Handbook of Fingerprint Recognition

Davide Maltoni
Dario Maio
Anil K. Jain
Salil Prabhakar

Second Edition

Handbook of Fingerprint Recognition

Springer

Davide Maltoni
Biometric Systems Lab (DEIS)
Università di Bologna
Via Sacchi, 3
47023 Cesena, Italy
maltoni@csr.unibo.it

Dario Maio
Biometric Systems Lab (DEIS)
Università di Bologna
Via Sacchi, 3
47023 Cesena, Italy
dmaio@deis.unibo.it

Anil K. Jain
Department of Computer Science
Michigan State University
3115, Engineering Building
East Lansing MI 48823, USA
jain@cse.msu.edu

Salil Prabhakar
DigitalPersona, Inc.
720 Bay Road
Redwood City CA 94063, USA
salilp@digitalpersona.com

ISBN: 978-1-84882-253-5 e-ISBN: 978-1-84882-254-2

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2009926293

Printed on acid-free paper

Springer Science+Business Media
springer.com

Contents

Preface

Overview

Biometric recognition, or simply biometrics, refers to the use of distinctive anatomical and behavioral characteristics or identifiers (e.g., fingerprints, face, iris, voice, hand geometry) for automatically recognizing a person. Questions such as “Is this person authorized to enter the facility?”, “Is this individual entitled to access the privileged information?”, and “Did this person previously apply for a passport?” are routinely asked in a variety of organizations in both public and private sectors. Traditional credential based systems no longer suffice to verify a person’s identity. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token- (e.g., keys or ID cards) or knowledge- (e.g., password or PIN) based methods. Biometric recognition provides better security, higher efficiency, and, in many instances, increased user convenience. It is for these reasons that biometric recognition systems are being increasingly deployed in a large number of government (e.g., border crossing, national ID card, e-passports) and civilian (e.g., computer network logon, mobile phone, Web access, smartcard) applications.

A number of biometric technologies have been developed and several of them have been successfully deployed. Among these, fingerprints, face, iris, voice, and hand geometry are the ones that are most commonly used. Each biometric trait has its strengths and weaknesses and the choice of a particular trait typically depends on the requirements of the application. Various biometric identifiers can also be compared on the following factors; universality, distinctiveness, permanence, collectability, performance, acceptability and circumvention. Because of the well-known distinctiveness (individuality) and persistence properties of fingerprints as well as cost and maturity of products, fingerprints are the most widely deployed biometric characteristics. It is generally believed that the pattern on each finger is unique. Given that there are about 6.5 billion living people on Earth and assuming each person has 10 fingers, there are 65 billion unique fingers! In fact, fingerprints and biometrics are often considered synonyms! Fingerprints were first introduced as a method for person identification over 100 years back. Now, every forensics and law enforcement agency worldwide routinely uses automatic fingerprint identification systems (AFIS). While law enforcement agencies were the earliest adopters of the fingerprint recognition technology, increasing concerns about national security, financial fraud and identity fraud have created a growing need for fingerprint technology for person recognition in a number of non-forensic applications.

Fingerprint recognition system can be viewed as a pattern recognition system. Designing algorithms capable of extracting salient features from fingerprints and matching them in a robust way are quite challenging problems. This is particularly so when the users are uncooperative, the finger surface is dirty or scarred and the resulting fingerprint image quality is poor. There is a popular misconception that automatic fingerprint recognition is a fully solved problem since automatic fingerprint systems have been around for almost 40 years. On the contrary, fingerprint recognition is still a challenging and important pattern recognition problem because of the large intra-class variability and large inter-class similarity in fingerprint patterns.

This book reflects the progress made in automatic techniques for fingerprint recognition over the past 4 decades. We have attempted to organize, classify and present hundreds of existing approaches to feature extraction and matching in a systematic way. We hope this book would be of value to researchers interested in making contributions to this area, and system integrators and experts in different application domains who desire to explore not only the general concepts but also the intricate details of this fascinating technology.

Objectives

The aims and objectives of this book are to:

- Introduce automatic techniques for fingerprint recognition. Introductory material is provided on all components/modules of a fingerprint recognition system.
- Provide an in-depth survey of the state-of-the-art in fingerprint recognition.
- Present in detail recent advances in fingerprint recognition, including sensing, feature extraction, matching and classification techniques, synthetic fingerprint generation, biometric fusion, fingerprint individuality and design of secure fingerprint systems.
- Provide a comprehensive reference book on fingerprint recognition, including an exhaustive bibliography.

Organization and Features

After an introductory chapter, the book chapters are organized logically into four parts: fingerprint sensing (Chapter 2); fingerprint representation, matching and classification (Chapters 3, 4, and 5); advanced topics, including synthetic fingerprint generation, biometric fusion, and fingerprint individuality (Chapters 6, 7, and 8); and fingerprint system security (Chapter 9).

Chapter 1 introduces biometric and fingerprint systems and provides some historical remarks on fingerprints and their adoption in forensic and civilian recognition applications. All the topics that are covered in detail in the successive chapters are introduced here in brief. This will provide the reader an overview of the various book chapters and let her choose a personalized reading path. Other non-technical but important topics such as “applications” and “privacy issues” are also discussed. Some background in image processing and pattern recognition techniques is necessary to fully understand the majority of the book chapters. To facilitate readers who do not have this background, references to basic readings on various topics are provided at the end of Chapter 1.

Chapter 2 surveys the existing fingerprint acquisition techniques: from the traditional “ink technique” to recent optical, capacitive, thermal, and ultrasonic live-scan fingerprint scanners, and discusses the factors that determine the quality of a fingerprint image. Chapter 2 also introduces the compression techniques that are used to efficiently store fingerprint images in a compact form.

