag{2.21}$$

The procedure above described is based on the assumption that the image I is totally covered by a fingerprint pattern. In order to calculate a global TSI value for a generic fingerprint image, a partitioning into non-overlapping sub-windows of fixed size and a fingerprint area segmentation (i.e. separation of the foreground from the background) is necessary. The partitioning is useful for two reasons:

a) it makes TSI independent of the image size;
b) it allows to estimate TSI also locally (e.g. the focusing in optical fingerprint scanners is usually better in the central region than near the borders).

The global TSI is obtained by averaging the TSI scores of each sub-image. The segmentation is required since the background does not contain significant edges and averaging over the whole image would produce a lower score. Several segmentation algorithms have been proposed for fingerprints [9]. In this work a simple method based on the gray level variance is used. In Figure 2.20 an example of fingerprint area segmentation is reported.

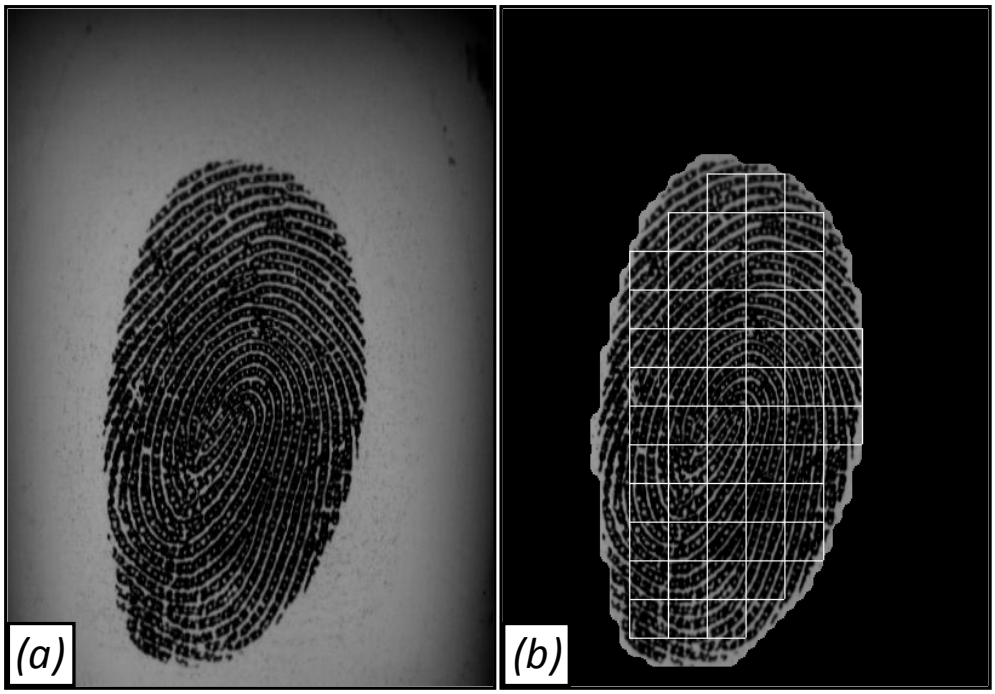


Figure 2.20 - Fingerprint image *(a)*, and the related segmented image where the sub-windows (32×32 pixels wide) used to calculate TSI are shown *(b)*.

2.6.4 Experimental results

Four sets of experiments have been carried out:

- to evaluate the TSI invariance with respect to the ridge/valley frequency and to the gray level range;
- to verify the relation between TSI value and the actual device focusing;
- to highlight similarities and differences between MTF, IQM and TSI;
- to show that TSI, analogously to IQM, is able to effectively measure fingerprint image focusing.

For all the following experiments the sub-windows size has been fixed to 32×32 pixels.

1. *Independence of ridge/valley frequency and gray level range.*

   For this set of experiments two kinds of images have been used:

   - Bar target images of varying frequency and gray level range. These computer generated targets exhibit a fixed steepness for the transition between two contiguous bars (see Figure 2.21).

- Fingerprint images of size $400x560$ pixels, $569dpi$, acquired with a high quality optical sensor (see Figure 2.22).

In Figure 2.21 a subset of the bar target images of different frequency and gray level range is shown. The associated plot of a horizontal section of the targets is reported in the last row. Different columns refer to different ridge/valley frequencies (from left to right the frequencies range from 1 to 4). The chosen values cover the different frequencies present in human fingerprints [9]. All the bar targets obtain the same TSI value, thus demonstrating the invariance to frequency and gray level range.

This property has been confirmed by the experiments carried out on fingerprint images. The fingerprints in Figure 2.22, characterized by different frequencies and gray level range, achieve very similar TSI values.

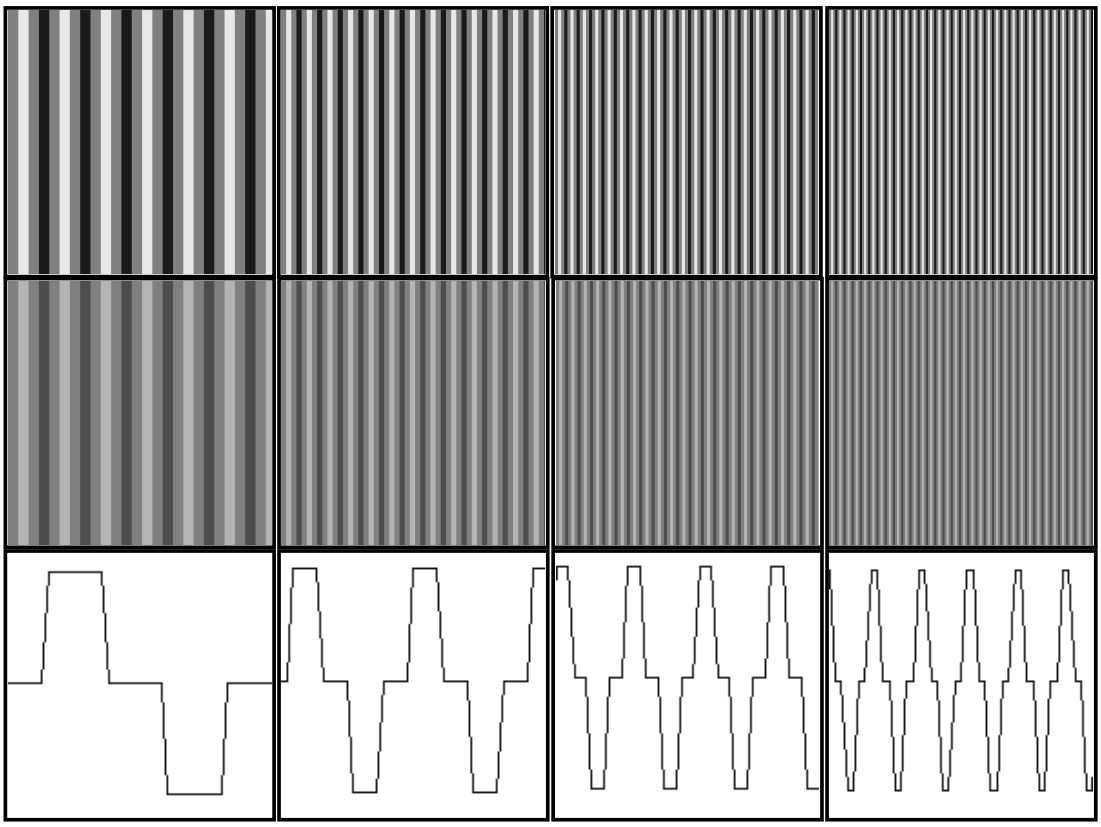


Figure 2.21 - Bar targets of different gray level range and frequencies (first and second row) and plots of a horizontal section (last row).

Figure 2.22 - Fingerprint images with different characteristics: high *(a)* and low *(b)* frequency, small *(c)* and large *(d)* gray level range. For each image the TSI value is reported as well.

2. *Relation to the device focusing*

   In order to verify the relation between TSI and the ability of a scanner to clearly focus a fingerprint, TSI value has been calculated for a set of images of the same finger acquired by using an optical sensor while the lens focus was manually degraded (by gradually moving the lens away from the ideal position). In Figure 2.23 a sequence of images progressively more out of focus is reported. In addition the related plot of a ridge/valley fingerprint section is shown to prove that the blurring produces a steepness reduction of the ridge/valley transitions.

Finally the TSI value of each image is given. The experimental results prove the strict relation between the proposed index and the device focusing.

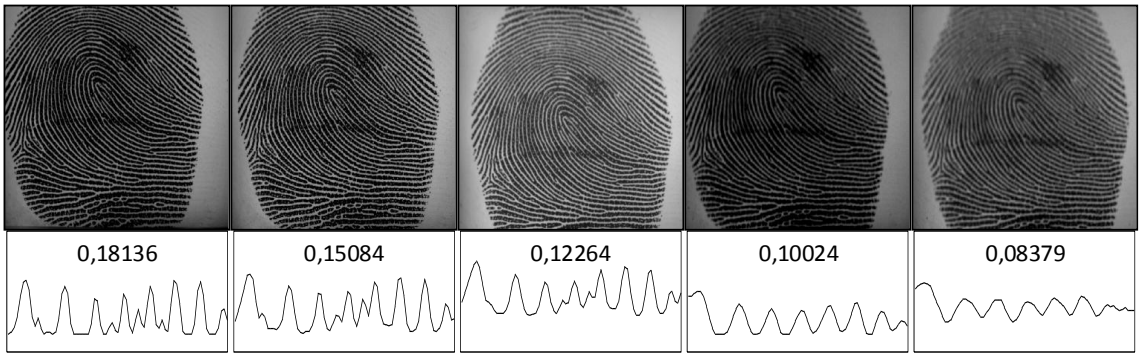


Figure 2.23 - In the first row a sequence of progressively defocused images of the same finger is shown. Plots of a fingerprint section and the TSI values are given in the second row.

3. *Comparison between MTF, IQM and TSI: sinusoidal targets*

   A set of experiments has been carried out to investigate the analogies/differences between MTF, IQM and TSI, and in particular to show the strict correlation between IQM and MTF. Since MTF can be easily measured only on sinusoidal targets, for this test a set of sinusoidal target images of various frequencies (from 1 to 10, typically adopted in the evaluation of $500dpi$ scanners [24] [25]) have been generated and progressively defocused by applying two different smoothing filters (Pillbox [38] and Butterworth [32]) to the original fingerprint images . In Figure 2.24 the effect of simulated defocusing is compared against physical scanner defocusing. The plots confirm the high similarity of the results. In Figure 2.25 an example of original and defocused target is reported.

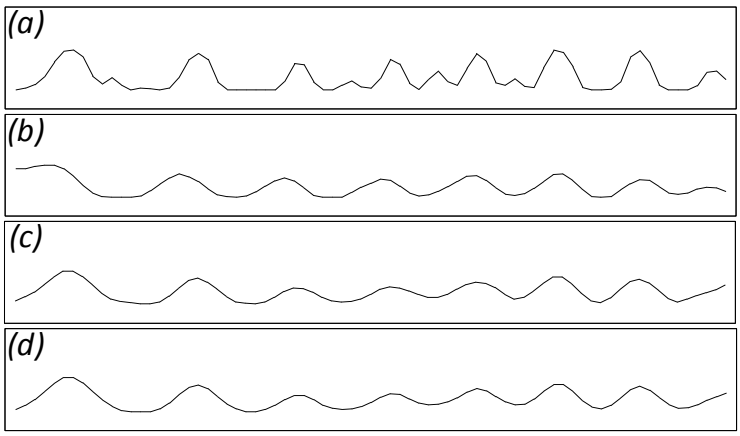


Figure 2.24 - Plot of a real fingerprint section *(a)* and plots obtained by: manually defocusing the device *(b)*, applying the Pillbox *(c)* and Butterworth *(d)* filters.

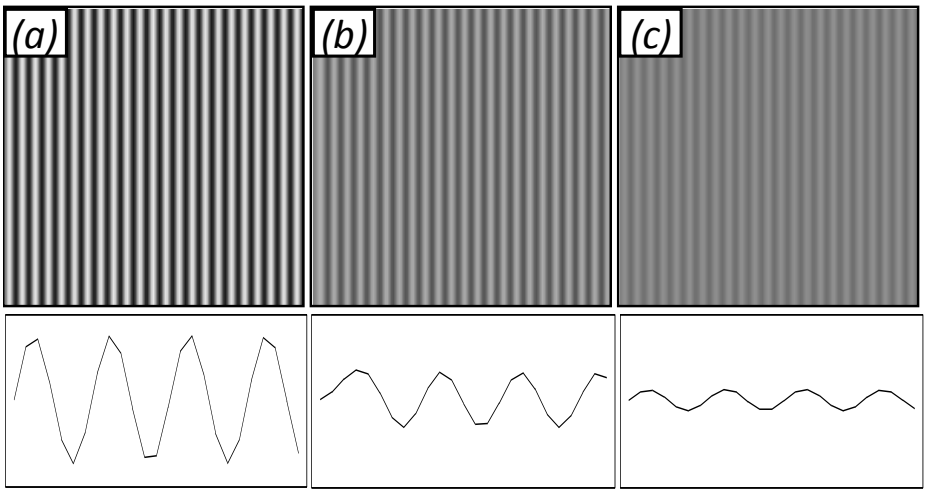


Figure 2.25 - First row: sinusoidal targets *(a)*, focus degradation using the Pillbox *(b)* and the Butterworth *(c)* filters. Second row: related plots of a horizontal section.

In Figure 2.26 the values of MTF, IQM and TSI are given as a function of the blurring grade introduced by applying different filters to targets of varying frequencies (F1-F10). The graphs show that, MTF and IQM are highly correlated (average correlation about 0,97) and exhibit the same decreasing trend.

As to TSI, the value measured for the lower frequencies is almost constant, while the trend related to the higher frequencies is decreasing. This is due to the invariance to given parameters that characterize TSI (see Subsection 2.6.3). In particular, for this kind of targets, the modification produced by the filters on the lower frequencies is mainly a reduction of the gray level range (see Figure 2.25) which is compensated by the pre-normalization step of TSI computation. In the higher frequency targets, the application of the filters produces an effective image deterioration, thus determining a lower TSI value. Differently from the test on the bar targets, the TSI value is different for varying frequencies due to the specific nature of the sinusoidal targets (the steepness of the transitions is not constant but depends on the frequency).

4. *Comparison between TSI and IQM: fingerprint images*

   The fourth set of experiments, carried out on fingerprint images, is aimed at comparing TSI and IQM in the evaluation of image focusing. Since MTF can only be calculated for sinusoidal targets, it will not be considered here; nevertheless the previous experiments showed the strict relation between IQM

and MTF and a comparison between IQM and TSI will give anyway a comprehensive analysis.

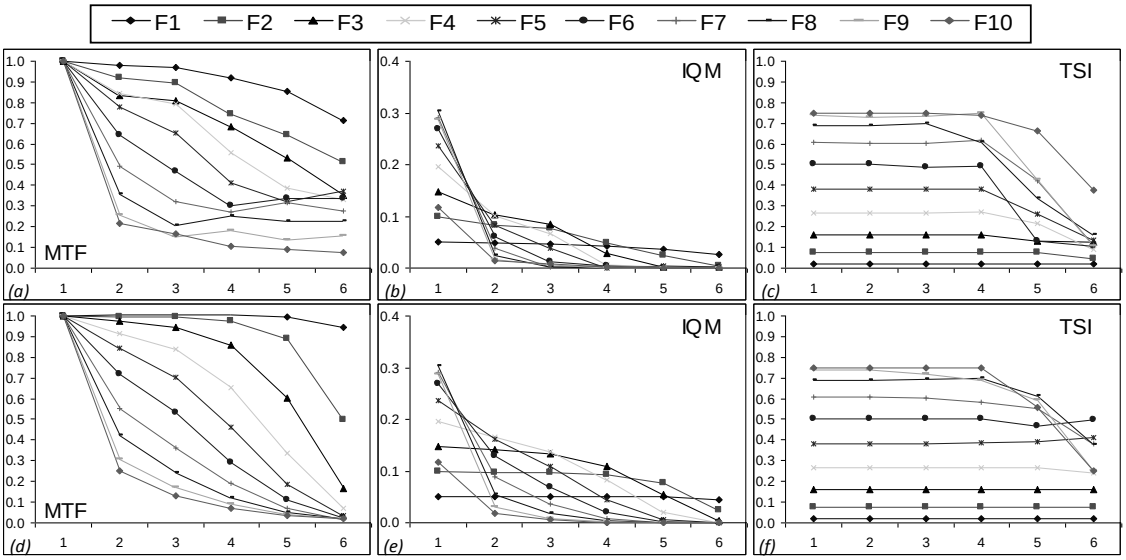
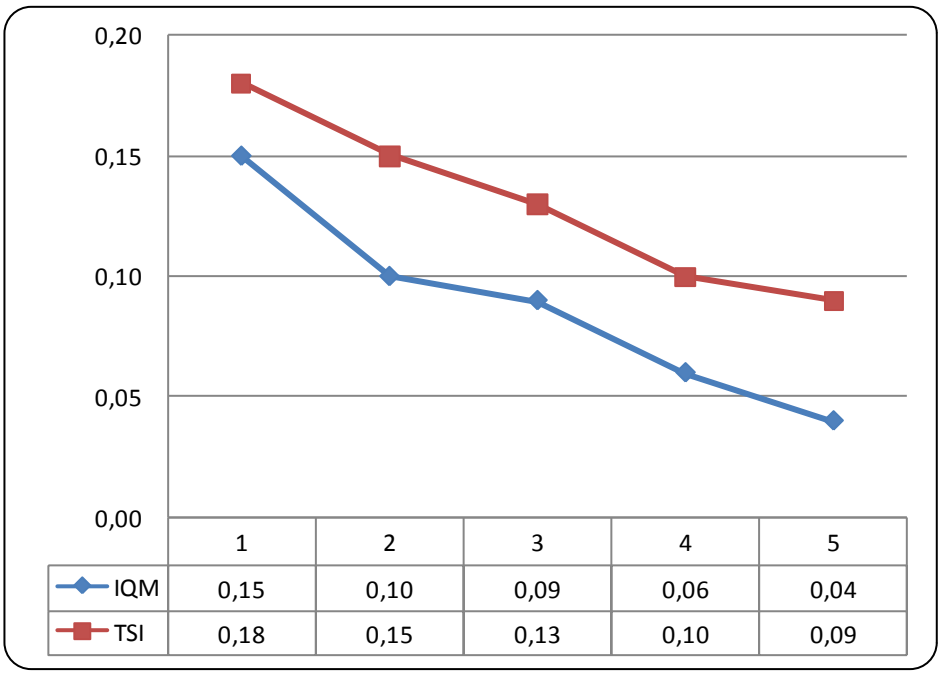


Figure 2.26 - MTF *(a,d)*, IQM *(b,e)* and TSI *(c,f)* values as a function of the blurring grade introduced by applying the Pillbox (first row) and Butterworth (second one) filters to sinusoidal targets.

TSI and IQM values have been calculated for a set of images of the same finger acquired by using an optical sensor while the lens focus was manually degraded (by gradually moving the lens away from the ideal position) (see Figure 2.23). Then the TSI and IQM values of each image are reported in Figure 2.27. The experimental results prove the strict relation between the proposed index, the IQM measurement and the device focusing.

Finally an extensive experimentation has been carried out on a large fingerprint database. It consists of 6400 images of 800 users. Each image has been gradually defocused by applying the two filtering techniques showed above. The results of the experiment are reported in Figure 2.28 were the TSI and IQM scores, averaged over the 6400 impressions, are plotted as a function of the blurring level introduced. In Figure 2.28a the Pillbox filter has been used, while the results in Figure 2.28b refer to the application of the Butterworth filter. Both the graphs confirm the relation between IQM and TSI (average correlation about 0,96), and the ability of the proposed index to effectively measure image focusing.



	1	2	3	4	5
IQM	0,15	0,10	0,09	0,06	0,04
TSI	0,18	0,15	0,13	0,10	0,09

Figure 2.27 - TSI and IQM values obtained from the images in Figure 2.23. The correlation between the two series is 0.99.

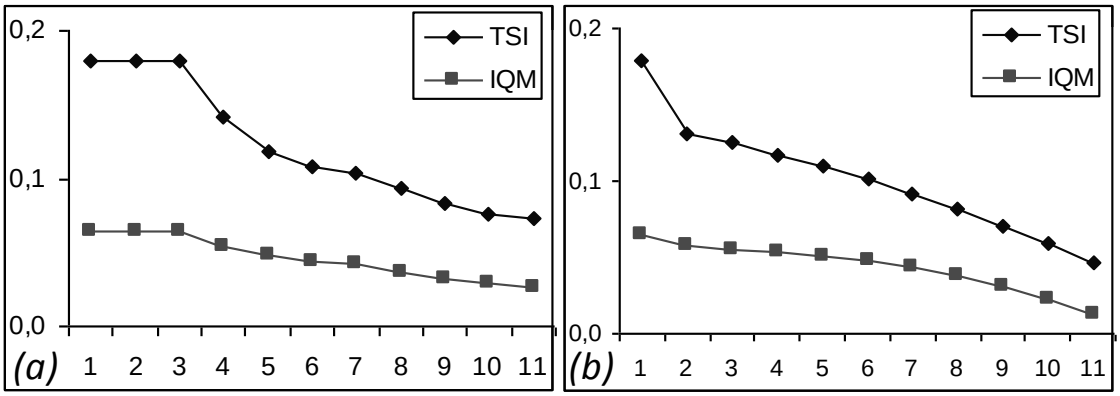


Figure 2.28 - Average TSI and IQM scores on fingerprint images as a function of the blurring level introduced by the application of the Pillbox *(a)* and Butterworth *(b)* filters.

To conclude, the experimental results confirmed the efficacy of TSI and its invariance with respect to the ridge/valley frequency and to the gray level range and showed that TSI behaves similarly to MTF and IQM in characterizing the level of image focusing but its computation is simpler and, more important, it is invariant with respect to those image characteristics (i.e. ridge/valley frequency and gray level range) that must not affect the measure.

2.7 Conclusions

This chapter addressed the problem of evaluating and certifying the "operational quality" of fingerprint scanners. To this purpose, the main quality parameters and the corresponding requirements defined in FBI IAFIS [20], PIV [22] and PassDEÜV [23] IQS have been considered and a large experimentation has been carried out to understand their effects on fingerprint recognition accuracy. To run the test described in Section 2.4, a total of 176,400 image transformations have been performed and a total of 16,314,200 fingerprint pairs have been compared.

These experiments shown that the most critical quality parameters are the Acquisition area and the Output resolution, which, at the PIV IQS minimum requirements, caused an average performance drop of 73% and 20%, respectively. On the other hand, other quality parameters (Signal to Noise Ratio, and Dynamic Range) do not seem to affect much the automated recognition performance.

Starting from these results, in cooperation with CNIPA, three new set of quality requirements, able to guarantee an optimal cost/performance tradeoff for (totally-automated) biometric applications, have been designed according to the above outcomes. Then, these new IQS are evaluated by comparing their potential effects on recognition accuracy with those caused by PIV and PassDEÜV ones.

Although the results of this analysis partially depend on the specific scanner used for collecting the test database, similar results would be obtained starting from images acquired by other scanners. According to the experimental results reported in Subsection 2.5.2, To conclude, the three proposed specifications are well suited for the applications they are targeted to. In particular:

- CNIPA-A specification is able to guarantee the best performance among the five IQS reviewed, thanks to the higher acquisition area, which proved to be the most important parameter;
- CNIPA-B specification is able to guarantee an accuracy that is clearly better than PIV and not too far from PassDEÜV; on the other hand, the cost of a device compliant to CNIPA-B would be definitely lower than that of one compliant to PassDEÜV, thanks to the less demanding requirements on five parameters;
- CNIPA-C specification can guarantee an accuracy similar to PIV but, also in this

case, the cost of a device compliant to CNIPA-C would be definitely lower than the cost of PIV-compliant devices.

Finally, a new quality index (TSI) to evaluate the fingerprint scanners focusing has been proposed and compared with two well known indicators, MTF and IQM. The experimental results show that TSI behaves similarly to MTF and IQM in characterizing the level of image focusing but its computation is simpler and, more important, it is invariant with respect to those image characteristics (i.e. ridge/valley frequency and gray level range) that must not affect the measure. Therefore it constitutes a very effective solution for measuring fingerprint scanner focusing.

3

MINUTIA CYLINDER-CODE

3.1 Introduction

Fingerprint recognition is an intriguing pattern recognition problem studied by more than forty years. Although very effective solutions are nowadays available, fingerprint recognition cannot be considered a fully solved problem, and the design of accurate, interoperable and computationally light algorithms is still an open issue [9].

Most fingerprint matching algorithms are based on minutiae (i.e., ridge ending and bifurcations). For a long time, minutiae matching had been treated as a 2D point pattern matching problem, aimed at determining the global (rigid) alignment leading to an optimal spatial (and directional) minutiae pairing. This formulation of the problem can be solved by searching the space of possible transformations: Hough transform is a common solution [39] [40]. Unfortunately, most of the global minutiae matching algorithms are computationally demanding, and lack of robustness with respect to non-linear fingerprint distortion.

In the last decade these weaknesses were addressed by introducing *local minutiae matching* techniques. Local minutiae structures are characterized by attributes that are invariant with respect to global transformations (e.g., translation, rotation, etc.) and therefore are suitable for matching without any a priori global alignment. Matching fingerprints based only on local minutiae arrangements relaxes global spatial relationships, which are highly distinctive, and therefore reduces the amount of information available for discriminating fingerprints. However, the benefits of both

local and global matching can be preserved by implementing hybrid strategies that perform a local structure matching followed by a consolidation stage. The local structure matching allows to quickly and robustly determine pairs of minutiae that match locally (i.e., whose neighboring features are compatible); the consolidation is aimed at verifying if and to what extent local matches hold at global level. It is worth noting that the consolidation step is not mandatory and a score can be directly derived from the local structure matching. The local matching itself can also lead to an early rejection in case of very different fingerprints.

Local minutiae matching algorithms evolved through three generations of methods: i) the earlier approaches whose local structures were typically formed by counting the number of minutiae falling inside some regions and no global consolidation was performed [41] [42]; ii) the approaches by Jiang and Yau [43] and Ratha et al. [44], who first effectively encoded the relationships between a minutia and its neighboring minutiae in term of invariant distances and angles, and proposed global consolidation; iii) the numerous variants and evolutions of Jiang and Yau [43] and Ratha et al. [44] methods, which typically extend the feature set by taking into account: local orientation field, local frequency, ridge shape, etc., see [45-70]. The reader may refer to [9] for an exhaustive review and classification of the literature on local minutiae matching.

Local minutiae structures can be classified into *nearest neighbor-based* and *fixed radius-based*. In the former family (well represented by Jiang and Yau's algorithm [43]), the neighbors of the central minutia are defined as its *K* spatially closest minutiae. This leads to fixed-length descriptors that can be usually matched very efficiently. In the latter (well represented by Ratha et al.'s algorithm [44]), the neighbors are defined as all the minutiae that are closer than a given radius *R* to the central minutia. The descriptor length is variable and depends on the local minutiae density; this can lead to a more complex local matching, but, in principle, is more tolerant against missing and spurious minutiae. Two drawbacks of [44] are: i) the absolute encoding of radial angles (whose corresponding relative encoding is denoted as d_R in Figure 3.7) that requires a sophisticated local matching and, ii) the missing directional difference between the central minutia and the neighboring ones (denoted as d_θ in Figure 3.7). Furthermore, the approach in [44], like most fixed-radius ones, can lead to border errors: in particular, minutiae close to the local-region border in one of the two fingerprints can be mismatched because local distortion or location inaccuracy may cause the same

minutiae to move out of the local region in the other fingerprint. The technique proposed by Feng in [49] does not suffer from the above drawbacks and can be considered a state-of-the-art fixed-radius local matching algorithm. In particular, the border problem is dealt with by considering minutiae not close to the border as *matchable* and minutiae near the border as *should-be-matchable*.

