

Computer Science, Technology and Applications

THE FINGERPRINT FRONTIER

The Evolution of Biometric Security



OTHMAN OMRAN KHALIFA
AISHA HASSAN ABDALLA

NOVA

Contributor Copy

Contributor Copy

The Fingerprint Frontier

The Evolution of Biometric Security



No part of this digital document may be reproduced, stored in a retrieval system or transmitted in any form or by any means. The publisher has taken reasonable care in the preparation of this digital document, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained herein. This digital document is sold with the clear understanding that the publisher is not engaged in rendering legal, medical or any other professional services.

Contributor Copy

Computer Science, Technology and Applications

More information about this series can be found at



Privacy and Identity Protection

More information about this series can be found at



Contributor Copy

Othman Omran Khalifa
Aisha Hassan Abdalla Hashim

The Fingerprint Frontier

The Evolution of Biometric Security



No part of this digital document may be reproduced, stored in a retrieval system or transmitted in any form or by any means. The publisher has taken reasonable care in the preparation of this digital document, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained herein. This digital document is sold with the clear understanding that the publisher is not engaged in rendering legal, medical or any other professional services.

Contributor Copy

Copyright © 2026 by Nova Science Publishers, Inc.

<https://doi.org/10.52305/TADU1443>

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means: electronic, electrostatic, magnetic, tape, mechanical photocopying, recording or otherwise without the written permission of the Publisher.

We have partnered with Copyright Clearance Center to make it easy for you to obtain permissions to reuse content from this publication. Simply navigate to this publication's page on Nova's website and locate the "Get Permission" button below the title description. This button is linked directly to the title's permission page on copyright.com. Alternatively, you can visit copyright.com and search by title, ISBN, or ISSN.

For further questions about using the service on copyright.com, please contact:

Copyright Clearance Center

Phone: +1-(978) 750-8400

Fax: +1-(978) 750-4470

E-mail: info@copyright.com.

NOTICE TO THE READER

The Publisher has taken reasonable care in the preparation of this book, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained in this book. The Publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the readers' use of, or reliance upon, this material. Any parts of this book based on government reports are so indicated and copyright is claimed for those parts to the extent applicable to compilations of such works.

Independent verification should be sought for any data, advice or recommendations contained in this book. In addition, no responsibility is assumed by the Publisher for any injury and/or damage to persons or property arising from any methods, products, instructions, ideas or otherwise contained in this publication.

The Publisher assumes no responsibility for any statements of fact or opinion expressed in the published contents.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered herein. It is sold with the clear understanding that the Publisher is not engaged in rendering legal or any other professional services. If legal or any other expert assistance is required, the services of a competent person should be sought. FROM A DECLARATION OF PARTICIPANTS JOINTLY ADOPTED BY A COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND A COMMITTEE OF PUBLISHERS.

Additional color graphics may be available in the e-book version of this book.

Library of Congress Cataloging-in-Publication Data

ISBN: 979-8-90134-451-4 (Hardcover)

ISBN: 979-8-90134-547-4 (eBook)

Published by Nova Science Publishers, Inc. † New York

Contributor Copy

The Fingerprint Frontier: The Evolution of Biometric Security is a timely and comprehensive contribution to the field of biometric technology and cybersecurity. The authors have successfully combined theoretical foundations with practical applications, offering readers a deep understanding of fingerprint recognition systems, security challenges, ethical considerations, and emerging technologies. This book serves as an invaluable resource for students, researchers, engineers, and security professionals seeking to understand the rapidly evolving world of biometric authentication.

