# Chapter 4
# Fingerprint Recognition

Fernando Alonso-Fernandez, (in alphabetical order) Josef Bigun, Julian Fierrez, Hartwig Fronthaler, Klaus Kollreider, and Javier Ortega-Garcia

**Abstract** First, an overview of the state of the art in fingerprint recognition is presented, including current issues and challenges. Fingerprint databases and evaluation campaigns, are also summarized. This is followed by the description of the BioSecure Benchmarking Framework for Fingerprints, using the NIST Fingerpint Image Software (NFIS2), the publicly available MCYT-100 database, and two evaluation protocols.

Two research systems are compared within the proposed framework. The evaluated systems follow different approaches for fingerprint processing and are discussed in detail. Fusion experiments involving different combinations of the presented systems are also given. The NFIS2 software is also used to obtain the fingerprint scores for the multimodal experiments conducted within the BioSecure Multimodal Evaluation Campaign (BMEC'2007) reported in Chap. 11.

## 4.1 Introduction

Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions. Among the most remarkable strengths of fingerprint recognition, we can mention the following:

- Its maturity, providing a high level of recognition accuracy.
- The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc.
- The use of easy-to-use, ergonomic devices, not requiring complex user-system interaction.

On the other hand, a number of weaknesses may influence the effectiveness of fingerprint recognition in certain cases:

D. Petrovska-Delacrétaz et al. (eds.), *Guide to Biometric Reference Systems and Performance Evaluation*, DOI 10.1007/978-1-84800-292-0_4,

- Its association with forensic or criminal applications.
- Factors such as finger injuries or manual working, can result in certain users being unable to use a fingerprint-based recognition system, either temporarily or permanently.
- Small-area sensors embedded in portable devices may result in less information available from a fingerprint and/or little overlap between different acquisitions.

In this chapter, we report experiments carried out using the BioSecure Reference Evaluation Framework for Fingerprints. It is composed of the minutiae-based NIST Fingerprint Image Software (NFIS2) [83], the publicly available MCYT-100 database (described in [70], and available at [64]) and two benchmarking protocols. The benchmarking experiments (one with the optical sensor and the other one with the capacitive sensor) can be easily reproduced, following the How-to documents provided on the companion website [16]. In such a way they could serve as further comparison points for newly proposed biometric systems.

As highlighted in Chap. 2, the comparison points are multiple, and are dependent of what the researchers want to study and what they have at their disposal. The points of comparisons that are illustrated in this book regarding the fingerprint experiments are the following:

- One comparison point could be obtained if the same system (NFIS2 software in this case) is applied to a different database. In such a way the performances of this software could be compared within the two databases. The results of such a comparison are reported in Chap. 11, where the NFIS2 software is applied on fingerprint data from the BioSecure Multimodal Evaluation Campaign.
- Yet another comparison could be done that is related to comparing different systems on the same database and same protocols. In such a way, the advantages of the proposed systems could be pinpointed. Furthermore if error analysis and/or fusion experiments are done the complementarities of the proposed systems could be studied, allowing further design of new, more powerful systems. In this chapter, two research fingerprint verification systems, one minutiae-based and the other ridge-based, are compared to the benchmarking system. The three systems tested include different approaches for feature extraction, fingerprint alignment and fingerprint matching. Fusion experiments using standard fusion approaches are also reported.

This chapter is structured as follows. Section 4.2 continues with a review of the state of the art, including current issues and challenges in fingerprint recognition. Sections 4.3 and 4.4 summarize existing fingerprint databases and evaluation campaigns, respectively. Section 4.5 introduces the benchmarking framework (open-source algorithms, database and testing protocols). In Sect. 4.6, two research systems are described. Experimental results within the benchmarking framework are given in Sect. 4.7, including evaluation of the individual systems and fusion experiments. Conclusions are finally drawn in Sect. 4.8.

## 4.2 State of the Art in Fingerprint Recognition

This section provides a basic introduction to fingerprint recognition systems and their main parts, including a brief description of the most widely used techniques and algorithms. A number of additional issues that are not in the scope of this book can be found in [59].

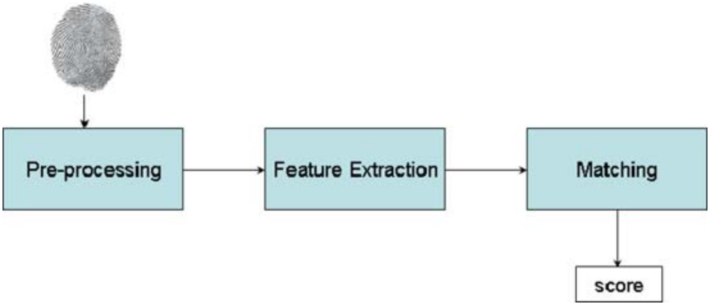


**Fig. 4.1** Main modules of a fingerprint verification system

The main modules of a fingerprint verification system (cf. Fig. 4.1) are: *a*) *fingerprint sensing*, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation; *b*) *preprocessing*, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; *c*) *feature extraction*, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and *d*) *matching*, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

### *4.2.1 Fingerprint Sensing*

The acquisition of fingerprint images has been historically carried out by spreading the finger with ink and pressing it against a paper card. The paper card is then scanned, resulting in a digital representation. This process is known as *off-line* acquisition and is still used in law enforcement applications. Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as *online* acquisition. There are three families of electronic fingerprint sensors based on the sensing technology [59]:

- *Solid-state* or silicon sensors (left part of Fig. 4.2): These consist of an array of pixels, each pixel being a sensor itself. Users place the finger on the surface

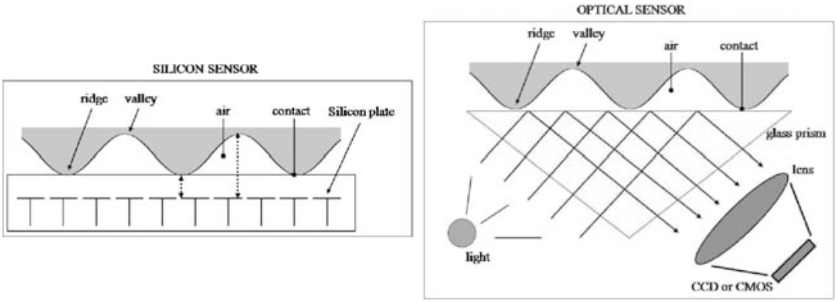


**Fig. 4.2** Acquisition principles of silicon and optical sensors

of the silicon, and four techniques are typically used to convert the ridge/valley information into an electrical signal: capacitive, thermal, electric field and piezoelectric. Since solid-state sensors do not use optical components, their size is considerably smaller and can be easily embedded. On the other hand, silicon sensors are expensive, so the sensing area of solid-state sensors is typically small.

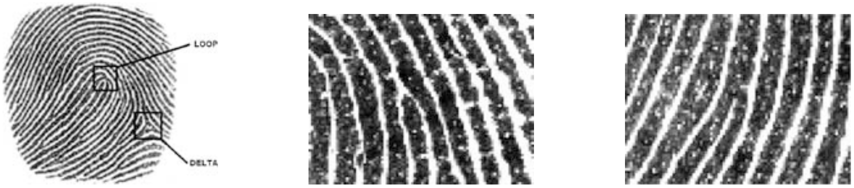
- *Optical* (right part of Fig. 4.2): The finger touches a glass prism and the prism is illuminated with diffused light. The light is reflected at the valleys and absorbed at the ridges. The reflected light is focused onto a CCD or CMOS sensor. Optical fingerprint sensors provide good image quality and large sensing area but they cannot be miniaturized because as the distance between the prism and the image sensor is reduced, more optical distortion is introduced in the acquired image.
- *Ultrasound*: Acoustic signals are sent, capturing the echo signals that are reflected at the fingerprint surface. Acoustic signals are able to cross dirt and oil that may be present in the finger, thus giving good quality images. On the other hand, ultrasound scanners are large and expensive, and take some seconds to acquire an image.

A new generation of touchless live scan devices that generate a 3D representation of fingerprints is appearing [22]. Several images of the finger are acquired from different views using a multicamera system, and a contact-free 3D representation of the fingerprint is constructed. This new sensing technology overcomes some of the problems that intrinsically appear in contact-based sensors such as improper finger placement, skin deformation, sensor noise or dirt.

### *4.2.2 Preprocessing and Feature Extraction*

A fingerprint is composed of a pattern of interleaved *ridges* and *valleys*. They smoothly flow in parallel and sometimes terminate or bifurcate. At a global level, this pattern sometimes exhibits a number of particular shapes called *singularities*, which can be classified into three types: *loop*, *delta* and *whorl*. In Fig. 4.3 a, we can see an example of loop and delta singularities (the whorl singularity can be defined as two opposing loops). At the local level, the ridges and valleys pattern can exhibit a particular shape called *minutia*. There are several types of minutiae, but for practical reasons, only two types of minutiae are considered: ridge ending (Fig. 4.3 b) and ridge bifurcation (Fig. 4.3 c).

Singularities at the global level are commonly used for fingerprint classification, which simplifies search and retrieval across a large database of fingerprint images. Based on the number and structure of loops and deltas, several classes are defined, as shown in Fig. 4.4.



(a) (b) (c)

**Fig. 4.3** Fingerprint singularities: (a) loop and delta singularities, (b) ridge ending, and (c) ridge bifurcation

The gray scale representation of a fingerprint image is known to be unstable for fingerprint recognition [59]. Although there are fingerprint matching techniques that directly compare gray images using correlation-based methods, most of the fingerprint matching algorithms use features which are extracted from the gray scale image. To make this extraction easy and reliable, a set of preprocessing steps is commonly performed: computation of local ridge frequency and local ridge orientation, enhancement of the fingerprint image, segmentation of the fingerprint area from the background, and detection of singularities.

The local ridge orientation at a pixel level is defined as the angle that the fingerprint ridges form with the horizontal axis [59]. Most of the algorithms do not compute the local ridge orientation at each pixel, but over a square-meshed grid (Fig. 4.5). The simplest approach for local ridge orientation estimation is based on the gray scale gradient. Since the gradient phase angle denotes the direction of the maximum pixel-intensity change, the ridge orientation is orthogonal to this phase angle. There are essentially two orientation estimation techniques: direction tensor sampling [13] and spectral tensor discretization [50] using Gabor filters. For its computational efficiency the method independently suggested by [13] is the most commonly used in fingerprint applications because the spectral approach needs more filtering. We refer to [12] for a detailed treatment of both approaches.

The local ridge frequency at a pixel level is defined as the number of ridges per unit length along a hypothetical segment centered at this pixel and orthogonal to the local ridge orientation [59]. As in the case of the local ridge orientation, the local ridge frequency is computed over a square-meshed grid. Existing methods [39, 56, 52] usually model the ridge-valley structure as a sinusoidal-shaped wave (Fig. 4.6), where the ridge frequency is set as the frequency of this sinusoid, and the orientation is used to angle the wave.