This chapter introduces a novel minutiae-only local representation aimed at combining the advantages of both neighbor-based and fixed-radius structures, without suffering from their respective drawbacks.

The rest of this chapter is organized as follows. Section 3.2 introduces the main motivations of this work and summarizes the advantages of the new technique. Section 3.3 defines the minutiae local structures and discusses how to measure the similarity between them. Section 3.4 proposes four simple approaches to consolidate local similarities into a global score. In Section 3.5, a large number of experiments are reported to compare the new approach with three "minutiae-only" implementations of the well-known approaches described in [43] [44] [49]. Finally Section 0 draws some concluding remarks.

3.2 Motivations and Contributions

The main motivations that induced us to design a new local minutiae matching technique are:

- *Need of accurate and interoperable minutiae-only algorithms*. Most of the fingerprint matching algorithms recently proposed exploit several extra features besides minutiae; in [10] some statistics about the features used by FVC2004 participants are reported. Researchers have shown that combining features (at least partially independent) is a very effective way to improve accuracy. On the other hand, unlike minutiae features, there is still no convergence on standards that precisely define and encode these extra features (one of the first attempt is CDEFFS (2008) [71] but it is still at an early stage). The world-wide large-scale deployment of fingerprint systems demands a new generation of accurate and highly interoperable algorithms and for this reason I believe that minutiae-only matching algorithms compliant to ISO/IEC 19794-2 (2005) [72] (or the very

similar ANSI/INCITS 378 (2004) [73]) will play a central role in the forthcoming years. Furthermore, minutiae-only templates also allow to compress into a few hundreds of bytes the salient fingerprint information, thus enabling their storage on inexpensive smart cards.

- *Portability on light architectures*. One effective way to secure biometric applications against external attacks is to confine the computation inside a closed system, that is a secure hardware platform such as a smart card or a system-on-a-chip. Unfortunately, the computational power of these low-cost secure platforms is hundred or thousand times lower than that of a modern PC [9] and resource demanding algorithms cannot be executed on board. Algorithms designers then concentrated on the development of simplified optimized versions, often based on local minutiae matching techniques and pre-computed information. However, recent MINEX II results [74] have shown that the best existing match-on-card algorithms cannot compete with the corresponding PC implementations and further research efforts are necessary. Analogous conclusions were drawn in [10] concerning the performance drop of the light category with respect to the open category in FVC2004.
- *Suitability for template protection techniques*. Template protection is currently receiving much attention because of the great benefits it can provide (e.g., non-reversibility, diversity and revocability): [75] [9]. Unfortunately, designing effective template protection techniques (e.g., fuzzy vault [76] [77] [78] [79] [80]), without incurring in a relevant accuracy drop, is very challenging and seems to require alignment free, fixed-length and noise-tolerant feature coding. At today, no fully satisfactory solution has been proposed.

The local minutiae representation introduced in this chapter is based on 3D data structures (called cylinders), built from invariant distances and angles in a neighborhood of each minutia. Cylinders can be created starting from a subset of mandatory features in standards like ISO/IEC 19794-2 (2005). In particular, only position and direction of the minutiae have been used, but not the minutiae type and the minutiae quality: in fact minutiae type is not a robust feature, and the definition of minutiae quality is not semantically clear in the standards (and could lead to interoperability problems). Thanks to the cylinder invariance, fixed-length and bit-oriented coding, some simple but effective metrics can be defined to compute cylinder similarity. Four global-scoring

techniques are then proposed to combine local similarities into a unique global score denoting the overall similarity between two fingerprints. The main advantages of the new method, called *Minutia Cylinder-Code* (MCC), are:

- MCC is a fixed-radius approach and therefore it tolerates missing and spurious minutiae better than nearest neighbor-based approaches.
- Unlike traditional fixed-radius techniques, MCC relies on a fixed-length invariant coding for each minutia and this makes the computation of local structure similarities very simple.
- Border problems are gracefully managed without extra burden in the coding and matching stages.
- Local distortion and small feature extraction errors are tolerated thanks to the adoption of smoothed functions (i.e., error tolerant) in the coding stage.
- MCC effectively deals with noisy fingerprint regions where minutiae extraction algorithms tend to place numerous spurious minutiae (close to each other); this is made possible by the saturation effect produced by a limiting function.
- The bit-oriented coding (one of the possible implementations of MCC) makes cylinder matching extremely simple and fast, reducing it to a sequence of bit-wise operations (e.g., AND, XOR) that can be efficiently implemented even on very simple CPUs.

3.3 The Local Structures

MCC representation associates a local structure to each minutia. This structure encodes spatial and directional relationships between the minutia and its (fixed-radius) neighborhood and can be conveniently represented as a cylinder whose base and height are related to the spatial and directional information, respectively (Figure 3.1).

Let $T = \{m_1, m_2, .., m_n\}$ be an ISO/IEC 19794-2 minutiae template [72]: each minutia m is a triplet $m = \{x_m, y_m, \theta_m\}$ where x_m and y_m are the minutia location, θ_m is the minutia direction (in the range $[0,2\pi[$). In the following, Subsection 3.3.1 describes how the local structure of a given minutia m is built; Subsection 3.3.2 discusses the creation of a whole cylinder-set from T, and Subsection 3.3.3 introduces a similarity measure between cylinders; finally, Subsection 3.3.4 focuses on a bit-oriented efficient

implementation.

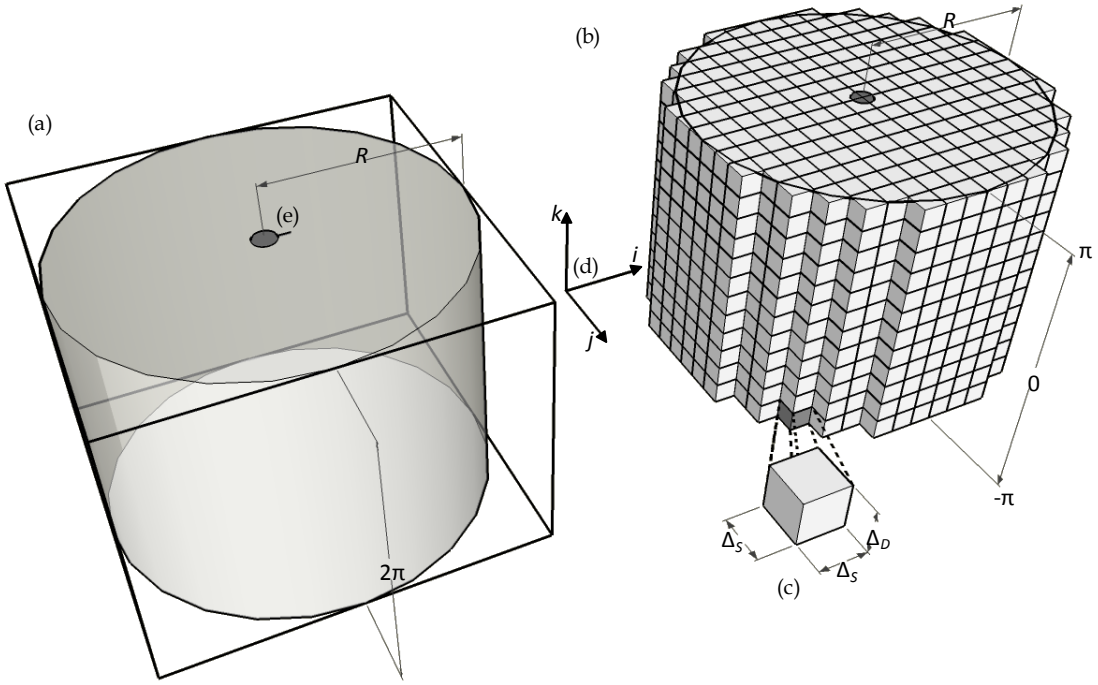


Figure 3.1 - A graphical representation of the local structure associated to a given minutia: (a) the cylinder with the enclosing cuboid; (b) the discretization of the cuboid into cells (c) of size $\Delta_S \times \Delta_S \times \Delta_D$: only cells whose center is within the cylinder are shown. Note that the cylinder is rotated so that axis i (d) is aligned to the direction of the corresponding minutia (e).

3.3.1 The Cylinder of a given minutia

The local structure associated to a given minutia $m = \{x_m, y_m, \theta_m\}$ is represented by a cylinder with radius R and height 2π, whose base is centered on the minutia location (x_m, y_m), see Figure 3.1.a.

The cylinder is enclosed inside a cuboid whose base is aligned according to the minutiae direction θ_m; the cuboid is discretized into $N_C = N_S \times N_S \times N_D$ cells. Each cell is a small cuboid with $\Delta_S \times \Delta_S$ base and Δ_D height, where $\Delta_S = \frac{2 \cdot R}{N_S}$ and $\Delta_D = \frac{2\pi}{N_D}$ (Figure 3.1.b).

Each cell can be uniquely identified by three indices (i, j, k) that denote its position in the cuboid enclosing the cylinder, with $i, j \in I_S = \{n \in \mathbb{N}, 1 \leq n \leq N_S\}$ and $k \in I_D = \{n \in \mathbb{N}, 1 \leq n \leq N_D\}$.

Let

$$d\varphi_k = -\pi + \left(k - \frac{1}{2}\right) \cdot \Delta_D \tag{3.1}$$

be the angle associated to all cells at height k in the cylinder, and let

$$p_{i,j}^m = \begin{bmatrix} x_m \\ y_m \end{bmatrix} + \Delta_S \cdot \begin{bmatrix} \cos(\theta_m) & \sin(\theta_m) \\ -\sin(\theta_m) & \cos(\theta_m) \end{bmatrix} \cdot \begin{bmatrix} i - \frac{N_S + 1}{2} \\ j - \frac{N_S + 1}{2} \end{bmatrix} \tag{3.2}$$

be the two-dimensional point corresponding to the center of the cells with indices i, j (projected onto the cylinder's base), expressed in the spatial coordinates of the minutiae template; since these points are projected onto the base, index k is not needed.
For each cell (i, j, k), a numerical value $C_m(i, j, k)$ is calculated by accumulating contributions from each minutia m_t belonging to the neighborhood $N_{p_{i,j}^m}$ of $p_{i,j}^m$:

$$N_{p_{i,j}^m} = \left\{ m_t \in T; m_t \neq m, d_S\left(m_t, p_{i,j}^m\right) \leq 3\sigma_S \right\} \tag{3.3}$$

where $3\sigma_S$ is the radius of the neighborhood (see Figure 3.2) and $d_S(m, p)$ is the Euclidean distance between minutia m and point p.
Function C_m: $I_S \times I_S \times I_D \rightarrow V$ is defined as follows:

$$C_m(i, j, k) = \begin{cases} \Psi\left(\sum_{m_t \in N_{p_{i,j}^m}} \left(C_m^S\left(m_t, p_{i,j}^m\right) \cdot C_m^D(m_t, d\varphi_k)\right)\right) & \text{if } \xi_m\left(p_{i,j}^m\right) = valid \\ invalid & \text{otherwise} \end{cases} \tag{3.4}$$

where:

- $V = [0,1] \cup \{invalid\}$ is the function codomain.
- The two terms $C_m^S\left(m_t, p_{i,j}^m\right)$ and $C_m^D(m_t, d\varphi_k)$ are the spatial and directional contribution of minutia m_t, respectively (they will be described in the following paragraphs).
- $\xi_m\left(p_{i,j}^m\right) = \begin{cases} valid & \text{if } d_S\left(m, p_{i,j}^m\right) \leq R \text{ and } p_{i,j}^m \in Conv_{Hull}(T, \Omega) \\ invalid & \text{otherwise} \end{cases}$
  where $Conv_{Hull}(T, \Omega)$ is the convex hull [81] of the minutiae in T, enlarged by

adding an offset of Ω pixels (see Fig. Figure 3.5.a). Intuitively, a cell is considered as $valid$ if and only if its center $p_{i,j}^m$ is contained in the intersection of the cylinder's base with the convex hull determined by all the minutiae in T (see Figure 3.5.b): this condition is important to avoid considering portions of the cylinder that probably lie outside the fingerprint area and hence cannot contain relevant information.

- $\Psi(v) = Z(v, \mu_\Psi, \tau_\Psi)$ is a sigmoid function, controlled by two parameters (μ_Ψ and τ_Ψ), that limits the contribution of dense minutiae clusters (typical of noisy regions), and ensures the final value is in the range $[0,1]$; the sigmoid function is defined as:

$$\mathrm{Z}(v, \mu, \tau) = \frac{1}{1 + e^{-\tau \cdot (v - \mu)}} \tag{3.5}$$

Basically, the value $C_m(i,j,k)$ of a valid cell represents the likelihood of finding minutiae near $p_{i,j}^m$ with a directional difference, with respect to m, close to $d\varphi_k$. This likelihood is obtained by summing the contributions of all the minutiae in neighborhood $N_{p_{i,j}^m}$. The contribution of each minutia m_t is defined as the product of C_m^S and C_m^D.

$C_m^S\left(m_t, p_{i,j}^m\right)$ is the spatial contribution that minutia m_t gives to cell (i,j,k); it is defined as a function of the Euclidean distance between m_t and $p_{i,j}^m$:

$$C_m^S\left(m_t, p_{i,j}^m\right) = G_S\left(d_S\left(m_t, p_{i,j}^m\right)\right) \tag{3.6}$$

where

$$G_S(t) = \frac{1}{\sigma_S\sqrt{2\pi}} e^{\left(-\frac{t^2}{2\sigma_S^2}\right)} \tag{3.7}$$

is the Gaussian function with zero mean and σ_S standard deviation.

Figure 3.2 graphically shows the values of $G_S(t)$ in the neighborhood of a given cell (darker areas represent higher values). It is worth noting that minutiae involved in the

computation of $C_m(i,j,k)$ do not necessarily lie inside the base of the cylinder centered in m with radius R; in fact, minutiae lying in the offset region $[R, R+3\sigma_S]$ still contribute to $C_m(i,j,k)$ and this allow to avoid the tedious border effect.

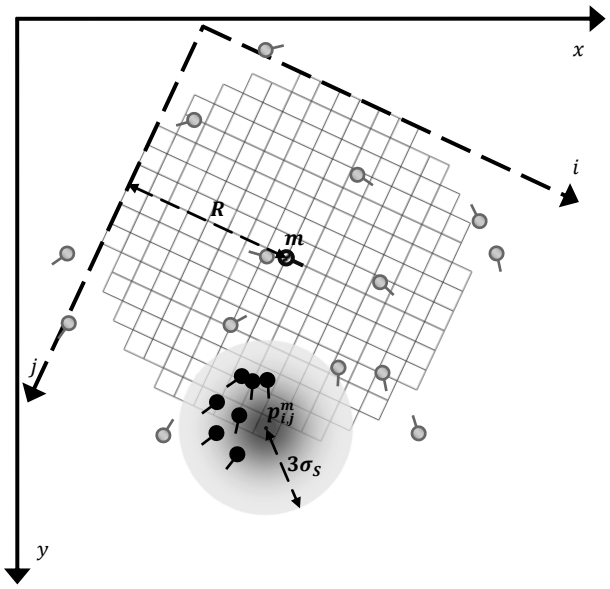


Figure 3.2 - Section of a cylinder associated to a minutia m. All the minutiae involved in the construction of the cylinder are shown. Note that they do not necessarily lie inside the cylinder base, since an offset of $3\sigma_S$ is allowed. $G_S(t)$ values in the neighborhood of a given cell (with center $p_{i,j}^m$) are highlighted (darker areas represents higher values). The black minutiae are those within neighborhood $N_{p_{i,j}^m}$.

$C_m^D(m_t, d\varphi_k)$ is the directional contribution of m_t; it is defined as a function of: i) $d\varphi_k$, and ii) the directional difference between θ_m and θ_{m_t}. Intuitively, the contribution is high when i) and ii) are close to each other.

$$C_m^D(m_t, d\varphi_k) = G_D\left(d\phi\left(d\varphi_k, d_\theta(m, m_t)\right)\right) \tag{3.8}$$

where $d\phi(\theta_1, \theta_2)$ is the difference between two angles θ_1, θ_2:

$$d\phi(\theta_1,\theta_2) = \begin{cases} \theta_1 - \theta_2 & \text{if } -\pi \le \theta_1 - \theta_2 < \pi \\ 2\pi + \theta_1 - \theta_2 & \text{if } \theta_1 - \theta_2 < -\pi \\ 2\pi - \theta_1 + \theta_2 & \text{if } \theta_1 - \theta_2 \ge \pi \end{cases} \tag{3.9}$$

and $d_\theta(m_1, m_2)$ is the directional difference between two minutiae:

$$d_\theta(m_1, m_2) = d\phi\left(\theta_{m_1}, \theta_{m_2}\right) \tag{3.10}$$

$G_D(\alpha)$ is the area under a Gaussian (with zero mean and standard deviation σ_D), in the interval $\left[\alpha - \frac{\Delta_D}{2}, \alpha + \frac{\Delta_D}{2}\right]$:

$$G_D(\alpha) = \frac{1}{\sigma_D\sqrt{2\pi}} \int_{\alpha-\frac{\Delta_D}{2}}^{\alpha+\frac{\Delta_D}{2}} e^{-\frac{t^2}{2\sigma_D^2}}\, dt \tag{3.11}$$

Figure 3.3 shows the local structure associated to a given minutia m in a simplified case where there is only one minutia that contributes to cell values $C_m(i, j, k)$. Figure 3.4 shows the cylinder associated to a minutia with five minutiae in its neighborhood.

3.3.2 Creation of a Cylinder-Set

The cylinder-set obtained from an ISO/IEC 19794-2 minutiae template T is defined as:

$$CS = \{C_m | C_m \; is \; not \; invalid, m \in T\} \tag{3.12}$$

where C_m is the cylinder associated to minutia m, containing values $C_m(i, j, k)$. A cylinder C_m is considered $invalid$ in the following cases:

- there are less than min_{VC} $valid$ cells in the cylinder;
- there are less than min_M minutiae that contribute to the cylinder (i.e., there are less than min_M minutiae m_t such that $d_S(m_t, m) \leq R + 3\sigma_S$, with $m_t \neq m$).

Figure 3.5 shows a minutia template and three valid cylinders from the corresponding cylinder-set.

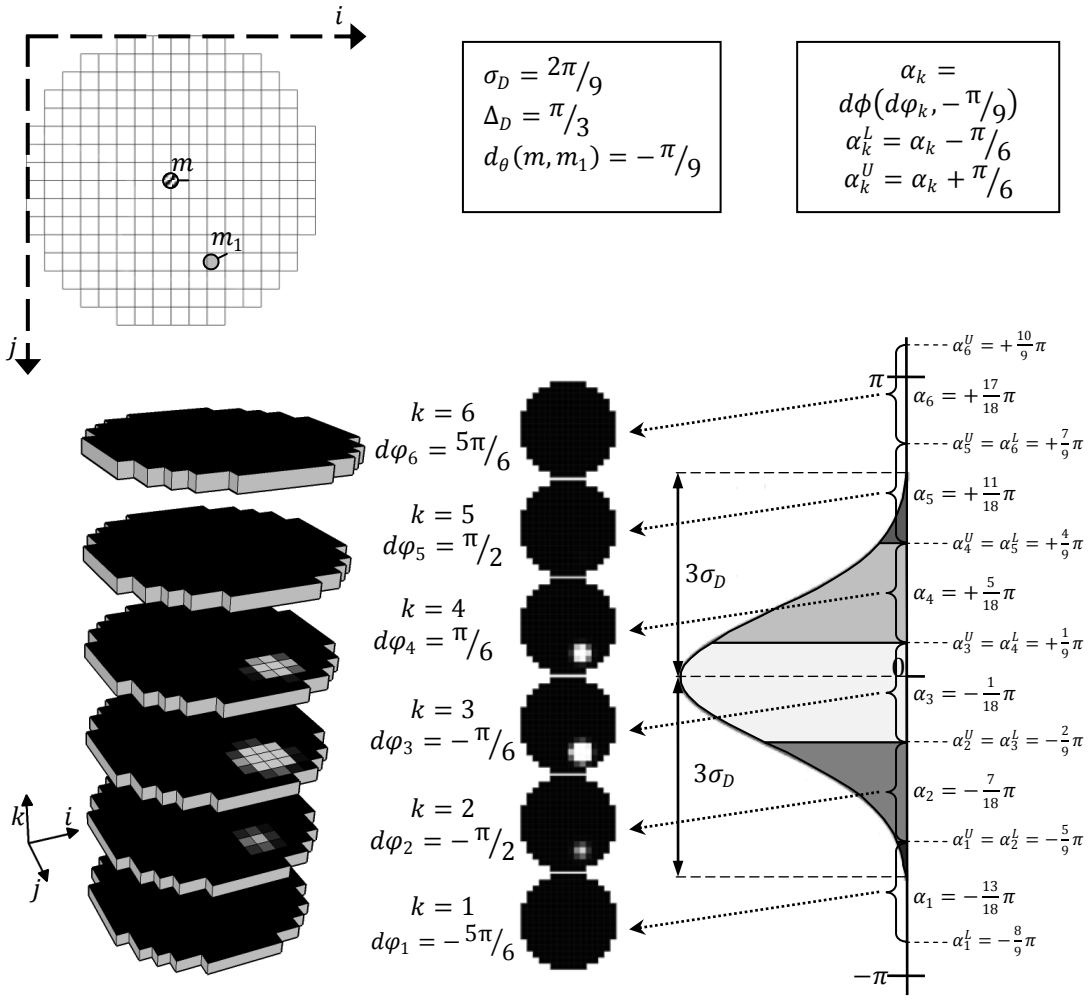


Figure 3.3 - A simplified case where only one minutia (m_1) contributes to the cylinder associated to minutia m. Different $C_m(i,j,k)$ values are represented by different gray levels (the lighter, the greater). The N_D areas (six in this example) under the Gaussian curve are graphically highlighted and the relevant values in equations (3.8) and (3.11) are numerically exemplified for each k: in particular, $\alpha_k = d\phi\left(d\varphi_k, d_\theta(m, m_1)\right)$ is the input value of function G_D in (3.8), while α_k^L and α_k^U are the lower and upper limits of the integral in (3.11), respectively. In practice, minutia m_1 contributes to more cylinder sections with different weights, according to its directional difference with m. Note that non-zero cell values are not perfectly symmetric with respect to the cell containing m_1: this is because m_1 does not exactly lie in the center of the cell.

3.3.3 The Similarity between Two Cylinders

Each cylinder is a local data structure:

- invariant for translation and rotation, since i) it only encodes distances and directional differences between minutiae (see equations (3.6) and (3.8)), and ii) its base is rotated according to the corresponding minutia direction, see equation

(3.2);

- robust against skin distortion (which is small at a local level) and against small feature extraction errors, thanks to the smoothed nature of the functions defining the contribution of each minutia (see (3.7) and (3.11)), and to the limiting function Ψ in (3.4);
- with a fixed-length given by the number of cells N_C.

For the above reasons, the similarity between two cylinders can be simply defined using a vector correlation measure, as described in the following paragraphs.

Given a cylinder C_m, let lin: $I_S \times I_S \times I_D \rightarrow \mathbb{N}$ be a function that linearizes the cylinder cell indices:

$$lin(i,j,k) = (k-1) \cdot (N_S)^2 + (j-1) \cdot N_S + i \tag{3.13}$$

and let $\mathbf{c}_m \in V^{N_C}$ be the vector derived from C_m (V is the codomain of (3.4)), according to (3.13):

$$\mathbf{c}_m[lin(i,j,k)] = C_m(i,j,k) \tag{3.14}$$

Given two minutiae a and b, let $\mathbf{c}_a$ and $\mathbf{c}_b$ be the vectors derived from cylinders C_a and C_b: two corresponding elements $\mathbf{c}_a[t]$ and $\mathbf{c}_b[t]$ are considered as *matchable* if and only if $\mathbf{c}_a[t] \neq invalid \wedge \mathbf{c}_b[t] \neq invalid$. Let $\mathbf{c}_{a|b}, \mathbf{c}_{b|a} \in [0,1]^{N_C}$ be the two vectors derived from $\mathbf{c}_a$ and $\mathbf{c}_b$ considering *matchable* elements only:

$$\mathbf{c}_{a|b}[t] = \begin{cases} \mathbf{c}_a[t] & \text{if } \mathbf{c}_a[t] \text{ and } \mathbf{c}_b[t] \text{ are } matchable \\ 0 & \text{otherwise} \end{cases} \tag{3.15}$$

$$\mathbf{c}_{b|a}[t] = \begin{cases} \mathbf{c}_b[t] & \text{if } \mathbf{c}_b[t] \text{ and } \mathbf{c}_a[t] \text{ are } matchable \\ 0 & \text{otherwise} \end{cases} \tag{3.16}$$

In practice, *matchable* elements corresponds to the intersection of the valid cells of the two cylinders.

The similarity between the two cylinders is defined as:

$$\gamma(a,b) = \begin{cases} 1 - \dfrac{\left\| \mathbf{c}_{a|b} - \mathbf{c}_{b|a} \right\|}{\left\| \mathbf{c}_{a|b} \right\| + \left\| \mathbf{c}_{b|a} \right\|} & \text{if } C_a \text{ and } C_b \text{ are } matchable \\ 0 & \text{otherwise} \end{cases} \tag{3.17}$$

where two cylinders are *matchable* if the following conditions are met:

1. the directional difference between the two minutiae is not greater than δ_θ ($d\phi(\theta_a, \theta_b) \leq \delta_\theta$);
2. at least min_{ME} corresponding elements in the two vectors $\mathbf{c}_a$ and $\mathbf{c}_b$ are *matchable*;
3. $\left\|\mathbf{c}_{a|b}\right\| + \left\|\mathbf{c}_{b|a}\right\| \neq 0$.

The first condition helps to reduce the number of *matchable* cylinders by assuming a maximum possible rotation between the two fingerprints; the second condition avoids to compare cylinders with a too small valid intersection; the third condition excludes the case where a sufficiently-large valid intersection of two valid cylinders does not contain any information.

Note that $\gamma(a, b)$ is always in the range $[0,1]$: zero means no similarity and one denotes maximum similarity. In the following, depending on the context, $\gamma(a, b)$ has been used to refer to the cylinder similarity, the local structure similarity or the minutiae similarity; because of the 1:1 relationship between minutiae and cylinders, this notation flexibility does not lead to ambiguities.