Chapters 3, 4, and 5 provide an in-depth treatment of fingerprint feature extraction, matching and classification, respectively. Published techniques (in over 700 technical papers) are divided into various categories to guide the reader through the large number of approaches proposed in the literature. The main approaches are explained in detail to help beginners and practitioners in the field understand the methodology used in building fingerprint systems.

Chapters 6, 7, and 8 are specifically dedicated to the three cutting edge topics: synthetic fingerprint generation, biometric fusion, and fingerprint individuality, respectively. Synthetic fingerprints have been accepted as a reasonable substitute for real fingerprints for the design and benchmarking of fingerprint recognition algorithms. Biometrics fusion techniques (e.g., fusion of fingerprints with iris or fusion of multiple fingers) can be exploited to overcome some of the limitations in the state-of-the-art technology to build practical solutions. Scientific evidence supporting fingerprint individuality is being increasingly demanded, particularly in forensic applications, and this has generated interest in designing accurate fingerprint individuality models.

Finally, Chapter 9 discusses the security issues and countermeasure techniques that are useful in building secure fingerprint recognition systems.

From the First to the Second Edition

This second edition of the “Handbook of Fingerprint Recognition” is not a simple retouch of the first version. While the overall chapter structure has been maintained, a large amount of new information has been included in order to:

- Provide additional details on topics that were only briefly discussed in the first edition.
- Shed light on emerging issues or consolidated trends.
- Organize and generalize the underlying ideas of the approaches published in the literature. Over 500 papers on fingerprint recognition were published in the last 5 years (2003 to 2008) alone! Fingerprint recognition literature is sometimes chaotic and, due

to different (and often cumbersome) notations and conventions followed in the literature, it is not easy to understand the differences among the plethora of published algorithms. Instead of systematically describing every single algorithm, we focused our attention on the contributions that advanced the state-of-the-art. Of course, this is a very difficult task and we apologize for excessive simplification or selectivity that we may have introduced.

The total length of the handbook grew from about 350 to about 500 pages and the number of references increased from about 600 to about 1,200. Several new figures, drawings and tables have been added with the aim of making the presentation illustrative and lucid. The DVD included with the book now also contains the databases used in the 2004 Fingerprint Verification Competition (FVC2004). Table 1 summarizes the new content included in this edition of the Handbook.

Chapter	**New content**
1	– Improved presentation of need and benefits of fingerprint recognition systems – More comprehensive analysis of system errors and their causes – Application categories – Updated introduction to individual book chapters
2	– New sensing technologies (e.g., multispectral imaging) – Image quality specifications (IQS) – Operational quality of fingerprint scanners – Examples of 1,000 dpi and multi-finger scanners – Examples of commercial single-finger scanners
3	– Level 3 features (pores, incipient ridges, creases) – Wider coverage of the methods for estimating ridge orientations – Learning-based segmentation techniques – Improved methods for singularity detection – Advances in fingerprint enhancement – Minutiae encoding standards – Estimation of fingerprint quality
4	– Advanced correlation filters – Computation of similarity score – Orientation image-based relative pre-alignment – Evolution of two-stage approaches: local structure matching + consolidation – Fingerprint distortion models – Improvements in texture-based matching – Fingerprint comparison based on Level 3 features

	– Fingerprint databases and recent third party evaluations – Interoperability of fingerprint recognition algorithms
5	– Improved exclusive classification techniques – Advances in continuous classification and fingerprint indexing – Performance evaluation on common benchmarks
6	– Physical and statistical models for fingerprint generation – Automatic generation of ground truth features corresponding to the synthetic images – Testing feature-extractor conformance to standards
7	– Major rewrite of the chapter with systematic presentation of fusion methods – More in-depth coverage of fusion methods and published techniques – Advances in image, feature, and score fusion techniques
8	– Coverage of the recent finite mixture minutiae placement model
9	– Major rewrite of the chapter with systematic presentation of security techniques – Advances in match-on-card (MoC) and system-on-a-chip (SoC) – Advances in template protection

Table 1. New content included in the Handbook.

Contents of the DVD

The book includes a DVD that contains the 12 fingerprint databases used in the 2000, 2002 and 2004 Fingerprint Verification Competitions (FVC). The DVD also contains a demonstration version of the SFINGE software that can be used to generate synthetic fingerprint images. These real and synthetic fingerprint images will allow interested readers to evaluate various modules of their own fingerprint recognition systems and to compare their developments with the state-of-the-art algorithms.

Intended Audience

This book will be useful to researchers, practicing engineers, system integrators and students who wish to understand and/or develop fingerprint recognition systems. It would also serve as a reference book for a graduate course on biometrics. For this reason, the book is written in an informal style and the concepts are explained in a simple language. A number of examples and figures are presented to visualize the concepts and methods before giving any mathematical definition. Although the core chapters on fingerprint feature extraction, matching and classification require some background in image processing and pattern recognition, the introduction, sensing and security chapters are accessible to a wider audience (e.g., developers of biometric applications, system integrators, security managers, designers of security systems).

Acknowledgments

A number of individuals helped in making this book a reality. Raffaele Cappelli of the University of Bologna wrote Chapter 6 on synthetic fingerprints, Alexander Ivanisov of Digital Persona Inc. provided invaluable suggestions throughout several revisions of Chapter 9, and Sharath Pankanti of the IBM T. J. Watson Research Center, Arun Ross of West Virginia University, and Abhishek Nagar of Michigan State University provided some portions of text and figures in Chapters 1, 7, and 8. We also thank Wayne Wheeler at Springer, for his encouragement in revising the first edition of this book.

