Handbook of Fingerprint Recognition

Davide Maltoni · Dario Maio · Anil K. Jain · Jianjiang Feng

Handbook of Fingerprint Recognition

Third Edition

Springer

Davide Maltoni
Department of Computer Science
and Engineering
University of Bologna
Cesena, Italy

Dario Maio
Department of Computer Science
and Engineering
University of Bologna
Cesena, Italy

Anil K. Jain
Department of Computer Science
and Engineering
Michigan State University
East Lansing, MI, USA

Jianjiang Feng
Department of Automation
Tsinghua University
Beijing, China

ISBN 978-3-030-83623-8 ISBN 978-3-030-83624-5 (eBook)
https://doi.org/10.1007/978-3-030-83624-5

1st edition: © Springer Science+Business Media New York 2003
2nd edition: © Springer-Verlag London Limited 2009
3rd edition: © Springer Nature Switzerland AG 2022
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Overview

Biometric recognition, or simply biometrics, refers to the use of distinctive anatomical and/or behavioral characteristics or identifiers (e.g., fingerprints, face, iris, voice, and 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 person recognition systems that are based on ID documents and password/PIN 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, offers better user convenience. It is for these reasons that biometric recognition systems have been deployed in a large number of government (e.g., border crossing, national ID card, and social benefit programs) and routine access control (e.g., mobile phone unlocking, computer logon, and access to buildings) applications.

A number of biometric recognition technologies have been developed, and several of them have been successfully deployed. Among these, fingerprints, face, and iris are the 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 be compared on a number of factors, including universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention. Because of the well-known distinctiveness (individuality) and persistence properties of fingerprints as well as the cost and maturity of sensors and matching algorithms, fingerprints are the most widely deployed biometric characteristics in use today. It is generally believed that the friction ridge pattern, composed of ridges and valleys, on each finger is unique. Given that there are about 7.8 billion living people on Earth and assuming each person has 10 fingers, there are 78 billion unique fingers! Hence, the biometric recognition

problem is the largest machine learning problem in terms of the number of classes. Fingerprints were first introduced as a method for person identification over 100 years ago. Now, every forensics and law enforcement agency worldwide routinely uses Automated 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 routine non-forensic applications.

Fingerprint recognition can be viewed as a pattern recognition system. Designing algorithms capable of extracting salient features from fingerprints and matching them in a robust way is not trivial. There is a popular misconception that automated fingerprint recognition is a fully solved problem since automated fingerprint systems have been around for almost 50 years. On the contrary, fingerprint recognition is still a challenging and stimulating recognition problem. This is particularly so when the users are uncooperative, the finger surface is dirty or scarred and the resulting fingerprint image quality is poor, and/or only small fingerprint fragments are available (e.g., due to a small sensing device). Latent fingerprints, obtained at crime scenes during forensics investigations, and their fully automated processing constitute a particularly challenging use case.

Deep learning (whose resurgence began around 2012) was a game-changer for computer vision and machine learning. The current state of the art for most biometric modalities can be attributed to the use of deep neural networks along with large training sets. Fingerprint recognition has also been approached in terms of data-driven learning techniques (as opposed to pre-specified minutiae features). This has resulted in new effective methods for automated processing of latent fingerprints and learning robust fixed-length fingerprint representations. However, top-down minutiae-based "geometric" matching still remains the best performing approach for most use cases of fingerprint recognition. This shows that tiny ridge details, first introduced for person recognition by Sir Francis Galton more than a century ago, are still competitive with the powerful representations learned by huge neural networks trained on big data.

This book reflects the progress made in automated techniques for fingerprint recognition over the past five decades, including recent deep learning-based methods. We have attempted to organize, classify, and present hundreds of existing approaches that span the end-to-end processing of fingerprints, from fingerprint sensing to final matching results 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 the fascinating technology behind fingerprint recognition.