3.3.4 Bit-based Implementation

The characteristics of the local structures and similarity measure introduced in the previous sections make MCC well suited for a bit-based implementation. To this purpose, $\Psi(v)$ in equation (3.4) may be changed from a sigmoid to a unit step function:

$$\Psi_{Bit}(v) = \begin{cases} 1 & \text{if } v \geq \mu_\Psi \\ 0 & \text{otherwise} \end{cases} \tag{3.18}$$

thus constraining the codomain of $C_m(i, j, k)$ to the binary values 0, 1 and $invalid$. In such an implementation, a given cylinder C_m can be stored as two bit-vectors $\mathbf{c}_m, \hat{\mathbf{c}}_m \in \{0,1\}^{N_C}$, the former storing the cell values, and the latter denoting the cell validities (see also (3.13)):

$$\begin{aligned} \mathbf{c}_m[lin(i, j, k)] &= \begin{cases} 1 & \text{if } C_m(i, j, k) = 1 \\ 0 & \text{otherwise} \end{cases} \\ \hat{\mathbf{c}}_m[lin(i, j, k)] &= \begin{cases} 1 & \text{if } C_m(i, j, k) \neq invalid \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{3.19}$$

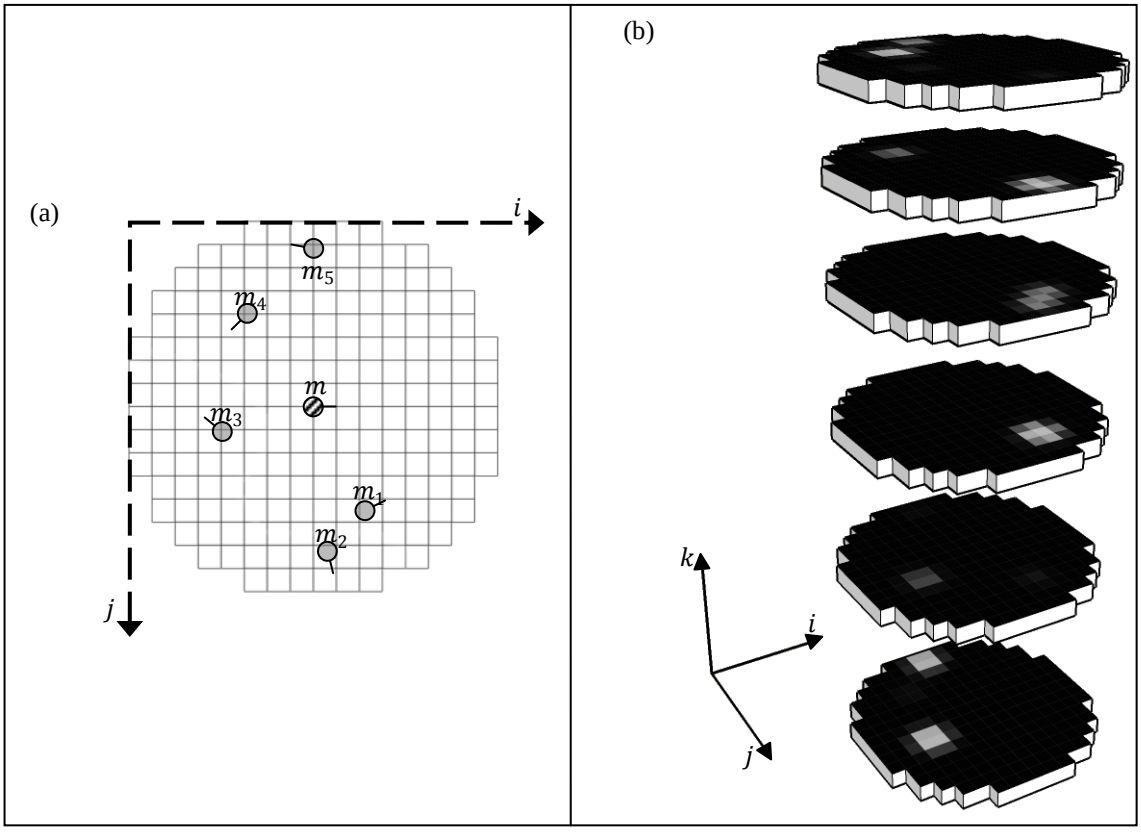


Figure 3.4 - A graphical representation of a cylinder: the minutiae involved (a) and the cell values (b): lighter areas represent higher values.

(3.15) and (3.16) can be calculated as follows:

$$\mathbf{c}_{a|b} = \mathbf{c}_a \text{ AND } \hat{\mathbf{c}}_{ab} \text{ , } \mathbf{c}_{b|a} = \mathbf{c}_b \text{ AND } \hat{\mathbf{c}}_{ab} \tag{3.20}$$

where AND denotes the *bitwise-and* between two bit-vectors, and $\hat{\mathbf{c}}_{ab} = \hat{\mathbf{c}}_a \text{AND } \hat{\mathbf{c}}_b$ is the intersection of the two masks. Finally, the similarity between the two cylinders can be computed as:

$$\gamma_{Bit}(a,b) = \begin{cases} 1 - \dfrac{\left\|\mathbf{c}_{a|b} \text{ XOR } \mathbf{c}_{b|a}\right\|}{\left\|\mathbf{c}_{a|b}\right\| + \left\|\mathbf{c}_{b|a}\right\|} & \text{if } C_a \text{ and } C_b \text{ are } matchable \\ 0 & \text{otherwise} \end{cases} \tag{3.21}$$

where XOR denotes the *bitwise-exclusive-or* between two bit-vectors. Note that the norm of a bit-vector can be simply computed by calculating the square root of the number of bits with value one. Figure 3.6 shows an example of cylinder obtained using the bit-based implementation.

Table 3.1 compares the number of floating point and integer operations involved in the computation of the similarity between two cylinders for a normal and bit-based implementation, respectively. Note that the bit-based implementation requires only five floating point operations and a very small number of integer and bitwise operations. Hence, (3.20) and (3.21) can be implemented very efficiently, even on light architectures (e.g., smart cards), where floating point operations are absent or very slow because they have to be replaced by surrogates (fixed point arithmetic or software emulation).

Table 3.1 - Number of operations required to compute the similarity between two cylinders.

	Normal implementation		*Bit-based implementation*	
	as a function of N_C	for $N_C = 1536^{\dagger}$	as a function of N_C and $rs^{\ddagger}$	for $N_C = 1536$, $rs = 32$
Square root extraction (float)	3	3	3	3
Multiplications and divisions (float)	$3 \cdot N_C + 1$	4609	1	1
Sums and subtractions (float)	$4 \cdot N_C - 1$	6143	1	1
Comparisons (i.e., checking if a value is $invalid$) (float)	$2 \cdot N_C$	3072	0	0
Sums (integer)	0	0	$\frac{3 \cdot N_C}{rs} - 2$	142
Counting number of 1's in a register	0	0	$\frac{3 \cdot N_C}{rs}$	144
Bitwise AND	0	0	$\frac{3 \cdot N_C}{rs}$	144
Bitwise XOR	0	0	$\frac{N_C}{rs}$	48

† $N_C = 1536$ *corresponds to* $N_S = 16$ *and* $N_D = 6$*, which are the default values in our implementation (see Table 3.2).*

‡ *Number of bits in the CPU registers.*

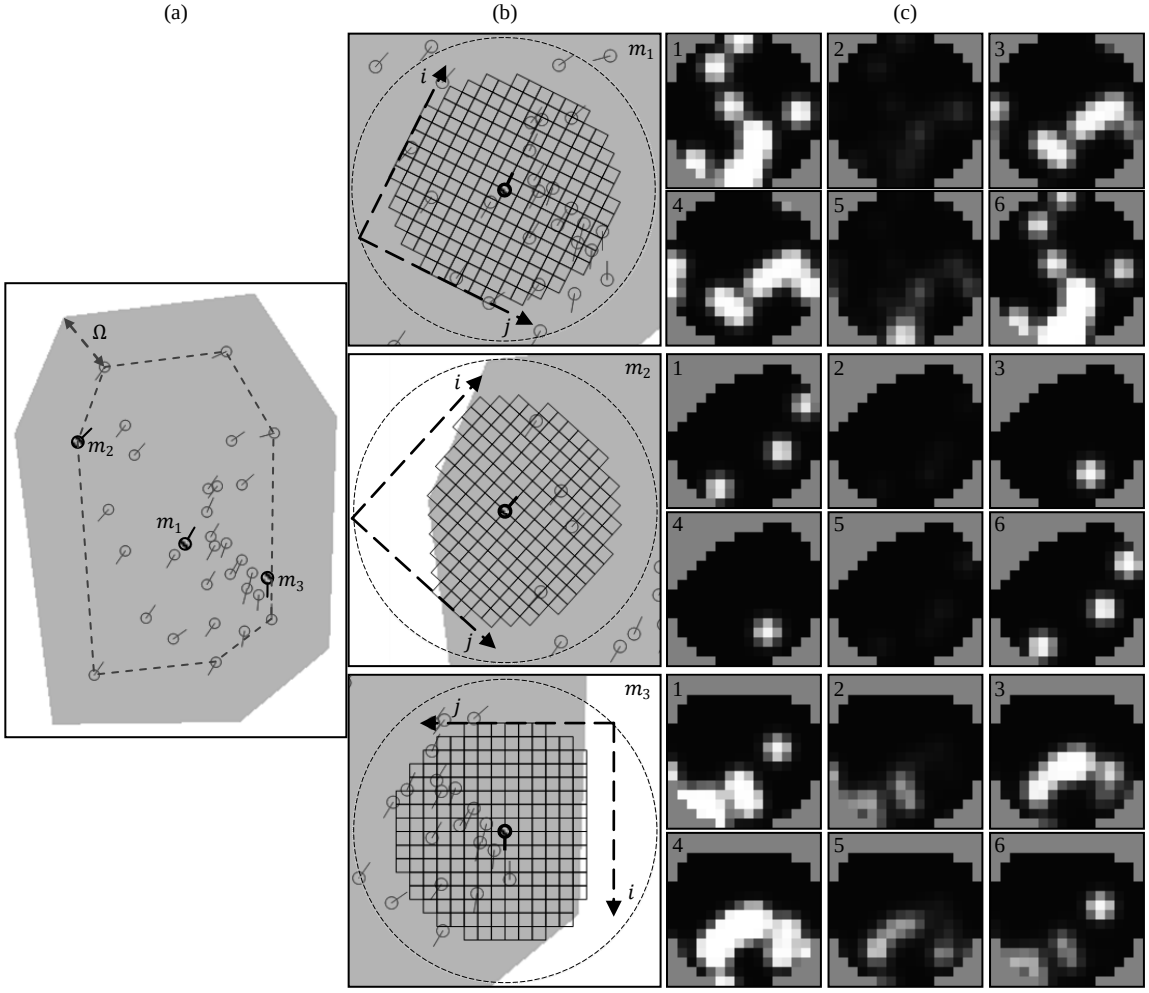


Figure 3.5 - A minutiae template with the corresponding convex hull (a). For each of the three minutiae highlighted in (a), column (b) shows the base of the corresponding cylinder (only valid cells are drawn); minutiae within the dashed circles are those that contribute to the cylinder cell values. Column (c) shows the cell values of the three cylinders for each value of $k \in \{1, \ldots, 6\}$ (lighter elements represent higher values); note that the cylinder sections in (c) are rotated according to the direction of the corresponding minutia.

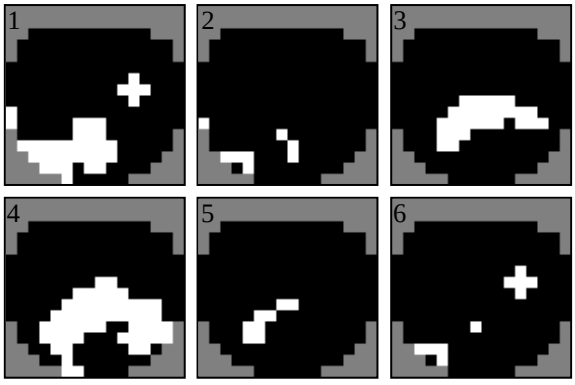


Figure 3.6 - The cell values of the cylinder associated to minutia m_3 in Figure 3.5 using the bit-based implementation (black=0, white=1, gray=$invalid$).

3.4 Global Score and Consolidation

In the previous section, a measure of local similarity between cylinders has been proposed. In order to compare two minutiae templates (i.e., two fingerprints), a single value (*global score*), denoting their overall similarity, has to be obtained from the local similarities. In the following, four simple techniques, inspired to ideas already proposed in the literature, are introduced to combine local similarities into a global score.

The first two may be classified as "pure local techniques", since they only combine local similarities; the other two implement a consolidation step to obtain a score that reflects to what extent the local relationships hold at global level. In the experimental evaluation, where MCC is compared to three well-known local algorithms, these four techniques are applied both to MCC and to the other ones.

Given two ISO/IEC 19794-2 minutiae templates $A = \{a_1, a_2, \dots, a_{n_A}\}$ and $B = \{b_1, b_2, \dots, b_{n_B}\}$, let:

- $\gamma(a, b)$ be the local similarity between minutia $a \in A$ and $b \in B$, with $\gamma: A \times B \rightarrow [0,1]$;
- $\Gamma \in [0,1]^{n_A \times n_B}$ be a matrix containing all the local similarities, with $\Gamma[r, c] = \gamma(a_r, b_c)$.

3.4.1 Local Similarity Sort (LSS)

This technique sorts all the local similarities and selects the top n_P; let P be the set of selected n_P minutiae-index pairs:

$$P = \{(r_t, c_t)\}, t = 1, \dots, n_P, 1 \leq r_t \leq n_A, 1 \leq c_t \leq n_B \tag{3.22}$$

the global score is calculated as the average of the corresponding local similarities:

$$S(A, B) = \frac{\sum_{(r,c) \in P} \Gamma[r, c]}{n_P} \tag{3.23}$$

The value of n_P is not an overall constant, since it partially depends on the number of minutiae in the two templates:

$$n_P = min_{n_P} + \left\lfloor \left(\mathrm{Z}(\min\{n_A, n_B\}\ , \mu_P, \tau_P)\right) \cdot \left(max_{n_p} - min_{n_p}\right) \right\rceil \qquad (3.24)$$

where μ_P, τ_P, min_{n_P}, and max_{n_p} are parameters, and Z is the sigmoid function defined in (3.5), and $\lfloor \cdot \rceil$ denotes the rounding operator.

3.4.2 Local Similarity Assignment (LSA)

The Hungarian algorithm [82] is used to solve the linear assignment problem on matrix Γ, that is to find the set of n_P pairs $P = \{(r_i, c_i)\}$ that maximizes $S(A, B)$ in (3.23) without considering the same minutia more than once (note that this is not guaranteed by LSS). The value of n_P and the global score are calculated as in (3.24) and (3.23), respectively.

3.4.3 Local Similarity Sort with Relaxation (LSS-R)

This technique is inspired from the relaxation approach initially proposed in [83] and recently applied to triangular minutiae structures in [70]. The basic idea is to iteratively modify the local similarities based on the compatibility among minutiae relationships. In particular, given a pair of minutiae (a, b), if the global relationships among a and some other minutiae in A are compatible with the global relationships among b and the corresponding minutiae in B, then the local similarity between a and b is strengthened, otherwise it is weakened.

As a preliminary step, n_R pairs (r_t, c_t) are selected using the LSS technique, with $n_R = \min\{n_A, n_B\}$ (usually $n_R \gg n_P$).

Let $\lambda_t^0 = \Gamma[r_t, c_t]$ be the initial similarity of pair t; the similarity at iteration i of the relaxation procedure is:

$$\lambda_t^i = w_R \cdot \lambda_t^{i-1} + (1 - w_R) \cdot \frac{\left(\sum_{\substack{k=1 \\ k \neq t}}^{n_R} \rho(t,k) \cdot \lambda_k^{i-1} \right)}{(n_R - 1)} \tag{3.25}$$

where $w_R \in [0,1]$ is a weighting factor and

$$\begin{aligned} \rho(t,k) &= \prod_{i=1}^{3} \mathrm{Z}\left(d_i, \mu_i^\rho, \tau_i^\rho\right) \\ d_1 &= \left| d_S\left(a_{r_t}, a_{r_k}\right) - d_S\left(b_{c_t}, b_{c_k}\right) \right| \\ d_2 &= \left| d\phi\left(d_\theta\left(a_{r_t}, a_{r_k}\right), d_\theta\left(b_{c_t}, b_{c_k}\right)\right) \right| \\ d_3 &= \left| d\phi\left(d_R\left(a_{r_t}, a_{r_k}\right), d_R\left(b_{c_t}, b_{c_k}\right)\right) \right| \end{aligned} \tag{3.26}$$

$\rho(t,k)$ is a measure of the compatibility between two pairs of minutiae: minutiae $\left(a_{r_t}, a_{r_k}\right)$ of template A and minutiae $\left(b_{c_t}, b_{c_k}\right)$ of template B. The compatibility value is based on the similarity between three features that are invariant for rotation and translation (see Figure 3.7); it is calculated as the product of three terms: d_1, d_2, and d_3, which are normalized by means of sigmoid functions (3.5) with specific parameters. d_1 denotes the similarity between the minutiae spatial distances, d_2 compares the directional differences, and d_3 compares the *radial angles*. The radial angle is defined as the angle subtended by the edge connecting the two minutiae and the direction of the first one (Figure 3.7):

$$d_R(m_1, m_2) = d\phi\left(\theta_{m_1}, \mathrm{atan2}\left(y_{m_2} - y_{m_1}, x_{m_2} - x_{m_1}\right)\right) \tag{3.27}$$

n_{rel} iterations of the relaxation procedure are executed on all the n_R pairs; then, similarly to [70], the *efficiency* of pair t is calculated as:

$$\varepsilon_t = \frac{\lambda_t^{n_{rel}}}{\lambda_t^0} \tag{3.28}$$

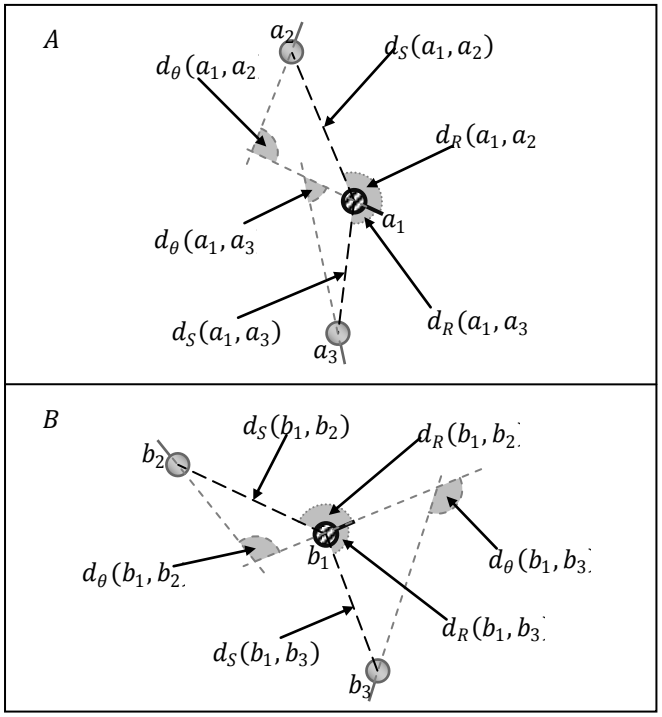


Figure 3.7 - An example of the global relationships considered in the relaxation procedure. The similarity λ_1^i between minutiae a_1 and b_1 is modified according to: i) the compatibility between the global relationships $a_1 \leftrightarrow a_2$ and $b_1 \leftrightarrow b_2$ ($\rho(1,2)$), ii) the compatibility between $a_1 \leftrightarrow a_3$ and $b_1 \leftrightarrow b_3$ ($\rho(1,3)$). The three invariant features used to calculate $\rho(t,k)$ are graphically highlighted: i) the spatial distances (dashed black lines), ii) the directional differences (gray angles with dashed border), and iii) the radial angles (gray angles with dotted border).

Intuitively, a high efficiency is achieved for the pairs of minutiae whose similarity is substantially strengthened because of high compatibility with other pairs, whereas pairs of local structures that initially obtained a high similarity by chance, will be penalized by the relaxation process and their final efficiency will be quite low.

To determine the global score, the n_P pairs with the largest efficiency are selected from the n_R pairs (the value of n_P is calculated as in (3.24)). The global score is computed as in (3.23), but using the relaxed similarity values $\lambda_t^{n_{rel}}$ instead of the values in matrix Γ.

3.4.4 Local Similarity Assignment with Relaxation (LSA-R)

This technique is identical to the previous one (LSS-R), except that, in the preliminary step, the n_R pairs (r_t, c_t) are selected with the LSA technique. The computation of the final score is identical to LSS-R as well: it is a simple average of the relaxed similarities $\lambda_t^{n_{rel}}$ of the n_P pairs with the largest efficiency.

3.5 Experimental Evaluation

In this section, in order to evaluate accuracy and efficiency of MCC, experiments aimed at comparing it with minutiae-only implementations of three well-known local minutiae matching methods [43] [44] [49] are reported.

3.5.1 Benchmark Datasets

In a first battery of experiments, all the algorithms have been extensively evaluated on five datasets (*DS2a*, *DS2b*, *DS2c*, *DS2d*, *DS2e*) of ISO/IEC 19794-2 templates, derived from the fingerprint images in FVC2006 [85] DB2.These datasets have been obtained using five ISO-compliant minutiae extractors (identified in the following by the letters *a*, *b*, *c*, *d*, *e*) provided by five of the best-performing FVC2006 participants. Figure 3.8 shows a fingerprint from FVC2006 DB2 with the five corresponding ISO templates. The choice of using FVC2006 DB2 as principal dataset is motivated by the fact that it was acquired with a large-area optical sensor of medium-high quality, which is well-suited for the algorithms evaluated, since it allows a sufficiently-large number of minutiae to be extracted. However the same tests have been also performed on the other three FVC2006 databases; hence, in the following, the results are reported on a total of 20 datasets: *DS*[*1-4*][*a-e*] (the number denotes the corresponding FVC2006 database and the letter the minutiae extractor). Each dataset contains 1680 ISO/IEC 19794-2 templates, obtained from the 1680 fingerprints in the corresponding FVC2006 database (140 fingers and 12 impressions per finger, see [85].
Figure 3.9 shows a sample fingerprint from each FVC2006 database; note that DB1 was acquired with a small area-scanner at 250 dpi, which is not well-suited for minutiae extraction and matching: this explains why error rates on the corresponding datasets *DS1*[*a-e*] are high, not only for MCC, but also for the other minutiae-only algorithms it is compared against, see Subsection 3.5.4.
In all the datasets, minutiae coordinates are encoded at 500 dpi.

3.5.2 Algorithms Evaluated

Three versions of MCC and three minutiae-only implementations of well-known algorithms have been compared on the 20 datasets:

- *MCC16* – MCC with $N_S = 16$ (see Table 3.2);
- *MCC16b* – MCC with $N_S = 16$ and bit-based implementation (see Subsection 3.3.4);
- *MCC8b* – MCC with $N_S = 8$ (see Table 3.2) and bit-based implementation;
- *Jiang* – the local matching phase of the approach proposed in [43];
- *Ratha* – the local matching phase of the approach proposed in [44];
- *Feng* – the local matching phase of the approach proposed in [49].

Except for parameter N_S, all the three versions of MCC use the same parameter values (Table 3.2); these values have been initially calibrated on *DB2d*, since *d* is the most accurate of the five minutiae extractors, and then maintained steady for all the 19 remaining datasets. As to the other three algorithms, the parameter values specified in the original papers have been used; for parameters whose values were not given in the original papers, optimal values have been determined on *DB2d*. The algorithms have been implemented as described in the corresponding papers, except for a few minor changes:

- in *Jiang* and *Ratha*, the contribution of ridge-count information has been neglected, since this information (not mandatory in the ISO/IEC 19794-2 template format) is not provided by any of the five extractors used in the experiments, and this work focuses on algorithms using only the mandatory information in the ISO/IEC 19794-2 format.
- in *Feng*, a minimum number of minutiae (three) has been required for a minutiae neighborhood to be valid (according to our experiments, without this correction, its accuracy markedly drops); furthermore, since information on the fingerprint pattern area (required in the original algorithm, see [49]) is not available in ISO/IEC 19794-2 templates, the fingerprint pattern area is approximated with the minutiae convex hull which is also used in MCC (see Subsection 3.3.1).

Both MCC and the other algorithms have been implemented in C#.

Each of the six algorithms has been combined with each of the global-scoring

techniques described in Section 4: LSS, LSA, LSS-R, and LSA-R, thus obtaining a total of 24 matching approaches to be tested.

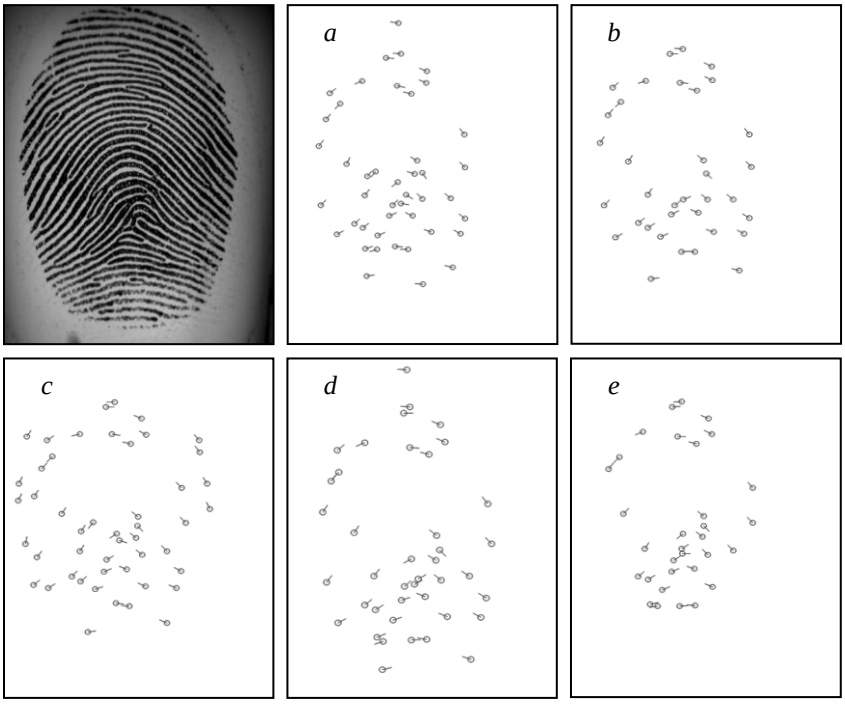


Figure 3.8 - A fingerprint from FVC2006 DB2 and the corresponding ISO templates obtained by the five minutiae extractors (*a*-*e*).

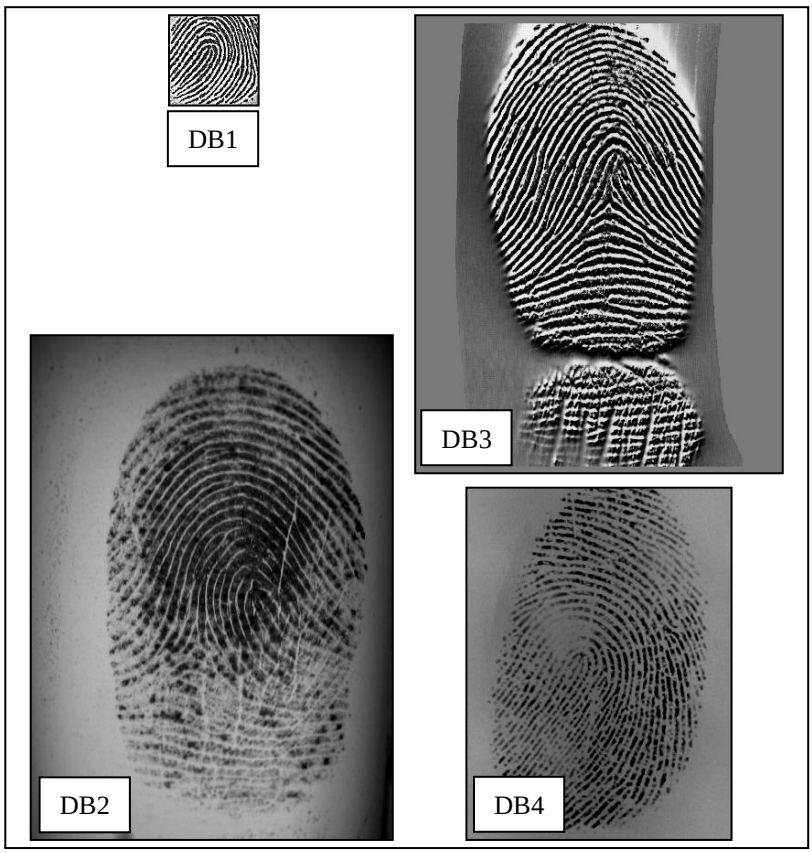


Figure 3.9 - A fingerprint from each FVC2006 database, at the same scale factor.