The first edition of the book received many positive feedbacks from readers and colleagues; the book also received the prestigious 2003 PSP award for the "Computer Science" category given by the Association of American Publishers. These accolades motivated us in our efforts to prepare this new edition of the book. One suggestion we received from several readers was to identify and focus on only the most effective algorithms for various stages of a fingerprint recognition system. While this would be very useful, it is not easy to make such a selection. All the evaluation studies on common benchmarks (e.g., FVC databases) are concerned with the accuracy of the entire recognition system. Therefore, it is not possible to determine if the performance improvement is due to a specific matching technique or is in large part due to a minor change to an existing feature extraction method. The only way to objectively compare algorithms is to factor out all the possible difference in the pre- or post- stages. Forthcoming FVC-onGoing (2009) is being organized with such an aim.

This book explores automatic techniques for fingerprint recognition, from the earliest approaches to the current state-of-the-art algorithms. However, with the development of novel sensor technologies, availability of faster processors at lower cost, and emerging applications of fingerprint recognition systems, there continues to be a vigorous activity in the design and development of faster, highly accurate, and robust algorithms. As a result, new algorithms for fingerprint recognition will continue to appear in the literature even after this book goes to press. We hope that the fundamental concepts presented in this book will provide some principled and proven approaches in the rapidly evolving and important field of automatic fingerprint recognition.

April 2009

Davide Maltoni
Dario Maio
Anil K. Jain
Salil Prabhakar

1
Introduction

1.1 Introduction

More than a century has passed since Alphonse Bertillon first conceived and then industriously practiced the idea of using body measurements for solving crimes (Rhodes, 1956). Just as his idea was gaining popularity, it faded into relative obscurity by a far more significant and practical discovery of the distinctiveness of the human fingerprints. In 1893, the Home Ministry Office, UK, accepted that no two individuals have the same fingerprints. Soon after this discovery, many major law enforcement departments saw potential of fingerprints in identifying repeat offenders who used an alias, i.e., changed their names with each arrest to evade the harshest penalties reserved for recidivists in law. The law enforcement departments embraced the idea of "booking" the fingerprints of criminals at the time of arrest, so that their records are readily available for later identification. Fingerprints found an application in forensics. By matching leftover fingerprint smudges (latents) from crime scenes to fingerprints collected during booking, authorities could determine the identity of criminals who have been previously arrested. The law enforcement agencies sponsored a rigorous study of fingerprints, developed scientific methods for visual matching of fingerprints and instituted strong programs/cultures for training fingerprint experts. They successfully applied the art of fingerprint recognition for nailing down the perpetrators (Scott (1951); Lee and Gaensslen (2001)).

Despite the ingenious methods improvised to increase the efficiency of the manual approach to fingerprint indexing and matching, the ever growing demands on fingerprint recognition quickly became overwhelming. The manual method of fingerprint indexing (based on the Henry system of classification) resulted in a highly skewed distribution of fingerprints into bins (types): most fingerprints fell into a few bins and this did not improve the search efficiency. Fingerprint training procedures were time-intensive and slow. Furthermore, demands imposed by the painstaking attention needed to visually compare two fingerprints of varied qualities, tedium of the monotonous nature of the work, and increasing workloads due to a higher demand on fingerprint recognition services, all prompted the law enforcement agencies to initiate research into acquiring fingerprints through electronic media and automate fingerprint recognition based on the digital representation of fingerprints. These efforts led to the development of *Automatic Fingerprint Identification Systems* (AFIS) over the past 4 decades. Law enforcement agencies were the earliest adopters of the automatic fingerprint recognition technology. More recently, however, increasing concerns about security and identity fraud

D. Maltoni et al., *Handbook of Fingerprint Recognition*, 1–56.

have created a growing need for fingerprint and other biometric technologies for person recognition in a large number of non-forensic applications.

1.2 Biometric Recognition

As our society has become electronically connected and more mobile, surrogate representations of identity such as passwords (prevalent in electronic access control) and cards (prevalent in banking and government applications) cannot be trusted to establish a person's identity. Cards can be lost or stolen and passwords or PIN can, in most cases, be guessed. Further, passwords and cards can be easily shared and so they do not provide non-repudiation.

Biometric recognition (or simply biometrics) refers to the use of distinctive *anatomical* (e.g., fingerprints, face, iris) and *behavioral* (e.g., speech) characteristics, called *biometric identifiers* or *traits* or *characteristics* for automatically recognizing individuals. Biometrics is becoming an essential component of effective person identification solutions because biometric identifiers cannot be shared or misplaced, and they intrinsically represent the individual's bodily identity. Recognition of a person by their body, then linking that body to an externally established "identity", forms a very powerful tool of identity management with tremendous potential consequences, both positive and negative. Consequently, biometrics is not only a fascinating pattern recognition research problem but, if carefully used, is an enabling technology with the potential to make our society safer, reduce fraud and provide user convenience (user friendly man–machine interface).

The word *biometrics* is derived from the Greek words *bios* (meaning life) and *metron* (meaning measurement); biometric identifiers are measurements from living human body. Perhaps all biometric identifiers are a combination of anatomical and behavioral characteristics and they should not be exclusively classified into either anatomical or behavioral characteristics. For example, fingerprints are anatomical in nature but the usage of the input device (e.g., how a user presents a finger to the fingerprint scanner) depends on the person's behavior. Thus, the input to the recognition engine is a combination of anatomical and behavioral characteristics. Similarly, speech is partly determined by the vocal tract that produces speech and partly by the way a person speaks. Often, a similarity can be noticed among parents, children, and siblings in their speech. The same argument applies to the face: faces of identical twins may be extremely similar at birth but during their growth and development, the faces change based on the person's behavior (e.g., lifestyle differences leading to a difference in bodyweight, etc.).