Objectives

The aims and objectives of this book are to

- Introduce automated 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 indexing (filtering) techniques, latent fingerprint recognition, synthetic fingerprint generation, 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 (Chap. 2); fingerprint representation, matching, and classification/indexing (Chaps. 3, 4, and 5); advanced topics including latent fingerprint recognition, synthetic fingerprint generation, and fingerprint individuality (Chaps. 6, 7, and 8); and fingerprint system security (Chap. 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, pattern recognition, and machine learning 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 Chap. 1.

Chapter 2 surveys the existing fingerprint acquisition techniques: from the traditional "ink technique" to live-scan sensing based on optical, capacitive, thermal, and ultrasonic technologies. The chapter also discusses the factors that determine the quality of a fingerprint image and introduces the technological advancements that enabled the in-display integration of fingerprint sensors in mobile phones.

Chapters 3–5 provide an in-depth treatment of fingerprint feature extraction, matching, and classification/indexing, respectively. Existing techniques 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 to understand the methodology used in building fingerprint systems.

Chapters 6–8 are specifically dedicated to the three cutting-edge topics: latent fingerprint recognition, synthetic fingerprint generation, and fingerprint individuality, respectively. Deep learning methods enabled the automated processing of latent fingerprints a reality, leading to the development of a new generation of AFIS. Synthetic fingerprints have been accepted as a reasonable substitute for real fingerprints for the design, training, and benchmarking of fingerprint recognition algorithms; this approach is particularly useful to deal with emerging restrictions (e.g., European Union General Data Protection Regulation (GDPR)) on the use of Personally Identifiable Information (PII) which is defined as any data that could potentially identify a specific individual. 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, Chap. 9 discusses the security issues and countermeasure techniques that are useful in building secure fingerprint recognition systems.

From the Second to the Third Edition

The third edition of the "Handbook of Fingerprint Recognition" is a major update of the second edition published in 2009. While the overall chapter structure has been mostly maintained, in the last 13 years (2009–2021) significant scientific and technological improvements have been made and this motivated us to update our manuscript to best reflect them.

The team of authors no longer includes Salil Prabhakar, now a full-time entrepreneur in the biometric business, but was enriched with the entrance of Jianjiang Feng whose scientific contributions to fingerprint recognition are well-known. A new chapter on latent fingerprint recognition was added (Chap. 6) because most advances have been made on this topic in the last decade, and it still remains a challenging problem. On the other hand, the "Biometric Fusion" chapter was removed because today multimodal biometric is mainstream, and a comprehensive introduction to this topic is already available (see Sect. 1.17).

The presentation style throughout the book chapters has also slightly changed. In the previous editions, we tried to organize and generalize the underlying ideas of all the approaches published in the literature (including minor contributions). However, with the constantly increasing number of papers appearing in journals and conferences, sticking to full coverage of the literature would lead to an over-chaotic and difficult-to-read essay. Hence, in this new edition, we have tried to balance at best a survey style with focused depth on the contributions we believe constitute major advancements.

The total length of the handbook grew from 494 to 523 pages and about 500 new papers have been cited to cover the period 2009–2021. Several new figures, drawings, and tables have been added with the aim of making the presentation illustrative and lucid. The Electronic Supplementary Material (ESM) included with the book contains the databases used in 2000, 2002, and 2004 Fingerprint Verification Competition (FVC2004). Table 1 summarizes the new content included in this edition of the Handbook.

Table 1 New content included in the Handbook

Chapter	New Content
1 Introduction	– Emerging applications and large-scale projects – Updated introduction to individual book chapters
2 Fingerprint sensing	– Evolution of sensing technology: from bulky optical devices to in-display integration in mobile phones. – New sensing technologies (e.g., OCT and touchless "on the fly") – From CMOS to TFT sensors – Examples of multi-fingers and single-finger scanners, sensing elements for mobile devices
3 Fingerprint Analysis and Representation	– Advanced segmentation techniques: total variation and deep learning models – Learning-based techniques for local orientation estimation: from dictionaries to CNN – New algorithms for fingerprint pose estimation – Neural network-based enhancement of low-quality fingerprints – Learning-based minutiae detection (e.g., FingerNet) – Benchmarking local orientation estimation and minutiae detection – Pore detection with classical and deep learning approaches – Novel approaches for global and local quality computation (e.g., NFIQ2)
4 Fingerprint Matching	– Updated categorization of global minutiae-matching approaches – Spectral minutiae representation – Evolution of local minutiae matching: from early methods to rich local descriptors to Minutiae Cylinder Code (MCC) – Improved techniques for distortion correction – Dense fingerprint registration – Evolution of feature-based matching: from FingerCode to handcrafted textural features to deep features – DeepPrint: combining fingerprint domain knowledge with deep networks to derive compact fixed-length fingerprint representations – Pore matching – Updated overview of benchmarks and evaluation campaigns.