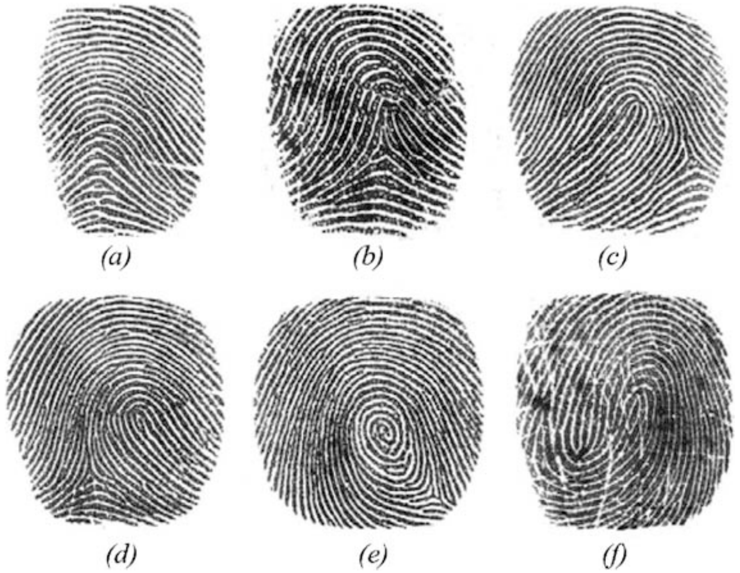


**Fig. 4.4** The six major fingerprint classes: (a) arch, (b) tented arch, (c) left loop, (d) right loop, (e) whorl, and (f) twin-loop

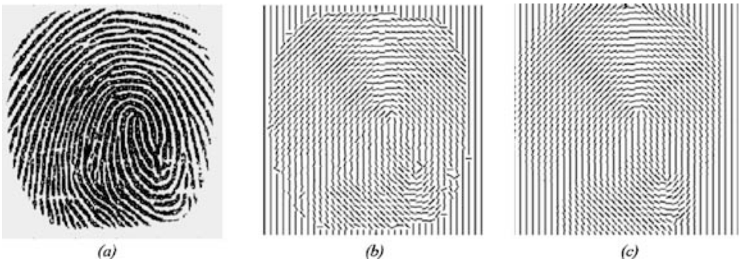


**Fig. 4.5** Local ridge orientation of a fingerprint image computed over a square-meshed grid: (a) original image, (b) orientation image, and (c) smoothed orientation image. Each element of (b) and (c) denotes the local orientation of the ridges

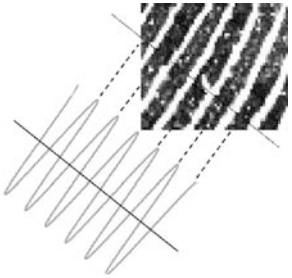


**Fig. 4.6** Modeling of ridges and valleys as a sinusoidal-shaped wave

Ideally, in a fingerprint image, ridges and valleys flow smoothly in a locally constant direction. In practice, however, there are factors that affect the quality of a fingerprint image (cf., Fig. 4.7): wetness or dryness of the skin, noise of the sensor, temporary or permanent cuts and bruises in the skin, variability in the pressure against the sensor, etc. Several enhancement algorithms have been proposed in the literature with the aim of improving the clarity of ridges and valleys. The most widely used fingerprint enhancement techniques use *contextual filters*, which means changing the filter parameters according to the local characteristics (context) of the image. Filters are tuned to the local ridge orientation and/or frequency, thus removing the imperfections and preserving ridges and valleys (cf. Fig. 4.8).

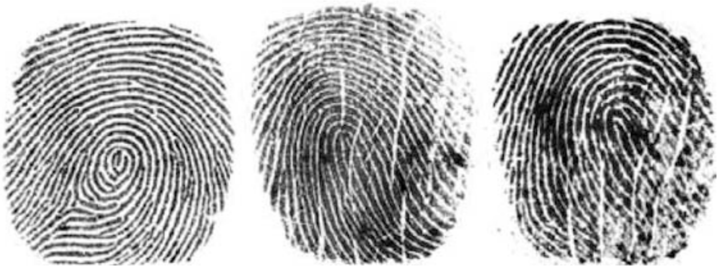


**Fig. 4.7** Fingerprint images with different quality. From left to right: high, medium and low quality, respectively

Fingerprint segmentation consists of the separation of the fingerprint area (foreground) from the background [59]. This is useful to avoid subsequent extraction of fingerprint features in the background, which is the noisy area. Global and local thresholding segmentation methods are not very effective, and more robust segmentation techniques are commonly used [65, 44, 55, 9, 79, 67]. These techniques exploit the existence of an oriented periodical pattern in the foreground and a nonoriented isotropic pattern in the background (Fig. 4.9).

As mentioned above, the pattern of ridges and valleys exhibits a number of particular shapes called *singularities* (Fig. 4.3 a). For the detection of singularities, most of the existing algorithms rely on the ridge orientation information (Fig. 4.5). The best-known algorithm for singularity detection is based on the *Poincaré* index [48, 47, 10]. Alternatively, detection of core and delta type singularities was shown to be efficient and precise using different filtering techniques.

Once the fingerprint image has been preprocessed, a feature extraction step is performed. Most of the existing fingerprint recognition systems are based on minutiae matching, so that reliable minutiae extraction is needed. Usually, the preprocessed fingerprint image is converted into a binary image, which is then thinned using morphology (Fig. 4.10). The thinning step reduces the ridge thickness to one pixel, allowing straightforward minutiae detection. During the thinning step, a number of spurious imperfections may appear (Fig. 4.11 a) and thus, a postprocessing step is sometimes performed (Fig. 4.11 b) in order to remove the imperfections from

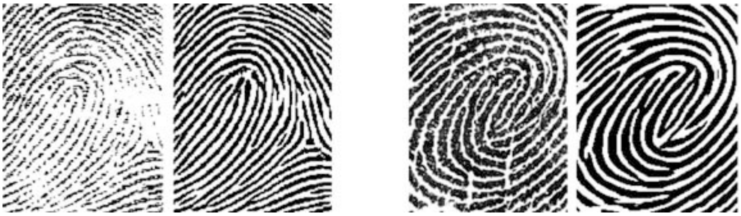


**Fig. 4.8** Examples of original and enhanced fingerprint images

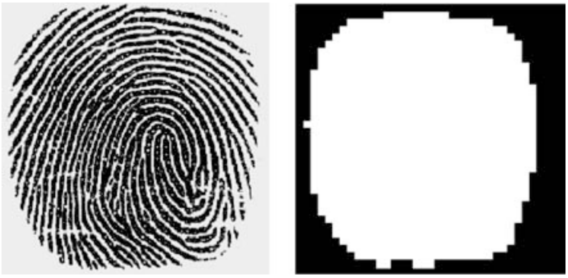


**Fig. 4.9** Segmentation of fingerprint images: (**left**) original image and (**right**) segmentation mask

the thinned image. Several approaches for binarization, thinning and minutiae detection have been proposed in literature [59]. However, binarization and thinning suffer from several problems: $a)$ spurious imperfections; $b)$ loss of structural information; $c)$ computational cost; and $d)$ lack of robustness in low quality fingerprint images. Because of that, other approaches that extract minutiae directly from the gray scale image have been also proposed [53, 55, 54, 46, 20, 17, 31].

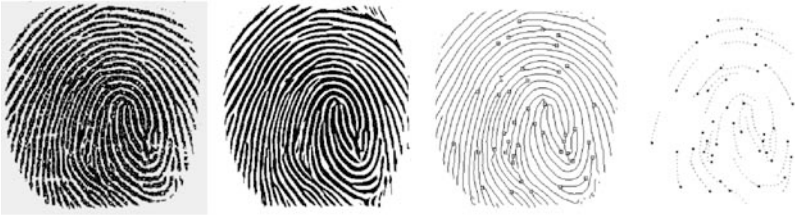


**Fig. 4.10** Binarization and thinning of fingerprint images using contextual filters

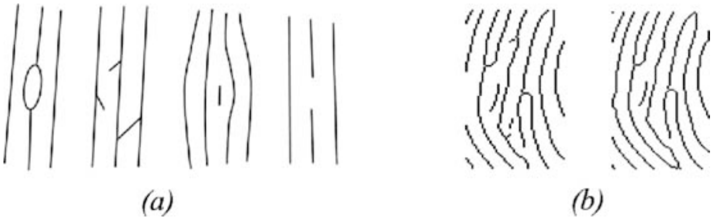


**Fig. 4.11** Thinning step: (a) typical imperfections appeared during the thinning step, and (b) a thinned fingerprint structure before and after removing imperfections

### *4.2.3 Fingerprint Matching*

In the matching step, features extracted from the input fingerprint are compared against those in a template, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images (or subimages) using correlation-based methods, so that the fingerprint template coincides with the gray scale image. However, most of the fingerprint matching algorithms use features that are extracted from the gray scale image (see Sect. 4.2.2).

One of the biggest challenges of fingerprint recognition is the high variability commonly found between different impressions of the same finger. This variability is known as *intraclass* variability and is caused by several factors, including: $a)$ displacement or rotation between different acquisitions; $b)$ partial overlap, specially in sensors of small area; $c)$ skin conditions, due to permanent or temporary factors (cuts, dirt, humidity, etc.); $d)$ noise in the sensor (for example, residues from previous acquisitions); and $e)$ nonlinear distortion due to skin plasticity and differences in pressure against the sensor. Fingerprint matching remains as a challenging pattern recognition problem due to the difficulty in matching fingerprints affected by one or several of the mentioned factors [59].

A large number of approaches to fingerprint matching can be found in literature. They can be classified into: $a)$ correlation-based approaches, $b)$ minutiae-based approaches, and $c)$ ridge feature-based approaches.

In the correlation-based approaches, the fingerprint images are superimposed and the gray scale images are directly compared using a measure of correlation. Due to nonlinear distortion, different impressions of the same finger may result in differences of the global structure, making the comparison unreliable. In addition, computing the correlation between two fingerprint images is computationally expensive. To deal with these problems, correlation can be computed only in certain local regions of the image, which can be selected following several criteria. Also, to speed up the process, correlation can be computed in the Fourier domain or using heuristic approaches, which allow the number of computational operations to be reduced.

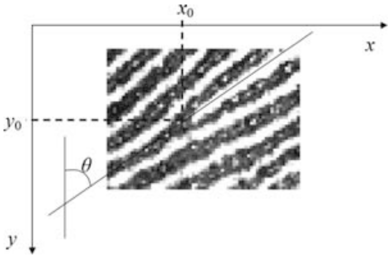


**Fig. 4.12** Minutia represented by its spatial coordinates and angle

Minutiae-based approaches are the most popular and widely used methods for fingerprint matching, since they are analogous with the way that forensic experts compare fingerprints. A fingerprint is modeled as a set of minutiae, which are usually represented by its spatial coordinates and the angle between the tangent to the ridge line at the minutiae position and the horizontal or vertical axis (Fig. 4.12). The minutiae sets of the two fingerprints to be compared are first aligned, requiring displacement and rotation to be computed (some approaches also compute scaling and other distortion-tolerant transformations). This alignment involves a minimization problem, the complexity of which can be reduced in various ways [23]. Once aligned, corresponding minutiae at similar positions in both fingerprints are looked for. A *region of tolerance* around the minutiae position is defined in order to compensate for the variations that may appear in the minutiae position due to noise and distortion. Likewise, differences in angle between corresponding minutia points are tolerated. Other approaches use *local minutia matching*, which means combining comparisons of local minutia configurations. These kind of techniques relax global spatial relationships that are highly distinctive [59] but naturally more vulnerable to nonlinear deformations. Some matching approaches combine both techniques by first carrying out a fast local matching and then, if the two fingerprints match at a local level, consolidating the matching at global level.

Unfortunately, minutiae are known to be unreliably extracted in low image quality conditions. For this and other reasons, alternative features have been proposed in the literature as an alternative to minutiae (or to be used in conjunction with minutiae) [59]. The alternative feature most widely studied for fingerprint matching is texture information. The fingerprint structure consists of periodical repetitions of a pattern of ridges and valleys that can be characterized by its local orientation, frequency, symmetry, etc. Texture information is less discriminative than minutiae, but more reliable under low quality conditions [29].

## *4.2.4 Current Issues and Challenges*

One of the open issues in fingerprint verification is the lack of robustness against image quality degradation [80, 2]. The performance of a fingerprint recognition system is heavily affected by fingerprint image quality. Several factors determine the quality of a fingerprint image: skin conditions (e.g., dryness, wetness, dirtiness, temporary or permanent cuts and bruises), sensor conditions (e.g., dirtiness, noise, size), user cooperation, etc. Some of these factors cannot be avoided and some of them vary along time. Poor quality images result in spurious and missed features, thus degrading the performance of the overall system. Therefore, it is very important for a fingerprint recognition system to estimate the quality and validity of the captured fingerprint images. We can either reject the degraded images or adjust some of the steps of the recognition system based on the estimated quality. Several algorithms for automatic fingerprint image quality assessment have been proposed in literature [2]. Also, the benefits of incorporating automatic quality measures in fingerprint verification have been shown in recent studies [28, 6, 32, 5].

A successful approach to enhance the performance of a fingerprint verification system is to combine the results of different recognition algorithms. A number of simple fusion rules and complex trained fusion rules have been proposed in literature [11, 49, 81]. Examples for combining minutia- and texture-based approaches are to be found in [75, 61, 28]. Also, a comprehensive study of the combination of different fingerprint recognition systems is done in [30]. However, it has been found that simple fusion approaches are not always outperformed by more complex fusion approaches, calling for further studies of the subject.

Another recent issue in fingerprint recognition is the use of multiple sensors, either for sensor fusion [60] or for sensor interoperability [74, 7]. Fusion of sensors offers some important potentialities [60]: *a*) the overall performance can be improved substantially, *b*) population coverage can be improved by reducing enrollment and verification failures, and *c*) it may naturally resist spoofing attempts against biometric systems. Regarding sensor interoperability, most biometric systems are designed under the assumption that the data to be compared is obtained uniquely and the same for every sensor, thus being restricted in their ability to match or compare biometric data originating from different sensors in practice. As a result, changing the sensor may affect the performance of the system. Recent progress has been made in the development of common data exchange formats to facilitate the exchange of feature sets between vendors [19]. However, little effort has been invested in the development of algorithms to alleviate the problem of sensor interoperability. Some approaches to handle this problem are given in [74], one example of which is the normalization of raw data and extracted features. As a future remark, interoperability scenarios should also be included in vendor and algorithm competitions, as done in [37].