A number of questions related to a person's identity are asked everyday in a variety of contexts. Is this person authorized to enter the facility? Is this individual entitled to access privileged information? Is this person wanted for a crime? Has this person already received certain benefits? Is the given service being administered exclusively to the enrolled users? Reliable answers to questions such as these are needed by business and government organizations. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token (ID cards) or knowledge-based (passwords or PIN) methods. The objectives of biometric recognition are user convenience (e.g., money withdrawal at an ATM machine without a card or PIN), better security (e.g., only authorized person can enter a facility), better accountability (e.g., difficult to deny having accessed confidential records), and higher efficiency (e.g., lower overhead than computer password maintenance). The tremendous success of fingerprint-based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all resulted in increasing use of fingerprint-based person recognition in commercial, government, civilian, and financial domains. In addition to fingerprints, some other traits, primarily hand shape, voice, iris and face have also been successfully deployed.

Thanks to the imaginative and flattering depiction of fingerprint systems in nightly television crime shows (e.g., CSI), the general perception is that automatic fingerprint identification is a foolproof technology! This is not true. There are a number of challenging issues that need to be addressed in order to broaden the scope of niche market for fingerprint recognition systems.

1.3 Biometric Systems

An important issue in designing a practical *biometric system* is to determine how an individual is going to be recognized. Depending on the application context, a biometric system may be called either a *verification* system or an *identification* system:

- A verification system authenticates a person's identity by comparing the captured biometric characteristic with her previously captured (enrolled) biometric reference template pre-stored in the system. It conducts one-to-one comparison to confirm whether the claim of identity by the individual is true. A verification system either rejects or accepts the submitted claim of identity.
- An identification system recognizes an individual by searching the entire enrollment template database for a match. It conducts one-to-many comparisons to establish if the individual is present in the database and if so, returns the identifier of the enrollment reference that matched. In an identification system, the system establishes a subject's identity (or determines that the subject is not enrolled in the system database) without the subject having to claim an identity.

The term *authentication* is also used in the biometric field, sometimes as a synonym for verification; actually, in the information technology language, authenticating a user means to let the system know the identity of the user regardless of the mode (verification or identification). Throughout this book we use the generic term *recognition* where we are not interested in distinguishing between verification and identification.

The block diagrams of verification and identification systems are depicted in Figure 1.1; user enrollment, which is common to both tasks is also graphically illustrated.

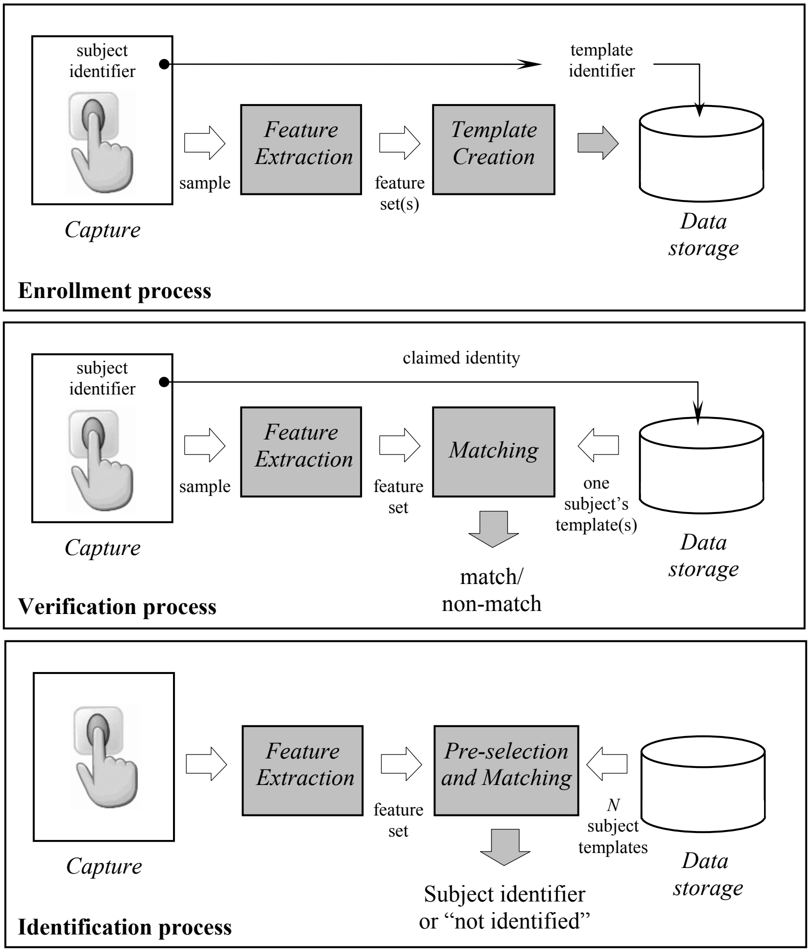

Figure 1.1. Enrollment, verification, and identification processes. These processes use the following modules: capture, feature extraction, template creation, matching, pre-selection, and data storage. In the identification process pre-selection and matching are often combined.

The enrollment, verification, and identification processes involved in user recognition make use of the following system modules:

- *Capture*: a digital representation of biometric characteristic needs to be sensed and captured. A biometric sensor, such as a fingerprint scanner, is one of the central pieces of a biometric capture module. The captured digital representation of the biometric characteristic is often known as a *sample*; for example, in the case of a fingerprint system, the raw digital fingerprint image captured by the fingerprint scanner is the sample. The data capture module may also contain other components (e.g., a keyboard and screen) to capture other (non-biometric) data.
- *Feature extraction*: in order to facilitate matching or comparison, the raw digital representation (sample) is usually further processed by a *feature extractor* to generate a compact but expressive representation, called a *feature set*.
- *Template creation*: the template creation module organizes one or more feature sets into an *enrollment template* that will be saved in some persistent storage. The enrollment template is sometimes also referred to as a *reference*.
- *Pre-selection and matching*: the pre-selection (or filtering) stage is primarily used in an identification system when the number of enrolled templates is large. Its role is to reduce the effective size of the template database so that the input needs to be matched to a relatively small number of templates. The matching (or comparison) stage (also know as a *matcher*) takes a feature set and an enrollment template as inputs and computes the similarity between them in terms of a *matching score*, also known as *similarity score*. The matching score is compared to a *system threshold* to make the final decision; if the match score is higher than the threshold, the person is recognized, otherwise not.
- *Data storage*: is devoted to storing templates and other demographic information about the user. Depending on the application, the template may be stored in internal or external storage devices or be recorded on a smart card issued to the individual.