(continued)

Table 1 (continued)

Chapter	New Content
5 Fingerprint Classification and Indexing	– Shortened the sections on exclusive classification techniques and expanded fingerprint indexing and retrieval – Novel minutiae-based indexing methods – Deep learning-based indexing – Benchmarking indexing techniques
6 (New) Latent Fingerprint Recognition	– Latent fingerprint recognition by human experts – Automated recognition: feature extraction and matching – Latent quality estimation – Performance evaluation
7 Fingerprint Synthesis	– Categorization of synthetic generation approaches – Generation of a master fingerprint and derivation of multiple impressions (e.g., SFINGE) – Generative models (e.g., GAN) for the direct synthesis of fingerprint images – Validation of synthetic generators and large-scale experiments
8 Individuality	– Empirical versus theoretical approaches – Persistence of fingerprints
9 Securing Fingerprint Systems	– Threat model for fingerprint systems – Methods of obtaining fingerprint data and countermeasures – Updated introduction to presentation attack instruments – State-of-the-art presentation attack detection techniques and their performance evaluation – Altered fingerprints and their detection – Novel template protection techniques (e.g., homomorphic encryption of fixed-length representations) – Challenges and open issues

Contents of the Electronic Supplementary Material (ESM)

The book includes ESM that contains the 12 fingerprint databases used in 2000, 2002, and 2004 Fingerprint Verification Competitions (FVC). The ESM 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 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 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, pattern recognition, and machine learning, the introduction, sensing, and security chapters are accessible to a wider audience (e.g., developers of biometric applications, system integrators, security managers, and designers of security systems).

Cesena, Italy — Davide Maltoni
Cesena, Italy — Dario Maio
East Lansing, USA — Anil K. Jain
Beijing, China — Jianjiang Feng
July 2021

Acknowledgments A number of individuals helped in making this book a reality. Raffaele Cappelli of the University of Bologna wrote Chap. 7 on synthetic fingerprints, and Karthik Nandakumar of MBZUAI University (Abu Dhabi) wrote Chap. 9 on securing fingerprint systems.

We also thank Wayne Wheeler at Springer, for his encouragement in revising the second edition of this book.

Contents

1 Introduction 1
1.1 Introduction 1
1.2 Biometric Recognition 2
1.3 Biometric Systems 4
1.4 Comparison of Traits 8
1.5 System Errors 13
1.5.1 Reasons Behind System Errors 13
1.5.2 Capture Module Errors 14
1.5.3 Feature Extraction Module Errors 15
1.5.4 Template Creation Module Errors 15
1.5.5 Matching Module Errors 15
1.5.6 Verification Error Rates 17
1.5.7 Identification Error Rates 21
1.5.8 Presentation Attack Detection Errors 23
1.6 System Evaluation 24
1.7 Applications of Fingerprint Systems 27
1.7.1 Application Characteristics 27
1.7.2 Application Categories 29
1.7.3 Barriers to Adoption 32
1.8 History of Fingerprints 33
1.9 Formation of Fingerprints 36
1.10 Individuality and Persistence of Fingerprints 37
1.11 Fingerprint Sensing 38
1.12 Fingerprint Representation and Feature Extraction 40
1.13 Fingerprint Matching 43
1.14 Fingerprint Classification and Indexing 45
1.15 Latent Fingerprint Recognition 47
1.16 Synthetic Fingerprints 47
1.17 Biometric Fusion 48
1.18 System Integration and Administration Issues 50