Professor, Dr. Sheroz Khan

Contributor Copy

Contributor Copy

*To our families, whose unwavering support, patience,
and encouragement have been the foundation of this work.
You have stood by us through long hours and endless dedication,
offering strength and encouragement when it was needed most.
This book is yours as much as it is ours.*

Contributor Copy

Contributor Copy

Contents

Foreword	 xvii
Ahmad Faris Ismail	
Preface	 xix
Acknowledgments	 xxi
Prologue	 xxiii
Chapter 1	An Introduction to Fingerprint Biometrics 1
	1.1. An Overview of Biometric Technology1
	1.2. The Role of Biometrics in Authentication2
	1.3. A Brief Introduction to Various Biometric Modalities3
	1.4. The Biometric System Recognition Process.....5
	1.5. Criteria for Selecting Biometric Modalities.....7
	1.6. A Historical Context of Fingerprint Identification9
	1.7. The Significance of Fingerprint Biometrics in Security10
	1.8. The Unique Nature of Fingerprints.....11
	1.9. Fingerprint Patterns12
	1.10. Distinct Advantages of Fingerprint Biometrics14
Chapter 2	The Fundamentals of Fingerprint Recognition17
	2.1. Introduction17
	2.2. Basic Anatomy of a Fingerprint18
	2.3. Fingerprint Acquisition Methods and Technologies.....20

2.4. Preprocessing Techniques for Enhancing
Image Quality24

2.5. Feature Extraction, Including Minutiae
Points and Ridge Patterns27

2.6. Algorithms for Minutiae Detection
and Matching29

Chapter 3

**Fingerprint Biometric Technology
and Recognition33**

3.1. Introduction33

3.2. Fingerprint Sensing and Imaging.....34

 3.2.1. *Optical Sensors: Pioneers
of Fingerprint Imaging*..... 34

 3.2.2. *Capacitive Scanners:
A Revolution in Fingerprint Recognition* 37

 3.2.3. *Ultrasonic Fingerprint Sensors:
Cutting-Edge Sensing Technology*..... 41

 3.2.4. *Optical Under-Display Scanners:
The Future of Fingerprint Sensing* 43

3.3. Fingerprint Feature Extraction.....45

 3.3.1. *Ridge Pattern Analysis* 45

 3.3.2. *Minutiae Points Identification* 47

 3.3.3. *Techniques for Detecting
and Extracting Minutiae Points*..... 48

3.4. Frequency Domain Techniques49

3.5. Image Enhancement for Feature Extraction50

 3.5.1. *The Contribution of Image
Enhancement to Feature
Extraction Accuracy* 51

3.6. Skeletonization and Thinning52

 3.6.1. *Ridge Structures Feature Extraction* 52

3.7. Hybrid Approaches and Machine Learning
in Feature Extraction53

Chapter 4

Fingerprint Data Acquisition and Processing.....55

4.1. Introduction55

4.2. Image Capture and Preprocessing56

 4.2.1. *Preprocessing methods*..... 58

 4.2.2. *Techniques for Noise Reduction* 59

4.2.3. Techniques for Image Enhancement.....	60
4.2.4. Techniques for Normalization	62
4.3. Fingerprint Data Storage and Encryption	63
4.4. Data Compression and Template Extraction	64
4.4.1. The Process of Extracting Templates from Fingerprint Images	65
4.5. Challenges in Fingerprint Data Acquisition and Processing	66
4.6. The Emerging Trends in Fingerprint Data Processing	67
Chapter 5 Fingerprint Database Management	69
5.1. Introduction	69
5.2. The Development and Evolution of Fingerprint Database Management.....	70
5.2.1. National and International Databases	71
5.3. Fingerprint Data Collection.....	72
5.3.1. High-Quality Fingerprint Images Collection.....	73
5.3.2. Biometric Standards Adhered Data Collection	73
5.4. Digitization and Template Creation.....	74
5.5. Fingerprint Database Structure	76
5.5.1. Centralized vs. Distributed Database Models.....	77
5.5.2. Scalability and Performance Considerations.....	77
5.5.3. Case Studies of Database Architectures	78
5.6. Data Storage and Management.....	78
5.6.1. Data Indexing and Retrieval Techniques.....	79
5.6.2. Large-Scale Fingerprint Databases Considerations.....	79
Chapter 6 Fingerprint Matching and Verification	81
6.1. Introduction	81
6.2. Matching Techniques and Algorithms.....	82
6.3. Pattern-Based and Ridge-Based Matching	83
6.3.1. Pattern-Based Fingerprint Matching	83