Table 3.2 - Parameter Values.

Parameter(s)	Description	Value
R	Cylinder radius (in pixel)	70
N_S	Number of cells along the cylinder diameter	16 [*MCC16(b)*] 8 [*MCC8b*]
N_D	Number of cylinder sections	6
σ_S	Standard deviation in (3.7)	$\frac{28}{3}$
σ_D	Standard deviation in (3.11)	$\frac{2}{9}\pi$
μ_Ψ, τ_Ψ	Sigmoid parameters for function Ψ	$\frac{1}{100}$, 400
Ω	Offset applied to enlarge the convex hull (in pixel)	50
min_{VC}	Minimum number of valid cells for a cylinder to be valid	75% of the max. number of valid cells in a cylinder
min_M	Minimum number of minutiae for a cylinder to be valid	2
min_{ME}	Minimum number of matching elements in two matchable cylinders	60% of the max. number of matching elements
δ_θ	Maximum global rotation allowed between two templates	$\frac{\pi}{2}$
μ_P, τ_P	Sigmoid parameters in (3.24)	20, $\frac{2}{5}$
min_{n_p}, max_{n_p}	Minimum and maximum number of minutiae in (3.24)	4, 12
w_R	Weight parameter in (3.25)	$\frac{1}{2}$
μ_1^ρ, τ_1^ρ	Sigmoid parameters for d_1 in (3.26)	5, $-\frac{8}{5}$
μ_2^ρ, τ_2^ρ	Sigmoid parameters for d_2 in (3.26)	$\frac{\pi}{12}$, -30
μ_3^ρ, τ_3^ρ	Sigmoid parameters for d_3 in (3.26)	$\frac{\pi}{12}$, -30
n_{rel}	Number of relaxation iterations for LSS-R and LSA-R	5

3.5.3 Test Protocol

For each dataset, the FVC2006 testing protocol has been adopted:

- each template is compared against the remaining templates of the same finger to obtain the False Non Match Rate (FNMR). If template T_1 is compared against T_2, the symmetric comparison (i.e., T_2 against T_1) is not executed, to avoid correlation in the matching scores. The total number of genuine tests is: $\frac{12\times11}{2} \times 140 = 9240$;
- the first template of each finger is compared against the first template of the remaining fingers in the dataset, to determine the False Match Rate (FMR). If template T_1 is compared to T_2, the symmetric comparison (i.e., T_2 against T_1) is not executed, to avoid correlation in the scores. The total number of impostor tests is: $\frac{140\times139}{2} = 9730$.

In case of failure to process or match templates, the corresponding matching scores are set to zero.

For each algorithm and for each dataset, the following performance indicators are considered:

- Equal-Error-Rate (EER) [26];
- FMR_{1000} (the lowest FNMR for FMR $\leq 0.1\%$) [10];
- Average matching time, subdivided into:
    - T_{cs}: average time to create the local structures from an ISO/IEC 19794-2 template;
    - T_{ls}: average time to compute all the local similarities between the local structures obtained from two templates (i.e., to fill matrix Γ);
    - T_{gs}: average time to calculate the global score from the local similarities (i.e., from Γ);
- Average memory size of the local structures created from a template, expressed in bytes.

3.5.4 Results: Accuracy

Table 3.3 reports the EER and FMR_{1000} of all the algorithms, combined with the four global-scoring techniques, on *DS*2[*a*-*e*]. For each global-scoring technique, the best result on each dataset is highlighted in bold; the overall best EER and FMR_{1000} are underlined. The graphs in Figure 3.10 and Figure 3.11 report, for each global-scoring technique, the average EER and FMR_{1000} over the five datasets, respectively; Figure 3.12 reports the DET graph on *DS2d*, using the LSA-R technique.

Table 3.3 - Accuracy of the Algorithms on the Five Datasets Obtained from FVC2006 DB2 (Percentage Values).

		DS2a		*DS2b*		*DS2c*		*DS2d*		*DS2e*	
		EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}
LSS	*MCC16*	**2.07**	**5.35**	**1.44**	**3.34**	**6.62**	**21.23**	**0.46**	**1.02**	**2.69**	**7.70**
	MCC16b	2.24	6.67	1.69	4.44	6.76	24.20	0.55	1.62	2.78	7.77
	MCC8b	2.28	7.12	1.73	5.23	7.54	26.43	0.59	1.92	2.88	8.34
	Jiang	5.37	16.50	6.50	13.82	16.48	38.33	3.23	7.72	8.82	19.69
	Ratha	9.11	34.72	11.68	39.73	18.68	51.28	7.78	32.20	10.93	37.33
	Feng	3.52	7.36	4.58	11.52	11.09	23.81	2.51	5.17	5.33	12.2
LSA	*MCC16*	**1.97**	**4.61**	**1.14**	**2.67**	**5.87**	**15.44**	**0.33**	**0.69**	**2.31**	**5.78**
	MCC16b	2.07	5.70	1.35	3.46	6.18	15.95	0.44	1.07	2.36	6.35
	MCC8b	2.07	5.99	1.47	3.81	7.03	21.37	0.45	1.12	2.57	6.09
	Jiang	5.11	15.57	6.75	13.92	17.27	36.85	3.20	6.97	9.08	21.23
	Ratha	8.06	26.99	10.41	33.02	17.56	44.63	6.87	24.63	9.88	30.36
	Feng	3.42	6.83	4.36	10.44	11.09	22.38	2.17	4.45	5.18	11.02
LSS-R	*MCC16*	**1.41**	**2.52**	**0.64**	1.20	**3.19**	**7.15**	0.21	**0.24**	**1.17**	**2.15**
	MCC16b	**1.41**	2.60	**0.64**	1.23	3.33	7.60	0.22	0.27	1.19	2.23
	MCC8b	1.46	3.05	0.67	**1.18**	3.82	7.99	**0.20**	0.28	1.37	2.62
	Jiang	3.66	7.91	3.60	5.89	11.48	22.13	1.22	2.04	5.47	9.67
	Ratha	2.34	3.76	0.96	1.72	6.82	9.36	0.41	0.46	2.16	3.44
	Feng	3.27	5.76	4.35	9.25	11.11	22.44	2.03	3.66	5.39	11.02
LSA-R	*MCC16*	1.23	1.98	0.48	**0.73**	**2.98**	**5.91**	**0.15**	**0.18**	**1.04**	**2.04**
	MCC16b	**1.21**	**1.97**	**0.47**	0.90	3.06	6.17	0.17	**0.18**	1.08	2.07
	MCC8b	1.23	2.14	0.59	0.89	3.66	7.11	0.18	0.25	1.28	2.41
	Jiang	4.06	7.98	3.54	6.40	11.00	20.83	1.22	2.02	5.12	9.56
	Ratha	2.91	5.10	1.12	1.93	8.03	10.94	0.49	0.58	2.78	4.42
	Feng	3.01	5.44	4.19	8.67	11.12	21.02	1.78	3.17	5.25	9.72

It is worth noting that the best result is always achieved by one of the three versions of MCC and that any of the three versions is always more accurate than the other

algorithms, except on *DS2c* with the LSS technique, where the FMR_{1000} of *Feng* (23.81%) is lower than that of *MCC16b* and *MCC8b* (24.20% and 26.43%, respectively). The overall best result is achieved by *MCC16* on *DS2d* using the LSA-R technique (EER=0.15%, FMR_{1000}=0.18%); this result would put *MCC16* at the ninth place in the ranking of the FVC2006 Open Category and at the second place in the Light Category (see [85]). Considering that FVC2006 algorithms do not rely only on ISO/IEC 19794-2 minutiae information, but typically exploit other features (e.g. orientation field, ridge density, etc.), the accuracy obtained by *MCC16* is definitely very good. It is also worth noting that the accuracy drop of MCC bit-based implementations (with respect to the MCC normal implementation) is very limited.

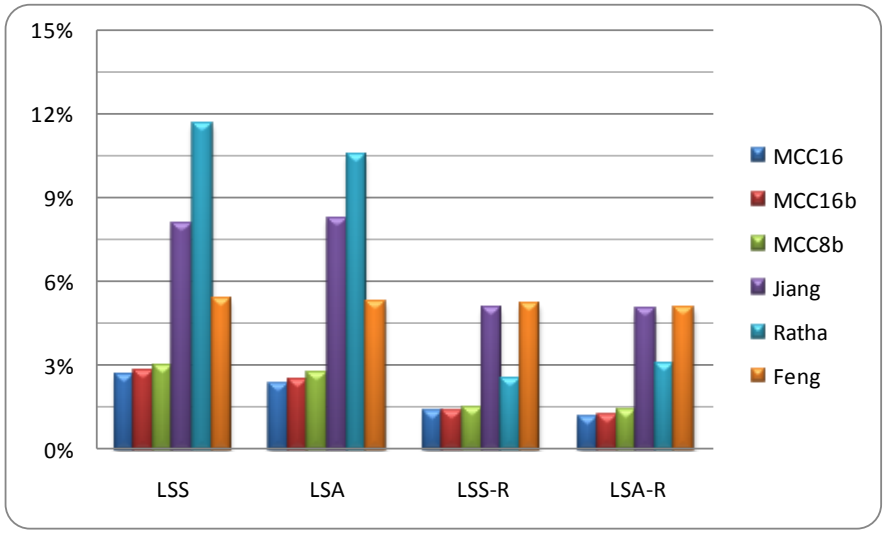


Figure 3.10 - Average EER over the five datasets *DS2*[*a-e*], for each of the four global-scoring techniques.

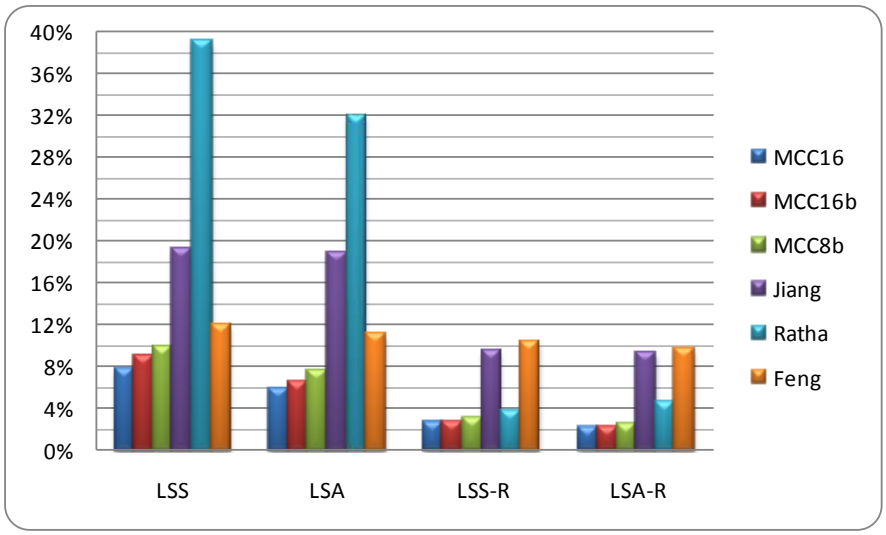


Figure 3.11 Average FMR_{1000} over the five datasets *DS2*[*a-e*], for each of the four global-scoring techniques.

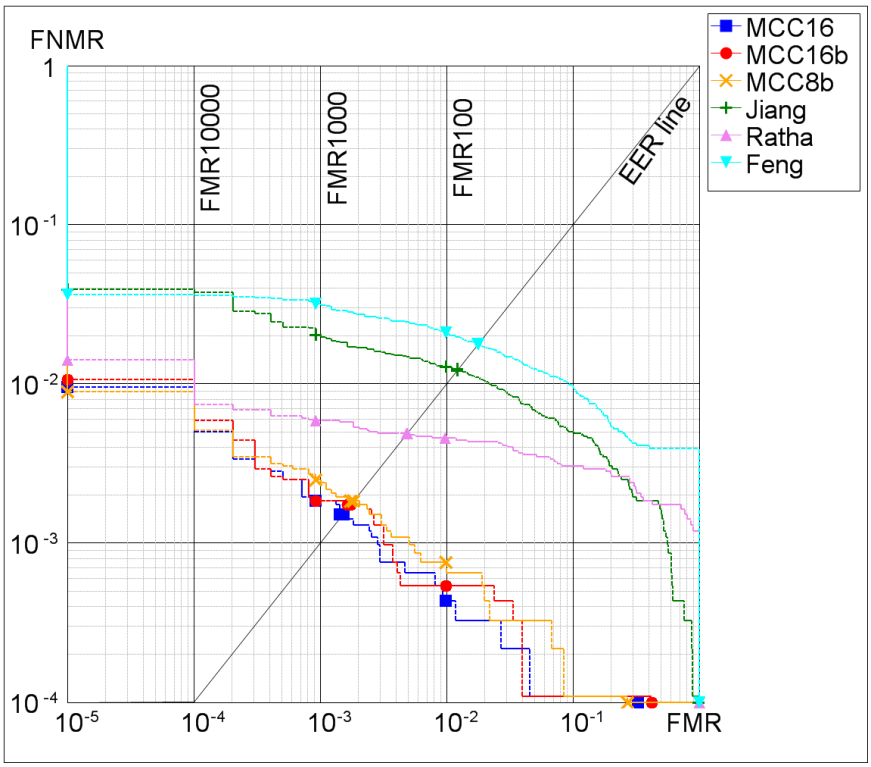


Figure 3.12 - DET graph of the six algorithms on *DS2d*, using LSA-R.

Table 3.4, Table 3.5 and Table 3.6 report the EER and FMR_{1000} of all the algorithms, combined with the four global-scoring techniques, on *DS*[1,3,4][*a*-*e*]. In each table, for each global-scoring technique, the best result on each dataset is highlighted in bold and the overall best EER and FMR_{1000} are underlined. The corresponding graphs in Figure 3.13, Figure 3.15, Figure 3.17 and Figure 3.14, Figure 3.16, Figure 3.18 report the average EER and FMR_{1000}, respectively. Note that, also in each of these datasets, the most accurate results are always achieved by one of the three versions of MCC; the superiority of MCC is well evident from the graphs, which show how the average error rates are always below those of the other algorithms. As to the four proposed global scoring techniques, from the experiments it is evident that:

- as expected, the consolidation stage markedly increases the accuracy; however MCC (and sometimes Feng) achieves a good accuracy even without consolidation;
- the use of the Hungarian algorithm to optimally solve the assignment algorithm, in spite of the computational overhead, leads to a small accuracy improvement and therefore its adoption is not advised when efficiency is a concern.

Table 3.4 - Accuracy of the Algorithms on the Five Datasets Obtained from FVC2006 DB1 (Percentage Values).

		DS2a		*DS2b*		*DS2c*		*DS2d*		*DS2e*	
		EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}
LSS	*MCC16*	**17.57**	**56.13**	**15.08**	**44.41**	**25.77**	**68.24**	**14.96**	**41.12**	**17.72**	**47.96**
	MCC16b	18.22	58.27	15.73	51.31	26.20	70.05	15.49	42.35	18.03	49.78
	MCC8b	18.46	59.19	16.23	51.95	26.80	74.87	15.21	45.78	18.96	53.41
	Jiang	31.58	85.30	26.74	71.57	32.17	84.18	23.95	73.28	26.73	75.50
	Ratha	43.14	99.57	34.44	99.41	35.52	92.15	28.58	98.43	30.31	90.22
	Feng	24.64	57.40	22.67	56.82	36.61	75.18	20.49	48.68	24.11	60.53
LSA	*MCC16*	**17.43**	**53.67**	**15.20**	**42.71**	**27.01**	**65.39**	**14.77**	39.13	**18.20**	**47.40**
	MCC16b	18.03	55.77	15.67	46.37	27.35	67.48	15.12	**39.02**	18.61	48.05
	MCC8b	18.17	56.36	16.27	50.81	27.91	71.63	15.01	41.34	19.29	50.77
	Jiang	32.24	85.30	26.64	70.48	31.73	84.12	24.61	72.14	26.61	72.97
	Ratha	42.83	99.08	34.10	97.50	34.67	89.91	31.62	98.04	29.72	84.21
	Feng	24.63	58.08	22.67	56.18	36.61	75.21	20.42	49.15	24.11	60.68
LSS-R	*MCC16*	**14.53**	41.14	**13.69**	**32.20**	**25.29**	**60.14**	**12.63**	28.28	**16.90**	**38.85**
	MCC16b	14.59	**40.88**	14.02	32.29	25.57	60.41	12.81	**28.03**	17.21	39.35
	MCC8b	14.92	42.06	14.42	32.92	25.86	61.48	12.64	28.20	17.42	39.57
	Jiang	27.68	70.66	23.74	57.38	32.26	78.10	20.64	59.88	25.08	63.20
	Ratha	27.32	52.12	23.82	43.29	34.39	64.87	20.84	39.85	27.40	47.70
	Feng	24.67	57.99	22.67	55.57	36.61	75.15	20.49	49.02	24.11	61.49
LSA-R	*MCC16*	**14.17**	**38.38**	**13.51**	**30.58**	**25.50**	**58.16**	**12.36**	**27.37**	**16.90**	**38.39**
	MCC16b	14.19	39.24	13.81	32.83	25.92	59.31	12.49	27.70	17.36	40.20
	MCC8b	14.78	40.41	14.66	33.16	26.72	59.97	12.65	27.65	17.40	39.03
	Jiang	27.11	68.54	23.65	56.81	31.81	78.68	20.47	59.50	24.82	63.85
	Ratha	35.19	56.19	28.93	45.49	33.68	66.31	27.16	42.76	27.73	46.98
	Feng	24.58	57.67	22.67	54.65	36.61	74.77	20.44	49.06	24.11	59.39

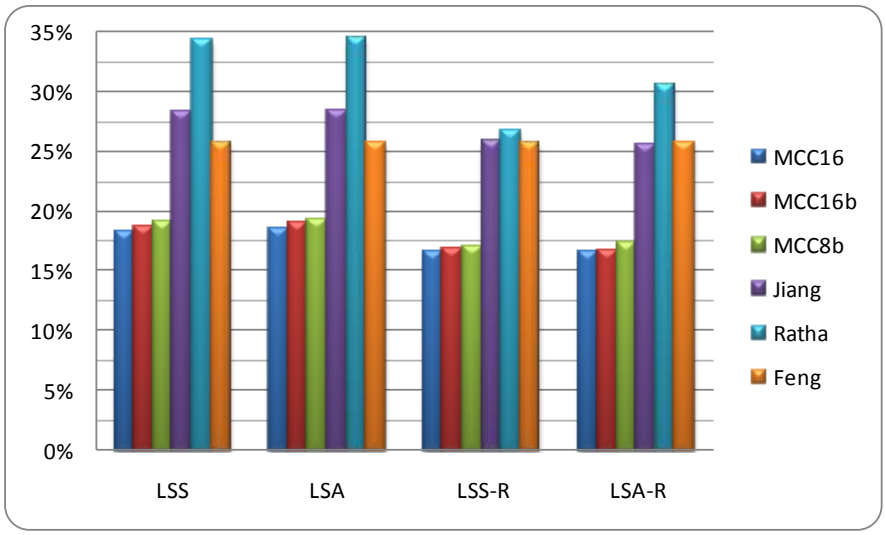


Figure 3.13 - Average EER over the five datasets *DS1*[*a*-*e*], for each of the four global-scoring techniques.

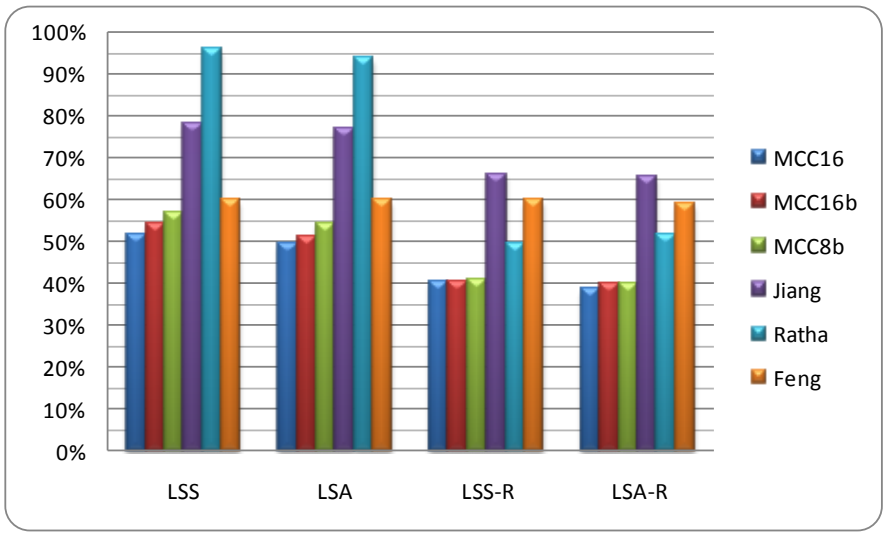


Figure 3.14 - Average FMR_{1000} over the five datasets *DS1*[*a-e*], for each of the four global-scoring techniques.

Table 3.5 - Accuracy of the Algorithms on the Five Datasets Obtained from FVC2006 DB3 (Percentage Values).

		DS2a		*DS2b*		*DS2c*		*DS2d*		*DS2e*	
		EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}	EER	FMR_{1000}
LSS	*MCC16*	**7.81**	**26.82**	**7.62**	**20.73**	**12.27**	**37.94**	**4.96**	**13.41**	**7.42**	**19.89**
	MCC16b	8.52	29.63	8.09	22.97	12.45	40.58	5.42	15.29	7.49	21.76
	MCC8b	8.78	29.92	8.57	23.24	14.04	49.17	5.47	14.83	8.47	33.82
	Jiang	15.91	49.90	18.91	48.23	22.34	59.58	11.34	37.18	16.16	42.22
	Ratha	25.99	68.93	27.91	87.77	28.13	79.09	20.11	67.32	22.74	74.24
	Feng	13.19	29.69	14.62	39.5	17.33	45.56	9.85	24.31	13.39	29.02
LSA	*MCC16*	**7.52**	**23.53**	**7.10**	**18.72**	**11.76**	32.23	**4.68**	**12.55**	**6.93**	**18.38**
	MCC16b	8.15	25.89	7.64	20.02	11.87	**31.17**	5.05	13.60	7.14	18.70
	MCC8b	8.39	27.29	8.35	21.63	13.68	43.81	5.34	13.84	8.02	29.47
	Jiang	16.30	47.31	19.47	47.71	22.89	57.93	11.80	35.81	16.33	42.06
	Ratha	24.70	58.29	26.35	81.62	27.27	72.17	18.51	61.27	21.12	62.26
	Feng	12.50	28.58	14.44	36.92	17.33	44.98	9.63	23.33	13.39	27.98
LSS-R	*MCC16*	**5.89**	**15.11**	**5.67**	**12.90**	**9.27**	**23.67**	**3.35**	**7.34**	**5.24**	12.54
	MCC16b	5.93	15.23	5.83	12.97	9.33	24.17	3.47	7.86	5.44	**12.39**
	MCC8b	6.23	15.53	5.95	13.23	10.17	26.15	3.66	9.18	5.57	13.67
	Jiang	12.38	29.02	13.99	40.18	19.24	45.86	7.40	29.42	12.52	30.38
	Ratha	9.88	18.58	8.60	17.37	16.76	31.49	6.32	10.25	9.91	16.99
	Feng	12.08	23.82	14.52	33.37	17.33	45.18	9.87	19.69	13.39	27.81
LSA-R	*MCC16*	**4.83**	**11.53**	**5.02**	**11.52**	**9.32**	23.05	3.08	6.23	4.72	12.81
	MCC16b	4.87	11.86	5.18	11.55	9.49	**22.53**	**3.06**	**6.14**	**4.71**	**12.05**
	MCC8b	5.29	12.32	5.57	12.24	10.46	24.58	3.35	7.40	5.35	14.33
	Jiang	12.63	29.51	13.53	37.50	18.98	47.23	7.12	25.68	12.10	33.45
	Ratha	11.30	21.65	10.01	18.64	19.51	31.83	7.42	11.59	11.63	19.59
	Feng	11.76	22.21	14.34	32.17	17.33	44.29	9.64	18.31	13.39	26.41

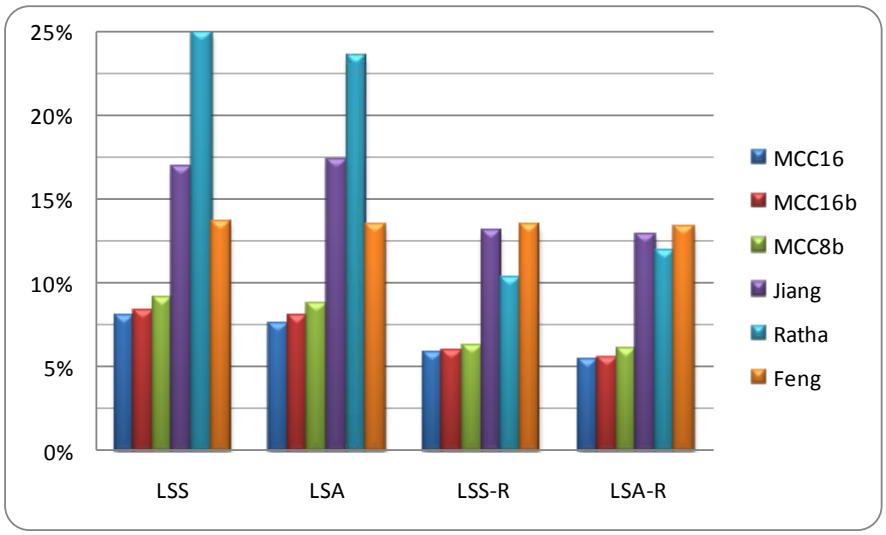


Figure 3.15 - Average EER over the five datasets *DS3*[*a*-*e*], for each of the four global-scoring techniques.

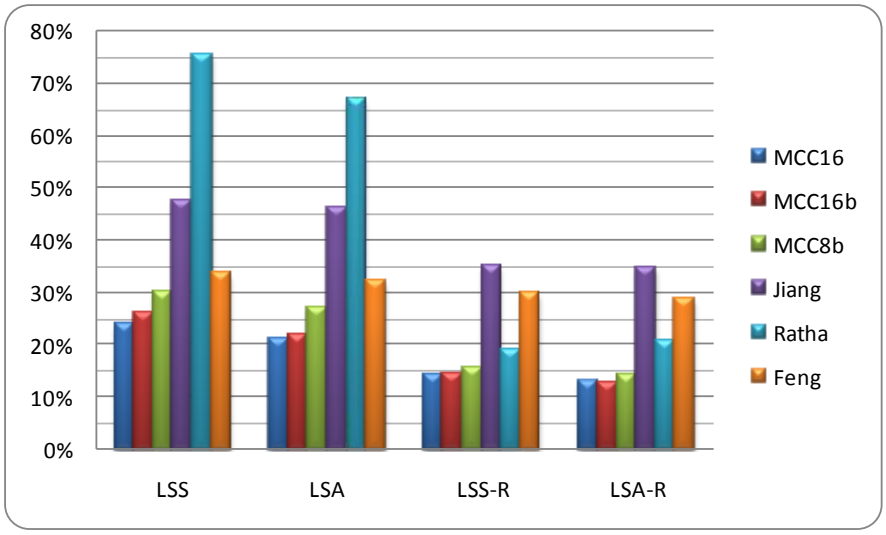


Figure 3.16 - Average FMR_{1000} over the five datasets *DS3*[*a*-*e*], for each of the four global-scoring techniques.

