Handbook of Fingerprint Recognition

Springer
New York
Berlin
Heidelberg
Hong Kong
London
Milan
Paris
Tokyo

Davide Maltoni
Dario Maio
Anil K. Jain
Salil Prabhakar

Handbook of Fingerprint Recognition

With 178 Illustrations

Davide Maltoni
Biometric Systems Laboratory
University of Bologna
Cesena, 47023
Italy
maltoni@csr.unibo.it

Dario Maio
DEIS-CSITE
University of Bologna
Bologna, 40136
Italy
dmaio@deis.unibo.it

Anil K. Jain
Department of Computer Science
and Engineering
Michigan State University
East Lansing, MI 48824
USA
jain@cse.msu.edu

Salil Prabhakar
DigitalPersona. Inc.
Redwood City, CA 94063
USA
salil@digitalpersona.com

Library of Congress Cataloging-in-Publication Data
Handbook of fingerprint recognition / Davide Maltoni . . . [et al.]
p. cm.
Includes bibliographical references and index.
ISBN 0-387-95431-7 (alk. paper)
1. Fingerprints—Identification. 2. Fingerprints—Classification I. Maltoni, Davide
HV6074.H25 2003
363.25′8—dc21 2003042439

ISBN 0-387-95431-7 Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 10864422

www.springer-ny.com

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

Contents

Preface

Overview

Biometric recognition refers to the use of distinctive physiological and behavioral characteristics (e.g., fingerprints, face, hang geometry, iris, gait, signature), called biometric identifiers or simply biometrics, 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 job?" are routinely asked in a variety of organizations in both public and private sectors. 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 knowledge- (e.g., password) based methods. Biometric recognition can provide better security, higher efficiency, and increased user convenience. It is for these reasons that biometric systems are being either increasingly deployed or evaluated in a large number of government (e.g., welfare disbursement, national ID card, issuing of driver's license) and civilian (e.g., computer network logon, automatic teller machine, cellular phone, Web access, smartcard) applications.

A number of biometric technologies have been developed and several of them are being used in a variety of applications. Among these, fingerprints, face, iris, speech, and hand geometry are the ones that are most commonly used. Each biometric has its strengths and weaknesses and the choice of a particular biometric typically depends on the requirements of an 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 over time, fingerprints are the most widely used biometric characteristics. In fact, fingerprints and biometrics are often considered synonyms! Fingerprints have been routinely used in the forensics community for over one hundred years and automatic fingerprint identification systems were first installed almost fifty years back. While law enforcement agencies were the earliest adopters of the fingerprint recognition technology, more recently, increasing identity fraud has created a growing need for biometric technology for person recognition in a number of non-forensic applications.

Fingerprint recognition is a complex pattern recognition problem; designing algorithms capable of extracting salient features and matching them in a robust way is quite hard, espe-

cially in poor quality fingerprint images. There is a popular misconception that automatic fingerprint recognition is a fully solved problem since it was one of the first applications of machine pattern recognition almost fifty years ago. On the contrary, fingerprint recognition is still a challenging and important pattern recognition problem.

This book reflects the progress made in automatic techniques for fingerprint recognition over the past four decades. We attempted to organize, classify and present hundreds of existing approaches in a systematic way. We believe this would greatly facilitate both beginners and experts of 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 the readers to 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, multimodal biometric systems, fingerprint individuality, and design of secure fingerprint systems;
- serve as the first complete 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 fingerprints, multimodal biometric systems, and fingerprint individuality (Chapters 6, 7, and 8); and securing fingerprint systems (Chapter 9).

Chapter 1 introduces biometric 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 and introductory surveys 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 on-line scanners, and discusses the factors that determine the quality of a fingerprint image. Chapter 2 also introduces the compression techniques that are used to store the fingerprint image data in a compact form.

Chapters 3, 4, and 5 provide an in-depth treatment of fingerprint feature extraction, representation, matching, classification, and retrieval algorithms. The existing techniques are divided into various categories to guide the reader through the large number of ideas proposed in more than 400 technical papers on the subject. The main approaches are explained in detail to help practitioners in the field understand the methodology used in commercial systems.

Chapters 6, 7, and 8 are specifically dedicated to the three cutting edge topics: synthetic fingerprint generation, multimodal biometric systems, and fingerprint individuality, respectively. Synthetic fingerprints have proven to be a valid substitute for real fingerprints for the design and benchmarking of fingerprint-based recognition systems. Multimodal biometric systems, that is, systems based on a combination of fingerprints with other biometrics (e.g., face) or a combination of different fingerprint feature extraction or matching algorithms, appear to be a promising research direction to overcome the intrinsic limitations of the existing solutions. Scientific evidence supporting fingerprint individuality is being increasingly demanded in forensic, civil and commercial applications, and this has generated interest in designing accurate fingerprint individuality models.

Finally, Chapter 9 discusses the design, implementation and administration of secure fingerprint-based biometric systems, whose building blocks (basic algorithms) have been presented in the previous chapters. Experience and care is necessary to design and develop secure systems. Techniques for securing biometric systems against attacks (to sensor, feature extraction and matching modules, template, and communication channels) are also discussed.

Contents of the DVD

The book includes a DVD that contains the four fingerprint databases used in the 2002 Fingerprint Verification Competition (FVC2002) and the four databases used in 2000 Fingerprint Verification Competition (FVC2000). 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 fingerprint recognition system and to compare their developments with the state-of-the-art algorithms.

Intended Audience

This book will be useful to researchers, practicing engineers, and students who wish to understand and/or develop fingerprint-based recognition systems. It would also be useful 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 plain language. A number of examples 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 people helped in making this book a reality. Raffaele Cappelli of the University of Bologna wrote Chapter 6 on synthetic fingerprints, Sharath Pankanti of the IBM T. J. Watson Research Center and Arun Ross of Michigan State University provided portions of text and figures in Chapters 1, 7, and 8, and Alexander Ivanisov of Digital Persona Inc. provided invaluable suggestions throughout several revisions of Chapter 9. We also thank Wayne Wheeler and Wayne Yuhasz, editors at Springer, for their suggestions and keeping us on schedule for the production of the book.

This book explores automatic techniques for fingerprint recognition, from the first approaches introduced more than forty years ago to the current state-of-the-art algorithms. However, with the development of sensor technologies, the availability of faster processors at lower cost, and new emerging applications of biometrics, there continues to be vigorous activity in the design and development of faster, more accurate, and robust fingerprint recognition systems. 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 constancy in this rapidly evolving and important field of automatic fingerprint recognition.

December 2002

Davide Maltoni
Dario Maio
Anil K. Jain
Salil Prabhakar