1.19 Securing Fingerprint Systems 52
1.20 Privacy Issues 54
1.21 Summary and Future Prospects 57
1.22 Image Processing, Pattern Recognition, and Machine Learning Background 58
1.22.1 Image Processing Books 58
1.22.2 Pattern Recognition and Machine Learning Books 58
1.22.3 Journals 59
References 59

2 Fingerprint Sensing 63
2.1 Introduction 63
2.2 Off-Line Fingerprint Acquisition 68
2.3 Live-Scan Fingerprint Sensing 69
2.3.1 Optical Sensors 70
2.3.2 Capacitive Sensors 76
2.3.3 Thermal Sensors 77
2.3.4 Pressure Sensors 78
2.3.5 Ultrasound Sensors 78
2.4 Swipe Sensors 79
2.5 Fingerprint Images and Their Parameters 81
2.6 Image Quality Specifications for Fingerprint Scanners 85
2.7 Operational Quality of Fingerprint Scanners 86
2.8 Examples of Fingerprint Scanners 90
2.9 Dealing with Small-Area Sensors 95
2.10 Storing and Compressing Fingerprint Images 101
2.11 Summary 103
References 105

3 Fingerprint Analysis and Representation 115
3.1 Introduction 115
3.2 Segmentation 120
3.2.1 Segmentation Based on Handcrafted Features and Thresholding 122
3.2.2 Learning-Based Segmentation with Simple Classifiers 123
3.2.3 Total Variation Models 124
3.2.4 Deep Learning Models 125
3.3 Local Ridge Orientation Estimation 126
3.3.1 Gradient-Based Approaches 127
3.3.2 Slit- and Projection-Based Approaches 129
3.3.3 Orientation Estimation in the Frequency Domain 131
3.3.4 Orientation Image Regularization 131

3.3.5 Global Models of Ridge Orientations 133
3.3.6 Learning-Based Methods 136
3.3.7 Benchmarking Fingerprint Orientation Extraction 138
3.4 Local Ridge Frequency Estimation 140
3.5 Singularity Detection and Pose Estimation 144
3.5.1 Poincaré 144
3.5.2 Methods Based on Local Characteristics of the Orientation Image 148
3.5.3 Partitioning-Based Methods 150
3.5.4 Methods Based on a Global Model of the Orientation Image 151
3.5.5 Fingerprint Pose Estimation 152
3.6 Enhancement 157
3.6.1 Pixel-Wise Enhancement 159
3.6.2 Contextual Filtering 160
3.6.3 Multi-Resolution and Iterative Enhancement 168
3.6.4 Learning-Based Enhancement 169
3.6.5 Crease Detection and Removal 171
3.7 Minutiae Detection 172
3.7.1 Binarization-Based Methods 174
3.7.2 Direct Gray-Scale Extraction 177
3.7.3 Learning-Based Approaches 181
3.7.4 Minutiae Encoding Standards 182
3.7.5 Benchmarking Minutiae Extraction 184
3.8 Minutiae Filtering 185
3.8.1 Structural Post-Processing 185
3.8.2 Minutiae Filtering in the Gray-Scale Domain 187
3.9 Estimation of Ridge Count 189
3.10 Pore Detection 190
3.10.1 Skeletonization 191
3.10.2 Filtering 191
3.10.3 Topological Approaches 192
3.10.4 Deep Learning Methods 193
3.11 Estimation of Fingerprint Quality 193
3.11.1 Local Quality Estimation 194
3.11.2 Global Quality Estimation 195
3.11.3 NFIQ (NIST Fingerprint Image Quality) 196
3.12 Summary 199
References 199