Using these five modules, three main processes can be performed, namely, enrollment, verification, and identification. A verification system uses the enrollment and verification processes while an identification system uses the enrollment and identification processes. The three processes are:

- *Enrollment*: user enrollment is a process that is responsible for registering individuals in the biometric system storage. During the enrollment process, the biometric characteristic of a subject is first captured by a biometric scanner to produce a sample. A quality check is often performed to ensure that the acquired sample can be reliably processed by successive stages. A feature extraction module is then used to produce a feature set. The template creation module uses the feature set to produce an enrollment template. Some systems collect multiple samples of a user and then either select the best image (or feature set) or fuse multiple images (or feature sets) to create a composite template. The enrollment process then takes the enrollment template and stores it in the system storage together with the demographic information about the user (such as an identifier, name, gender, height, etc.).

- *Verification*: the verification process is responsible for confirming the claim of identity of the subject. During the recognition phase, an identifier of the subject (such as username or PIN [Personal Identification Number]) is provided (e.g., through a keyboard or a keypad or a proximity card) to claim an identity; the biometric scanner captures the characteristic of the subject and converts it to a sample, which is further processed by the feature extraction module to produce a feature set. The resulting feature set is fed to the matcher, where it is compared against the enrollment template(s) of that subject (retrieved from the system storage based on the subject's identifier). The verification process produces a match/non-match decision.
- *Identification*: in the identification process, the subject does not explicitly claim an identity and the system compares the feature set (extracted from the captured biometric sample) against the templates of all (or a subset of) the subjects in the system storage; the output is a *candidate list* that may be empty (if no match is found) or contain one (or more) identifier(s) of matching enrollment templates. Because identification in large databases is computationally expensive, a pre-selection stage is often used to filter the number of enrollment templates that have to be matched against the input feature set.

Depending on the application domain, a biometric system could operate either as an *on-line* system or an *off-line* system. An on-line system requires the recognition to be performed quickly and an immediate response is imposed (e.g., a computer network logon application). On the other hand, an off-line system does not require the recognition to be performed immediately and a relatively longer response delay is allowed (e.g., background check of an applicant). On-line systems are often *fully automatic* and require that the biometric characteristic be captured using a live-scan scanner, the enrollment process be unattended, there be no (manual) quality control, and the matching and decision making be fully automatic. Off-line systems, however, are often *semi-automatic*, where the biometric acquisition could be through an off-line scanner (e.g., scanning a fingerprint image from a latent or inked fingerprint card), the enrollment may be supervised (e.g., when a suspect is "booked," a police officer guides the fingerprint acquisition process), a manual quality check may be performed to ensure good quality acquisition, and the matcher may return a list of candidates which are then manually examined by a forensic expert to arrive at a final decision.

The verification and identification processes differ in whether an identity is claimed or not by the subject. A biometric *claim* (or *claim of identity*) is defined as the implicit or explicit claim that a subject *is* or *is not* the source of a specified or unspecified biometric enrollment template. A claim may be:

- *Positive*: the subject is enrolled.
- *Negative*: the subject is not enrolled.
- *Specific*: the subject is or is not enrolled as a specified biometric enrollee.
- *Non-specific*: the subject is or is not among a set or subset of biometric enrollees.

The application context defines the type of claim. In certain applications, it is in the interest of the subject to make a positive claim of identity. Such applications are typically trying to prevent multiple people from using the same identity. For example, if only Alice is authorized to enter a certain secure area, then it is in the interest of any subject to make a positive claim of identity (of being Alice) to gain access. But the system should grant access only to Alice. If the system fails to match the enrolled template of Alice with the input feature set, access is denied, otherwise, access is granted. In other applications, it is in the interest of the subject to make a negative claim of identity. Such applications are typically trying to prevent a single person from using multiple identities. For example, if Alice has already received certain welfare benefits, it is in her interest to now make a negative claim of identity (that she is not among the people who have already received benefits), so that she can double-dip. The system should establish that Alice's negative claim of identity is false by finding a match between the input feature set of Alice and enrollment templates of all people who have already received the benefits.

The following three types of claims are used depending on the application context:

- *Specific positive claim*: applications such as logical access control (e.g., network-logon) may require a specific positive claim of identity (e.g., through a username or PIN). A verification biometric system is sufficient in this case to confirm whether the specific claim is true or not through a one-to-one comparison.
- *Non-specific positive claim*: applications such as physical access control may assume a non-specific positive claim that the subject is someone who is authorized to access the facility. One of the advantages of this scenario is that the subject does not need to make a specific claim of identity (no need to provide a username, PIN, or any other token), which is quite convenient. However, the disadvantage of this scenario is that an identification biometric system is necessary (which has longer response time and lower accuracy due to one-to-many comparisons).
- *Non-specific negative claim*: applications such as border crossing typically assume a non-specific negative claim, i.e., the subject is not present in a "watch list". Again, an identification system must be used in this scenario. Note that such applications cannot use traditional knowledge-based or possession-based methods of recognition. Surrogates tokens such as passports have been traditionally used in such applications but if passports are forged (or if people obtain duplicate passports under different names), traditional recognition methods cannot solve the problem of duplicate identities or *multiple enrollments*.