Due to the low cost and reduced size of new fingerprint sensors, several devices in daily use already include embedded fingerprint sensors (e.g., mobile telephones, PC peripherals, PDAs, etc.) However, using small-area sensors implies having less information available from a fingerprint and little overlap between different acquisitions of the same finger, which has great impact on the performance of the recognition system [59]. Some fingerprint sensors are equipped with mechanical guides in order to constrain the finger position. Another alternative is to perform several acquisitions of a finger, gathering (partially) overlapping information during the enrollment, and reconstruct a full fingerprint image.

In spite of the numerous advantages of biometric systems, they are also vulnerable to attacks [82]. Recent studies have shown the vulnerability of fingerprint systems to fake fingerprints [35, 72, 71, 63]. Surprisingly, fake biometric input to the sensor is shown to be quite successful. Aliveness detection could be a solution and it is receiving great attention [26, 78, 8]. It has also been shown that the matching score is a valuable piece of information for the attacker [82, 73, 62]. Using the feedback provided by this score, signals in the channels of the verification system can be modified iteratively and the system is compromised in a number of iterations. A solution could be given by concealing the matching score and just releasing an acceptance/rejection decision, but this may not be suitable in certain biometric systems [82].

With the advances in fingerprint sensing technology, new high resolution sensors are able to acquire ridge pores and even perspiration activities of the pores [40, 21]. These features can provide additional discriminative information to existing fingerprint recognition systems. In addition, acquiring perspiration activities of the pores can be used to detect spoofing attacks.

## 4.3 Fingerprint Databases

Research in biometrics profoundly depends on the availability of sensed data. The growth that the field has experienced over the past two decades has led to the appearance of increasing numbers of biometric databases, either monomodal (one biometric trait sensed) or multimodal (two or more biometric traits sensed). Previous to the International Fingerprint Verification Competitions (FVC, see Sect. 4.4), the only large, publicly available datasets were the NIST databases [69]. However, these databases were not well suited for the evaluation of algorithms operating with live-scan images [59] and will not be described here. In this section, we present some of the most important publicly available biometric databases, either monomodal or multimodal, that include the fingerprint trait acquired with live-scan sensors. A summary of these databases with some additional information are shown in Table 4.1.

### *4.3.1 FVC Databases*

Four international Fingerprint Verification Competitions (FVC) were organized in 2000, 2002, 2004 and 2006 [57, 58, 18, 33], see Sect. 4.4. For each competition, four databases were acquired using three different sensors and the SFinGE synthetic generator [59]. Each database has 110 fingers (150 in FVC2006) with eight impressions per finger (twelve in FVC2006), resulting in 880 impressions (1,800 in FVC2006). In the four competitions, the SFinGe synthetic generator was tuned to simulate the main perturbations introduced in the acquisition of the three "real" databases.

In FVC2000, the acquisition conditions were different for each database (e.g., interleaving/not interleaving the acquisition of different fingers, periodical cleaning/no cleaning of the sensor). For all the databases, no care was taken to assure a minimum quality of the fingerprints; in addition, a maximum rotation and a nonnull overlapping area were assured for impressions from the same finger.

In FVC2002, the acquisition conditions were the same for each database: interleaved acquisition of different fingers to maximize differences in finger placement, no care was taken in assuring a minimum quality of the fingerprints and the sensors were not periodically cleaned. During some sessions, individuals were asked to: *a*) exaggerate displacement or rotation or, *b*) dry or moisten their fingers.

The FVC2004 databases were collected with the aim of creating a more difficult benchmark because, in FVC2002, top algorithms achieved accuracies close to 100% [18]: simply more intraclass variation was introduced. During the different sessions, individuals were asked to: *a*) put the finger at slightly different vertical position, *b*) apply low or high pressure against the sensor, *c*) exaggerate skin distortion and rotation, and *d*) dry or moisten their fingers. No care was taken to assure a minimum quality of the fingerprints and the sensors were not periodically cleaned. Also, the acquisition of different fingers were interleaved to maximize differences in finger placement.

For the 2006 edition [33], no deliberate difficulties were introduced in the acquisition as it was done in the previous editions (such as exaggerated distortion, large amounts of rotation and displacement, wet/dry impressions, etc.), but the population is more heterogeneous, including manual workers and elderly people. Also, no constraints were enforced to guarantee a minimum quality in the acquired images and the final datasets were selected from a larger database by choosing the most difficult fingers according to a quality index, to make the benchmark sufficiently difficult for an evaluation.

### 4.3.2 MCYT Bimodal Database

In the MCYT database [70], fingerprints and online signatures were acquired. The fingerprint subcorpus of this database (MCYT Fingerprint subcorpus) includes tenprint acquisition of each of the 330 subjects enrolled in the database. For each individual, 12 samples of each finger were acquired using an optical and a capacitive sensor. With the aim of including variability in fingerprint positioning on the sensor, the 12 different samples of each fingerprint were acquired under human supervision and considering three different levels of control. For this purpose, the fingerprint core had to be located inside a size-varying rectangle displayed in the acquisition software interface viewer.

### 4.3.3 BIOMET Multimodal Database

In the multimodal BIOMET database [36], the fingerprint acquisitions were done with an optical and a capacitive sensor. During the first acquisition campaign, only the optical sensor was used, whereas both the optical and capacitive sensors were employed for the second and third campaigns. The total number of available fingerprints per sensor is six for the middle and index fingers of each contributor.

### 4.3.4 Michigan State University (MSU) Database

The MSU fingerprint database [45] was acquired within the Pattern Recognition and Image Processing Laboratory (PRIP) at Michigan State University. Data was acquired from nonhabituated cooperative subjects using optical and solid-state sensors connected to IBM Thinkpads. A live feedback of the acquired image was provided and users were guided to place their fingers in the center of the sensor and in upright position. Because of that, most of the fingerprint images are centered and no significant rotation is found. Some images were acquired while the subject was removing the finger from the sensor due to time lag in providing the feedback, resulting in partial fingerprints. It was also observed that subjects had greasier fingers during and after the lunch hour, whereas drier fingers were registered in the evening compared to the morning sessions.

With the aim of studying user adaptation within the fingerprint image acquisition process, a second database using the solid-state sensor was acquired. Eight subjects were asked to choose the finger that they felt most comfortable with and then use the same finger every day to give one fingerprint image during six consecutive weeks. The subjects were cooperative but unattended.

### 4.3.5 BioSec Multimodal Database

Among the five modalities present in the BioSec Database, recorded in the framework of an Integrated Project of the 6th European Framework Programme [14], fingerprints are also present. The baseline corpus [27] comprises 200 subjects with two acquisition sessions per subject. The extended version of the BioSec database comprises 250 subjects with four sessions per subject (about one month between sessions). Fingerprint data have been acquired using three different sensors.

### *4.3.6 BiosecurID Multimodal Database*

The BiosecurID database [34] has been collected in an office-like uncontrolled environment (in order to simulate a realistic scenario). The fingerprint part comprises data from 400 subjects, with two different sensors and four sessions distributed in a four-month time span.

### *4.3.7 BioSecure Multimodal Database*

One of the main integrative efforts of the BioSecure Network of Excellence was the design and collection of a new multimodal database [4], allowing to create a common and repeatable benchmarking of algorithms. Acquisition of the BioSecure Multimodal Database has been jointly conducted by 11 European institutions participating in the BioSecure Network of Excellence [15]. Among the three different datasets that are present in this database, fingerprints are captured in the *Data Set 2 (DS2)* and *Data Set 3 (DS3)*. Pending integration, the BioSecure database has approximately 700 individuals participating in the collections of DS2 and DS3. Fingerprint data in DS2 were acquired using an optical and a capacitive sensor. Fingerprint data in DS3 were acquired with a PDA, and they are considered degraded in acquisition condition with respect to DS2, since they were acquired while subjects were standing with a PDA in the hand.

## 4.4 Fingerprint Evaluation Campaigns

The most important evaluation campaigns carried out in the fingerprint modality are the NIST Fingerprint Vendor Technology Evaluation (FpVTE2003) [84] and the four Fingerprint Verification Competitions (FVC), which took place in 2000 [57], 2002 [58], 2004 [18] and 2006 [33]. A comparative summary of FVC2004, FVC2006 and FpVTE2003 is given in Table 4.2. An important evaluation is also the NIST Minutiae Interoperability Exchange Test (MINEX) [37].

### *4.4.1 Fingerprint Verification Competitions*

The Fingerprint Verification Competitions (FVC) were organized with the aim of determining the state of the art in fingerprint verification. These competitions have received great attention from both academic and commercial organizations, and several research groups have used the FVC datasets for their own experiments later on. The number of participants and algorithms evaluated has increased in each new edition. Also, to increase the number of participants, anonymous participation was

**Table 4.1** Summary of existing databases that include the fingerprint trait (where # S. denotes number of sessions)

| Name | Type | Sensor | Image Size | Resolution | Subjects | # S. | Samples | Distributor |
|---|---|---|---|---|---|---|---|---|
| FVC2000 | monomodal | Low cost optical (KeyTronic) | 300 × 300 | 500 dpi | 110 | 2 | 880 | Univ. Bologna<br>http://biolab.csr.unibo.it |
| | | Low cost capacitive (ST Microelectronics) | 256 × 364 | 500 dpi | 110 | 2 | 880 | |
| | | Optical (Identicator technology) | 448 × 478 | 500 dpi | 110 | 2 | 880 | |
| | | Synthetic (SFinGe v2.0) | 240 × 320 | 500 dpi | 110 | 2 | 880 | |
| FVC2002 | monomodal | Optical (Identix) | 388 × 374 | 500 dpi | 110 | 3 | 880 | Univ. Bologna<br>http://biolab.csr.unibo.it |
| | | Optical (Biometrika) | 296 × 560 | 569 dpi | 110 | 3 | 880 | |
| | | Capacitive (Precise Biometrics) | 300 × 300 | 500 dpi | 110 | 3 | 880 | |
| | | Synthetic (SFinGe v2.51) | 288 × 384 | 500 dpi | 110 | 3 | 880 | |
| FVC2004 | monomodal | Optical (CrossMatch) | 640 × 480 | 500 dpi | 110 | 3 | 880 | Univ. Bologna<br>http://biolab.csr.unibo.it |
| | | Optical (Digital Persona) | 328 × 364 | 500 dpi | 110 | 3 | 880 | |
| | | Thermal sweeping (Atmel FingerChip) | 300 × 480 | 512 dpi | 110 | 3 | 880 | |
| | | Synthetic (SFinGe v3.0) | 288 × 384 | 500 dpi | 110 | 3 | 880 | |
| FVC2006 | monomodal | Capacitive (Authentec) | 96 × 96 | 250 dpi | 150 | 3 | 1800 | http://biolab.csr.unibo.it<br>http://atvs.ii.uam.es |
| | | Optical (Biometrika) | 400 × 560 | 569 dpi | 150 | 3 | 1800 | |
| | | Thermal sweeping Atmel) | 400 × 500 | 500 dpi | 150 | 3 | 1800 | |
| | | Synthetic (SFinGe v3.0) | 288 × 384 | 500 dpi | 150 | 3 | 1800 | |
| MCYT | multimodal<br>(fingerprint, signature) | Capacitive (Precise Biometrics) | 300 × 300 | 500 dpi | 330 | 1 | 39600 | ATVS (Biometric Recognition Group)<br>http://atvs.ii.uam.es |
| | | Optical (Digital Persona) | 256 × 400 | 500 dpi | 330 | 1 | 39600 | |
| BIOMET | multimodal<br>(audio, face, hand, fingerprint, signature) | Optical (SAGEM) | N/A | N/A | 327 | 3 | N/A | Association BioSecure<br>http://biosecure.info |
| | | Capacitive (GEMPLUS) | N/A | N/A | 327 | 3 | N/A | |
| MSU | monomodal | Optical (Digital Biometrics) | 640 × 480 | 500 dpi | 160 | 2 | 2560 | MSU (Michigan State Univ.) |
| | | Solid-state (Veridicom) | 300 × 300 | 500 dpi | 160 | 2 | 2560 | |
| | | Solid-state (Veridicom) | 300 × 300 | 500 dpi | 8 | 30 | 240 | |
| Smartkom | multimodal<br>(hand, signature, fingerprint, voice) | N/A | N/A | N/A | 96 | N/A | N/A | ELDA (European Language<br>Resources Distribution Agency) |
| BioSec | multimodal<br>(face, speech, fingerprint, iris) | Optical (Biometrika) | 400 × 560 | 569 dpi | 250 | 4 | 16000 | ATVS (Biometric Recognition Group)<br>http://atvs.ii.uam.es |
| | | Thermal sweeping (Atmel) | 400 × 500 | 500 dpi | 250 | 4 | 16000 | |
| | | Capacitive (Authentec) | 96 × 96 | 250 dpi | 250 | 4 | 16000 | |
| BiosecurID | multimodal (speech, iris, face, signature,<br>hand, handwriting, fingerprints, keystroking) | Optical (Biometrika) | 400 × 560 | 569 dpi | 400 | 4 | 25600 | ATVS (Biometric Recognition Group)<br>http://atvs.ii.uam.es |
| | | Thermal sweeping (Yubee) | 400 × 500 | 5 dpi | 400 | 4 | 25600 | |
| BioSecure | multimodal (face, speech,<br>signature, fingerprint, hand, iris) | Optical (Biometrika) | 400 × 560 | 569 dpi | 700 | 2 | 16800 | Association BioSecure<br>http://biosecure.info |
| | | Thermal sweeping (Atmel) | 400 × 500 | 500 dpi | 700 | 2 | 16800 | |
| | | Thermal Sweeping (HP iPAQ hx2790 PDA) | 300 × 470 | 96 dpi | 700 | 2 | 16800 | |

allowed in 2002, 2004 and 2006. Additionally, the FVC2004 and FVC2006 were subdivided into: *a*) *open category* and *b*) *light category*. The light category aimed at evaluating algorithms under low computational resources, limited memory usage and small template size.