4 Fingerprint Matching 217
4.1 Introduction 218
4.2 Correlation-Based Techniques 223
4.3 Minutiae-Based Methods 228
4.3.1 Problem Formulation 229
4.3.2 Similarity Score 233
4.3.3 Global Minutiae Matching Approaches 234
4.3.4 Hough Transform-Based Approaches 236
4.3.5 Consensus-Based Approaches 237
4.3.6 Spectral Minutiae Representation 241
4.3.7 Minutiae Matching with Pre-Alignment 243
4.4 Global Versus Local Minutiae Matching 244
4.4.1 Archetype Methods for Nearest Neighbor-Based and Fixed Radius-Based Local Minutiae Structures 245
4.4.2 Evolution of Local Structure Matching 247
4.4.3 Minutiae Cylinder Code 251
4.4.4 Consolidation 253
4.5 Dealing with Distortion 256
4.5.1 Fingerprint Distortion Models 257
4.5.2 Tolerance Box Adaptation 260
4.5.3 Warping 260
4.5.4 Dense Registration 262
4.5.5 A-Priori Distortion Removal 264
4.6 Feature-Based Matching Techniques 266
4.6.1 Early Global Methods 267
4.6.2 Local Orientation and Frequencies 269
4.6.3 Geometrical Attributes and Spatial Relationship of the Ridge Lines 269
4.6.4 Handcrafted Textural Features 270
4.6.5 Deep Features 271
4.6.6 Pore Matching 272
4.7 Comparing the Performance of Matching Algorithms 275
4.7.1 Fingerprint Databases 275
4.7.2 Fingerprint Evaluation Campaigns 280
4.7.3 Interoperability of Fingerprint Recognition Algorithms 281
4.8 Summary 282
References 283

5 Fingerprint Classification and Indexing 299
5.1 Introduction 299
5.2 Classification 301
5.2.1 Rule-Based Approaches 305

5.2.2 Syntactic Approaches 306
5.2.3 Structural Approaches 306
5.2.4 Statistical Approaches 307
5.2.5 Neural Network-Based Approaches 309
5.2.6 Multiple Classifier-Based Approaches 310
5.2.7 Fingerprint Sub-Classification 312
5.3 Benchmarking Fingerprint Classification Techniques 313
5.3.1 Metrics 313
5.3.2 Datasets 315
5.3.3 Search Strategies for Exclusive Classification 316
5.4 Fingerprint Indexing and Retrieval 318
5.4.1 Methods Based on Orientation and Frequency Images 320
5.4.2 Methods Based on Matching Scores 320
5.4.3 Methods Based on Minutiae 321
5.4.4 Hybrid and Ensemble Methods 324
5.4.5 Deep Learning-Based Methods 324
5.5 Benchmarking Fingerprint Indexing Techniques 330
5.5.1 Metrics and Benchmarks 330
5.5.2 Comparison of Existing Approaches 331
5.6 Summary 331
References 332

6 Latent Fingerprint Recognition 339
6.1 Introduction 339
6.2 Latent Fingerprint Recognition by Latent Examiners 342
6.2.1 ACE-V 342
6.2.2 Criticisms 343
6.2.3 Recent Advances 344
6.3 Automated Latent Fingerprint Recognition 346
6.4 Feature Extraction 348
6.4.1 Challenges 348
6.4.2 Pose Estimation 349
6.4.3 Foreground Segmentation 352
6.4.4 Local Ridge Orientation Estimation 355
6.4.5 Overlapping Fingerprint Separation 362
6.4.6 Ridge Enhancement and Minutiae Detection 363
6.4.7 Quality Estimation 367
6.5 Matching 371
6.5.1 Challenges 371
6.5.2 Latent Matching with Manually Marked Features 374
6.5.3 Latent Matching with Automatically Extracted Features 375
6.5.4 Performance Evaluation 378

6.6 Summary . . . 379
References . . . 380

7 Fingerprint Synthesis . . . 385
7.1 Introduction . . . 385
7.2 Generation of a Master Fingerprint . . . 387
7.2.1 Fingerprint Area Generation . . . 389
7.2.2 Orientation Image Generation . . . 390
7.2.3 Frequency Image Generation . . . 395
7.2.4 Ridge Pattern Generation . . . 395
7.3 Generation of Fingerprints from a Master Fingerprint . . . 400
7.3.1 Variation in Ridge Thickness . . . 401
7.3.2 Fingerprint Distortion . . . 402
7.3.3 Perturbation and Rendering . . . 403
7.3.4 Background Generation . . . 404
7.4 Direct Generation of Synthetic Fingerprints . . . 407
7.5 Validation of Synthetic Generators . . . 410
7.5.1 Ranking Difference Among Comparison Algorithms . . . 411
7.5.2 Match Score Distributions . . . 412
7.5.3 Fingerprint Quality Measures . . . 412
7.5.4 Minutiae Histograms . . . 413
7.5.5 Analysis of Multiple Features . . . 414
7.5.6 Large Scale Experiments . . . 415
7.6 The "SFinGe" Software . . . 417
7.7 Summary . . . 422
References . . . 424