1.4 Comparison of Traits

Any human anatomical or behavioral trait can be used as a biometric identifier to recognize a person as long as it satisfies the following requirements:

- *Universality:* each person should possess the biometric trait.
- *Distinctiveness*: any two persons should be sufficiently different in terms of their biometric traits.
- *Permanence*: biometric trait should be invariant (with respect to the matching criterion) over time.
- *Collectability*: biometric trait can be measured quantitatively.

However, in a practical biometric system, there are a number of other issues that should be considered in selecting a trait, including:

- *Performance*: recognition accuracy, speed (throughput), resource requirements, and robustness to operational and environmental factors.
- *Acceptability*: extent to which users are willing to accept the biometric identifier in their daily lives.
- *Circumvention*: ease with which the biometric system can be circumvented by fraudulent methods.

A practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, harmless to the users, accepted by the intended population, and sufficiently robust to various fraudulent methods.

A number of biometric traits are in use in various applications. Each biometric trait has its own strengths and weaknesses and the choice typically depends on the application. No single trait is expected to effectively meet the requirements of all the applications. The match between a biometric trait and an application is determined depending upon the characteristics of the application and the properties of the trait. Some of the issues that need to be addressed in selecting a biometric trait for a particular application are:

- Does the application need a verification or identification system? If an application requires an identification of a subject from a large database, it needs a very distinctive biometric trait (e.g., fingerprints or iris).
- What are the operational characteristics of the application? For example, is the application attended (semi-automatic) or unattended (fully automatic)? Are the users habituated (or willing to become habituated) to the given biometric? Is the application covert or overt? Are subjects cooperative or non-cooperative?
- What is the template storage requirement of the application? For example, an application that performs the recognition on a smart card may require a small template size.
- How stringent are the performance requirements? For example, an application that demands very high accuracy needs a more distinctive biometric.

- What types of biometric traits are acceptable to the target user population? Biometric traits have different degrees of acceptability in different demographic regions depending on the cultural, ethical, social, religious, and hygienic standards. The acceptability of a biometric in an application is often a compromise between the sensitivity of the targeted population to various perceptions or taboos and the value or convenience offered by biometrics-based recognition.

A brief introduction to the most common biometric traits is provided below. We do not cover fingerprints in this list since it is extensively covered in the rest of this book. Figure 1.2 shows several biometric traits that have been either adopted in commercial systems or are being investigated.

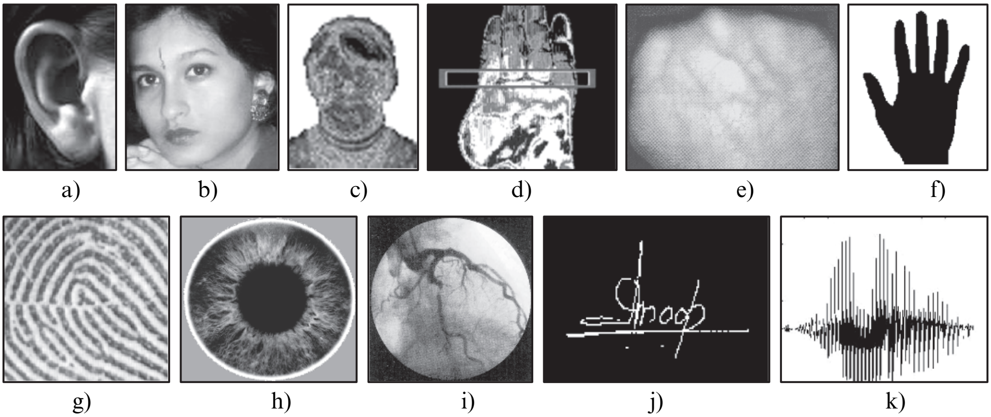

Figure 1.2. Examples of biometrics traits: a) ear, b) face, c) facial thermogram, d) hand thermogram, e) hand vein, f) hand geometry, g) fingerprint, h) iris, i) retina, j) signature, and k) voice.

- *Iris*: visual texture of the human iris is determined by the chaotic morphogenetic processes during embryonic development and is posited to be distinctive for each person and each eye (Daugman, 1999). An iris image is typically captured using a non-contact imaging process. Capturing an iris image often involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera. The iris recognition technology has been shown to be extremely accurate and fast on high resolution well-captured iris images.
- *Face*: face is one of the most acceptable biometric traits because it is one of the most common methods of recognition that humans use in their daily visual interactions. In addition, the method of acquiring face images is nonintrusive. Facial disguise is of

concern in unattended recognition applications. It is very challenging to develop face recognition techniques that can tolerate the effects of aging, facial expression, variations in the imaging environment, and facial pose with respect to the camera.

- *Hand and finger geometry*: some features related to the human hand (e.g., length of fingers) are relatively invariant and peculiar (although not very distinctive) to an individual. The image acquisition system requires cooperation of the subject to capture frontal and side view images of the palm flatly placed on a panel with outstretched fingers. The template storage requirements of the hand are very small, which is an attractive feature for bandwidth- and memory-limited systems. Due to its limited distinctiveness, hand geometry-based systems are only used for verification and do not scale well for identification applications. Finger geometry systems (which measure the geometry of at most two fingers as opposed to the whole hand) may be preferred because of their compact size.
- *Hand or finger vein*: near-infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Veins could also be detected in a finger using infra-red or near-infra-red sensing. Systems for vein capture use inexpensive infra-red light emitting diodes (LEDs), leading to commercial systems for hand and finger vein biometrics.
- *Voice*: voice capture is unobtrusive and voice may be the only feasible biometric in applications requiring person recognition over a telephone. Voice is not expected to be sufficiently distinctive to permit identification of an individual from a large database of identities. Moreover, a voice signal available for recognition is typically degraded in quality by the microphone, communication channel, and digitizer characteristics. Voice is also affected by factors such as a person's health (e.g., cold), stress and emotional state. Besides, some people seem to be extraordinarily skilled in mimicking others voice.
- *Signature*: the way a person signs his name is known to be a characteristic of that individual. Signatures have been acceptable in government, legal, and commercial transactions as a method of verification for a long time. Signature is a behavioral biometric that changes over time and is influenced by physical and emotional conditions of the signatories. Signatures of some subjects vary a lot: even successive impressions of their signature are significantly different. Furthermore, professional forgers can reproduce signatures of others to fool the unskilled eye.