**Table 4.2** Comparative summary between FVC2004, FVC2006 and FpVTE2003

| | **FVC 2004** | **FVC 2006** | **FpVTE 2003** |
|---|---|---|---|
| **Participants** | 43 | 53 | 18 |
| **Algorithms** | Open Category: 41<br>Light Category: 26 | Open Category: 44<br>Light Category: 26 | Large Scale Test (LST): 13<br>Medium Scale Test (MST): 18<br>Small Scale Test (SST): 3 |
| **Population** | Students | Heterogeneous (incl. manual workers and elderly people) | Operational data from U.S. Government sources |
| **Fingerprint format** | Flat impressions from low-cost scanners | | Mixed formats from various sources |
| **Perturbations** | Deliberate perturbations | Selection of the most difficult images based on a quality index | Intrinsic low quality fingers and/or noncooperative users |
| **Data collection** | Acquired for the event | From the BioSec database | U.S. Government sources |
| **Database size** | 4 databases, each containing 1800 fingerprints from 150 fingers | | 48105 fingerprints from 25309 subjects |
| **Anonymous partic.** | Allowed | Allowed | Not allowed |
| **Best EER** | 2.07 %<br>(avg, Open Category) | 2.16 %<br>(avg, Open Category) | 0.2 % (MST, the closest to the FVC Open Category) |

For each FVC competition, four databases are acquired using three different sensors and the SFinGE synthetic generator [59] (see Sect. 4.3.1). The size of each database was set at 110 fingers with eight impressions per finger (150 fingers with 12 impressions per finger in FVC2006). A subset of each database (all the impressions from 10 fingers) was made available to the participants prior to the competition for algorithm tuning. The impressions from the remaining fingers are used for testing. Once tuned, participants submit their algorithms as executable files to the evaluators. The executable files are tested at the evaluator's site and the test data are not released until the evaluation concludes. In order to benchmark the algorithms, the evaluation is divided into: *a*) genuine attempts: each fingerprint image is compared to the remaining images of the same finger, and *b*) impostor attempts: the first impression of each finger is compared to the first image of the remaining fingers. In both cases, symmetric matches are avoided.

The FVC2004 databases were collected with the aim of creating a more difficult benchmark compared to the previous competitions [18]. During the acquisition sessions, individuals were requested to: *a*) put a finger at slightly different vertical position, *b*) apply low or high pressure against the sensor, *c*) exaggerate skin distortion and rotation, and *d*) dry or moisten their fingers. Data for the FVC2006 edition were collected without introducing deliberate difficulties, but the population is more heterogeneous, including manual workers and elderly people. Also, the final datasets in FVC2006 were selected from a larger database by choosing the most difficult fingers according to a quality index. In Table 4.3, results of the best performing algorithm in each FVC competition are shown. Data in the 2000 and 2002 editions were acquired without special restrictions and, as observed in Table 4.3, error rates decreased significantly from 2000 to 2002, demonstrating in some sense the maturity of fingerprint verification systems. However, in the 2004 and 2006 editions, it is observed that error rates increase with respect to the 2002 edition due to the deliberate difficulties and/or low quality sources introduced in the data, thus revealing that degradation of quality has a severe impact on the recognition rates.

**Table 4.3** Results in terms of Equal Error Rate (EER) % of the best performing algorithm in each of the four databases of the FVC competitions

| **Database** | **2000** | **2002** | **2004** | **2006** |
|---|---|---|---|---|
| DB1 | 0.67 | 0.10 | 1.97 | 5.56 |
| DB2 | 0.61 | 0.14 | 1.58 | 0.02 |
| DB3 | 3.64 | 0.37 | 1.18 | 1.53 |
| DB4 | 1.99 | 0.10 | 0.61 | 0.27 |
| **Average** | **1.73** | **0.19** | **2.07** | **2.16** |

### *4.4.2 NIST Fingerprint Vendor Technology Evaluation*

The NIST Fingerprint Vendor Technology Evaluation (FpVTE2003) aimed at: $a$) comparing systems on a variety of fingerprint data and identifying the most accurate systems; $b$) measuring the accuracy of fingerprint matching, identification, and verification on actual operational fingerprint data; and $c$) determining the effect of a variety of variables on matcher accuracy. Eighteen different companies competed in the FpVTE, and 34 systems were evaluated.

Three separate subtests were performed in the FpVTE2003: $a$) the Large-Scale Test (LST), $b$) the Medium-Scale Test (MST), and $c$) the Small-Scale Test (SST). SST and MST tested matching accuracy using individual fingerprints, whereas LST used sets of fingerprint images. The size and structure of each test were designed to optimize competing analysis objectives, available data, available resources, computational characteristics of the algorithms and the desire to include all qualified participants. In particular, the sizes of MST and LST were only determined after a great deal of analysis of a variety of issues. Designing a well-balanced test to accommodate heterogeneous system architectures was a significant challenge.

Data in the FpVTE2003 came from a variety of existing U.S. Government sources (paper cards, scanners), including low quality fingers. 48,105 sets of flat, slap or rolled fingerprint sets from 25,309 individuals were used, with a total of 393,370 fingerprint images. The systems that resulted in the best accuracy performed consistently well over a variety of image types and data sources. Also, the accuracy of these systems was considerably better than the rest of the systems. Further important conclusions drawn from the FpVTE2003 included: $a$) the number of fingers used and the fingerprint quality had the largest effect on system accuracy; $b$)

accuracy on controlled data was significantly higher than accuracy on operational data; *c*) some systems were highly sensitive to the sources or types of fingerprints; and *d*) accuracy dropped as subject age at time of capture increased.

### *4.4.3 Minutiae Interoperability NIST Exchange Test*

The purpose of the NIST Minutiae Interoperability Exchange Test (MINEX) [37] is to determine the feasibility of using minutiae data (rather than image data) as the interchange medium for fingerprint information between different fingerprint matching systems, and to quantify the verification accuracy changes when minutiae from dissimilar systems are used for matching fingerprints. Interoperability of templates is affected by the method used to encode minutiae and the matcher used to compare the templates. There are different schemes for defining the method of locating, extracting, formatting and matching the minutiae information from a fingerprint image [59]. In the MINEX evaluation, proprietary template formats are also compared with the ANSI INCITS 378-2004 template standard [1].

The images used for this test come from a variety of sensors, and include both live-scanned and non live-scanned rolled and plain impression types. No latent fingerprint images are used. Participants submitting a system had to provide an algorithm capable of extracting and matching a minutiae template using both their *proprietary* minutiae format and the ANSI INCITS 378-2004 minutiae data format standard [1]. The most relevant results of the MINEX evaluation were:

- Proprietary templates are superior to the ANSI INCITS 378-2004 templates.
- Some template generators produce standard templates that are matched more accurately than others. Some matchers compare templates more accurately than others. The leading vendors in generation are not always the leaders in matching and vice-versa.
- Verification accuracy of some matchers can be improved by replacing the vendors' template generator with that from another vendor.
- Performance is sensitive to the quality of the dataset. This applies to both proprietary and interoperable templates. Higher quality datasets provide reasonable interoperability, whereas lower quality datasets do not.

## 4.5 The BioSecure Benchmarking Framework

In order to ensure a fair comparison of various fingerprint recognition algorithms, a common evaluation framework has to be defined. In this section a reference system that can be used as a baseline for future improvements and comparisons is first defined. The database and the corresponding protocols are then described along with the associated performance measures. The benchmarking experiments presented in this section can be easily reproduced using the material and relevant information provided on the companion site [16].

## 4.5.1 Reference System: NFIS2

[1]The reference system for the fingerprint modality in the BioSecure Network of Excellence is the minutiae-based NIST Fingerprint Image Software (NFIS2–rel.28–2.2) [83]. NFIS2 contains software technology, developed for the Federal Bureau of Investigation (FBI), designed to facilitate and support the automated manipulation and processing of fingerprint images. Source code for over 50 different utilities or packages and an extensive User's Guide are distributed on CD-ROM free of charge [83]. For the evaluations and tests with the NFIS2 software presented in this chapter, two packages are used: the minutiae extraction MINDTCT package and the fingerprint matching BOZORTH3 package. These two packages are described next.

### 4.5.1.1 Minutiae Extraction Using MINDTCT

MINDTCT takes a fingerprint image and locates all minutiae in the image, assigning to each minutia point its location, orientation, type, and quality. The architecture of MINDTCT is shown in Fig. 4.13 and it can be divided in the following phases: *a*) generation of image quality map; *b*) binarization; *c*) minutiae detection; *d*) removal of false minutiae (including islands, lakes, holes, minutiae in regions of poor image quality, side minutiae, hooks, overlaps, minutiae that are too wide, and minutiae that are too narrow-pores); *e*) counting of ridges between a minutia point and its nearest neighbors; and *f*) minutiae quality assessment. Additional details of these phases are given below.

Because of the variation of image quality within a fingerprint, NFIS2 analyzes the image and determines areas that are degraded. Several characteristics are measured, including regions of low contrast, incoherent ridge flow, and high curvature. These three conditions represent unstable areas in the image where minutiae detection is unreliable, and together they are used to represent levels of quality in the image. An image quality map is generated integrating these three characteristics. Images are divided into nonoverlapping blocks, where one out of five levels of quality is assigned to each block.

The minutiae detection step scans the binary image of the fingerprint, identifying local pixel patterns that indicate the ending or splitting of a ridge. A set of minutia patterns is used to detect candidate minutia points. Subsequently, false minutiae are removed and the remaining candidates are considered as the true minutiae of the image. Fingerprint minutiae marchers often use other information in addition to just the points themselves. Apart from minutia's position, direction, and type,

[1] Material from this section is reproduced with permission from Annals of Telecommunication; source [3].

MINDTCT computes ridge counts between a minutia point and each of its nearest neighbors.

In the last step, a quality/reliability measure is associated with each detected minutia point. Even after performing the removal step, false minutiae potentially remain in the list. A robust quality measure can help to manage this. Two factors are combined to produce a quality measure for each detected minutia point. The first factor is taken directly from the location of the minutia point within the quality map described before. The second factor is based on simple pixel intensity statistics (mean and standard deviation) within the immediate neighborhood of the minutia point. A high quality region within a fingerprint image is expected to have significant contrast that will cover the full grayscale spectrum [83].