Table 3.6 - Accuracy of the Algorithms on the Five Datasets Obtained from FVC2006 DB4 (Percentage Values).

		DS2a		*DS2b*		*DS2c*		*DS2d*		*DS2e*	
		EER	FMR$_{1000}$	EER	FMR$_{1000}$	EER	FMR$_{1000}$	EER	FMR$_{1000}$	EER	FMR$_{1000}$
LSS	*MCC16*	**7.67**	**32.60**	**10.24**	**36.46**	**19.86**	**67.07**	**5.51**	**22.15**	**7.58**	**26.56**
	MCC16b	8.57	36.63	11.44	44.18	20.49	70.91	6.27	31.95	8.50	34.23
	MCC8b	8.84	42.07	11.81	44.59	21.16	72.26	6.54	33.03	9.04	34.56
	Jiang	19.36	64.30	23.12	71.28	31.55	82.00	13.65	48.30	15.13	55.20
	Ratha	28.65	94.99	28.88	91.48	37.06	94.74	19.71	83.02	20.44	80.76
	Feng	15.50	40.31	17.74	52.83	25.61	71.99	11.67	27.75	11.67	36.46
LSA	*MCC16*	**4.06**	11.73	**5.62**	**13.29**	**12.38**	**35.28**	2.60	**6.12**	**3.63**	**9.31**
	MCC16b	4.28	**10.66**	5.78	13.98	12.41	35.76	**2.57**	6.93	3.78	9.37
	MCC8b	4.43	11.94	6.04	15.20	13.23	38.02	2.83	6.88	3.93	9.47
	Jiang	11.72	27.36	17.23	42.15	27.25	62.31	6.78	14.98	8.86	20.33
	Ratha	7.45	15.70	10.63	22.58	22.73	40.15	4.77	8.63	6.63	12.62
	Feng	14.24	29.50	17.71	44.72	25.61	65.47	9.57	20.39	11.57	28.66
LSS-R	*MCC16*	**6.66**	**27.87**	**9.04**	**30.49**	**18.65**	**62.36**	**5.03**	**17.88**	**6.64**	**21.99**
	MCC16b	7.51	33.67	10.00	37.15	19.23	65.79	5.65	24.08	7.32	28.55
	MCC8b	7.80	34.88	10.32	38.71	20.04	68.60	5.93	26.00	7.87	27.75
	Jiang	18.88	60.36	22.21	64.62	32.17	80.20	13.35	43.78	14.90	51.36
	Ratha	27.24	92.91	27.02	89.78	36.38	94.69	18.08	76.26	18.76	76.61
	Feng	14.02	37.27	17.66	50.71	25.61	65.49	10.57	25.54	10.93	32.80
LSA-R	*MCC16*	**3.09**	8.12	**4.91**	**11.74**	**11.77**	**28.21**	**2.10**	4.60	**2.95**	**6.94**
	MCC16b	3.17	**7.97**	5.00	12.23	11.84	29.41	2.27	**4.45**	2.97	7.04
	MCC8b	3.52	9.74	5.44	14.30	12.99	32.23	2.46	5.31	3.23	8.51
	Jiang	11.48	27.96	16.45	40.15	26.37	62.58	6.58	14.48	8.39	20.09
	Ratha	9.66	18.60	13.30	27.06	26.68	45.64	5.92	9.44	8.51	13.94
	Feng	13.24	29.92	17.52	41.80	25.61	62.85	9.01	17.74	10.72	24.13

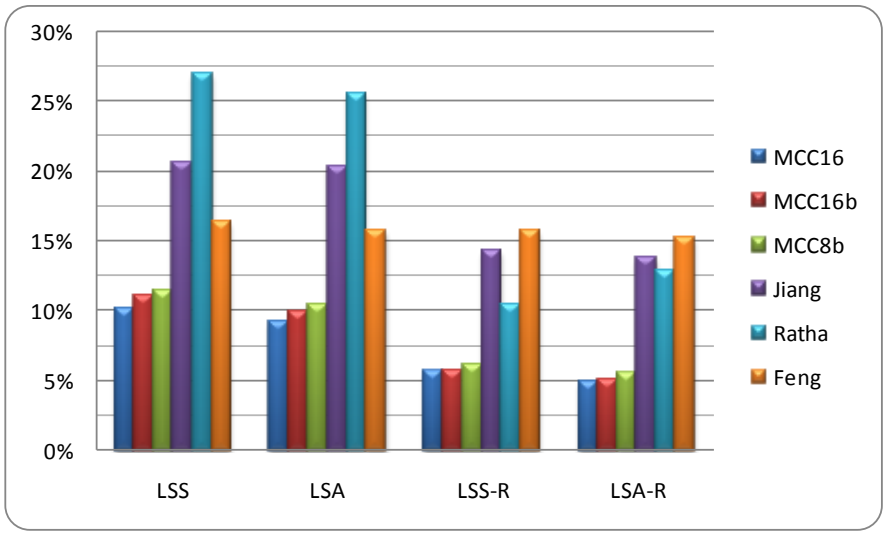


Figure 3.17 - Average EER over the five datasets *DS4*[*a-e*], for each of the four global-scoring techniques.

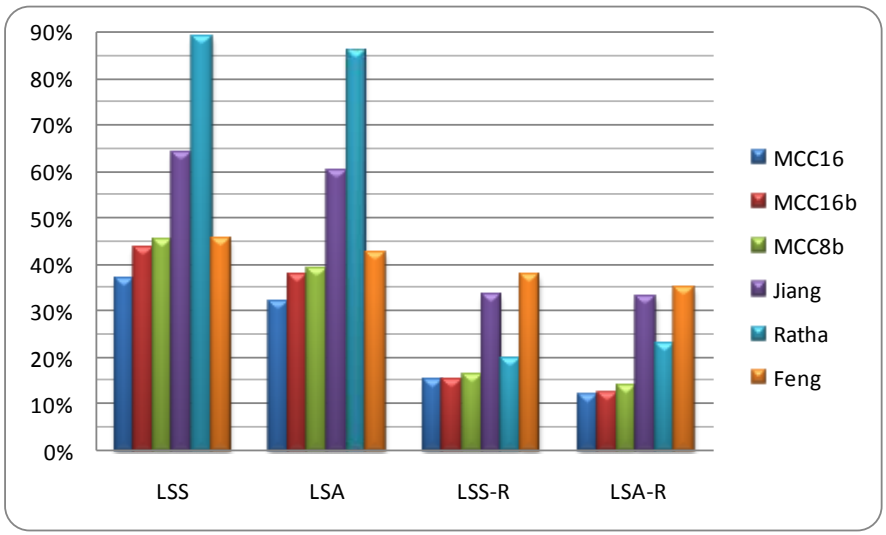


Figure 3.18 - Average FMR_{1000} over the five datasets *DS4*[*a*-*e*], for each of the four global-scoring techniques.

3.5.5 Results: Efficiency

Table 3.7 reports the average matching times measured over all the 20 datasets: note that four columns are reported for T_{gs}, since it depends on the specific global-scoring technique used. From the table, the following observations may be made.

- The average time taken by MCC to create the local structures from an ISO/IEC 19794-2 template (T_{cs}) is within 4.2ms and 21ms. As it was reasonable to expect, this time is higher than in the other algorithms, however I believe this does not limit the applicability of MCC, for the following reasons: i) according to our experience (and having in mind the high margin for code optimization), even if this step would be implemented on very light architectures, the 4.2ms of *MCC8b* should not become more than one second; ii) match-on-card solutions would not need to perform the cylinder computation at verification time; in fact, the cylinder-set of the acquired fingerprint may be computed on the PC and the template stored inside the smart-card may already contain the cylinder-set pre-computed at enrollment stage; iii) in identification (one-to-many) applications, cylinder-set needs to be pre-computed only once for each template and not at each comparison.
- *MCC8b* exhibits the lowest local similarity computation time (the average T_{ls} is 0.3ms): note that this time refers to a C# implementation, without any assembly-

language or hardware-oriented optimization that the bit-based nature of the similarity measure could allow.

- The average time taken to calculate the global score (T_{gs}) in general does not depend on the specific local matching algorithm, with a noticeable exception: the techniques based on the assignment problem (LSA and LSA-R) are definitely faster when coupled to *Feng*; this may be due to the specific distribution of local similarities produced by such an algorithm that, on the average, requires less iterations of the Hungarian method.
- To provide a reference, the average matching time over the four databases of the top ten FVC2006 participants is much higher than MCC: 416ms for the Open Category and 53ms for the Light Category. However a direct comparison is not feasible, since times reported in FVC2006 corresponds to "template against image" matching and therefore include one feature extraction which is a time demanding task (see [85] and [10]).

Table 3.8 shows, for each algorithm, the average memory size of the local structures created from an ISO/IEC 19794-2 template: the average has been calculated over all the 20 datasets. The memory size is reported considering both raw format and compression with two general-purpose lossless compression techniques: rar [86] and zip [87]. It is worth noting that:

- *MCC16* require a considerable amount of memory because it encodes cell values as floating point data and therefore it is not suitable to run on resource-limited platforms. This is not the case of *MCC16b* and *MCC8b*;
- without any compression, the local structures of *MCC16b* and *MCC8b*, although larger than those of *Jiang* and *Feng*, can be stored and managed into a typical smart card;
- the local structures of *MCC16b* and *MCC8b* can be compressed much more than the others, probably due to their bit-based composition: once compressed, the local structure size of *MCC8b* is comparable to that of *Jiang* and *Feng*;
- the average template size of the top ten FVC2006 participants is: 4478 bytes for the Open Category (hence higher than *MCC8b*) and 1175 bytes for the Light Category (not far from *MCC8b*).

Table 3.7 - Average Matching Times Over All Datasets (milliseconds).

	T_{cs}	T_{ls}	T_{gs}			
			LSS	LSA	LSS-R	LSA-R
MCC16	21.0	21.0	0.5	4.3	2.7	4.7
MCC16b	17.3	1.2	0.5	4.3	2.8	4.7
MCC8b	4.2	0.3	0.5	4.2	2.9	4.8
Jiang	1.0	0.8	0.4	4.3	2.6	4.1
Ratha	1.0	250.7	0.5	4.3	2.8	4.4
Feng	0.2	12.3	0.5	2.4	2.8	3.1

Table 3.8 - Average Memory Size of the Local Structures, Over All Datasets, Measured in Bytes.

	Raw format	Compressed format (rar)		Compressed format (zip)	
	Size	*Size*	*Ratio*	*Size*	*Ratio*
MCC16	209253	103766	202%	104595	200%
MCC16b	7630	1457	524%	1642	465%
MCC8b	1913	605	316%	655	292%
Jiang	1068	608	176%	647	165%
Ratha	26543	19487	136%	20046	132%
Feng	1428	567	252%	614	233%

3.6 Conclusion

In this chapter Minutia Cylinder-Code (MCC) has been introduced: a novel minutiae-only representation and matching technique for fingerprint recognition. MCC relies on a robust discretization of the neighborhood of each minutia into a 3D cell-based structure named cylinder. Simple but effective techniques for the computation and consolidation of cylinder similarities are provided, to determine the global similarity between two fingerprints.

In order to compare MCC with three well-known approaches, a systematic experimentation has been carried out, involving a total of 24 matching approaches (6 algorithms and 4 global-scoring techniques) over 20 minutiae datasets extracted from FVC2006 databases, resulting in more than nine millions matching attempts.

Experimental results demonstrate that MCC is more accurate than well-known minutiae-only local matching techniques ([43] [44] [49]). MCC is also very fast and suitable to be simply coded in hardware, due to the bit-wise nature of the matching technique; this allows its porting on inexpensive secure platforms such as a smart-card or a system-on-a-chip. The new algorithms is so promising that a patent has been filed on it.

While in this work the problem of robustly and efficiently matching two fingerprints has been focused, I believe that the peculiarities of MCC also allow to develop new effective techniques for fingerprint indexing and template protection: these two issues are the main targets of our future research efforts.

4

PERFORMANCE EVALUATION OF FINGERPRINT VERIFICATION SYSTEMS

4.1 Introduction

Although the accuracy of fingerprint-based biometric systems can be very high, no fingerprint recognition algorithm is perfect. Performance evaluation is important for all biometric systems and particularly so for fingerprint recognition, which is receiving widespread international attention for citizen identity verification and identification. The most-widely known performance evaluation efforts in this field are the Fingerprint Verification Competitions (FVC) [87] and the Fingerprint Vendor Technology Evaluation (FpVTE) [88]; other initiatives include the NIST SDK Testing [89] and the MINEX campaign aimed at evaluating interoperability [90]. Fortunately, controlled, scientific testing initiatives are not limited within the biometrics community to fingerprint recognition. Other biometric modalities have been the target of excellent evaluation efforts as well. The (U.S.) National Institute of Standards and Technology (NIST) has sponsored scientifically-controlled tests of text-independent speaker recognition algorithms [91] [92] for a number of years, and more recently of facial recognition technologies as well [93].

NIST and others have suggested [94] [95] that biometric testing can be classified into "technology", "scenario" and "operational" evaluations. "Technology" evaluations test computer algorithms with archived biometric data collected using a "universal" (algorithm-independent) sensor; "Scenario" evaluations test biometric systems placed in a controlled, volunteer-user environment modelled on a proposed application; "Operational" evaluations attempt to analyze performance of biometric systems placed into real applications. Tests can also be characterized as "on-line" or "off-line", depending upon whether the test computations are conducted in the presence of the

human user (on-line) or after-the-fact on stored data (off-line). An off-line test requires a pre-collected database of samples and makes it possible to reproduce the test and to evaluate different algorithms under identical conditions.

Off-line tests can be classified as follows (Figure 4.1):

- *In-house - self defined test*: the database is internally collected and the testing protocol is self-defined. Generally the database is not publicly released, perhaps because of human-subject privacy concerns, and the protocols are not completely explained. As a consequence, results may not be comparable across such tests or reproducible by a third party;
- *In-house - existing benchmark*: the test is performed over a publicly available database, according to an existing protocol. Results are comparable with others obtained using the same protocol on the same database. Besides the trustworthiness problem, the main drawback is the risk of overfitting the data - that is, tuning the parameters of the algorithms to match only the data specific to this test. In fact, even if the protocol defines disjoint training, validation, and test sets, the entire evaluation (including learning) might be repeated a number of times to improve performance over the final test set. Examples of recent biometric evaluations of this type are [96] and [97];
- *Independent - weakly supervised*: the database is sequestered and is made available just before the beginning of the test. Samples are unlabelled (the filename does not carry information about the sample's owner identity). The test is executed at the testee's site and must be concluded within given time constraints. Results are determined by the evaluator from the comparison scores obtained by the testee during the test. The main criticism against this kind of evaluation is that it cannot prevent human intervention: visual inspection of the samples, result editing, etc., could be in principle carried out with sufficient resources. Examples of recent biometric evaluations of this type are: [98], [91] and [99].
- *Independent - supervised*: this approach is very similar to the independent weakly supervised evaluation but here the test is executed at the evaluator's site on the testee's hardware. The evaluator can better control the evaluation but: i) there is no way to compare computational efficiency (i.e., different hardware

systems can be used); ii) some interesting statistics (e.g., template size, memory usage) cannot be obtained; iii) there is no way to prevent score normalization and template consolidation [9] [100] (i.e., techniques where information from previous comparisons are unfairly exploited to increase the accuracy in successive comparisons). Examples of recent biometric evaluations of this type are [93] and [88];

- *Independent - strongly supervised*: data are sequestered and not released before the conclusion of the test. Software components compliant to a given input/output protocol are tested at the evaluator's site on the evaluator's hardware. The tested algorithm is executed in a totally-controlled environment, where all input/output operations are strictly monitored. The main drawbacks are the large amount of time and resources necessary for the organization of such events. Examples of recent biometric evaluations of this type are [26], [101], [102] and, the FVC2006 [4] [5] [85] and FVC-onGoing [103] [104] evaluation discussed in this chapter.

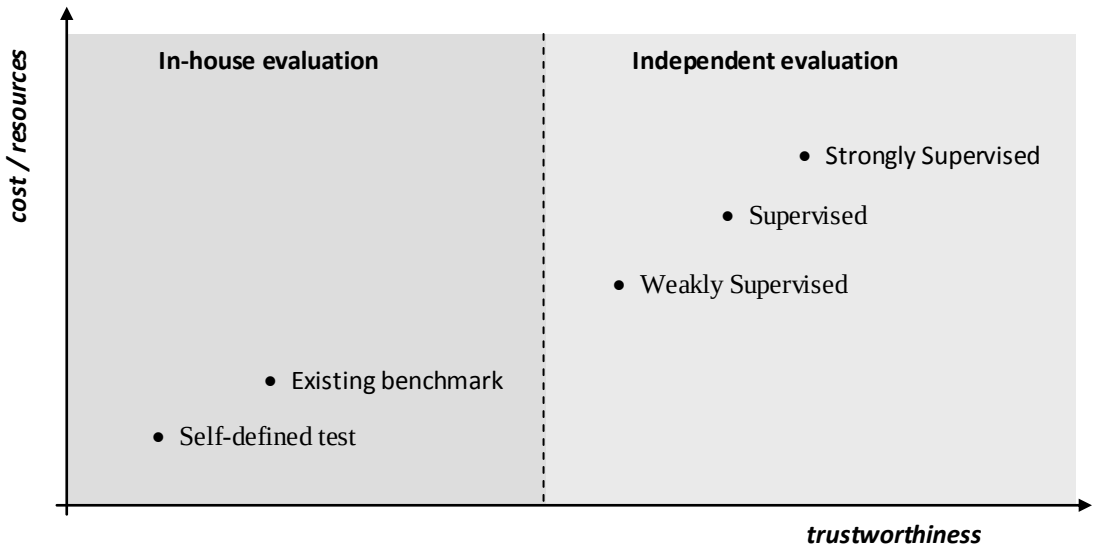


Figure 4.1 - Classification of off-line biometric evaluations.

FVC2006 follows FVC2000 [105] [26], FVC2002 [106] [101] and FVC2004 [107] [108], the first three international Fingerprint Verification Competitions organized by the authors in the years 2000, 2002 and 2004 with results presented at the 15th

International Conference on Pattern Recognition (ICPR), the 16th ICPR and the 1st International Conference on Biometric Authentication (ICBA), respectively. The previous contests received significant attention from both academic and commercial organizations. Several research groups have used FVC2000, FVC2002 and FVC2004 datasets for their own experiments and some companies not participating in the original competitions later requested the organizers to measure their performance against the FVC2000, FVC2002 and/or FVC2004 benchmarks. Beginning with FVC2002, to increase the number of companies and therefore to provide a more complete overview of the state-of-the-art, anonymous participation was allowed. Table 4.1 compares the four competitions from a general point of view, highlighting the main differences.

FVC2006 was extensively publicized starting in March 2006 with the creation of the FVC2006 web site [85]. All companies and research groups in the field known to the authors were invited to participate in the contest. All participants in the past FVC competitions were informed of the new evaluation. FVC2006 was also announced through mailing lists and biometric-related on-line magazines. Four new databases were collected using three commercially available scanners and the synthetic fingerprint generator SFinGe [109] [110] [9] (see Section 4.2). A representative subset of each database (sets B: 120 fingerprints from ten fingers) was made available to the participants prior to the competition for algorithm tuning to accommodate the image size and the variability of the fingerprints in the databases.

Two different sub-competitions (*Open* category and *Light* category) were organized using the same databases. Each participating group was allowed to submit one algorithm in each category. The Light category was intended for algorithms characterized by low computational resources, limited memory usage and small template size (see Section 4.3).

By the June 30th, 2006 registration deadline, 150 registrations had been received. All registered participants received the training subsets and detailed instructions for algorithm submission. By the October 31st, 2006 deadline for submission, a total of 70 algorithms from 53 participating groups had been received (Table 4.2). Once all the executables were submitted to the evaluators, feedback was sent to the participants by providing them with the results of their algorithms over sets B (the same data set they had previously been given for algorithm tuning), thus allowing them to verify that run-time problems were not occurring on the evaluator side. Four algorithms from two

participants (P030 and P144) were disqualified, since they were attempting to cheat by gaining additional information from the file names to improve their matching performance.

Table 4.1 - The four Fingerprint Verification Competitions: A summary.

	FVC2000	FVC2002	FVC2004	FVC2006
Call for participation	November, 1999	October, 2001	April, 2003	March, 2006
Registration deadline	March 1st, 2000	January 10th, 2002	October 15th, 2003	June 30th, 2006
Submission deadline	June 1st, 2000	March 1st, 2002	November 30th, 2003	October 31st, 2006
Evaluation period	July–August, 2000	April–July, 2002	January–February 2004	January–February 2007
Anonymous participation	Not allowed	Allowed		
Categories	-		Open and Light	
Registered participants	25 (15 withdrew)	48 (19 withdrew)	110 (64 withdrew)	150 (97 withdrew)
Algorithms evaluated	11	31	Open Category: 41 Light Category: 26	Open Category: 44 Light Category: 26
Presentation of the results	15th ICPR	16th ICPR [101]	1st ICBA [108]	BIOSECURE Project [5]
Databases	Four new databases, each one containing: set A (100x8) and set B (10x8)			Set A (140x12) set B (10x12)
DB1	Optical	Optical	Optical	Electric Field
DB2	Capacitive	Optical	Optical	Optical
DB3	Optical	Capacitive	Thermal-sweeping	Thermal-sweeping
DB4	Synthetic (SFinGe v2.0)	Synthetic (SFinGe v2.51)	Synthetic (SFinGe v3.0)	Synthetic (SFinGe v3.0)
Databases availability	DVD accompanying "Handbook of Fingerprint Recognition" [9]		http://biometrics.cse.msu.edu/fvc04db	Not available yet
Website	http://bias.csr.unibo.it/fvc200{0|2|4|6}			
HW/SW	Pentium III (450 MHz) Windows NT FVC Test suite v1.0	Pentium III (933 MHz) Windows 2000 FVC Test suite v1.2	Athlon 1600+ (1,41 GHz) Windows XP FVC Test suite v2.0	Pentium IV (3,20Ghz) Windows XP FVC Test suite v2.1

The rest of this chapter is organized as follows: Section 4.2 describes data collection procedure and shows examples of the fingerprints included in the four databases. Section 4.3 introduces the testing protocol with particular emphasis on the test procedures, the performance indicators used, and the treatment of failures and in Section 4.4, results of the top algorithms are reported.

Table 4.2 - The 53 FVC2006 participants: 17 of them submitted two algorithms (one for each category), 27 participated only in the Open category and 9 participated only in the Light category. The two struck-out rows denote participants that were disqualified due to unfair behaviour of their algorithms.

ID	Type	Open	Light
P006	Academy	✓	
P009	Independent developer	✓	
P015	Industry	✓	
P017	Industry	✓	✓
P022	Industry	✓	
P024	Industry	✓	
~~P030~~	~~Independent developer~~	~~✓~~	~~✓~~
P036	Academy	✓	
P041	Independent developer	✓	
P045	Industry	✓	✓
P050	Academy	✓	
P052	Academy		✓
P053	Independent developer	✓	
P054	Independent developer	✓	✓
P058	Industry	✓	✓
P060	Independent developer	✓	✓
P065	Independent developer	✓	✓
P066	Industry	✓	
P067	Industry	✓	
P072	Industry	✓	✓
P073	Academy	✓	
P074	Industry	✓	
P081	Industry	✓	✓
P083	Industry	✓	
P085	Academy	✓	
P088	Industry	✓	

ID	Type	Open	Light
P090	Industry	✓	✓
P092	Industry	✓	✓
P095	Academy	✓	
P096	Industry	✓	✓
P097	Industry	✓	
P098	Academy	✓	
P101	Independent developer	✓	✓
P103	Independent developer		✓
P106	Academy	✓	
P109	Industry	✓	
P118	Academy	✓	
P119	Academy	✓	
P120	Industry	✓	
P121	Independent developer		✓
P122	Independent developer		✓
P123	Academy		✓
P124	Industry	✓	
P129	Industry		✓
P131	Academy	✓	✓
P133	Industry		✓
P138	Academy	✓	✓
P141	Independent developer	✓	✓
P143	Industry		✓
~~P144~~	~~Industry~~	~~✓~~	~~✓~~
P148	Industry	✓	
P151	Industry	✓	
P153	Industry		✓

4.2 Databases

Four databases created using three different scanners and the SFinGe synthetic generator [109] [110] [9] were used in the FVC2006 benchmark (see Table 4.3). Figure 4.2 shows an example image at the same scale factor from each database.

Data collection in FVC2006 was performed without deliberately introducing difficulties

such as exaggerated distortion, large amounts of rotation and displacement, wet/dry impressions, etc. (as it was done in the previous editions), but the population is more heterogeneous and also includes manual workers and elderly people. The volunteers were simply asked to put their fingers naturally on the acquisition device, but no constraints were enforced to guarantee a minimum quality in the acquired images. The final datasets were selected from a larger database by choosing the most difficult fingers according to the NIST quality index, to make the benchmark sufficiently difficult for a technology evaluation.

Table 4.3 - Scanners/technologies used for collecting the databases.

	Technology	Image	Resolution
DB1	Electric Field Sensor (AuthenTec)	96×96	250 dpi
DB2	Optical Sensor (BiometriKa)	400×560	569 dpi
DB3	Thermal Sweeping Sensor (Atmel)	400×500	500 dpi
DB4	Synthetic Generator (SFinGe v3.0)	288×384	About 500 dpi

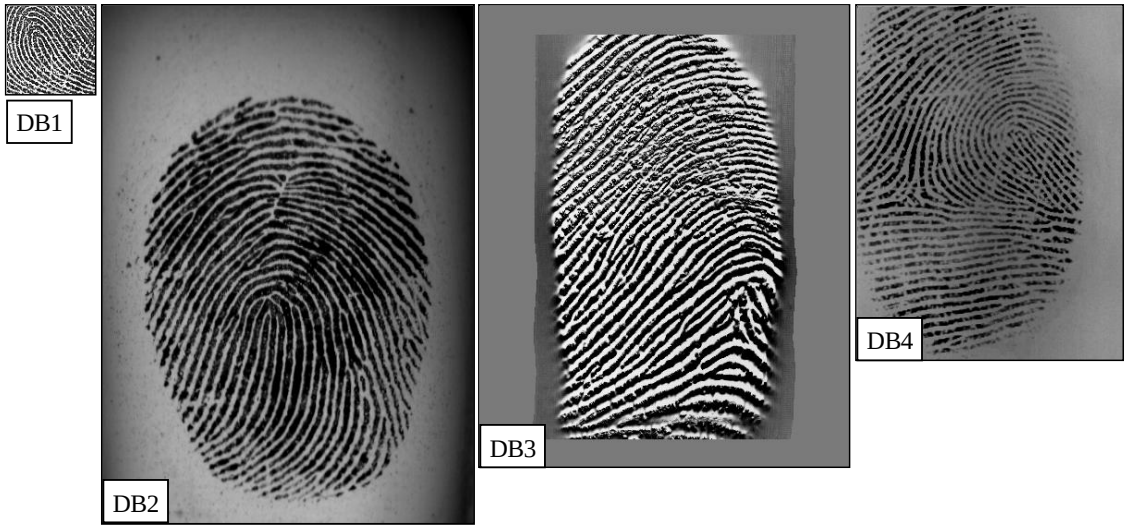


Figure 4.2 - A fingerprint image from each database, at the same scale factor.