The biometric identifiers described above are compared in Table 1.1. Note that fingerprint has a nice balance among all the desirable properties. Every human being possesses fingers (with the exception of hand-related disability) and hence fingerprints. Fingerprints are very distinctive (see Chapter 8) and they are permanent; even if they temporarily change slightly due to cuts and bruises on the skin, the fingerprint reappears after the finger heals. Live-scan fingerprint scanners can easily capture high-quality fingerprint images and unlike face recognition, they do not suffer from the problem of segmenting the fingerprint from the background. However, they are not suitable for covert applications (e.g., surveillance) as live-scan fingerprint scanners cannot capture a fingerprint image from a distance and without the knowledge of the person. The deployed fingerprint recognition systems offer good performance and fingerprint scanners have become quite compact and affordable (see Chapter 2). Because fingerprints have a long history of use in forensic divisions worldwide for criminal investigations, they have some stigma of criminality associated with them. However, this is rapidly changing with the high demand for automatic person recognition to fight identity fraud and security threats. With a layered approach involving fingerprint and other security technologies, fingerprint systems are difficult to circumvent (see Chapter 9). Fingerprint recognition is one of the most mature biometric technologies and is suitable for a large number of recognition applications. This is also reflected in the revenues generated by various biometric technologies (see Figure 1.3).

Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Hand/finger vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1.1. Comparison of commonly used biometric traits. Entries in the table are based on the perception of the authors. High, Medium, and Low are denoted by H, M, and L, respectively.

1.5 System Errors

The critical promise of the ideal biometric trait is that when a sample is presented to the biometric system, it will offer the correct decision. In practice, a biometric system is a pattern recognition system that inevitably makes some incorrect decisions. Let us first try to understand why a biometric system makes errors and then discuss the various types of errors. We also encouraged the readers to refer to ISO/IEC 19795-2 (2007) and to the other sections of ISO/IEC 19795 for a comprehensive treatment of biometric system errors.

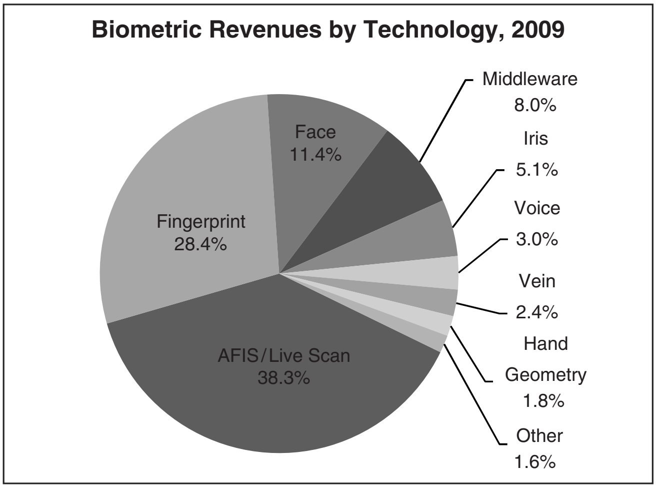

Figure 1.3. Revenue by biometric traits as estimated by International Biometric Group in 2009. Fingerprint-based systems (both forensic and non-forensic applications) continue to be the leading biometric technology in terms of market share, commanding more than 50% of biometric revenue.

1.5.1 Reasons behind system errors

There are three primary reasons that explain the errors made by a biometric system (see Jain et al. (2004b)):

- *Information limitation*: the invariant and distinctive information content in the biometric samples may be inherently limited due to the intrinsic signal capacity (e.g., individuality information) of the biometric identifier. For instance, the distinctive information in hand geometry is less than that in fingerprints. Consequently, hand geometry measurements can differentiate fewer identities than fingerprint even under ideal conditions. Information limitation may also be due to poorly controlled biometric presentation by the users (user interface issue) or inconsistent signal acquisition. Differently acquired measurements of a biometric identifier limit the invariance across different samples of the pattern. For example, information limitation occurs when there is very little overlap between the enrolled and sample fingerprints (e.g., left and right half of the finger). In such situations, even a perfect matcher cannot offer a correct decision. An extreme example of information limitation is when the person does not possess or cannot present the particular biometric needed by the identification system (e.g., amputees with missing hands and fingers).

- *Representation limitation*: the ideal representation scheme should be designed to retain all the invariance as well as discriminatory information in the sensed measurements. Practical feature extraction modules, typically based on simplistic models of biometric signal, fail to capture the richness of information in a realistic biometric signal resulting in the inclusion of erroneous features and exclusion of true features. Consequently, a fraction of legitimate pattern space cannot be handled by the biometric system, resulting in errors.
- *Invariance limitation*: finally, given a representation scheme, the design of an ideal matcher should perfectly model the invariance relationship among different patterns from the same class (user), even when imaged under different presentation conditions. Again, in practice (e.g., due to non-availability of sufficient number of training samples, uncontrolled or unexpected variance in the collection conditions) a matcher may not correctly model the invariance relationship resulting in matcher errors.