### 4.5.1.2 Fingerprint Matching Using the BOZORTH3 Algorithm

The BOZORTH3 matching algorithm computes a match score between the minutiae from any two fingerprints to help determine if they are from the same finger. This matcher uses only the location and orientation of the minutia points to match the fingerprints. It is rotation and translation invariant. The algorithm can be described by the following three steps: *a*) construction of two IntraFingerprint Minutia Comparison Tables, one table for each of the two fingerprints; *b*) construction of an InterFingerprint Compatibility Table; and *c*) generation of the matching score using the InterFingerprint Compatibility Table. These steps are described in Fig. 4.13. The first step is to compute relative measurements from each minutia in a fingerprint to all other minutia in the same fingerprint. These relative measurements are stored in the IntraFingerprint Minutia Comparison Table and are used to provide rotation and translation invariance. The invariant measurements computed are the distance

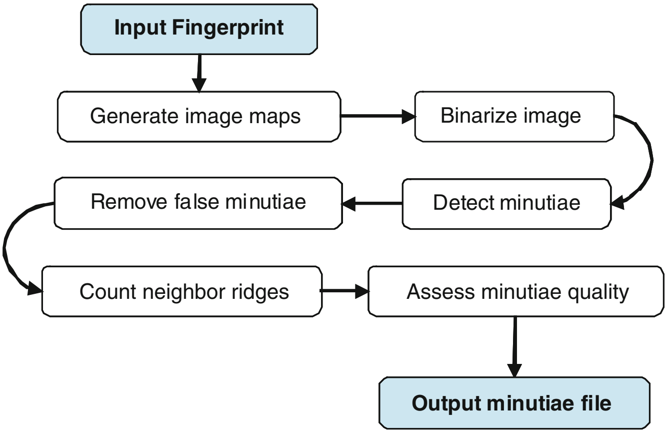


**Fig. 4.13** System architecture of the MINDTCT package of the NIST Fingerprint Image Software 2 (NFIS2), [83]

between two minutiae and angle between each minutia's orientation and the intervening line between both minutiae. A comparison table is constructed for each of the two fingerprints.

The next step is to take the IntraFingerprint Minutia Comparison Tables from the two fingerprints and look for "compatible" entries between the two tables. Table entries are "compatible" if: *a*) the corresponding distances and *b*) the relative minutia angles are within a specified tolerance. An InterFingerprint Compatibility Table is generated, only including entries that are compatible. A compatibility table entry therefore incorporates two pairs of minutia, one pair from the template fingerprint and one pair from the test fingerprint. The entry into the compatibility table indicates that the minutiae pair of the template fingerprint corresponds to the minutiae pair of the test fingerprint.

At the end of the second step, we have constructed a compatibility table that consists of a list of compatibility associations between two pairs of potentially corresponding minutiae. These associations represent single links in a compatibility graph. The matching algorithm then traverses and links table entries into clusters, combining compatible clusters and accumulating a match score. The larger the number of linked compatibility associations, the higher the match score, and the more likely the two fingerprints originate from the same person.

### *4.5.2 Benchmarking Database: MCYT-100*

A large biometric database acquisition process was launched in 2001 within the MCYT project [70]. For the experiments reported in this chapter, the freely available MCYT-100 subcorpus [64], which contains 100 individuals extracted from the MCYT database is used. The single-session fingerprint database acquisition was designed to include different types of sensors and different acquisition conditions. Two types of acquisition devices were used: *a*) a CMOS-based capacitive capture device, model 100SC from Precise Biometrics, producing a 500 dpi, 300 × 300 pixel image; and *b*) an optical scanning device, model UareU from Digital Persona, producing a 500 dpi, 256 × 400 pixel image. Some example images of the MCYT database acquired with the optical and the capacitive sensor are shown in Fig. 4.14.

With the aim of including variability in fingerprint positioning on the sensor, the MCYT database includes 12 different samples of each fingerprint, all of which were acquired under human supervision and with three different levels of control. For this purpose, the fingerprint core must be located inside a size-varying rectangle displayed in the acquisition software interface viewer. In Fig. 4.15, three samples of the same fingerprint are shown, so that variability in fingerprint positioning can be clearly observed. Depending on the size of the rectangle, the different levels of control will be referred to as: *a*) "low," with three fingerprint acquisitions using the biggest rectangle; *b*) "medium," with three fingerprint acquisitions; and *c*) "high," with six fingerprint acquisitions using the smallest rectangle. Therefore, each individual provides a total number of 240 fingerprint images for the database (10 prints × 12 samples/print × 2 sensors).

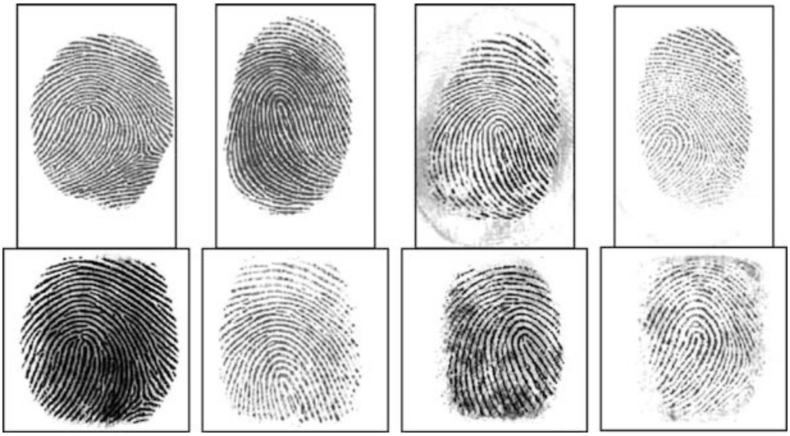


**Fig. 4.14** Examples of MCYT fingerprints, of four different fingerprints (*one per column*); acquired with the optical (*top line*) or with the capacitive sensor (*bottom line*)

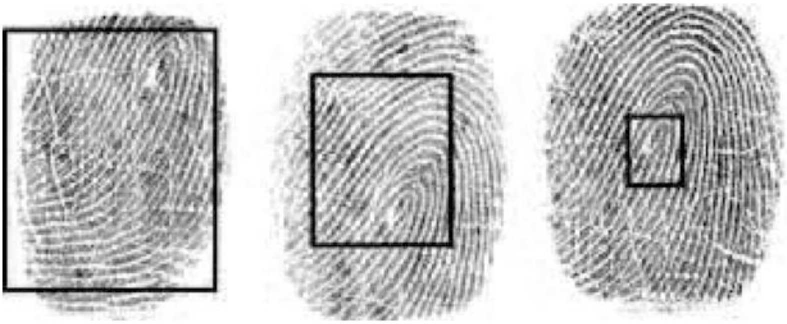


**Fig. 4.15** Examples of the same MCYT fingerprint samples acquired at different levels of control

### 4.5.3 Benchmarking Protocols

For the experiments, data consist of 12,000 fingerprint images per sensor from the 10 fingers of the 100 contributors. We consider the different fingers as different users enrolled in the system, thus resulting in 1,000 users with 12 impressions per user. The experimental protocol is applied to each sensor separately.

We use one impression per finger with low control during the acquisition as a template. In genuine trials, the template is compared to the other 11 impressions available (two with low control, three with medium control and six with high control). The impostor trials are obtained by comparing the template to one impression with high control of the same finger of all the other contributors. The total number of genuine and impostor trials are therefore $1{,}000 \times 11 = 11{,}000$ and $1{,}000 \times 99 = 99{,}000$, respectively, per sensor.

### *4.5.4 Benchmarking Results*

The minutiae-based NIST Fingerprint Image Software (NFIS2–rel.28–2.2) [83] was used to provide the benchmarking results, on the MCYT-100 database (see Sect. 4.5.2) according to the reference protocols (see Sect. 4.5.3). The benchmarking results obtained with both sensors (optical and capacitive) are presented in Table 4.4. Corresponding DET curves are displayed in Fig. 4.16.

**Table 4.4** Fingerprint verification results (EER%) with Confidence Intervals [CI], obtained by applying the NIST Fingerprint Image Software (NFIS2–rel.28–2.2) [83] on the MCYT-100 database, according to the proposed benchmarking protocols, for the optical and capacitive sensors

| | Optical (dp) | Capacitive (pb) |
|---|---|---|
| EER (in %) | 3.18 [±0.18] | 8.58 [±0.29] |

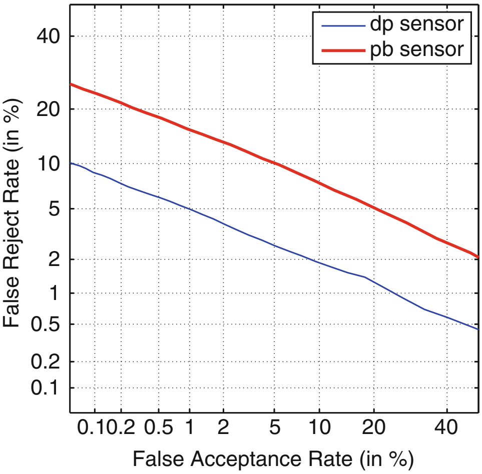


**Fig. 4.16** DET plots for the benchmarking experiments obtained by applying the NIST Fingerprint Image Software (NFIS2–rel.28–2.2) [83] on the MCYT-100 database according to the proposed benchmarking protocols. The experiment with the fingerprint images acquired with the optical Digital Persona device is denoted as *db* and with the capacitive Precise Biometrics sensor is denoted as *pb*. The corresponding EER are 3.18% and 8.58%, respectively

## 4.6 Research Algorithms Evaluated within the Benchmarking Framework

We have also tested the minutiae-based fingerprint matcher developed by Halmstad University [HH] in Sweden [31] and the ridge-based fingerprint matcher developed by the ATVS/Biometric Recognition Group at Universidad Politecnica de Madrid [UPM], Spain [29].

### *4.6.1 Halmstad University Minutiae-based Fingerprint Verification System [HH]*

[2]The fingerprint recognition software developed by Halmstad University [31] includes a novel way to detect the minutia points' position and direction, as well as ridge orientation, by using filters sensitive to parabolic and linear symmetries. The minutiae are exclusively used for alignment of two fingerprints. The number of paired minutiae can be low, which is advantageous in partial or low-quality fingerprints. After a global alignment, a matching is performed by distinctive area correlation, involving the minutiae's neighborhood. We briefly describe the four phases of the system: $a$) local feature extraction, $b$) pairing of minutiae, $c$) fingerprint alignment, and $d$) matching.

#### 4.6.1.1 Local Feature Extraction

Two prominent minutia types, ridge bifurcation and termination have parabolic symmetry properties [67], whereas they lack linear symmetry [68]. The leftmost image in Fig. 4.17 shows a perfectly parabolic pattern. On the contrary, the local ridge and

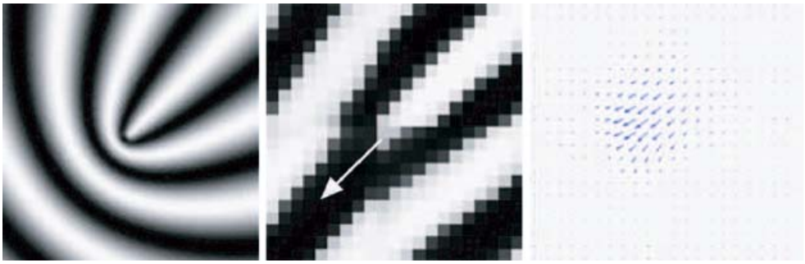


**Fig. 4.17** (**Left-hand side**) perfectly parabolic pattern; (**center**) ridge bifurcation neighborhood with indicated minutia direction; (**right-hand side**) corresponding complex response of $h_1$ when convoluted with $z$

[2] Material from this section is reproduced with permission from Annals of Telecommunication; source [3].

valley structure is linearly symmetric. Perfect linearly symmetric patterns include planar waves, which have the same orientation at each point.

Averaging the orientation tensor $z = (f_x + if_y)^2$ of an image (with $f_x$ and $f_y$ as its partial derivatives) gives an orientation estimation and its error. A signal energy independent linear symmetry measure, *LS*, can be computed by dividing averaged $z$ with averaged $|z|$. The result is a complex number, having the ridge orientation (in double angle) as argument and the reliability of its estimation as magnitude. Parabolic symmetry *PS* is retrieved by convolving $z$ with a filter $h_n = (x + iy)^n \cdot g$ where $g$ denotes a 2D Gaussian, with $n = 1$. The result is again a complex number, having the minutiae's direction as argument and an occurrence certainty as magnitude (compare Fig. 4.17). Note that $h_0$ can be used for the calculation of *LS*. All filtering is done in 1D involving separable Gaussians and their derivatives.

At the beginning, an image enhancement [24] is applied prior to the calculation of linear and parabolic symmetries. Some additional measures are then taken in order to reliably detect minutiae points. First, the selectivity of the parabolic symmetry filter response is improved, using a simple inhibition scheme to get $PSi = PS(1 - |LS|)$. Basically, parabolic symmetry is attenuated if the linear symmetry is high, whereas it is preserved in the opposite case. In Fig. 4.18, the overall minutia detection process is depicted. The first two images show the initial fingerprint and its enhanced version, respectively. The extracted parabolic symmetry is displayed in image IV ($|PS|$), whereas the linear part is shown in image III (*LS*). The sharpened magnitudes $|PSi|$ are displayed in image V.