8 Fingerprint Individuality . . . 427
8.1 Introduction . . . 427
8.2 Theoretical Approach . . . 430
8.2.1 Early Individuality Models . . . 430
8.2.2 Uniform Minutiae Placement Model . . . 438
8.2.3 Other Models . . . 447
8.3 Empirical Approach . . . 448
8.4 Persistence of Fingerprints . . . 451
8.5 Summary . . . 453
References . . . 453

9 Securing Fingerprint Systems . . . 457
9.1 Introduction . . . 458
9.2 Threat Model for Fingerprint Systems . . . 461
9.2.1 Insider Attacks . . . 462
9.2.2 External Adversarial Attacks . . . 464

9.3 Methods of Obtaining Fingerprint Data and Countermeasures 466
9.3.1 Lifting Latent Fingerprints 468
9.3.2 Extracting Fingerprints from High-Resolution Photos 468
9.3.3 Guessing Fingerprint Data by Hill Climbing 470
9.3.4 Stealing Fingerprint Data from the Template Database 470
9.3.5 Countermeasures for Protecting Fingerprint Data 471
9.4 Presentation Attacks 474
9.4.1 Fingerprint Spoofs 475
9.4.2 Altered Fingerprints 476
9.5 Presentation Attack Detection 479
9.5.1 Hardware-Based Approaches for Spoof Detection 479
9.5.2 Software-Based Approaches for Spoof Detection 482
9.5.3 Altered Fingerprint Detection 485
9.5.4 PAD Performance Evaluation 487
9.5.5 Challenges and Open Issues 491
9.6 Template Protection 492
9.6.1 Desired Characteristics 494
9.6.2 Template Protection Approaches 496
9.6.3 Feature Transformation 500
9.6.4 Fingerprint Cryptosystems 504
9.6.5 Feature Adaptation 506
9.6.6 Challenges and Open Issues 510
9.7 Building a Closed Fingerprint System 512
9.8 Summary 515
References 516

Acronyms

ACER	Average Classification Error Rate
ACE-V	Analysis, Comparison, Evaluation and Verification
AD	Auxiliary Data
AES	Advanced Encryption Standard
AFIS	Automated Fingerprint Identification System
AM	Amplitude Modulation
APCER	Attack Presentation Classification Error Rate
API	Application Programming Interface
ASPP	Atrous Spatial Pyramid Pooling
ATM	Automatic Teller Machine
BPCER	Bonafide Presentation Classification Error Rate
CCTV	Closed Circuit Television
CDEFFS	Committee to Define an Extended Fingerprint Feature Set
CJIS	Criminal Justice Information Service
CMC	Cumulative Match Characteristic
CMOS	Complementary Metal Oxide Semiconductor
CNN	Convolutional Neural Network
COTS	Commercial Off-The-Shelf
CSI	Crime Scene Investigation
CTF	Contrast Transfer Function
DCT	Discrete Cosine Transformation
DET	Detection Error Tradeoff
DoG	Difference of Gaussians
DoS	Denial of Service
DPI	Dots Per Inch
DWT	Discrete Wavelet Transform
EER	Equal Error Rate
EFS	Extended Feature Set
EFTS	Electronic Fingerprint Transmission Specification
ELFT	Evaluation of Latent Fingerprint Technology