- 6.3.2. Ridge-Based Fingerprint Matching 84
 - 6.4. Minutiae-Based Matching and Its Variations85
 - 6.4.1. Minutiae-Based Matching Process..... 86
 - 6.5. Performance Evaluation and Accuracy Metrics87
 - 6.6. Advanced Matching Techniques88
 - 6.7. Fingerprint Verification Process.....89
 - 6.8. Advances in Fingerprint Matching and Verification91
- Chapter 7 Security Challenges in Fingerprint Biometrics.....93**
 - 7.1. Introduction93
 - 7.2. Attacks on Fingerprint Biometric Systems.....94
 - 7.3. Techniques for Preventing Spoofing Attacks96
 - 7.3.1. Handling Spoofing Attacks: Prevention, Detection, and Mitigation 97
 - 7.4. Secure Enrollment and Storage of Templates.....98
 - 7.4.1. Enrollment Security 98
 - 7.4.2. Secure Storage of Templates 99
 - 7.5. Cryptographic Protection for Fingerprint Data.....99
- Chapter 8 Fingerprint Biometric System Integration101**
 - 8.1. Introduction101
 - 8.2. Architecture and Design of Fingerprint Biometric Systems.....102
 - 8.3. Integrating Fingerprint Biometrics into Access Control Systems103
 - 8.3.1. Design Principles for Fingerprint Biometric Integration 104
 - 8.3.2. Considerations in Choosing Fingerprint Sensors for Integration 105
 - 8.3.3. Database Integration in Fingerprint Biometric Systems..... 106
 - 8.4. Integration with Surveillance Systems106
 - 8.5. Integration with Time and Attendance Systems108
 - 8.6. Integration with Mobile Device Security.....109
 - 8.7. Integration with Financial Services109
 - 8.8. Integration with Healthcare110
 - 8.9. Forensic and Law Enforcement110
 - 8.10. Border Control and Immigration111

	<i>8.10.1. The Role of Fingerprint Biometrics in Border Control</i>	111
	8.11. User Experience and Human Factors in Integration	112
Chapter 9	Human Factors in Fingerprint Biometric Systems	115
	9.1. Introduction	115
	9.2. Psychological and Behavioral Aspects in Biometric Identification.....	116
	9.3. Fingerprint Recognition Perception and Acceptance.....	116
	9.4. Usability and User Experience in Fingerprint Systems.....	118
	<i>9.4.1. User Familiarity with Fingerprint Authentication</i>	118
	9.5. Aging and Environmental Factors	119
	9.6. Accessibility and Inclusivity.....	120
	9.7. Human Errors and Biometric Identification	121
	9.8. Cultural and Ethical Considerations	122
	9.9. Human Factors in Next-Generation Biometric Systems.....	123
Chapter 10	Privacy and Ethical Considerations in Fingerprint Biometric Systems	125
	10.1. Introduction	125
	10.2. Privacy Concerns in Fingerprint Biometric System	126
	10.3. Fingerprint Biometric Accuracy and Bias	128
	<i>10.3.1. Accuracy Challenges in Fingerprint Biometrics</i>	128
	<i>10.3.2. Potential Bias in Fingerprint Recognition Algorithms</i>	128
	<i>10.3.3. Case Studies of Bias in Biometric Systems (e.g., Skin Tone Bias)</i>	129
	10.4. Privacy-Enhancing Technologies	130
	<i>10.4.1. Encryption and Secure Storage of Biometric Data</i>	130
	10.5. Ethical Implications of Fingerprint Biometrics.....	131