To avoid multiple detections of the same minutia, neighborhoods of $9 \times 9$ pixels are considered when looking for the highest responses in *PSi*. At this stage, *LS* can be reused to verify minutia candidates. First, a minimum $|LS|$ is employed to segment the fingerprint area from the image background. Second, each minutia is required to have full surround of high linear symmetry, in order to exclude spurious and false minutiae. Minutiae's coordinates and direction are stored in a list ordered by magnitude. In image VI of Fig. 4.18, its first 30 entries are indicated by circles.

In Fig. 4.18, the overall minutia detection process is depicted. The first two images show the initial fingerprint and its enhanced version, respectively. The extracted parabolic symmetry is displayed in image IV ($|PS|$), whereas the linear part is shown in image III (*LS*). The sharpened magnitudes $|PSi|$ are displayed in image V.

#### 4.6.1.2 Pairing of Minutiae

In order to establish correspondences between two fingerprints, a local minutia matching approach inspired by triangular matching [51] is implemented. This approach essentially means establishing a connected series of triangles, which are equal with respect to both fingerprints and have corresponding minutiae as their corners.

For each minutia in a fingerprint, additional attributes are derived, which describe their within-fingerprint relation. For two arbitrary minutiae $m_i$ and $m_j$ of one fingerprint, the following attributes are derived: *a*) the distance $d_{ij} = d_{ji}$ between

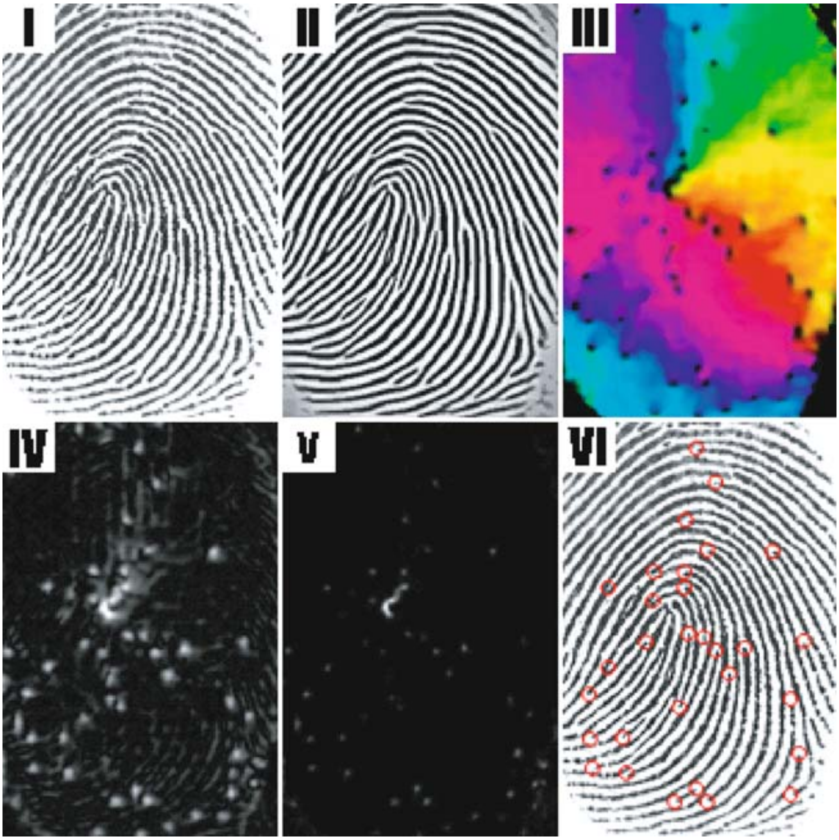


**Fig. 4.18** Local feature extraction using complex filtering (HH system): (**I, II**) show the initial fingerprint and its enhanced version; (**III**) linear symmetry *LS*; (**IV**) parabolic symmetry *PS*; (**V**) sharpened magnitudes $|PSi|$; and (**VI**) the first ordered 30 minutiae; (see insert for color reproduction of this figure)

the two minutiae; and $b)$ the angles $\alpha_{ij}$ and $\alpha_{ji}$ of the minutiae with respect to the line between each other (compare Fig. 4.19). Next, corresponding couples in the two fingerprints are selected. Having two arbitrary minutiae $m_k$ and $m_l$ of the second fingerprint, the correspondence is fulfilled if $\left|d_{ij} - d_{kl}\right| < \lambda_{dist}$ and $\left(\left|\alpha_{ij} - \alpha_{kl}\right| + \left|\alpha_{ji} - \alpha_{lk}\right|\right) < \lambda_{angle}$. Thus, a corresponding couple means two pairs of minutiae, — e.g. $\{m_i, m_j; m_k, m_l\}$ — which at least correspond in a local scope.

Among all corresponding couples, we look for those that have a minutia in common in both of the fingerprints. Taking $\{m_i, m_j; m_k, m_l\}$ as a reference, it may be that $\{m_i, m_o; m_k, m_p\}$ and $\{m_j, m_o; m_l, m_p\}$ are corresponding couples as well. This is also visualized right, in Fig. 4.19. Such a constellation suggests $m_o$ and $m_p$ being neighbors to $\{m_i, m_j\}$ and $\{m_k, m_l\}$, respectively. To verify neighbors, we additionally check the closing angles $\gamma_1$ and $\gamma_2$ in order to favor uniqueness. In this way neighbors are consecutively assigned to the corresponding reference couples, the

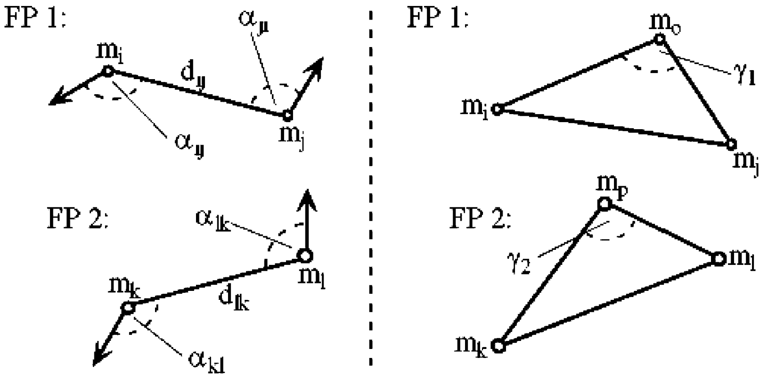


**Fig. 4.19** Corresponding couples (**left-hand side**) and triangles (**right-hand side**) for two fingerprints; all angles are signed in order to be unambiguous

equivalent of establishing equal triangles with respect to both fingerprints sharing a common side. Each corresponding couple is taken as a reference once. The corresponding couple to which most neighbors can be found is considered for further processing. This couple and its mated neighbors are stored in a pairing list.

#### 4.6.1.3 Fingerprint Alignment

Here, global alignment of two fingerprints is assumed to be a rigid transformation since only translation and rotation is considered. The corresponding parameters are computed using the established minutia pairs (list): translation is given by the difference of the position vectors for the first minutia pair. The rotation parameter is determined as the averaged angle among vectors between the first minutia pair and all others. Following the estimated parameters, the coordinate transformation for all points in *LS* is done, as the latter is needed for the final step. No further alignment efforts, e.g., fine adjustment, are performed.

#### 4.6.1.4 Fingerprint Matching

Finally, a simple matching using normalized correlation at several sites of the fingerprint is performed (similar to [66]). Small areas in *LS* around the detected minutia points in the first fingerprint are correlated with areas at the same position in the second fingerprint. Only areas having an average linear symmetry higher than a threshold are considered. This is done to favor well-defined (reliable) fingerprint regions for comparison. The final matching score is given by the mean value of the single similarity measures.

## *4.6.2 UPM Ridge-based Fingerprint Verification System [UPM]*

[3]The UPM ridge-based matcher uses a set of Gabor filters to capture the ridge strength. The image is tessellated into square cells, and the variance of the filter responses in each cell across all filtered images is used as feature vector. This feature vector is called FingerCode because of the similarity to previous research works [75, 25]. The automatic alignment is based on the system described in [76] in which the correlation between the two FingerCodes is computed, obtaining the optimal offset. The UPM ridge-based matcher can be divided in two phases: *a*) extraction of the FingerCode; and *b*) matching of the FingerCodes.

### 4.6.2.1 Feature Extraction (the FingerCode)

No image enhancement is performed since Gabor filters extract information that is in a specific (usually low-pass) band that is not affected by noise to the same extent as the original image is. The complete processing for extracting the feature vectors consists of the following three steps: *a*) convolution of the input fingerprint image with eight Gabor filters, obtaining eight filtered images $F_\theta$; *b*) tessellation of the filtered images into equal-sized square disjoint cells; and *c*) extraction of the FingerCode. For each cell of each filtered image $F_\theta$, we compute the variance of the pixel intensities. These standard deviation values constitute the FingerCode of a fingerprint image. A sample fingerprint image, the resulting convolved image with a Gabor filter of orientation $\theta = 0°$, the tessellated image and its FingerCode are shown in Fig. 4.20.

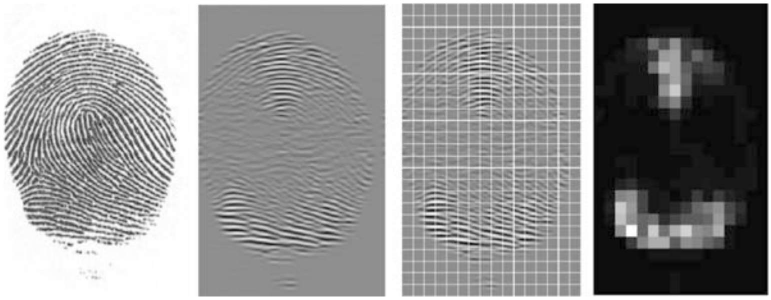


**Fig. 4.20** Processing steps of the UPM ridge-based verification system

[3] Material from this section is reproduced with permission from Annals of Telecommunication; source [3].

#### 4.6.2.2 Matching of FingerCodes

The complete sequence of stages performed is: $a)$ alignment of the two fingerprints to be compared; and $b)$ similarity computation between the FingerCodes. The matching score is computed as the Euclidean distance between the two FingerCodes.

To determine the alignment between two fingerprints, the 2D correlation of the two FingerCodes [76] is computed. Correlation involves multiplying corresponding entries between the two FingerCodes at all possible translation offsets, and determining the sum, which is computed more efficiently in the Fourier domain. The offset that results in the maximum sum is chosen to be the optimal alignment. Every offset is properly weighted to account for the amount of overlap between the two FingerCodes. It is worth noting that this procedure does not account for rotational offset between the two fingerprints. For the MCYT database used in this work, which is acquired under realistic conditions with an optical sensor, we have observed that typical rotations between different impressions of the same fingerprint are compensated by using the tessellation.

## 4.7 Experimental Results within the Benchmarking Framework

### *4.7.1 Evaluation of the Individual Systems*

In Fig. 4.21 we show the verification results of the reference system and research systems described in Sects. 4.5.1 and 4.6. Furthermore, a general algorithmic description of these individual systems is given in Table 4.5. In Table 4.6 we also show the verification performance in terms of EER[4].

As expected, we can observe that minutiae-based matchers perform better than the ridge-based matcher. It is also supported by other findings that minutiae are more discriminative than other features of fingerprints, such as local orientation and frequency, ridge shape or texture information [59]. Regarding the technology of the sensor, we observe that the optical sensor performs better than the capacitive one. This could be because acquisition area is lower for the capacitive sensor, as can be seen in Fig. 4.14. Smaller acquisition surface implies less overlap between different acquisitions of the same finger and less amount of discriminative information in the fingerprint image [59].

By considering only minutiae-based approaches, HH algorithm results in the best performance. This result may be justified as follows:

- HH algorithm relies on complex filtering for minutiae extraction, considering the surrounding ridge information directly in the gray scale image. On the other

[4] The experimental protocol (individuals, enrollment and test images) for the results reported in this section is different from the one used for the experiments reported in [4].