4.3 Test protocol

4.3.1 Test procedure

Participants submitted each algorithm in the form of two executable programs: the first for enrolling a fingerprint image and producing the corresponding template, and the second for comparing a fingerprint template to a fingerprint image and producing a comparison score in the range [0,1]. The executables take the input from command-line arguments and append the output to a text file. The input includes a database-specific configuration file. For each database, participants were allowed to submit a distinct configuration file to adjust the algorithm's internal parameters (e.g. to accommodate the different image sizes). Configuration files are text or binary files and their I/O is the responsibility of the participant's code. These files can also contain pre-computed data to save time during enrollment and comparison. Each algorithm is tested by performing, for each database, the following comparisons:

- *genuine recognition attempts*: the template of each fingerprint image is compared to the remaining images of the same finger, but avoiding symmetric matches (i.e. if the template of image j is matched against image k, template k is not matched against image j);
- *impostor recognition attempts*: the template of the first image of each finger is compared to the first image of the remaining fingers, but avoiding symmetric matches.

Then, for each database:

- a total of 1540 enrollment attempts are performed (the enrollment of the last image of any finger does not need to be performed);
- if all the enrollments are correctly performed (no enrollment failures), the total number of genuine and impostor comparison attempts is 9240 and 9730, respectively.

All the algorithms are tested at the evaluators' site on evaluators' hardware: the evaluation is performed in a totally-controlled environment, where all input/output operations are strictly monitored. This enables us to:

- evaluate other useful performance indicators such as processing time, amount of

memory used, and template size (see Subsection 4.3.2);

- enforce a maximum response time of the algorithms;
- implement measures that guarantee algorithms cannot cheat (for instance matching filenames instead of fingerprints);
- ensure that, at each comparison, one and only one template is matched against one and only one image and that techniques such as template consolidation [100] and score normalization [95] are not used to improve performance.

The schema in Figure 4.3 summarizes the testing procedure of FVC2006.

In the Open category, for practical testing reasons, the maximum response time of the algorithms was limited to 10 seconds for enrollment and 5 seconds for comparison; no other limits were imposed.

In the Light category, in order to create a benchmark for algorithms running on light architectures, the following limits were imposed:

- maximum time for enrollment: 0.3 seconds;
- maximum time for comparison: 0.1 seconds;
- maximum template size: 2 KBytes;
- maximum amount of memory allocated: 4 MBytes.

The evaluation (for both categories) was executed using Windows XP Professional O.S. PCs with Intel Pentium 4 at 3.20Ghz and 1GB of RAM.

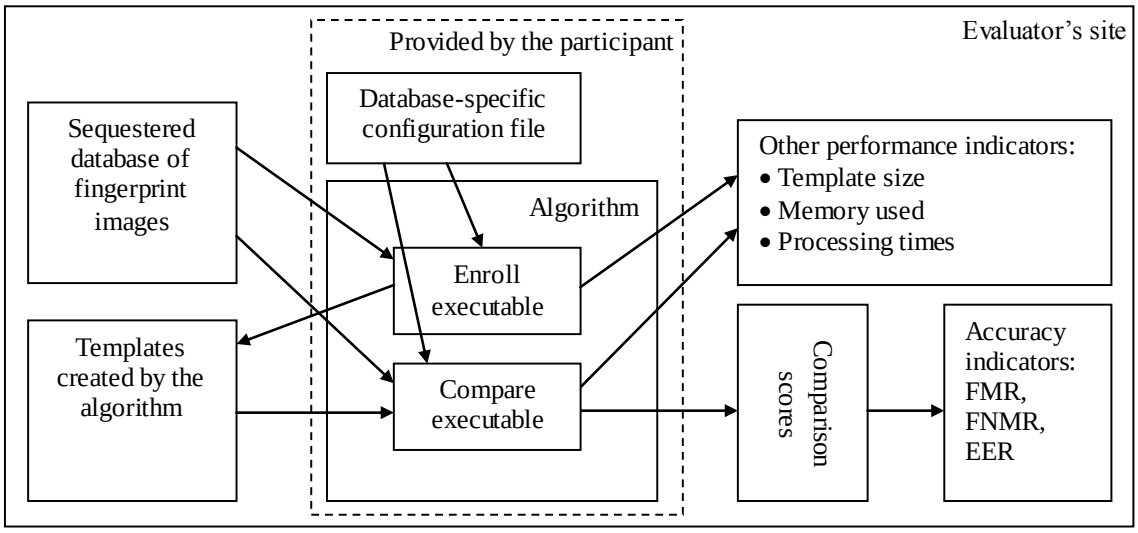


Figure 4.3 - Testing procedure.

4.3.2 Performance evaluation

For each database and for each algorithm, the following performance indicators were measured and reported:

- genuine and impostor score histograms;
- False Match Rate (FMR) and False Non-Match Rate (FNMR) graphs and Decision Error Tradeoff (DET) graph;
- Failure-to-Enroll Rate and Failure-to-Compare Rate;
- Equal Error Rate (EER), FMR100, FMR1000, ZeroFMR and ZeroFNMR;
- average enrollment time and average comparison time;
- maximum memory allocated for enrollment and for comparison;
- average and maximum template size.

A formal definition of FMR (False Match Rate), FNMR (False Non-Match Rate) and Equal Error Rate (EER) is given in [26]. Note that in single-attempt, positive recognition applications, FMR (False Match Rate) and FNMR (False Non-Match Rate) are often referred to as FAR (False Acceptance Rate) and FRR (False Rejection Rate), respectively. ZeroFMR is given as the lowest FNMR at which no False Matches occur and ZeroFNMR is the lowest FMR at which no False Non-Matches occur.

FMR100 and FMR1000 are the values of FNMR for $FMR = \frac{1}{100}$ and $\frac{1}{1000}$, respectively. These measures are useful to characterize the accuracy of fingerprint-based systems, which are often operated far from the EER point using thresholds which reduce FMR at the cost of higher FNMR (see also Subsection 1.1.3).

4.3.3 Treatment of failures

An enrollment or comparison attempt can fail, thus resulting in a Failure-to-Enroll (FTE) or Failure-to-Compare (FTC) error, respectively. Failures can be reported by the algorithm (which declares itself to be unable to process a given fingerprint), or imposed by the test procedure in the following cases:

- *timeout*: the algorithm exceeds the maximum processing time allowed;
- *crash*: the program crashes during its execution;

- *memory limit*: the amount of memory allocated by the algorithm exceeds the maximum allowed;
- *template limit* (only for enrollment): the size of the template exceeds the maximum allowed;
- *missing template* (only for comparison): the required template has not been created due to enrollment failure, such that the comparison cannot be performed.

4.4 Results

This section, after a structured overview of the algorithms (Subsection 4.4.1), reports: the results of the top algorithms in the two categories (Subsections 4.4.2 and 4.4.3). Note that in the following graphs and tables, participant IDs (e.g. P001, P002) are used to denote the different algorithms. For instance, "P001" indicates the algorithm submitted by participant P001; since many participants submitted two algorithms (one for each category), the same participant ID may refer to the Open category algorithm or to the Light category algorithm, according to the context.

4.4.1 Overview of the algorithms

Reporting low-level details about the approaches and techniques adopted by the participating algorithms would be unfeasible, since most of the participants are commercial entities and the details of their algorithms are proprietary. For this reason, as in FVC2004, all the participants had to provide a high-level structured description of their algorithms by answering a few questions about:

- *Pre-processing*: Is segmentation (separation of the fingerprint area from the background) and/or image enhancement performed?
- *Alignment*: Is alignment carried out before or during comparison? What kind of transformations are dealt with (displacement, rotation, scale, non-linear mapping)?
- *Features*: Which features are extracted from the fingerprint images?
- *Comparison*: Is the algorithm minutiae-based? If so, is minutiae comparison

global or local [9]? If not, what is the approach (correlation-based, ridge-pattern-texture-based, ridge-line-geometry-based)?

All the participants except P095 provided the requested data; Table 4.4 compares the algorithms by summarizing the main information. The two histograms in Figure 4.4 highlight the distribution of the features adopted and of the matching approaches, respectively. Figure 4.5 and Figure 4.6 compare the two distributions with those of FVC2004.

Table 4.4 - High-level description of the algorithms from 52 participants. Notes: P030 - Raw image parts and Correlation are used only in the Open category. P058 - Ridge counts is used only in the Open category. P101 - Ridge pattern (texture) and Correlation are used only in the Open category. P131 - alignment type is Non-linear in the Open category and Displacement + Rotation + Scale in the Light one; Ridge Count is used only in the Light category, all the other bracketed elements only in the Open category. P141 - alignment type is Non-linear in the Open category. P144 - Local ridge frequency and Texture measures are used only in the Open category.

Preprocessing			**Alignment**		**Features**								**Comparison**				
Participant	Segmentation	Enhancement	Before matching, During matching	Displacement, Rotation, Scale, Non-linear	Minutiae	Singular points	Ridges	Ridge counts	Orientation field	Local ridge frequency	Texture measures	Raw/Enh. image parts	Minutiae (global)	Minutiae (local)	Ridge pattern (geometry)	Ridge pattern (texture)	Correlation
P006	✓	✓	D	DR	✓					✓	✓		✓			✓	✓
P009	✓	✓	D	N	✓								✓				
P015	✓	✓	D	DR	✓	✓	✓		✓	✓	✓		✓	✓	✓		
P017	✓	✓	BD	DRS	✓	✓	✓	✓	✓	✓			✓				
P022	✓	✓	-	-	✓	✓		✓					✓				
P024	✓	✓	-	-	✓									✓			
P030		✓	B	DRS	✓	✓			✓			(✓)	✓	✓			(✓)
P036	✓	✓	D	DR	✓			✓	✓				✓				
P041	✓	✓	-	-	✓		✓						✓		✓		✓
P045	✓	✓	D	DR	✓	✓			✓	✓		✓	✓				✓
P050	✓	✓	B	DR	✓	✓								✓			
P052	✓	✓	D	DR	✓								✓	✓			
P053	✓	✓	B	DR	✓		✓		✓				✓				
P054	✓	✓	D	DRS	✓				✓				✓				
P058	✓	✓	D	DRS	✓		✓	(✓)		✓				✓			
P060	✓	✓	-	-	✓				✓	✓			✓	✓			
P065	✓	✓	D	DRS	✓	✓							✓	✓			
P066	✓	✓	D	DR	✓	✓	✓	✓	✓		✓			✓	✓	✓	
P067	✓	✓	D	N	✓		✓		✓			✓	✓	✓	✓		✓
P072	✓	✓	D	DR	✓		✓						✓		✓		

Preprocessing			Alignment		Features								Comparison				
Participant	Segmentation	Enhancement	Before matching, During matching	Displacement, Rotation, Scale, Non-linear	Minutiae	Singular points	Ridges	Ridge counts	Orientation field	Local ridge frequency	Texture measures	Raw/Enh. image parts	Minutiae (global)	Minutiae (local)	Ridge pattern (geometry)	Ridge pattern (texture)	Correlation
P073	✓	✓	D	DRS	✓			✓	✓	✓			✓	✓			
P074	✓	✓	VB	N	✓		✓		✓	✓				✓			
P081			-	-	✓									✓			
P083	✓	✓	D	DR	✓	✓		✓	✓			✓		✓	✓		
P085	✓	✓	D	DRS	✓		✓		✓						✓		
P088	✓		D	DRS	✓	✓	✓	✓	✓	✓			✓	✓	✓		
P090	✓	✓	D	DR	✓	✓					✓			✓			✓
P092	✓	✓	-	-	✓		✓		✓					✓			
P096		✓	D	DR	✓		✓	✓	✓		✓		✓				
P097	✓	✓	-	-	✓		✓		✓					✓	✓		
P098	✓	✓	D	DR	✓								✓	✓			
P101	✓	✓	D	N	✓	✓			✓				✓	✓		(✓)	(✓)
P103	✓	✓	-	-	✓	✓			✓					✓			
P106	✓	✓	D	DR	✓				✓	✓	✓		✓			✓	✓
P109	✓	✓	D	DR	✓	✓			✓	✓			✓				
P118	✓	✓	D	DR	✓		✓		✓				✓		✓		✓
P119	✓	✓	D	DR	✓								✓				
P120	✓	✓	B	DR		✓			✓	✓	✓					✓	
P121	✓	✓	D	DR	✓	✓	✓		✓					✓	✓		
P122	✓	✓	D	DR	✓		✓		✓					✓	✓		
P123			-	-	✓			✓						✓			
P124	✓	✓	D	DR	✓	✓	✓							✓	✓		
P129	✓	✓	D	DR	✓				✓	✓	✓		✓			✓	
P131	✓	✓	D	(N)(DRS)	✓	(✓)	(✓)	(✓)	✓	✓		(✓)		✓	(✓)		(✓)
P133	✓	✓	D	DR	✓				✓		✓		✓	✓		✓	
P138	✓	✓	D	DR	✓				✓	✓			✓				
P141	✓	✓	D	DR(N)	✓				✓	✓			✓	✓	✓		✓
P143	✓	✓	D	DR	✓	✓	✓						✓	✓	✓		
P144	✓	✓	D	DRS	✓		✓		✓	(✓)	(✓)		✓		✓		✓
P148	✓	✓	B	D		✓			✓	✓	✓					✓	
P151	✓		D	N	✓	✓				✓			✓				
P153	✓	✓	D	DR	✓								✓				

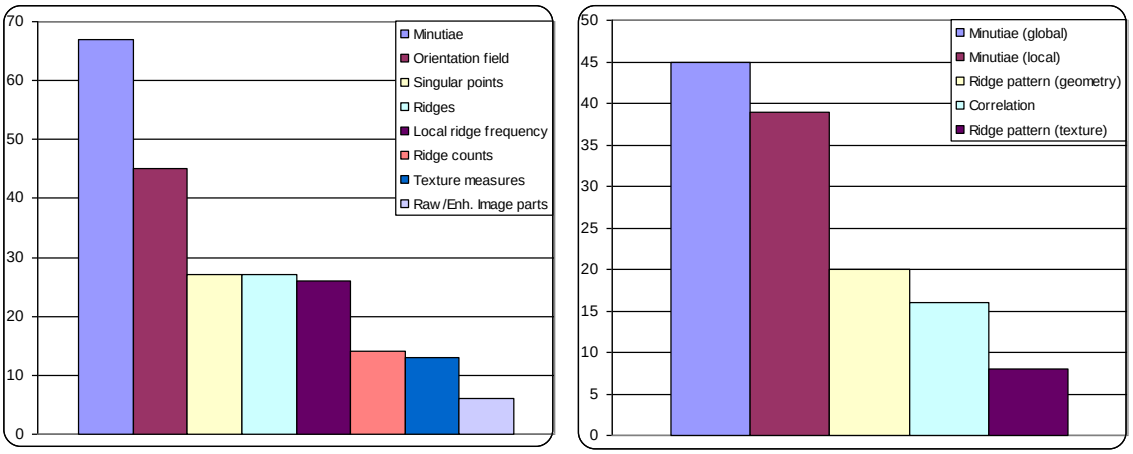


Figure 4.4 - Histograms of the distribution of the different features (on the left) and of the different matching strategies (on the right) exploited by the algorithms.

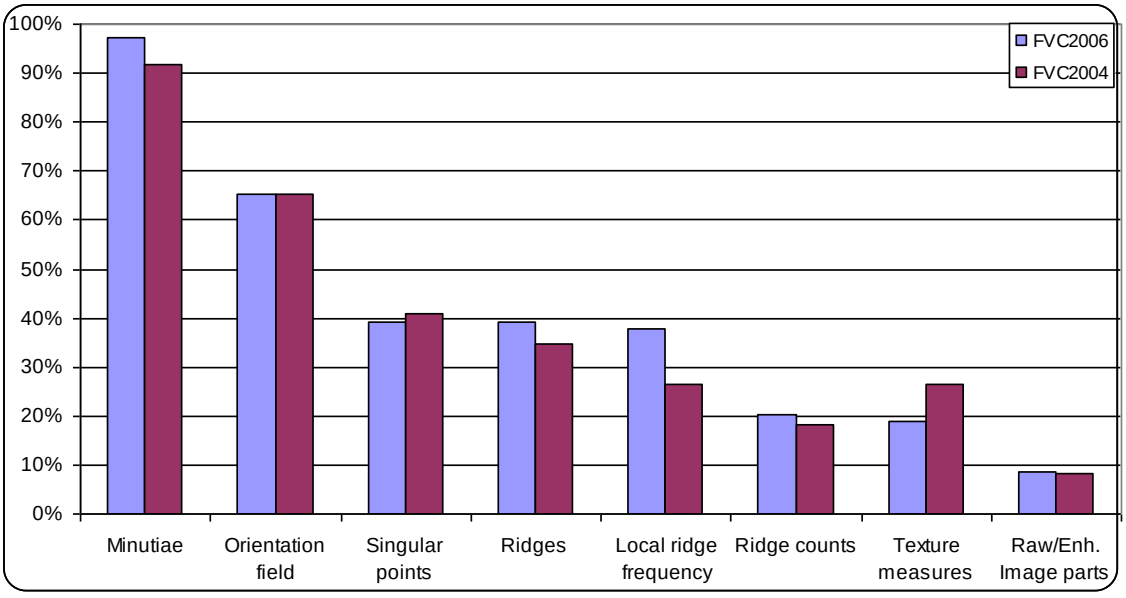


Figure 4.5 - Comparison between the features exploited by the algorithms in FVC2006 and FVC2004.

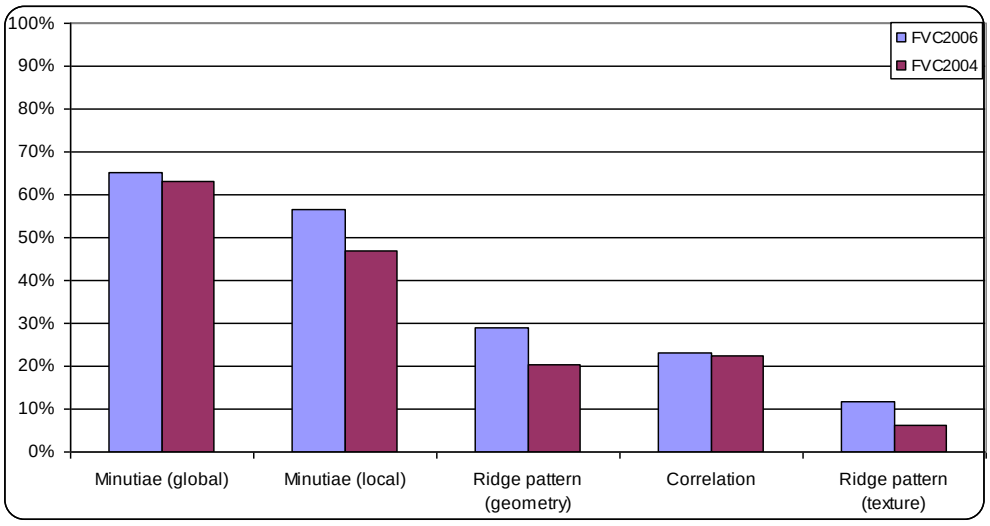


Figure 4.6 - Comparison between the matching approaches of the algorithms in FVC2006 and FVC2004.

4.4.2 Open category - results on the four databases

In the following, results from the top 15 algorithms on each of the four databases are reported for the Open category. Detailed results, of all the algorithms, are reported in the FVC2006 Web Site [85].

Table 4.5 - Open category - database 1: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P017	5.564	9.708	15.335	22.922	0.00	0.00	0.038	0.039	1.22	1.66	1472	2172
P066	5.978	9.556	14.167	19.405	0.00	0.00	0.430	0.506	5.63	10.84	8080	8520
P045	6.122	10.498	22.348	41.494	0.00	0.00	0.074	0.311	3.88	5.23	1476	1916
P131	6.922	8.712	21.299	29.675	0.00	0.00	0.068	0.205	8.02	11.91	5772	6724
P067	7.044	12.435	15.325	24.177	0.00	0.00	0.108	0.120	24.01	25.37	3404	3600
P009	7.370	10.584	13.344	20.303	0.00	0.00	0.265	0.304	1.43	2.10	4028	4208
P058	7.496	10.779	13.041	15.671	0.00	0.00	0.103	0.103	2.07	4.22	1636	1660
P074	7.733	12.619	17.576	28.701	0.00	0.00	0.092	0.094	2.04	3.52	1468	1480
P015	7.823	11.201	14.156	17.814	0.00	0.00	0.572	0.597	1.31	3.26	14264	20324
P101	7.928	12.424	57.413	57.413	0.00	0.00	0.176	0.283	4.16	4.84	1856	7496
P024	8.255	10.898	13.669	16.926	0.00	0.00	0.065	0.067	1.01	1.37	2100	2360
P088	8.794	13.864	18.431	26.840	0.00	0.00	0.503	0.515	0.89	3.24	1832	4288
P072	8.887	13.247	17.792	23.853	0.00	0.00	0.024	0.035	1.38	1.38	724	760
P060	9.124	21.190	51.115	79.513	0.00	0.00	0.134	0.136	0.34	0.73	1176	1184

P041	9.468	12.641	16.061	20.444	0.00	0.00	0.033	0.049	0.50	0.68	1808	2308

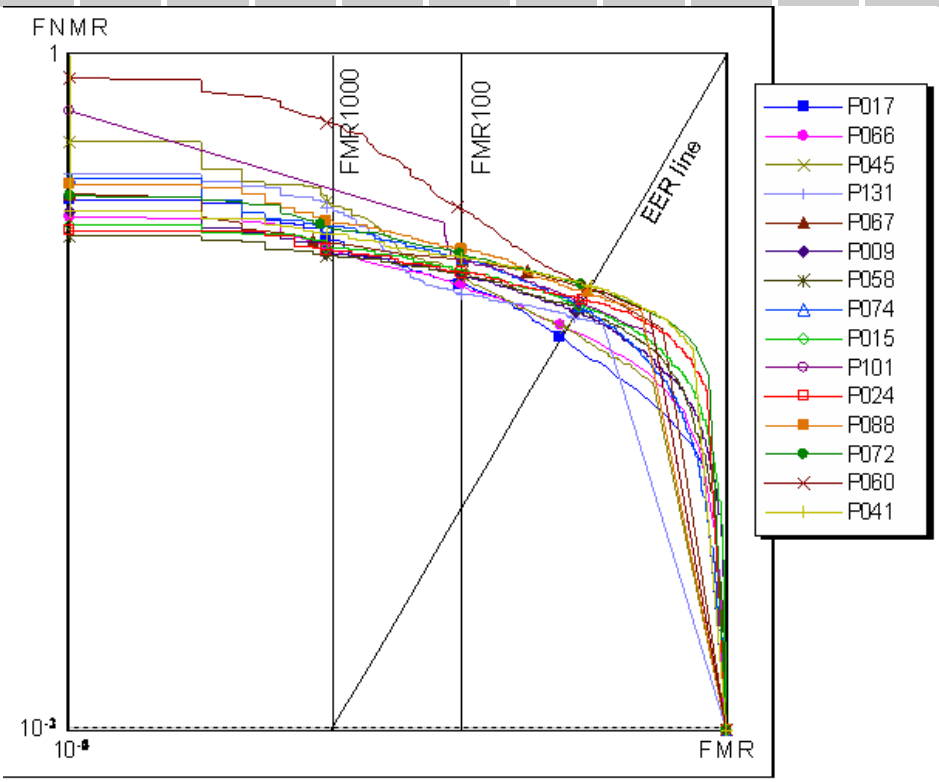


Figure 4.7 - Open category – database 1: DET graph of the top 15 algorithms (according to EER).

Table 4.6 - Open category - database 2: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P088	0.021	0.011	0.022	0.022	0.00	0.00	1.085	1.100	1.60	3.17	6224	7460
P015	0.032	0.022	0.032	0.032	0.00	0.00	1.434	1.461	2.76	5.54	19744	24956
P009	0.095	0.000	0.097	0.249	0.00	0.00	0.799	0.899	2.00	3.19	6228	6404
P058	0.100	0.076	0.108	0.141	0.00	0.00	0.587	0.589	5.28	10.22	3644	3672
P101	0.121	0.076	0.141	0.346	0.00	0.00	0.727	0.769	6.27	7.30	4208	7728
P066	0.122	0.065	0.152	0.281	0.00	0.00	0.771	1.002	9.56	17.04	4728	7156
P065	0.137	0.087	0.162	0.422	0.00	0.00	0.091	0.091	0.23	0.46	1924	1948
P045	0.138	0.043	0.173	0.606	0.00	0.00	0.226	0.253	9.73	14.30	2304	3168
P067	0.185	0.130	0.335	0.509	0.00	0.00	0.403	0.427	81.42	111.33	7312	7684
P141	0.237	0.195	0.346	0.909	0.00	0.00	0.158	0.168	2.07	2.74	2104	2108
P074	0.248	0.184	0.368	1.028	0.00	0.00	0.257	0.270	5.64	9.27	2440	2456
P072	0.268	0.130	0.465	0.952	0.00	0.00	0.072	0.116	4.89	4.89	904	932
P022	0.290	0.216	0.411	0.898	0.00	0.00	0.655	0.666	1.93	1.93	3756	4676
P090	0.374	0.335	0.552	7.900	0.00	0.00	0.141	0.085	0.72	1.01	1964	3104
P024	0.474	0.368	0.682	100.000	0.00	0.00	0.214	0.146	2.36	3.46	3060	3836

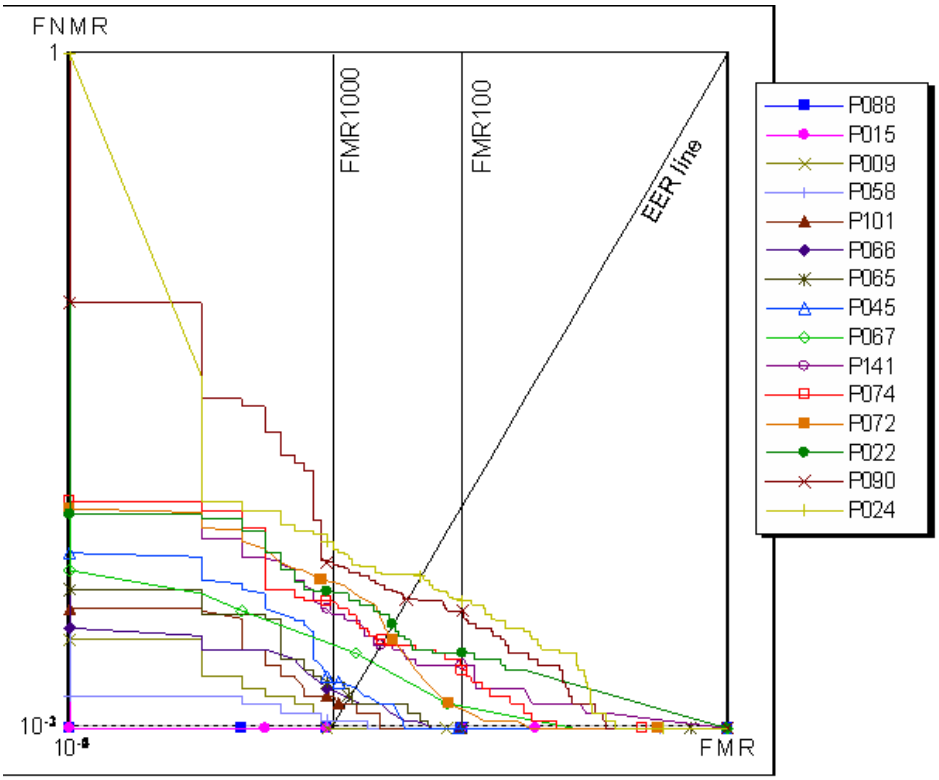


Figure 4.8 - Open category – database 2: DET graph of the top 15 algorithms (according to EER).