ESD	Electrostatic Discharge
FAP	Fingerprint Acquisition Profile
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FFT	Fast Fourier Transform
FHE	Fully Homomorphic Encryption
FM	Frequency Modulation
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False Non-Match Rate
FOE	Fingerprint Orientation Extraction
FOMFE	Fingerprint Orientation Model based on 2D Fourier Expansions
FPGA	Field Programmable Gate Array
FPIR	False Positive Identification Rate
FpVTE	Fingerprint Vendor Technology Evaluation
FRR	False Rejection Rate
FTA	Failure to Acquire
FTC	Failure to Capture
FTD	Failure to Detect
FTE	Failure to Enroll
FTIR	Frustrated Total Internal Reflection
FTP	Failure to Process
FVC DB #	FVC Database #
FVC	Fingerprint Verification Competition
FVC2000	Fingerprint Verification Competition (2000 edition)
FVC2002	Fingerprint Verification Competition (2002 edition)
FVC2004	Fingerprint Verification Competition (2004 edition)
FVC2006	Fingerprint Verification Competition (2006 edition)
FVC-onGoing	Fingerprint Verification Competition on Going
GAN	Generative Adversarial Network
GLCM	Gray-Level Co-occurrence Matrix
GPU	Graphic Processing Unit
HE	Homomorphic Encryption
HMM	Hidden Markov Model
HR	Hit Rate
i.i.d.	Independent and Identically Distributed
IAFIS	Integrated Automated Fingerprint Identification System
IARPA	Intelligence Advanced Research Projects Activity
IBIA	International Biometrics Industry Association
ICP	Iterative Closest Point
ID	Identity

IEC	International Electrotechnical Commission
IQS	Image Quality Specification
ISO	International Standards Organization
JPEG	Joint Photographic Experts Group
KL	Karhunen–Loève
LBP	Local Binary Pattern
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
LFIQ	Latent Fingerprint Image Quality
LR	Likelihood Ratio
LSH	Locality-Sensitive Hashing
MCC	Minutiae Cylinder Code
MEMS	Micro-Electro-Mechanical System
MINEX	Minutiae Interoperability Exchange Test
MoC	Match-on-Card
MRF	Markov Random Field
MTF	Modulation Transfer Function
MUT	Micromachined Ultrasound Transducer
NFIQ	NIST Fingerprint Image Quality
NGI	Next Generation Identification
NIST DB #	NIST Database #
NIST PFT	NIST Proprietary Fingerprint Template program
NIST	National Institute of Standards and Technology
NMP	Non-Match Probability
NN	Nearest Neighbor
NRC	National Research Council
NV	No Value
OCT	Optical Coherence Tomography
OTP	One Time Password
PA	Presentation Attack
PAD	Presentation Attack Detection
PAI	Presentation Attack Instrument
PC	Personal Computer
PCA	Principal Component Analysis
PCASYS	Pattern-level Classification Automation SYStem
PCB	Printed Circuit Board
PDE	Partial Differential Equation
PI	Pseudonymous Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PMUT	Piezoelectric Micromachined Ultrasound Transducer

PPI	Pixels Per Inch
PR	Penetration Rate
RANSAC	RANdom Sample Consensus
RBF	Radial Basis Function
RBM	Restricted Boltzmann Machine
R-CNN	Region-based Convolutional Neural Network
RF	Radio Frequency
RLC	Run Length Code
RMSD	Root Mean Square Deviation
ROC	Receiver Operating Characteristic
ROI	Region of Interest
SDK	Software Development Kit
SFinGe	Synthetic Fingerprint Generator
SIFT	Scale Invariant Feature Transformation
SNR	Signal-to-Noise Ratio
SoC	System-on-a-Chip, or System-on-Card
SoD	System on Device
SPI	Serial Peripheral Interface
SPOF	Symmetric Phase Only Filter
STFT	Short-Time Fourier Transform
SVM	Support Vector Machine
TEE	Trusted Execution Environment
TFT	Thin-Film Transistor
TPS	Thin Plate Spline
TSI	Top Sharpening Index
TV	Total Variation
USB	Universal Serial Bus
VAE	Variational AutoEncoder
VEO	Value for Exclusion Only
VID	Value for Individualization
WGAN	Wasserstein Generative Adversarial Network
WSQ	Wavelet Scalar Quantization