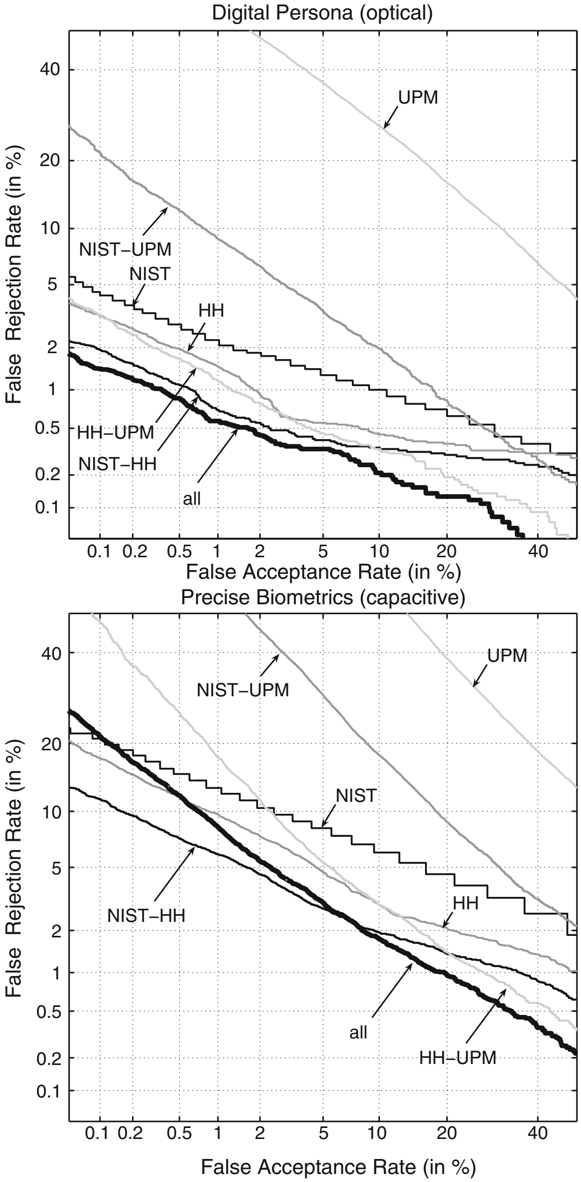


**Fig. 4.21** Verification performance of the individual systems and of the fusion experiments carried out using the mean rule

hand, NIST algorithm relies on binarization and morphological analysis, which does not take the surrounding ridge information of the gray scale image into account, but only the information contained in small neighborhoods of the binarized image. Binarization-based methods usually result in a significant loss of information during the binarization process and in a large number of spurious minutiae introduced during thinning [59], thus decreasing the performance of the system.

- For fingerprint alignment, the NIST algorithm matches minutia pairs, whereas the HH algorithm performs triangular matching of minutiae. As the complexity of the alignment method increases, more conditions are implicitly imposed for a fingerprint to be correctly aligned, resulting in higher accuracy.
- In the same way, for fingerprint matching, the NIST algorithm looks for compatibility of minutiae pairs, whereas the HH algorithm does not perform minutiae matching but local orientation correlation of areas around the minutiae. Thus, the HH algorithm combines the accuracy of a minutiae-based representation with the robustness of a correlation-based matching, which is known to perform properly in low image quality conditions [59].

It should be noted that there are other reasons that justify significantly different performance between different implementations of systems that exploit the same features and use the same basic techniques. In the FVC experience [18], it was noted that commercial systems typically outperform academic approaches. Although they are based on the same ideas, commercial systems usually are strongly tuned and optimized.

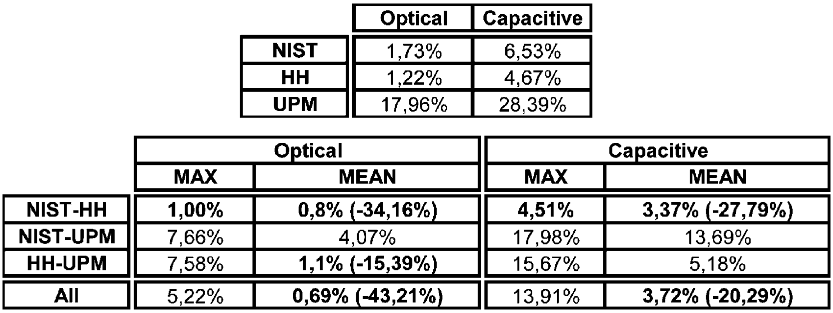
**Table 4.5** High-level description of the individual systems tested (reproduced with permission from Annals of Telecommunication; source [3])

| | Segmentation (Y/N) | Enhancement (Y/N) | Features | Alignment | | Matching |
|---|---|---|---|---|---|---|
| | | | | Translation<br>Rotation | | |
| **NIST** | Y | Y | Minutiae by binarization | TR | Minutiae-based by compatibility between minutiae pairs | Compatibility association between pairs of minutiae |
| **HH** | Y | Y | Minutiae by complex filtering (parabolic and linear symmetry) | TR | Minutiae-based by triangular matching | Normalized correlation of the neighborhood around minutiae |
| **UPM** | N | N | Ridge information by Gabor filtering and square tessellation | T | Correlation between the extracted features | Euclidean distance between extracted features |

## *4.7.2 Multialgorithmic Fusion Experiments*

We have evaluated two different simple fusion approaches based on the max rule and the mean rule. These schemes have been used to combine multiple classifiers in biometric authentication with good results reported [11, 49]. More advanced fusion rules currently form the basis of an intensive research topic. The use of these simple fusion rules is motivated by their simplicity, as complex fusion approaches may

**Table 4.6** Verification performance in terms of EER of the individual systems and of the fusion experiments carried out using the mean and the max rule. The relative performance gain compared to the best individual matcher involved is also given for the mean rule



| | Optical | Capacitive |
|---|---|---|
| **NIST** | 1,73% | 6,53% |
| **HH** | 1,22% | 4,67% |
| **UPM** | 17,96% | 28,39% |

| | Optical | | Capacitive | |
|---|---|---|---|---|
| | MAX | MEAN | MAX | MEAN |
| **NIST-HH** | **1,00%** | **0,8% (-34,16%)** | **4,51%** | **3,37% (-27,79%)** |
| **NIST-UPM** | 7,66% | 4,07% | 17,98% | 13,69% |
| **HH-UPM** | 7,58% | **1,1% (-15,39%)** | 15,67% | 5,18% |
| **All** | 5,22% | **0,69% (-43,21%)** | 13,91% | **3,72% (-20,29%)** |

need training to outperform simple fusion approaches, which even then cannot be guaranteed, e.g., see [30].

Each matching score has been normalized to be a similarity score in the $[0,1]$ range using the tanh-estimators described in [41]:

$$s' = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{s-\mu_s}{\sigma_s}\right)\right)+1\right\} \tag{4.1}$$

where $s$ is the raw similarity score, $s'$ denotes the normalized similarity score, and $\mu_s$ and $\sigma_s$ are respectively the estimated mean and standard deviation of the genuine score distribution.

In Table 4.6 we show the verification performance in terms of EER of the fusion experiments carried out using the max and mean rule. In addition, Fig. 4.21 depicts the DET plots only using the mean rule, which is the fusion rule that results in the best performance, based on the results of Table 4.6.

From Table 4.6, it is worth noting that an important relative improvement is obtained when fusing HH and NIST algorithms. Both of them use minutiae-based features, but they rely on completely different strategies for feature extraction (complex filtering vs. binarization) and matching (normalized correlation vs. minutiae compatibility), see Table 4.5. Fusing the three available systems results in an additional improvement for the optical sensor. For the capacitive one, however, improvement is obtained only for low FRR values (see Fig. 4.21). Interestingly enough, combining the ridge-based system (UPM) with minutiae-based systems does not always result in better performance, although they are systems based on heterogeneous strategies for feature extraction and/or matching. Only the combination of UPM and HH systems results in lower error rates for certain regions of the DET plot.

In terms of EER, the best combination of two systems (HH and NIST) results in a significant performance improvement. Subsequent inclusion of the third system (UPM) only produces a slight improvement of the performance or even no improvement, as it is the case of the capacitive sensor. Interestingly, the best combinations always include the best individual systems (HH and NIST). This should not be taken as a general statement because none of our fusion methods used training. Other studies have revealed that the combination of the best individual systems can be outperformed by other combinations [30], especially if the supervisor is data or expert adaptive.

## 4.8 Conclusions

In this work, we have reported on experiments carried out using the publicly available MCYT-100, database which includes fingerprint images acquired with an optical and a capacitive sensor. Three published systems [31, 83, 29] have been tested and the results discussed. The three systems implement different approaches for feature extraction, fingerprint alignment, and matching. Furthermore, several combinations of the systems using simple fusion schemes have been reported.

A number of experimental findings can be put forward as a result. We can confirm that minutiae have discriminative power but that complementary information, such as second and higher order minutiae constellation, local orientation, frequency, ridge shape or texture information encoding alternative features, improves the performance, in particular in low-quality fingerprints [59]. The minutiae-based algorithm that results in the best performance (HH) exploits both a minutiae-based correspondence and a correlation-based matching, instead of using only either of them. Moreover, the HH algorithm extracts minutiae by means of complex filtering, instead of using the classical approach based on binarization, which is known to result in loss of information and spurious minutiae [59].

When combining only two systems we generally obtain a significant performance improvement compared to including a third system. Though the latter combination produces the overall best EER of $\sim$0.69 for the optical sensor, it is not the scope of this work to work towards a perfect verification rate but to give an incentive to combine different methods within the same modality and reveal the fundamental reasons for such improvements.

In this study, which used untrained supervisors, the best combinations of two/three systems always included the best individual systems. Other studies have shown that however the performance of different individual systems can be influenced by database acquisition and the sensors [60]. This motivates us to extend the presented experiments to different databases and complementary method combinations to obtain compact and efficient systems.

## Acknowledgments

This work was partially funded by the IST-FP6 BioSecure Network of Excellence. F. Alonso-Fernandez is supported by a FPI Scolarship from Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo. J. Fierrez is supported by a Marie-Curie Fellowship from the European Commission.

# References

1. ANSI-INCITS 378, Fingerprint Minutiae Format for Data Interchange. American National Standard (2004)
2. Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J., Fronthaler, H., Kollreider, K., Bigun, J.: A comparative study of fingerprint image quality estimation methods. IEEE Trans. on Information Forensics and Security **2**(4), 734–743 (2007)
3. Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., Fronthaler, H., Kollreider, K., Bigun, J.: Combining Multiple Matchers for fingerprint verification: a case study in BioSecure Network of Excellence. Annals of Telecommunications, Multimodal Biometrics, Eds. B.Dorizzi and C.Garcia-Mateo, Vol. 62, (2007)
4. Alonso-Fernandez, F., Fierrez, J., Ramos, D., Ortega-Garcia, J.: Dealingwith sensor interoperability in multi-biometrics: The UPM experience at the Biosecure Multimodal Evaluation 2007. Defense and Security Symposium, Biometric Technologies for Human Identification, BTHI, Proc. SPIE (2008)
5. Alonso-Fernandez, F., Roli, F., Marcialis, G., Fierrez, J., Ortega-Garcia, J.: Performance of fingerprint quality measures depending on sensor technology. Journal of Electronic Imaging, Special Section on Biometrics: Advances in Security, Usability and Interoperability (to appear) (2008)
6. Alonso-Fernandez, F., Veldhuis, R., Bazen, A., Fierrez-Aguilar, J., Ortega-Garcia, J.: On the relation between biometric quality and user-dependent score distributions in fingerprint verification. Proc. of Workshop on Multimodal User Authentication – MMUA (2006)
7. Alonso-Fernandez, F., Veldhuis, R., Bazen, A., Fierrez-Aguilar, J., Ortega-Garcia, J.: Sensor interoperability and fusion in fingerprint verification: A case study using minutiae- and ridge-based matchers. Proc. IEEE Intl. Conf. on Control, Automation, Robotics and Vision, ICARCV, Special Session on Biometrics (2006)
8. Antonelli, A., Capelli, R., Maio, D., Maltoni, D.: Fake finger detection by skin distortion analysis. IEEE Trans. on Information Forensics and Security **1**, 306–373 (2006)
9. Bazen, A., Gerez, S.: Segmentation of fingerprint images. Proc. Workshop on Circuits Systems and Signal Processing, ProRISC pp. 276–280 (2001)
10. Bazen, A., Gerez, S.: Systematic methods for the computation of the directional fields and singular points of fingerprints. IEEE Trans. on Pattern Analysis and Machine Intelligence **24**, 905–919 (2002)
11. Bigun, E., Bigun, J., Duc, B., Fischer, S.: Expert conciliation for multi modal person authentication systems by bayesian statistics. Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA **LNCS-1206**, 291–300 (1997)
12. Bigun, J.: Vision with Direction. Springer (2006)
13. Bigun, J., Granlund, G.: Optimal orientation detection of linear symmetry. First International Conference on Computer Vision pp. 433–438 (1987)
14. BioSec: Biometrics and security, FP6 IP, IST – 2002-001766 – http://www.biosec.org (2004)
15. BioSecure: Biometrics for secure authentication, FP6 NoE, IST – 2002-507634 – http://www.biosecure.info (2004)
16. BioSecure Benchmarking Framework. http://share.int-evry.fr/svnview-eph
17. Bolle, R., Serior, A., Ratha, N., Pankanti, S.: Fingerprint minutiae: A constructive definition. Proc. Workshop on Biometric Authentication, BIOAW **LNCS-2359**, 58–66 (2002)
18. Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., Jain, A.K.: Performance evaluation of fingerprint verification systems. IEEE Trans. on Pattern Analysis and Machine Intelligence **28**(1), 3–18 (2006)
19. CBEFF: Common Biometric Exchange File Format – http://www.itl.nist.gov/div893/biometrics/documents/NISTIR6529A.pdf (2001)
20. Chang, J., Fan, K.: Fingerprint ridge allocation in direct gray scale domain. Pattern Recognition **34**, 1907–1925 (2001)
21. Chen, Y., Jain, A.: Dots and incipients: Extended features for partial fingerprint matching. Proceedings of Biometric Symposium, Biometric Consortium Conference (2007)