Table 4.7 - Open category - database 3: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P015	1.534	1.753	2.760	7.175	0.00	0.00	1.682	1.678	5.88	10.67	20324	25528
P058	1.608	1.786	2.413	3.755	0.00	0.00	0.307	0.307	4.34	12.31	3272	3292
P009	1.645	1.937	3.030	3.929	0.00	0.00	0.583	0.641	1.81	3.06	6020	6196
P074	1.681	1.851	3.268	4.719	0.00	0.00	0.235	0.242	4.73	10.12	2376	2392
P045	1.890	2.468	5.260	7.587	0.00	0.00	0.194	0.223	8.32	12.79	2276	3300
P066	2.054	2.738	3.864	7.597	0.00	0.00	0.517	0.661	7.23	13.39	3648	6808
P072	2.135	2.900	4.545	5.584	0.00	0.00	0.071	0.114	5.88	5.88	876	912
P088	2.156	2.392	3.669	5.725	0.00	0.00	0.844	0.847	1.38	3.11	6844	8076
P067	2.203	3.420	6.234	7.024	0.00	0.00	0.255	0.274	51.87	86.09	6644	6960
P024	2.335	2.781	4.340	100.000	0.00	0.00	0.239	0.169	2.01	3.20	3924	4600
P131	2.615	3.214	6.753	18.929	0.00	0.00	0.275	0.437	16.42	28.13	9528	8660
P017	2.762	3.734	5.974	10.022	0.00	0.00	0.097	0.097	1.59	2.00	2348	2740
P041	2.810	3.409	5.195	8.019	0.00	0.00	0.123	0.135	0.99	1.63	3716	4600
P065	2.979	3.680	5.054	7.240	0.00	0.00	0.058	0.057	0.21	0.55	1828	1852
P101	3.019	3.810	4.297	5.076	0.00	0.00	0.508	0.543	5.74	7.19	3896	7712

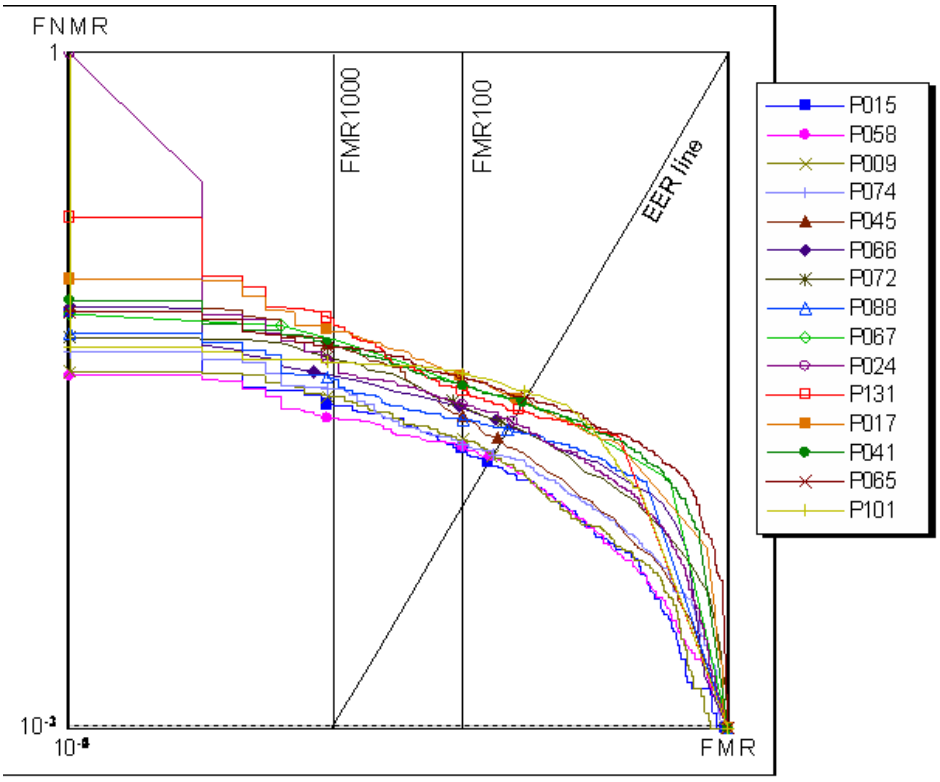


Figure 4.9 - Open category – database 3: DET graph of the top 15 algorithms (according to EER).

Table 4.8 - Open category - database 4: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P009	0.269	0.141	0.400	0.703	0.00	0.00	0.564	0.601	1.69	2.43	5268	5436
P074	0.453	0.368	0.823	1.732	0.00	0.00	0.230	0.238	5.04	8.51	2068	2084
P066	0.466	0.465	0.855	2.045	0.00	0.00	0.725	1.023	7.21	11.00	3284	6688
P015	0.627	0.595	0.952	1.450	0.00	0.00	1.085	1.113	2.51	5.44	17132	22316
P101	0.691	0.693	0.942	2.229	0.00	0.00	0.636	0.679	6.39	7.51	3804	7728
P131	0.701	0.671	0.974	17.251	0.13	0.07	0.185	0.291	16.45	30.29	7648	7216
P045	0.759	0.714	1.883	10.411	0.00	0.00	0.146	0.178	8.43	12.45	1916	2664
P088	0.891	0.877	1.699	3.712	0.00	0.00	1.528	1.549	1.64	4.63	3444	6620
P058	0.991	0.996	1.959	3.398	0.00	0.00	0.292	0.294	3.88	8.23	2340	2368
P017	1.112	1.147	1.677	3.907	0.00	0.00	0.072	0.073	1.52	1.97	1964	2152
P090	1.218	1.299	2.262	3.690	0.00	0.00	0.088	0.055	0.50	0.75	1620	2620
P072	1.345	1.558	2.976	6.894	0.00	0.00	0.045	0.074	3.30	3.30	792	828
P024	1.350	1.483	2.879	100.000	0.32	0.65	0.133	0.109	1.93	2.76	2440	3136
P041	1.486	1.591	2.857	100.000	0.32	0.65	0.062	0.080	0.95	1.32	2008	3012
P067	1.570	2.348	4.740	5.823	0.00	0.00	0.197	0.244	40.68	55.78	4712	9740

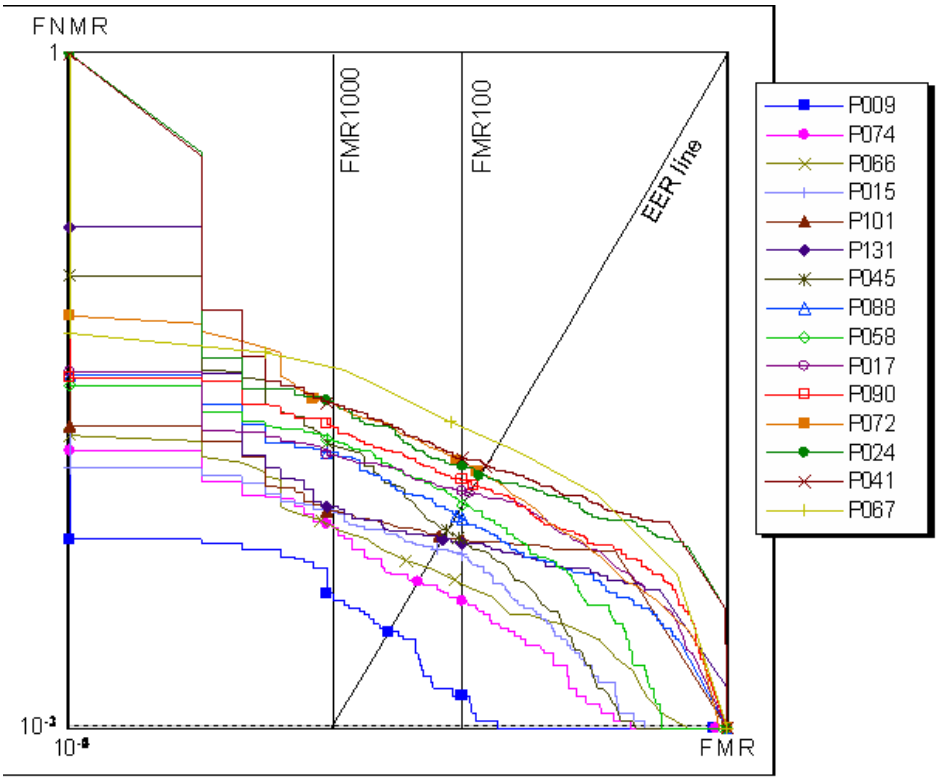


Figure 4.10 - Open category – database 4: DET graph of the top 15 algorithms (according to EER).

4.4.3 Light category - results on the four databases

In the following, results from the top 15 algorithms on each of the four databases are reported for the Light category. Detailed results, of all the algorithms, are reported in the FVC2006 Web Site [85].

Table 4.9 - Light category - database 1: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P129	5.356	8.225	13.323	100.000	0.32	1.01	0.031	0.029	1.94	1.94	1860	2028
P017	5.564	9.708	15.335	22.922	0.00	0.00	0.037	0.039	1.22	1.66	1472	2172
P133	5.888	8.506	12.890	100.000	0.32	1.01	0.039	0.036	1.71	1.71	2888	3032
P045	6.420	12.251	20.303	28.669	0.00	0.00	0.048	0.052	1.43	1.64	1328	1740
P121	7.877	11.634	17.348	22.489	0.00	0.00	0.027	0.027	0.46	0.74	1412	1436
P058	8.019	11.310	15.368	21.742	0.00	0.47	0.075	0.075	0.49	1.03	1532	1552
P072	9.412	13.994	18.929	22.890	0.00	0.00	0.024	0.032	1.20	1.20	724	756
P131	9.942	20.022	35.595	46.970	0.00	0.00	0.035	0.036	0.79	1.41	1404	1284
P143	10.116	17.652	27.662	54.221	0.00	0.00	0.022	0.023	0.42	0.77	1008	1120
P065	10.385	15.411	20.530	30.271	0.00	0.14	0.023	0.022	0.09	0.18	1196	1804
P141	10.514	25.032	45.335	78.712	0.00	0.00	0.024	0.026	0.67	0.91	1000	1384
P052	11.026	18.853	25.693	35.952	0.00	0.00	0.019	0.022	0.18	0.44	1080	1592
P096	11.573	21.732	32.154	50.541	0.13	1.58	0.039	0.041	1.67	1.67	1172	1248
P054	11.746	21.494	32.381	50.509	0.13	1.58	0.040	0.041	1.58	1.58	1172	1244
P101	11.839	19.978	27.965	34.621	0.00	0.00	0.079	0.075	0.28	0.68	1700	2496

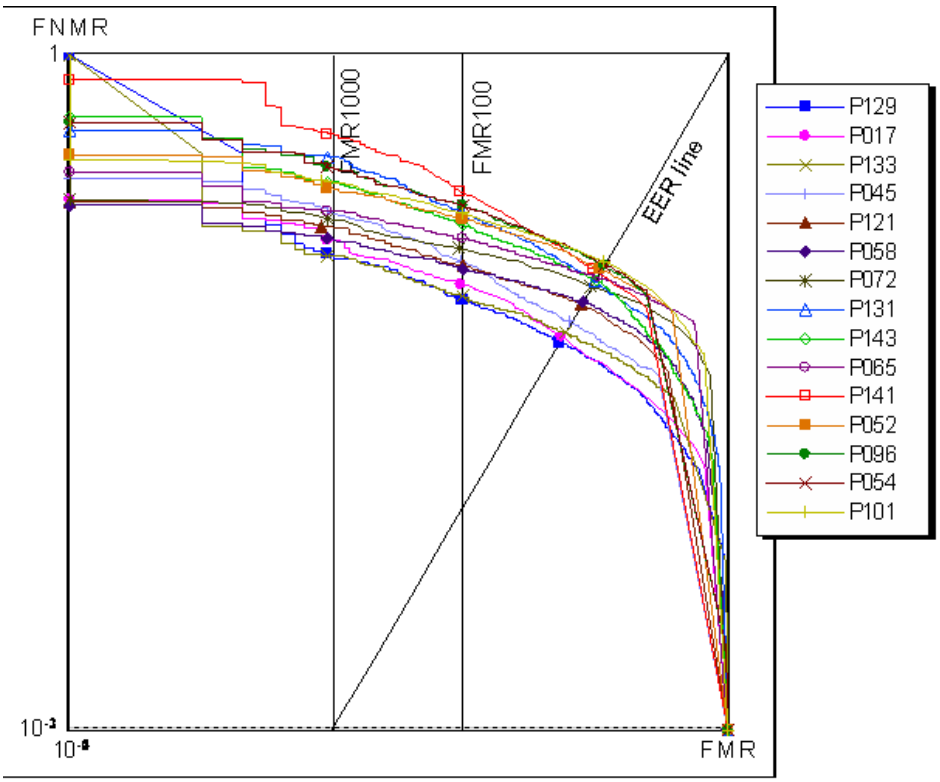


Figure 4.11 - Light category – database 1: DET graph of the top 15 algorithms (according to

EER).

Table 4.10 - Light category - database 2: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P065	0.148	0.087	0.173	0.422	0.00	0.01	0.092	0.091	0.23	0.46	1924	1948
P133	0.158	0.087	0.195	0.335	0.00	0.00	0.064	0.066	1.71	1.71	3272	3416
P129	0.169	0.087	0.206	0.325	0.00	0.00	0.056	0.056	1.94	1.94	2236	2420
P121	0.190	0.119	0.260	0.346	0.00	0.00	0.070	0.067	1.24	1.99	2008	1948
P045	0.290	0.141	0.628	2.229	0.00	0.00	0.101	0.047	0.55	0.82	2284	2328
P141	0.295	0.206	0.606	1.439	0.00	0.00	0.044	0.052	1.00	1.34	1536	1596
P058	0.295	0.249	0.368	0.855	0.00	0.00	0.181	0.082	1.05	1.81	2236	1708
P090	0.411	0.314	2.240	7.727	0.00	0.00	0.114	0.064	0.72	1.01	2016	3248
P143	0.474	0.390	0.812	1.396	0.00	0.00	0.045	0.044	1.18	1.81	1728	1816
P017	0.585	0.509	0.920	1.872	0.00	0.00	0.109	0.069	1.65	2.00	2356	2224
P072	0.586	0.574	1.017	1.732	0.00	0.00	0.043	0.061	2.00	2.00	900	936
P081	0.680	0.660	0.768	0.909	0.00	0.00	0.037	0.038	1.01	1.83	1028	1092
P096	0.707	0.703	1.526	2.814	0.00	0.00	0.069	0.072	1.67	1.67	1380	1488
P092	0.712	0.671	1.342	2.641	0.00	0.00	0.070	0.072	1.74	1.74	1380	1480
P054	0.807	0.736	1.558	2.965	0.00	0.00	0.072	0.071	1.58	1.58	1380	1476

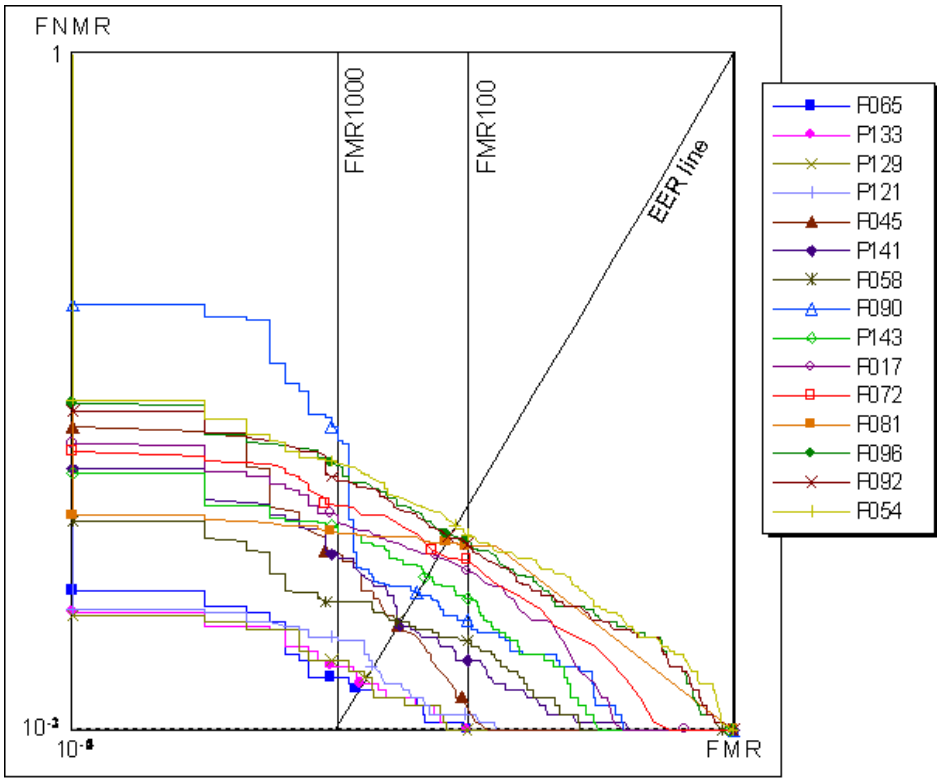


Figure 4.12 - Light category – database 2: DET graph of the top 15 algorithms (according to EER).

Table 4.11 - Light category - database 3: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P133	1.634	1.742	3.009	4.329	0.06	0.79	0.054	0.056	1.71	1.71	3252	3396
P129	1.645	1.753	2.987	4.210	0.06	0.79	0.047	0.046	1.94	1.94	2216	2392
P058	2.351	2.738	4.686	6.526	0.00	0.00	0.121	0.082	0.87	1.83	2208	1708
P045	2.489	3.582	7.814	11.223	0.00	0.00	0.084	0.040	0.47	0.79	2192	2236
P017	2.887	3.885	6.439	18.128	0.00	0.00	0.091	0.070	1.54	1.94	2208	2164
P065	2.952	3.669	5.087	7.511	0.00	0.00	0.058	0.057	0.21	0.55	1828	1852
P141	3.063	4.156	7.110	13.149	0.00	0.00	0.047	0.051	0.95	1.54	1752	1756
P072	3.205	4.145	6.017	8.182	0.00	0.00	0.041	0.058	2.00	2.00	876	912
P121	3.338	4.177	5.898	7.424	0.00	0.00	0.058	0.055	1.09	2.00	2124	2056
P052	3.502	4.848	7.413	15.909	0.00	0.00	0.061	0.067	0.34	0.44	1596	1924
P143	3.548	5.011	8.366	11.374	0.00	0.00	0.029	0.033	0.95	1.74	1620	1712
P131	3.632	5.281	10.173	19.535	0.00	0.00	0.077	0.058	1.26	1.74	1884	1592
P090	4.360	5.357	7.338	17.013	0.00	0.00	0.093	0.058	0.56	0.97	2124	3332
P096	4.850	7.641	11.266	18.268	0.00	0.00	0.065	0.067	1.67	1.67	1360	1464
P054	4.871	7.771	11.115	18.225	0.00	0.00	0.068	0.067	1.58	1.58	1360	1460

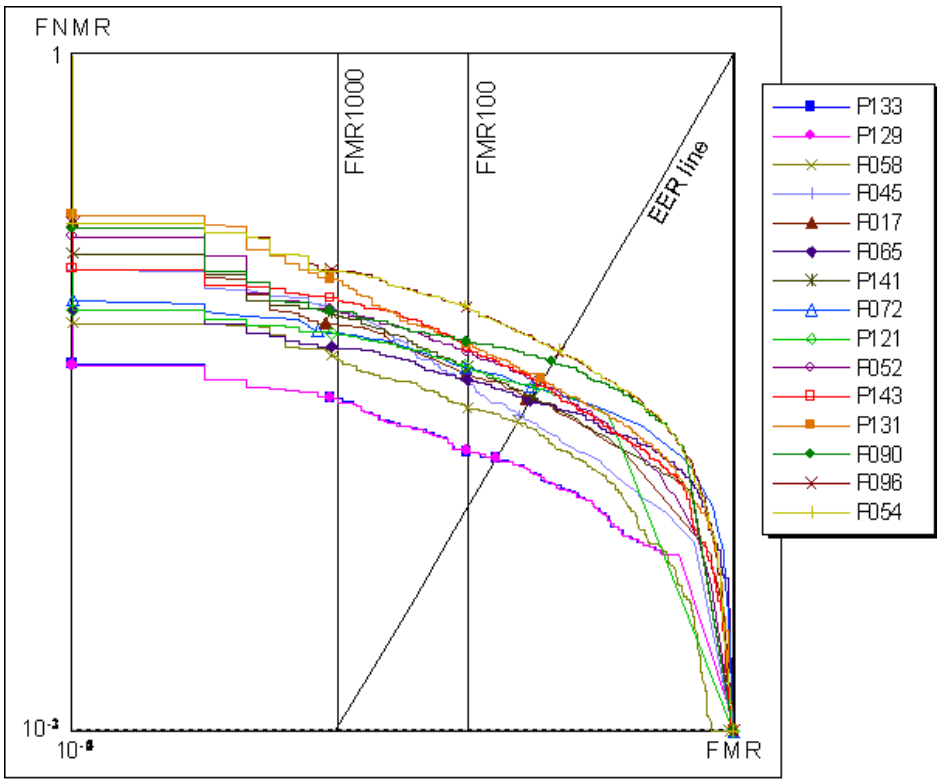


Figure 4.13 - Light category – database 3: DET graph of the top 15 algorithms (according to EER).

Table 4.12 - Light category - database 4: top 15 algorithms, sorted by EER.

Algorithm	EER (%)	FMR100 (%)	FMR1000 (%)	ZeroFMR (%)	FTE (%)	FTC (%)	Avg Enroll Time (s)	Avg Comparison Time (s)	Avg Model Size (KB)	Max Model Size (KB)	Max Enroll Memory (KB)	Max Match Memory (KB)
P121	0.427	0.249	0.747	1.039	0.00	0.00	0.049	0.049	0.87	1.61	1736	1760
P129	0.496	0.400	1.115	1.742	0.00	0.00	0.055	0.054	1.94	1.94	2176	2344
P133	0.522	0.465	1.039	2.327	0.00	0.00	0.063	0.062	1.71	1.71	3212	3344
P045	0.564	0.400	2.424	10.725	0.00	0.00	0.071	0.053	0.78	1.29	1856	2056
P141	0.680	0.498	1.613	2.976	0.00	0.00	0.050	0.056	1.36	1.80	1540	1544
P143	0.875	0.844	1.916	3.323	0.00	0.00	0.027	0.032	0.84	1.53	1272	1348
P017	1.135	1.190	1.710	3.810	0.00	0.00	0.071	0.066	1.52	1.98	1896	2128
P090	1.144	1.169	2.229	6.742	0.00	0.00	0.083	0.054	0.51	0.78	1672	2816
P131	1.603	1.861	4.113	6.396	0.00	0.00	0.073	0.060	1.15	1.63	1596	1436
P065	1.666	1.775	2.468	4.675	0.00	0.00	0.050	0.049	0.17	0.37	1484	1508
P052	1.877	2.327	4.794	25.779	0.00	0.00	0.042	0.048	0.28	0.44	1324	1648
P072	2.024	2.684	4.794	13.961	0.00	0.00	0.036	0.053	2.00	2.00	792	824
P058	3.443	4.816	7.338	10.065	0.00	0.00	0.116	0.084	0.80	1.77	1732	1624
P092	5.245	7.890	12.814	26.071	0.00	0.00	0.056	0.060	1.74	1.74	1272	1408
P096	5.432	8.690	13.745	28.193	0.00	0.00	0.056	0.059	1.67	1.67	1276	1408

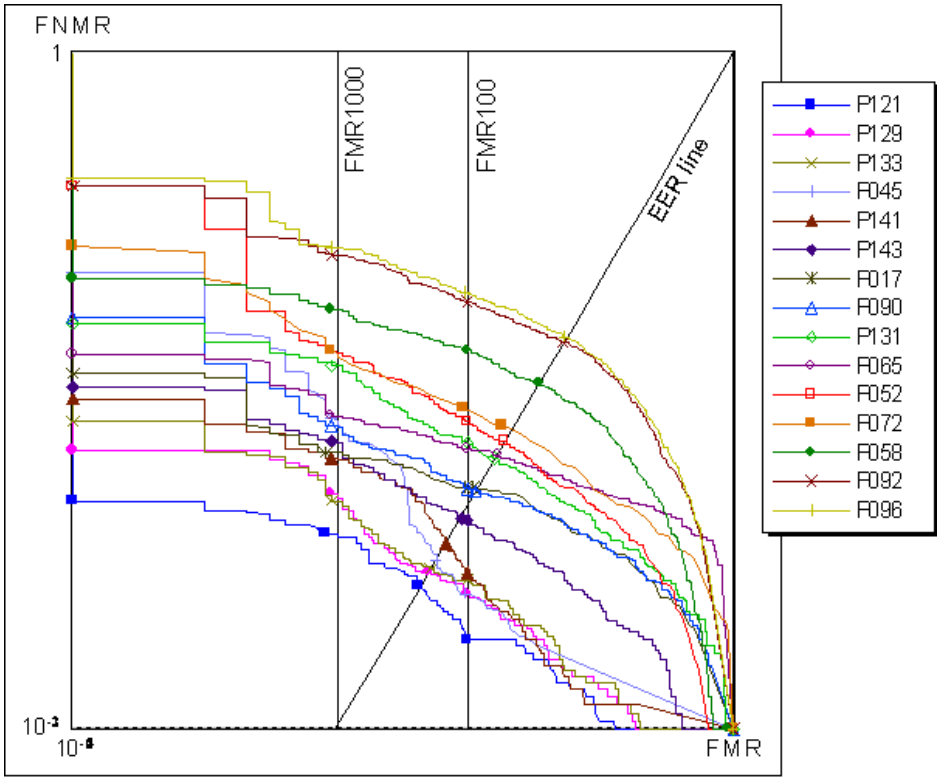


Figure 4.14 - Light category – database 4: DET graph of the top 15 algorithms (according to EER).

4.5 FVC-onGoing

FVC-onGoing [103] [104] will offer web-based automatic evaluation of fingerprint recognition algorithms on a set of sequestered datasets, reporting results using well known performance indicators and metrics.

The aim is to track the advances in fingerprint recognition technologies, through continuously updated independent testing and reporting of performances on given benchmarks. The benchmark datasets will not evolve over time; in case new datasets will be added in the future, they will form a different benchmark or a new version of an existing one: in this way, only results obtained on the same data will be compared.

The algorithms will be evaluated using strongly supervised approaches (see [10]), to maximize trustworthiness of the results.

While previous FVC initiatives were organized as "competitions", with specific calls and fixed time frames, FVC-onGoing will be:

- an "on going competition" always open to new participants;
- an evolving online repository of evaluation metrics and results.