The challenge is to be able to arrive at a realistic and invariant representation of the biometric identifier from a few samples acquired under inconsistent conditions, and then, formally estimate the discriminatory information in the signal from the samples. This is especially difficult in a large-scale identification system where the number of enrolled users is huge (e.g., in the millions).

1.5.2 Capture module errors

In a fully automated biometric system, the biometric data is captured without human supervision and assistance. Such a biometric system typically uses a live-scan device that automatically detects the presence of a biometric characteristic as it appears in the field of view. For example, a live-scan fingerprint scanner may wait in a low-power-consumption mode, with a finger detection algorithm continually polling for the approach/presence of a finger. When the finger detection algorithm detects a finger, the scanner may switch to a finger capture mode to automatically capture a good quality fingerprint image. The automated biometric capture system can produce two types of errors: *Failure To Detect* (FTD) and *Failure To Capture* (FTC). Failure to detect error occurs when a finger indeed approaches the fingerprint scanner but the scanner fails to detect its presence. The failure to capture error occurs when the system knows that a finger is present but fails to capture a sample. The rate of these two failures is usually inversely proportions to each other. These failures occur when either the captured image is of very poor quality (e.g., if the scanner surface is dirty) or when the capture module is used inappropriately (e.g., only tip of the finger instead of the central pad of the finger is presented to the scanner or a finger is moved across on a swipe scanner with dramatically varying speed and skew).

1.5.3 Feature extraction module errors

After capture the biometric sample is sent to the feature extraction module for processing. If the captured image is of poor quality, the feature extraction algorithm may fail to extract a usable feature set. This error is known as *Failure To Process* (FTP). Since capture module and feature extraction module are common to all the processes (enrollment, verification, and identification), the three types of errors (FTD, FTC, and FTP) mentioned here are often combined into one single measure called the *Failure To Acquire* (FTA). A high FTA rate will affect the throughput of the resulting biometric system and increase user frustration. One way to lower FTA is by increasing the sensitivity of the capture and feature extraction modules. But this will put additional burden on the later modules (such as matching).

1.5.4 Template creation module errors

The template creation module that takes one (or more) feature sets extracted from samples during the enrollment process and produces a template may also fail. Again, this typically happens either when there is not enough discriminatory information present in the feature sets (e.g., too small fingerprint area) or when the fingerprint images are of poor quality and consequently the feature set(s) are very noisy. Since template creation module is used only in the enrollment process and is the most critical part of the enrollment process, the failure of template creation module is known as *Failure To Enroll* (FTE). There is a tradeoff between the FTE rate and the error rates of the matching module discussed below. If the failure to enroll is disabled, then templates can be created from poor quality fingerprints but such noisy templates would result in higher matching errors.

1.5.5 Matching module errors

The result of a fingerprint matching module is typically a matching score (without loss of generality, lying in the interval [0,1]) that quantifies the similarity between the recognition feature set and the enrollment template. The closer the score is to 1, the more certain is the system that the recognition feature set comes from the same finger as the enrollment template. The decision module regulates its decision by using a threshold t; pairs of feature set and template generating scores higher than or equal to t are inferred as *matching pairs* (i.e., belonging to the same finger) and pairs of feature set and template generating scores lower than t are inferred as *non-matching pairs* (i.e., belonging to different fingers).

When the matching module is operating in a one-to-one comparison mode (it compares feature set from one finger with template from one finger), it gives a *match* or *non-match* decision depending on whether the comparison score exceeded the threshold or not, respectively. The matching module, operating in one-to-one comparison mode, can commit two types of errors: (i) mistaking feature set and template from two different fingers to be from the same finger (called *false match*), and (ii) mistaking feature set and template from the same finger to be from two different fingers (called *false non-match*).

It is important to understand the difference between false match and false non-match errors and the more commonly used *false acceptance* and *false rejection* errors. The false match and false non-match are errors of the matching module in one-to-one comparison mode while false acceptance and false rejection are the error rates associated with verification and identification processes and in fact their exact meaning is dependent upon the type of identity claim made by the user. For example, in applications with positive claim of identity (e.g., an access control system) a false match from the matching module results in the false acceptance of an impostor into the system, whereas a false non-match from the matching module causes the false rejection of a genuine user in the system. On the other hand, in an application with negative claim of identity (e.g., preventing users from obtaining welfare benefits under false identities), a false match from the matching module results in rejecting a genuine request, whereas a false non-match from the matching module results in falsely accepting an impostor request. Further, an application may use other criteria for acceptance/rejection in addition to match/non-match decision. The notion of "false match/false non-match" is not application dependent and therefore, in principle, is more appropriate than "false acceptance/false rejection". However, the use of false acceptance (and False Acceptance Rate, abbreviated as FAR) and false rejection (and False Rejection Rate, abbreviated as FRR) is more popular, especially in the commercial sector. In the rest of this book, while we will try to avoid the use of false acceptance and false rejection, they are synonyms for false match and false non-match, respectively.

When a biometric system operates in the identification mode, matching module works in one-to-many comparison mode. In its simplest form, one-to-many comparison against N templates can be viewed as a series of N one-to-one comparisons. If identification is performed only for subjects who are present in the enrollment database, the identification is known as *closed-set identification*. Closed-set identification always returns a non-empty candidate list. While closed-set identification has been studied extensively by researchers, it is rarely used in practice. In *open-set identification*, some of the identification attempts are made by subjects who are not enrolled. In the rest of this book when we refer to identification we will focus only on the open-set scenario. If the matching module is given a feature set from finger A and a set of templates that includes at least one template of A, and the matching module produces an empty candidate list, the error is called a *false negative identification error*. If the matching module is given a feature set from finger A and a set of templates that does not include any template from A, and the matching module returns a non-empty candidate list, the error is called a *false positive identification error*.