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