Furthermore, the evaluation will be not only limited to fingerprint verification algorithms: ad hoc metrics and datasets for testing specific modules of fingerprint verification systems will be available. In fact, since results are always reported as FMR/FNMR values (see Subsection 1.1.3) of the entire fingerprint recognition system developed, it is practically impossible to understand if an advancement in performance is due to a specific matching technique or is in large part due to a minor change in an existing feature extraction method. For example, the only way to objectively compare fingerprint matchers is to start from the same set of features (i.e., the set of minutiae for minutiae based matchers). This will allow to better understand the limits and the challenges not only of the whole recognition problem, but also of its building blocks, with clear benefits for researchers and algorithms' developers.

Benchmarks (witch specific datasets and testing protocols) for the following (sub)problems are currently being developed, and others may be added in the future:

- Fingerprint Verification (assessment of the accuracy of one-to-one fingerprint matching algorithms);
- Orientation Image Extraction (assessment of the accuracy of orientation image

extraction algorithms);

- Minutiae Extraction (assessment of the accuracy of minutiae extraction algorithms);
- Minutiae Matching (assessment of the accuracy of minutiae matching algorithms on datasets of minutiae templates).

One of the main goals of FVC-onGoing is to fully automate the main steps of the evaluation: participant registration, algorithm submission, performance evaluation, and reporting of the results. To this purpose, a new web-based evaluation framework, whose architecture and typical workflow are shown in Figure 4.15, was developed.

4.6 Conclusions

Performance evaluation is important for all pattern recognition applications and particularly so for biometrics, which is receiving widespread international attention for citizen identity verification and identification in large-scale applications. Unambiguously and reliably assessing the current state of the technology is mandatory for understanding its limitations and addressing future research requirements. This document reviews and classifies current biometric testing initiatives and assesses the state-of-the-art in fingerprint verification through presentation of the results of the fourth international Fingerprint Verification Competition (FVC2006). The interest shown in the FVC testing program by algorithm developers continues to be very high: the fingerprint databases of the three previous editions constitute the most frequently used benchmarking databases in scientific publications on fingerprint recognition; in this fourth edition (FVC2006), a total of 70 algorithms, submitted by 53 participants, have been evaluated by the organizers. The huge amount of data collected during the tests (not only match scores, but also execution times, template size, etc.), together with the high-level information on the algorithms is currently being analyzed to gain more insights into the current state-of-the art of this challenging pattern recognition problem.
However, as far as FVC-onGoing is concerned, the development of the evaluation framework is completed (see Figure 4.15); in the next months a beta testing phase will be carried out with some invited participants and the official start of FVC-onGoing is planned to be held in conjunction with the *3rd International Conference on Biometrics* (ICB2009) [111].

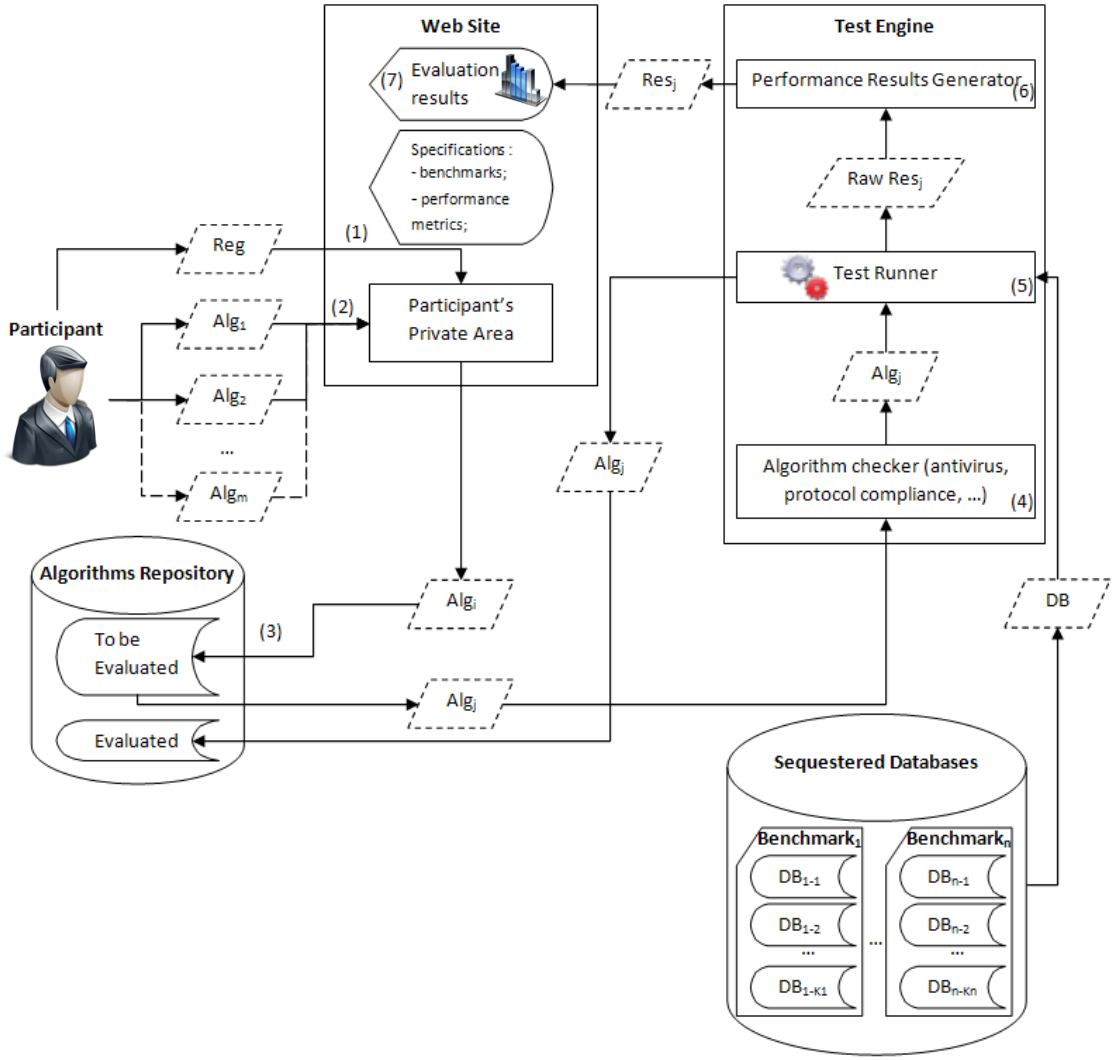


Figure 4.15 - The diagram shows the architecture of the FVC-onGoing evaluation framework and an example of a typical workflow: a given participant, after registering to the Web Site (1), submits some algorithms (2) to one or more of the available benchmarks; the algorithms (binary executable programs compliant to a given protocol) are stored in a specific repository (3). Each algorithm is evaluated by the Test Engine that, after some preliminary checks (4), executes it on the dataset of the corresponding benchmark (5) and processes its outputs (e.g. matching scores) to generate (6) all the results (e.g. EER, score graphs, …), which are finally published (7) on the Web Site.

CONCLUSIONS

In this work, various problems of fingerprint-based biometric systems have been analyzed and original solutions to some fundamental problems have been provided. In particular, the following topics have been addressed: i) definition of new specifications to certify the quality of fingerprint acquisition devices, ii) study and development of a new recognition algorithm, based on minutiae local structures, able to efficiently run even on light architectures (e.g. smartcards, embedded systems) and iii) performance evaluation of fingerprint recognition systems and their individual components.

The quality of the acquisition device can have a large impact on the accuracy of the whole recognition system. This mean, that a low-quality sensor could, on one hand, heavily affect the performance and the reliability, on the other, cause low interoperability between different fingerprint-recognition systems. For these reasons the work in this thesis started by studying the specifications and the standards, at the state-of-the-art, used to certify the quality of fingerprint acquisition devices. Then, a well-defined testing protocol to evaluate the real effect of these specifications on the accuracy of a generic fingerprint-recognition system has been defined. Successively, extensive experiments have been carried out following a well-defined protocol and, thanks to the obtained results, three new specifications, with a better cost/performance trade-off, have been defined.

It is well-known that, to improve the global reliability of these systems, the recognition algorithms, being the "core" of any biometric system, hold a primary role. Recently, the growing demand for personal privacy and security against external attacks has increased the interest of the scientific community in developing new algorithms that could be used even on secure platforms such as smartcards or systems-on-a-chip. For these reasons, after studying the state-of-the-art of fingerprint recognition algorithms, a novel approach that uses an innovative 3D cylindrical representation of the neighborhood of

each minutia has been developed. Thanks to the cylinder invariance, fixed-length, bit-oriented coding and to the local similarity measure used, the new approach met all the design goals. Its performance has been measured on a reference benchmark and compared with three among the best techniques at the state-of-the-art, with extremely good results.

Finally, part of the work has been devoted to two international competitions to evaluate the performance of fingerprint recognition algorithms: *FVC2006* and *FVC-onGoing*. Thanks to these competitions, it is possible on the one hand to track the state-of-the-art of this type of algorithms and of their components; on the other, to offer to the scientific community new reference benchmarks and well-defined testing protocols.

The interesting results obtained in this work lay the foundations for new important developments. Concerning the new recognition algorithm, future research will be mainly targeted towards new approaches for *fingerprint indexing* and *template protection*. This because the 3D representation of the local structures (fixed-length and bit-oriented coding) seems very well-suited to be combined with such techniques. The new specifications to certify the quality of fingerprint acquisition devices will be promoted in the scientific and industrial community, since they are well-defined and can aim at becoming a standard in the field. Moreover, a new software tool able to measure the characteristics of a given scanner and evaluate its compliance to the specification requirements will be developed. As to the international competition *FVC-onGoing*, a beta testing phase is being carried out with some invited participants and the official starting is planned to be held in conjunction with the *3rd International Conference on Biometrics*.

INDEX OF FIGURES

Indices of Figures

Indices of Figures

Indices of Figures

INDEX OF TABLES

Index of Tables

BIBLIOGRAPHY

[1] A. Alessandroni, R. Cappelli, M. Ferrara, and D. Maltoni, "Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality," in *Proceedings European Workshop on Biometrics and Identity Management (BIOID 2008)*, Roskilde, Denmark, 2008, pp. 29-35.

[2] R. Cappelli, M. Ferrara, and D. Maltoni, "On the Operational Quality of Fingerprint Scanners," *Information Forensics and Security, IEEE Transactions on*, vol. 3, pp. 192--202, 2008.

[3] R. Cappelli, M. Ferrara, and D. Maltoni, "The Quality of Fingerprint Scanners and Its Impact on the Accuracy of Fingerprint Recognition Algorithms," *Lecture Notes in Computer Science*, vol. 4105, pp. 10-16, 2006.

[4] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technology Today*, vol. 15, no. 7-8, pp. 7-9, August 2007.

[5] R. Cappelli et al., "Report describing FVC 2006 technology evaluation," BioSecure Deliverable D2.1.3, 2007.

[6] M. Ferrara, A. Franco, and D. Maltoni, "Estimating Image Focusing in Fingerprint Scanners," in *proceedings Workshop on Automatic Identification Advances Technologies (AutoID07)*, Alghero, Italy, 2007, pp. 30-34.

[7] M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint scanner focusing estimation by Top Sharpening Index," in *proceedings 14th International Conference on Image Analysis and Processing (ICIAP07)*, Modena, Italy, 2007, pp. 223-228.

[8] B. Dorizzi et al., "Fingerprint and On-line signature Verification Competitions at ICB 2009," in *Proceedings 3rd IAPR/IEEE International Conference on Biometrics (ICB09)*, Alghero, 2009.

[9] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*.: Springer, 2008.

[10] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed.: Springer-Verlag New York, NJ, USA, 2009.

[11] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance Evaluation of Fingerprint Verification Systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 3-18, 2006.

[12] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*.: Kluwer Academic Publishers, 1999.

Bibliography

[13] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, pp. 4--20, 2004.

[14] A. K. Jain, S. Prabhakar, and S. Pankanti, "On the similarity of identical twin fingerprints," *Pattern Recognition*, vol. 35, pp. 2653--2663, 2002.

[15] J. Wayman, A. K. Jain, D. Maltoni, and D. Maio, *Biometric systems*.: Springer, 2005.

[16] (2009, March) US-VISIT Program Web Site. [Online]. http://www.dhs.gov/us-visit

[17] NIST. (2009, March) PIV Program web site. [Online]. http://csrc.nist.gov/piv-program

[18] Council of EU, 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, December 29, 2004, Official Journal of the EU.

[19] (2008, February) GMPC Project Web Site. [Online]. http://www.jpn.gov.my/kppk1/Index2.htm

[20] (2008, February) Singapore Biometric Passport Web Site. [Online]. http://app.ica.gov.sg

[21] Department of Justice, F.B.I., "Electronic Fingerprint Transmission Specification," *CJIS-RS-0010 (V7)*, January 1999.

[22] F.B.I., CJIS Division, Image Quality Specifications for Single Finger Capture Devices, July 2006, version 071006; download at: http://www.fbi.gov/hq/cjisd/iafis/piv/pivspec.pdf, March 2009.

[23] BSI, Quality requirements for the acquisition and transmission of fingerprint image data as biometric feature for electronic identification documents, March 2009, available online at: http://www.bsi.de/english/publications/techguidelines/tr03104.

[24] R. D. Forkert, G. T. Kearnan, N. B. Nill, and P. N. Topiwala, Test Procedures for Verifying IAFIS Scanner Image Quality Requirements, November 1994, MITRE document number MP 94B0000039R1.

[25] N. B. Nil, Test Procedures for Verifying IAFIS Image Quality Requirements for Fingerprint Scanners and Printers, April 2005, MITRE Technical Report MTR 05B0000016.

[26] N. B. Nill, Test Procedures for Verifying Image Quality Requirements for Personal Identity Verification (PIV) Single Finger Capture Devices, December 2006, MITRE Technical Report MTR 060170.

[27] 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, pp. 402-412, 2002.

[28] BioLab. (2009, March) FVC2006 Web Site. [Online]. http://bias.csr.unibo.it/fvc2006

[29] O. Sanchez, "BioSec: a European project," *Biometric Technology Today*, vol. 13, no. 6, June 2005.

[30] J. Fierrez, J. Ortega-Garcia, D. T. Toledano, and J. Gonzalez-Rodriguez, "Biosec baseline corpus: A multimodal biometric database," *Pattern Recognition*, vol. 40, no. 4, pp. 1389-1392, April 2007.

[31] C. C. Slama, C. Theurer, and S. W. Henriksen, *Manual of photogrammetry*, 4th ed. Falls Church, VA: American Society of Photogrammetry, 1980.

[32] G. Vass and T. Perlaki, "Applying and removing lens distortion in post production," in *The Second Hungarian Conference on Computer Graphics and Geometry*, Budapest, 2003.

[33] S. Butterworth, ", On the theory of filter amplifiers," *Wireless Engineer*, vol. 7, pp. 536-541, October 1930.

[34] P. Heckbert, "Color image quantization for frame buffer display," *ACM SIGGRAPH Computer Graphics*, vol. 16, pp. 297-307, 1982.

[35] (2009, March) SWGFAST, Scientific Working Group on Friction Ridge Analysis, Study and Technology. [Online]. http://www.swgfast.org

[36] (2009, March) CNIPA Web Site. [Online]. http://www.cnipa.gov.it/site/it-IT/

[37] N. B. Nill and B. H. Bouzas, "Objective Image Quality Measure Derived from Digital Image Power Spectra," *Optical Engineering*, vol. 31, no. 4, pp. 813-825, 1992.

[38] X. Zhang et al., "A signal processing system on chip for digital cameras," *IEEE Annual Conference on Industrial Electronics Society*, vol. 2, pp. 1243-1248, 2000.

[39] S. W. Smith, *The scientist and engineer's guide to digital signal processing*, 2nd ed. San Diego, California, CA, USA: California Technical Publishing, 2003.

[40] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A Real-Time Matching System for Large Fingerprint Databases," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, pp. 799-813, 1996.

[41] S. H. Chang, F. H. Cheng, W. H. Hsu, and G. Z. Wu, "Fast algorithm for point pattern matching: Invariant to translations, rotations and scale changes," *Pattern Recognition*, vol. 30, pp. 311-320, 1997.

[42] A. K. Hrechak and J. A. McHugh, "Automated fingerprint recognition using structural matching," *Pattern Recognition*, vol. 23, pp. 893-904, 1990.

[43] A. J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips," *Pattern Recognition*, vol. 34, pp. 255-270, 2001.

[44] X. Jiang and W. Y. Yau, "Fingerprint Minutiae Matching Based on the Local and Global Structures," *Pattern Recognition, International Conference on*, vol. 2, p. 6038, 2000.

[45] N. K. Ratha, V. D. Pandit, R. M. Bolle, and V. Vaish, "Robust Fingerprint Authentication Using Local Structural Similarity," *Applications of Computer Vision, IEEE Workshop on*, p. 29, 2000.

[46] T. Y. Jea and V. Govindaraju, "A minutia-based partial fingerprint recognition system," *Pattern Recognition*, vol. 38, pp. 1672-1684, 2005.

[47] S. Chikkerur, A. N. Cartwright, and V. Govindaraju, "K-plet and Coupled BFS: A Graph Based Fingerprint Representation and Matching Algorithm," *Lecture Notes in Computer Science*, vol. 3832, p. 309, 2006.

[48] D. Kwon, I. D. Yun, D. H. Kim, and S. U. Lee, "Fingerprint Matching Method Using Minutiae Clustering and Warping," , vol. 4.

[49] H. Chen, J. Tian, and X. Yang, "Fingerprint Matching with Registration Pattern Inspection," *Lecture Notes in Computer Science*, pp. 327-334, 2003.

[50] J. Feng, "Combining minutiae descriptors for fingerprint matching," *Pattern Recognition*, vol. 41, pp. 342 - 352, 2008.

[51] X. Tan and B. Bhanu, "A robust two step approach for fingerprint identification," *Pattern Recognition Letters*, vol. 24, pp. 2127-2134, 2003.

[52] G. Parziale and A. Niel, "A Fingerprint Matching Using Minutiae Triangulation," *Lecture Notes in Computer Science*, pp. 241-248, 2004.

[53] X. Chen, J. Tian, J. Yang, and Y. Zhang, "An algorithm for distorted fingerprint matching based on local triangle feature set," *IEEE Transactions on Information Forensics and Security*, vol. 1, pp. 169-177, 2006.

Bibliography

[54] D. Q. Zhao, F. Su, and A. Cai, "Fingerprint Registration Using Minutia Clusters and Centroid Structure," , 2006, pp. 413-416.

[55] W. Xu, X. Chen, and J. Feng, "A Robust Fingerprint Matching Approach: Growing and Fusing of Local Structures," *Lecture Notes in Computer Science*, vol. 4642, p. 134, 2007.

[56] X. Linag, A. Bishnu, and T. Asano, "A Robust Fingerprint Indexing Scheme Using Minutia Neighborhood Structure and Low-Order Delaunay Triangles," *Information Forensics and Security, IEEE Transactions on*, vol. 2, pp. 721-733, 2007.

[57] M. Tico and P. Kuosmanen, "Fingerprint Matching Using an Orientation-Based Minutia Descriptor," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1009-1014, 2003.

[58] J. Qi and Y. Wang, "A robust fingerprint matching method," *Pattern Recognition*, vol. 38, pp. 1665-1671, 2005.

[59] E. Zhu, J. Yin, and G. Zhang, "Fingerprint matching based on global alignment of multiple reference minutiae," *Pattern Recognition*, vol. 38, pp. 1685-1694, 2005.

[60] X. Wang, J. Li, and Y. Niu, "Fingerprint matching using OrientationCodes and PolyLines," *Pattern Recognition*, vol. 40, pp. 3164-3177, 2007.

[61] Y. He, J. Tian, L. Li, H. Chen, and X. Yang, "Fingerprint Matching Based on Global Comprehensive Similarity," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 850-862, 2006.

[62] X. He, J. Tian, L. Li, Y. He, and X. Yang, "Modeling and Analysis of Local Comprehensive Minutia Relation for Fingerprint Matching," *Systems, Man and Cybernetics, Part B, IEEE Transactions on*, vol. 37, pp. 1204-1211, 2007.

[63] H. Wei, M. Guo, and Z. Ou, "Fingerprint Verification Based on Multistage Minutiae Matching," , 2006, pp. 1058-1061.

[64] G. S. Ng, X. Tong, X. Tang, and D. Shi, "Adjacent Orientation Vector Based Fingerprint Minutiae Matching System," , 2004, pp. 528-531.

[65] X. Tong, J. Huang, X. Tang, and D. Shi, "Fingerprint minutiae matching using the adjacent feature vector," *Pattern Recognition Letters*, vol. 26, pp. 1337-1345, 2005.

[66] L. Sha, F. Zhao, and X. Tang, "Minutiae-based Fingerprint Matching Using Subset Combination," , 2006, pp. 566-569.

[67] J. Feng, Z. Ouyang, and A. Cai, "Fingerprint matching using ridges," *Pattern Recognition*, vol. 39, pp. 2131-2140, 2006.

[68] Y. Zhang, X. Yang, Q. Su, and J. Tian, "Fingerprint Recognition Based on Combined Features," *Lecture Notes in Computer Science*, vol. 4642, p. 281, 2007.

[69] D. Lee, K. Choi, and J. Kim, "A Robust Fingerprint Matching Algorithm Using Local Alignment," , vol. 16, 2002, pp. 803-806.

[70] L. Sha and X. Tang, "Orientation-improved minutiae for fingerprint matching," , vol. 4, 2004, pp. 432-435.

[71] Y. Feng, J. Feng, X. Chen, and Z. Song, "A Novel Fingerprint Matching Scheme Based on Local Structure Compatibility," , 2006, pp. 374-377.

[72] "Data Format for the Interchange of Extended Fingerprint and Palmprint Features - Addendum to ANSI/NIST-ITL 1-2007," *ANSI/NIST, Working Draft 0.2*, 2008.

[73] ISO/IEC 19794-2:2005, Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data, 2005.

[74] "INCITS 378-2004 - Finger Minutiae Format for Data Interchange," *ANSI/INCITS standard*, 2004.

[75] P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan, "MINEX II: Performance of Fingerprint Match-on-Card Algorithms," techreport 2007.

[76] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, vol. 8, 2008.

[77] A. Jules and M. Sudan, "A Fuzzy Vault Scheme," in *Int. Symp. on Information Theory*, 2002.

[78] U. Uludag and A. K. Jain, "Fuzzy fingerprint vault," in *Workshop on Biometrics: Challenges Arising from Theory to Practice*, 2004, pp. 13-16.

[79] U. Uludag and A. K. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Computer Vision and Pattern Recognition Workshop*, 2006, pp. 163-171.

[80] J. Jeffers and A. Arakala, "Minutiae-Based Structures for A Fuzzy Vault," in *Biometric Consortium Conference*, 2006, pp. 1-6.

[81] J. Jeffers and A. Arakala, "Fingerprint Alignment for A Minutiae-Based Fuzzy Vault," in *Biometrics Symposium*, 2007, pp. 1-6.

[82] F. P. Preparata and M. I. Shamos, *Computational Geometry: An Introduction*.: Springer, 1985.

[83] H. W. Kuhn, "The Hungarian Method for the assignment problem," *Naval Research Logistics Quarterly*, vol. 2, pp. 83-97, 1955.

[84] A. Rosenfeld, R. A. Hummel, and S. W. Zucker, "Scene Labeling by Relaxation Operations," *Systems, Man and Cybernetics, IEEE Transactions on*, vol. 6, pp. 420-433, 1976.

[85] BioLab. (2009, March) FVC2006 web site. [Online]. http://bias.csr.unibo.it/fvc2006

[86] Wikipedia. (2009, March) Rar file format. [Online]. http://en.wikipedia.org/wiki/Rar

[87] Wikipedia. (2009, March) Zip file format. [Online]. http://en.wikipedia.org/wiki/ZIP_(file_format)

[88] 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, pp. 402-412, 2002.

[89] C. Wilson et al., "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report," National Institute of Standards and Technology, web site: http://fpvte.nist.gov., NISTIR 7123, 2004.

[90] C. Watson et al., "Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers," National Institute of Standards and Technology, NISTIR 7221, 2005.

[91] P. Grother et al., "MINEX, Performance and Interoperability of the INCITS 378 Fingerprint Template," National Institute of Standards and Technology, NISTIR 7296, 2006.

[92] A. Martin, M. Przybocki, and J. Campbell, "The NIST Speaker Recognition Evaluation Program," in *Biometric Systems Technology, Design and Performance Evaluation*. London: Springer-Verlag, 2004.

[93] NIST. (2009, January) Speaker Recognition Evaluation web site. [Online]. http://www.nist.gov/speech/tests/spk/index.htm

[94] P. J. Philips et al., "Facial Recognition Vendor Test 2002 Evaluation Report," FRVT2002 web site: http://www.frvt.org/FRVT2002., 2003.

Bibliography

[95] P. J. Philips, A. Martin, C. L. Wilson, and M, Przybocki, "An Introduction to Evaluating Biometric Systems," *IEEE Computer Magazine*, February 2000.

[96] UK Government's Biometrics Working Group, "Best Practices in Testing and Reporting Performance of Biometric Devices," v2.01, 2002.

[97] J. Matas et al., "Comparison of Face Verification Results on the XM2VTS Database," in *Proceedings of 15th International Conference on Pattern Recognition*, vol. 4, Barcelona, 2000, pp. 858-863.

[98] K. Messer et al., "Face Authentication Competition on the BANCA Database," in *Proceedings International Conference on Biometric Authentication (ICBA04)*, Hong Kong, 2004, pp. 8-15.

[99] P. J. Philips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090-1104, October 2000.

[100] D. M. Blackburn, J. M. Bone, and P.J. Philips, "Facial Recognition Vendor Test 2000 Evaluation Report," FRVT2000 web site: http://www.frvt.org/FRVT2000, 2001.

[101] A. K. Jain and A. Ross, "Fingerprint Mosaicking," in *Proceedings International Conference on Acoustic Speech and Signal Processing*, vol. 4, 2002, pp. 4064-4067.

[102] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second Fingerprint Verification Competition," in *Proceedings 16th International Conference on Pattern Recognition (ICPR2002)*, vol. 3, Québec City, 2002, pp. 811-814.

[103] Y. Dit-Yan et al., "SVC2004: First International Signature Verification Competition", in proceedings International Conference on Biometric Authentication (ICBA04)," , Hong Kong, 2004, pp. 16-22.

[104] BioLab. (2009, BioLab) FVC-onGoing web site. [Online]. http://bias.csr.unibo.it/fvcongoing

[105] BioLab. (2009, March) FVC2000 web site. [Online]. http://bias.csr.unibo.it/fvc2000

[106] BioLab. (2009, March) FVC2002 web site. [Online]. http://bias.csr.unibo.it/fvc2002

[107] BioLab. (2009, March) FVC2004 web site. [Online]. http://bias.csr.unibo.it/fvc2004

[108] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition", in proceedings International Conference on Biometric Authentication (ICBA04)," , Hong Kong, 2004, pp. 1-7.

[109] R. Cappelli, A. Erol, D. Maio, and D. Maltoni, "Synthetic Fingerprint-image Generation," in *Proceedings 15th International Conference on Pattern Recognition (ICPR2000)*, Barcelona, 2000, pp. 475-478.

[110] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic Fingerprint-Database Generation," in *Proceedings 16th International Conference on Pattern Recognition (ICPR2002)*, vol. 3, Québec City, 2002, pp. 744-747.

[111] Vision Lab. (2009, March) ICB09 web site. [Online]. http://icb09.uniss.it/