10.5.1. *Mass Surveillance
and Civil Liberties* 132

10.6. Workplace Implications:
Employee Monitoring and Consent 133

10.7. User Understanding in Fingerprint Biometrics 134

10.8. Balancing Information Sharing
and User Privacy 135

**Chapter 11 The Role of Fingerprint Biometrics
in National Security** 137

11.1. Introduction 137

11.2. Early Adoption in National Security 138

11.3. The Evolution of Fingerprint Biometrics
in National Security 139

11.4. Government and National Security
Applications 139

11.4.1. *Law Enforcement
and Criminal Identification* 140

11.4.2. *Biometric Identification
in Immigration* 141

11.5. Sensitive Government Installations 142

11.6. Intelligence Gathering and Analysis 143

11.7. Forensic Applications 144

11.8. International Collaborations 145

**Chapter 12 Fingerprint Biometrics and Global
Security Challenges** 147

12.1. Introduction 147

12.2. Cybersecurity and Fingerprint
Data Protection 147

12.2.1. *Security Audits and Monitoring* 149

12.2.2. *International Crimes
and Security Threats* 149

12.2.3. *Cybercrime* 150

12.2.4. *International Cooperation
and Data Sharing* 151

12.2.5. *Diplomatic and Political
Implications* 152

12.3. Data Security in Globalized Information
Exchange 153

	12.3.1. <i>International Standards and Regulations in Fingerprint Biometrics</i>	154
	12.4. Ongoing Evolution of Fingerprint Biometrics in Global Security	155
Chapter 13	Best Practices for Fingerprint Biometric Security	157
	13.1. Introduction	157
	13.2. Secure Storage of Fingerprint Data	158
	13.3. Protection Against Spoofing	159
	13.3.1. <i>Case Studies of Successful Spoofing Attempts and How to Prevent Them</i>	159
	13.3.2. <i>Prevention Measures and Best Practices</i>	160
	13.4. Data Privacy Compliance	161
	13.5. User Education and Awareness: Empowering Fingerprint Security	162
	13.6. Regular Security Audits	163
	13.7. Secure Physical Access Control	164
	13.7.1. <i>Case Studies of Unauthorized Access and Its Consequences</i>	165
	13.8. Secure Enrollment and Storage of Templates	167
	13.9. Secure Communication and Data Transmission	168
	13.10. The Role of Encryption	168
Chapter 14	Emerging Technologies in Fingerprint Biometrics and Security	171
	14.1. Introduction	171
	14.2. Advances in Fingerprint Sensor Technology	172
	14.3. Fingerprint Biometrics and IoT Integration	174
	14.4. Blockchain and Fingerprint Security	175
	14.5. Cloud-Based Fingerprint Biometric Systems	176
	14.6. Behavioral Biometrics and Multimodal Systems	177
	14.7. AI and Machine Learning for Fingerprint Security Enhancement	178
	14.8. Multimodal Biometrics and Fusion of Different Modalities	180
	14.8.1. <i>Multimodal Biometrics</i>	180

14.8.2. *Fusion of Different Modalities*..... 181

Chapter 15 Beyond Fingerprint Biometrics183

15.1. Introduction183

15.2. Beyond Fingerprint Biometrics
in Future Technologies184

15.2.1. *Human Augmentation and
the Fusion of Biometrics with Technology* 185

15.3. Biometric Wearables: Fusion of Fashion
and Security186

15.4. Emerging Biometric Modalities187

15.4.1. *Artificial Intelligence
in Fingerprint Biometrics* 188

15.4.2. *Advantages of Combining
Different Biometric Modalities*..... 189

15.5. The Impact of Quantum Computing
on Fingerprint Biometric Security190

15.6. Biometrics in Space Exploration191

Epilogue193

References195

About the Authors197

Index199

Foreword

In an era where digital transformation shapes nearly every aspect of modern life, the importance of secure and reliable identity verification has never been greater. From personal mobile devices and financial systems to border security and national infrastructures, biometric technologies have emerged as essential tools for protecting sensitive information and ensuring trusted authentication. Among these technologies, fingerprint biometrics remains one of the most dependable, accessible, and widely adopted methods of identification.

The Fingerprint Frontier: The Evolution of Biometric Security offers a comprehensive and insightful exploration into this fascinating and rapidly advancing field. This book provides readers with a thorough understanding of fingerprint biometrics, beginning with its historical foundations and progressing toward advanced applications in security, forensics, and digital identity management. The authors skillfully bridge theory and practice, presenting complex technical concepts in a clear and accessible manner while emphasizing the broader social, ethical, and security implications of biometric systems.

One of the strengths of this book lies in its balanced approach. It not only examines the scientific and technological principles behind fingerprint recognition, image processing, feature extraction, and biometric system integration, but also addresses critical issues such as privacy protection, user acceptance, ethical considerations, and emerging cybersecurity threats. In doing so, the book reflects the interdisciplinary nature of biometric security and its growing relevance in our interconnected world.