22. Chen, Y., Parziale, G., Diaz-Santana, E., Jain, A.: 3d touchless fingerprints: Compatibility with legacy rolled images. Proceedings of Biometric Symposium, Biometric Consortium Conference (2006)
23. Chikkerur, S., Ratha, N.K.: Impact of singular point detection on fingerprint matching performance. Proc. IEEE AutoID pp. 207–212 (2005)
24. Chikkerur, S., Wu, C., Govindaraju, V.: A systematic approach for feature extraction in fingerprint images. Intl. Conf. on Bioinformatics and its Applications pp. 344–350 (2004)
25. Daugman, J.: How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology **14**, 21–30 (2004)
26. Derakhshani, R., Schuckers, S., Hornak, L., O'Gorman, L.: Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition **36**, 383–396 (2003)
27. Fierrez, J., Torre-Toledano, J.D., Gonzalez-Rodriguez, J.: BioSec baseline corpus: A multimodal biometric database. Pattern Recognition **40**(4), 1389–1392 (2007)
28. Fierrez-Aguilar, J., Chen, Y., Ortega-Garcia, J., Jain, A.: Incorporating image quality in multi-algorithm fingerprint verification. Proc. International Conference on Biometrics, ICB **LNCS-3832**, 213–220 (2006)
29. Fierrez-Aguilar, J., Munoz-Serrano, L., Alonso-Fernandez, F., Ortega-Garcia, J.: On the effects of image quality degradation on minutiae- and ridge-based automatic fingerprint recognition. Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST pp. 79–82 (2005)
30. Fierrez-Aguilar, J., Nanni, L., Ortega-Garcia, J., Capelli, R., Maltoni, D.: Combining multiple matchers for fingerprint verification: A case study in FVC2004. Proc. Int Conf on Image Analysis and Processing, ICIAP **LNCS-3617**, 1035–1042 (2005)
31. Fronthaler, H., Kollreider, K., Bigun, J.: Local feature extraction in fingerprints by complex filtering. Proc. Intl. Workshop on Biometric Recognition Systems, IWBRS **LNCS-3781**, 77–84 (2005)
32. Fronthaler, H., Kollreider, K., Bigun, J., Fierrez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Gonzalez-Rodriguez, J.: Fingerprint image quality estimation and its application to multi-algorithm verification. IEEE Trans. on Information Forensics and Security (to appear) (2008)
33. FVC2006: Fingerprint Verification Competition – http://bias.csr.unibo.it/fvc2006/default.asp (2006)
34. Galbally, J., Fierrez, J., Ortega-Garcia, J., Freire, M., Alonso-Fernandez, F., Siguenza, J., Garrido-Salas, J., Anguiano-Rey, E., Gonzalez-de-Rivera, G., Ribalda, R., Faundez-Zanuy, M., Ortega, J., Cardeoso-Payo, V., Viloria, A., Vivaracho, C., Moro, Q., Igarza, J., Sanchez, J., Hernaez, I., Orrite-Uruuela, C.: Biosecurid: a multimodal biometric database. Proc. MADRINET Workshop pp. 68–76 (2007)
35. Galbally-Herrero, J., Fierrez-Aguilar, J., Rodriguez-Gonzalez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Tapiador, M.: On the vulnerability of fingerprint verification systems to fake fingerprint attacks. Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST (2006)
36. Garcia-Salicetti, S., Beumier, C., Chollet, G., Dorizzi, B., les Jardins, J., Lunter, J., Ni, Y., Petrovska-Delacretaz, D.: BIOMET: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities. Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA p. 845853 (2003)
37. Grother, P., McCabe, M., Watson, C., Indovina, M., Salamon, W., Flanagan, P., Tabassi, E., Newton, E., Wilson, C.: MINEX – Performance and interoperability of the INCITS 378 fingerprint template. NISTIR 7296 – http://fingerprint.nist.gov/minex (2005)
38. Guyon, I., Makhoul, J., Schwartz, R., Vapnik, V.: What size test set gives good error rate estimates? IEEE Trans. on Pattern Analysis and Machine Intelligence **20**, 52–64 (1998)
39. Hong, L., Wan, Y., Jain, A.: Fingerprint imagen enhancement: Algorithm and performance evaluation. IEEE Trans. on Pattern Analysis and Machine Intelligence **20**(8), 777–789 (1998)
40. Jain, A., Chen, Y., Demirkus, M.: Pores and ridges: High resolution fingerprint matching using level 3 features. IEEE Trans. on Pattern Analysis and Machine Intelligence **29**(1), 15–27 (2007)

41. Jain, A., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recognition **38**(12), 2270–2285 (2005)
42. Jain, A., Ross, A., Pankanti, S.: Biometrics: A tool for information security. IEEE Trans. on Information Forensics and Security **1**, 125–143 (2006)
43. Jain, A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology **14**(1), 4–20 (2004)
44. Jain, A.K., Hong, L., Pankanti, S., Bolle, R.: An identity authentication system using fingerprints. Proc. IEEE **85**(9), 1365–1388 (1997)
45. Jain, A.K., Prabhakar, S., Ross, A.: Fingerprint matching: Data acquisition and performance evaluation". Tech. Rep. TR99-14, MSU (1999)
46. Jiang, X., Yau, W., Ser, W.: Detecting the fingerprint minutiae by adaptive tracing the gray level ridge. Pattern Recognition **34**, 999–1013 (2001)
47. Karu, K., Jain, A.: Fingerprint classification. Pattern Recognition **29**(3), 389–404 (1996)
48. Kawagoe, M., Tojo, A.: Fingerprint pattern classification. Pattern Recognition **17**, 295–303 (1984)
49. Kittler, J., Hatef, M., Duin, R., Matas, J.: On combining classifiers. IEEE Trans. on Pattern Analysis and Machine Intelligence **20**(3), 226–239 (1998)
50. Knutsson, H.: Filtering and reconstruction in image processing. Ph.D. thesis, Linköping University (1982)
51. Kovacs-Vajna, Z.: A fingerprint verification system based on triangular matching and dynamic time warping. IEEE Trans. on Pattern Analysis and Machine Intelligence **22**, 1266–1276 (2000)
52. Kovacs-Vajna, Z., Rovatti, R., Frazzoni, M.: Fingerprint ridge distance computation methodologies. Pattern Recognition **33**, 69–80 (2000)
53. Leung, M., Engeler, W., Frank, P.: Fingerprint image processing using neural network. Proc. IEEE Region 10 Conf. on Computer and Comm. Systems (1990)
54. Liu, J., Huang, Z., Chan, K.: Direct minutiae extraction from gray level fingerprint image by relationship examination. Proc. Int. Conf. on Image Processing **2**, 427–300 (2000)
55. Maio, D., Maltoni, D.: Direct gray scale minutiae detection in fingerprints. IEEE Trans. on Pattern Analysis and Machine Inteligence **19**(1), 27–40 (1997)
56. Maio, D., Maltoni, D.: Ridge-line density estimation in digital images. Proc. Int. Conf. on Pattern Recognition pp. 534–538 (1998)
57. Maio, D., Maltoni, D., Capelli, R., Wayman, J., Jain, A.: FVC2000: Fingerprint verification competition. IEEE Trans. on Pattern Analysis and Machine Intelligence **24**(3), 402–412 (2002)
58. Maio, D., Maltoni, D., Capelli, R., Wayman, J., Jain, A.: FVC2002: Second fingerprint verification competition. Proc. Intl. Conf. on Pattern Recognition, ICPR **3**, 811–814 (2002)
59. Maltoni, D., Maio, D., Jain, A., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, New York (2003)
60. Marcialis, G., Roli, F.: Fingerprint verification by fusion of optical and capacitive sensors. Pattern Recognition Letters **25**, 1315–1322 (2004)
61. Marcialis, G., Roli, F.: Fusion of multiple fingerprint matchers by single-layer perceptron with class-separation loss function. Pattern Recognition Letters **26**, 1830–1839 (2005)
62. Martinez-Diaz, M., Fierrez-Aguilar, J., Alonso-Fernandez, F., Ortega-Garcia, J., Siguenza, J.: Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST (2006)
63. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV **4677**, 275–289 (2002)
64. MCYT multimodal database http://atvs.ii.uam.es
65. Mehtre, B.: Fingerprint image analysis for automatic identification. Machine Vision and Applications **6**, 124–139 (1993)
66. Nandakumar, K., Jain, A.: Local correlation-based fingerprint matching. Proc. of Indian Conference on Computer Vision, Graphics and Image Processing pp. 503–508 (2004)

67. Nilsson, K.: Symmetry filters applied to fingerprints. Ph.D. thesis, Chalmers University of Technology, Sweden (2005)
68. Nilsson, K., Bigun, J.: Using linear symmetry features as a pre-processing step for fingerprint images. Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA **LNCS-2091**, 247–252 (2001)
69. NIST special databases and software from the image group – http://www.itl.nist.gov/iad/894.03/databases/defs/dbases.html
70. Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J., Vivaracho, C., Escudero, D., Moro, Q.: MCYT baseline corpus: a bimodal biometric database. IEE Proceedings on Vision, Image and Signal Processing **150**(6), 395–401 (2003)
71. Putte, T., Keuning, J.: Biometrical fingerprint recognition: dont get your fingers burned. Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App. pp. 289–303 (2000)
72. Ratha, N., Connell, J., Bolle, R.: An analysis of minutiae matching strength. Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA **LNCS-2091**, 223–228 (2001)
73. Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal **40**(3), 614–634 (2001)
74. Ross, A., Jain, A.: Biometric sensor interoperability: A case study in fingerprints. Proc. Workshop on Biometric Authentication, BIOAW **LNCS-3087**, 134–145 (2004)
75. Ross, A., Jain, A., Reisman, J.: A hybrid fingerprint matcher. Pattern Recognition **36**(7), 1661–1673 (2003)
76. Ross, A., Reisman, K., Jain, A.: Fingerprint matching using feature space correlation. Proc. Workshop on Biometric Authentication, BIOAW **LNCS-2359**, 48–57 (2002)
77. Schiel, F., Steininger, S., Trk, U.: The SmartKom multimodal corpus at BAS. Proc. Intl. Conf. on Language Resources and Evaluation (2002)
78. Schuckers, S., Parthasaradhi, S., Derakshani, R., Hornak, L.: Comparison of classification methods for time-series detection of perspiration as a liveness test in fingerprint devices. Proc. International Conference on Biometric Authentication, ICBA, **LNCS-3072**, 256–263 (2004)
79. Shen, L., Kot, A., Koo, W.: Quality measures of fingerprint images. Proc. 3rd International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA **LNCS-2091**, 266–271 (2001)
80. Simon-Zorita, D., Ortega-Garcia, J., Fierrez-Aguilar, J., Gonzalez-Rodriguez, J.: Image quality and position variability assessment in minutiae-based fingerprint verification. IEE Proceedings - Vis. Image Signal Process. **150**(6), 402–408 (2003)
81. Snelick, R., Uludag, U., Mink, A., Indovina, M., Jain, A.: Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. IEEE Trans. on Pattern Analysis and Machine Intelligence **27**(3), 450–455 (2005)
82. Uludag, U., Jain, A.: Attacks on biometric systems: a case study in fingerprints. Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI pp. 622–633 (2004)
83. Watson, C., Garris, M., Tabassi, E., Wilson, C., McCabe, R., Janet, S.: User's Guide to Fingerprint Image Software 2 – NFIS2 (http://fingerprint.nist.gov/NFIS). NIST (2004)
84. Wilson, C., Hicklin, R., Korves, H., Ulery, B., Zoepfl, M., Bone, M., Grother, P., Micheals, R., Otto, S., Watson, C.: Fingerprint Vendor Techonology Evaluation 2003: Summary of results and analysis report. NISTIR 7123, http://fpvte.nist.gov (2004)