The detailed discussion of fingerprint acquisition technologies, preprocessing methods, minutiae extraction, matching algorithms, and advanced sensing systems demonstrates the authors' strong academic and professional expertise. Equally important is the book's forward-looking perspective, which examines future developments in biometric authentication and the evolving challenges associated with global security and digital trust.

Contributor Copy

This book will undoubtedly serve as a valuable resource for students, researchers, engineers, security professionals, policymakers, and anyone interested in understanding the evolving landscape of biometric technology. Its combination of academic rigor, practical examples, and accessible explanations makes it suitable for both newcomers and experienced specialists in the field.

I am confident that *The Fingerprint Frontier: The Evolution of Biometric Security* will inspire further research, innovation, and thoughtful discussion in this important domain, while serving as a trusted reference for years to come.

Professor, Dr. Ahmad Faris Ismail
Deputy Rector (Academic and Internationalization)
International Islamic University Malaysia

Contributor Copy

Preface

Fingerprint biometrics is a key technology in the rapidly evolving field of identity verification and security, establishing a global context where secure, efficient, and reliable identification is paramount. This book aims to provide a comprehensive examination of the several aspects and implications of fingerprint biometrics in the context of global identity management and security. It explores the fundamentals of fingerprint recognition through chapters meticulously crafted by subject experts in the field. The book begins with an introduction to technology and a detailed examination of fingerprint data, acquisition, and pre-processing thereof. A detailed analysis of fingerprint database management, a crucial element in the digital age, underscores the need for secure storage and access to biometric data.

The book then discusses the crucial aspects of fingerprint matching and verification, exploring the complexities of system integration and the security challenges that inevitably arise with these advancements. It highlights the importance of user experience and acceptance in the widespread adoption of this technology by emphasizing the significant integration of human factors into fingerprint biometrics systems.

An exploration of privacy and ethical issues is crucial to the moral use of biometric data, paving the way for discussing fingerprinting in the context of national security. Chapter by chapter, the book addresses the global security challenges that fingerprinting seeks to address, as well as the best practices for its implementation.

By exploring emerging technologies in fingerprint security, the authors transcend the present and look to the future as we read the pages of this book. In Chapter Fifteen is presented a forward-looking question that goes beyond the boundaries, pointing to the revolutionary frontier where identity and technology intersect. This collaborative effort brings together the knowledge and perspectives of experienced researchers, academics, and career professionals combined in this cooperative effort. It is sincerely hoped that this book will be an invaluable tool for researchers, practitioners, and

Contributor Copy

enthusiasts alike as they navigate the complex world of fingerprint biometric technology.

We extend our sincere thanks and appreciation to everyone who contributed to the completion of this book, recognizing the importance of collective collaboration in enriching the dialogue on biometrics and international security. We hope that this book will serve as a beacon for readers as they navigate the complex world of fingerprint biometrics and its critical role in protecting our globalized society.

Othman Omran Khalifa
Aisha Hassan Abdalla Hashim

Contributor Copy

Acknowledgments

We would like to express our sincere gratitude to all those who have contributed to the completion of this book on fingerprint biometrics. First and foremost, we extend our deepest appreciation to our families for their unwavering support, patience, and encouragement throughout this journey. Their continuous motivation and understanding have been the foundation that enabled us to complete this work.

We are also grateful to our colleagues, researchers, and academic peers for their valuable insights, discussions, and constructive feedback, which greatly enriched the quality of this book. Special thanks go to all contributors and reviewers whose expertise helped shape the content and improve its clarity and depth.

Finally, we acknowledge everyone who has indirectly contributed to this effort. May this book serve as a meaningful contribution to the field of fingerprint biometrics and inspire further research and innovation.

Othman Omran Khalifa
Aisha Hassan Abdalla

Contributor Copy

Contributor Copy

Prologue

Human identity has always been at the center of civilization. From ancient signatures and seals to modern digital credentials, societies have continuously searched for reliable methods to distinguish individuals, protect information, and establish trust. In today's interconnected and technology-driven world, where digital interactions shape communication, commerce, governance, and security, the challenge of reliable identification has become more critical than ever before. The rapid growth of cyber threats, identity fraud, unauthorized access, and data breaches has intensified the global demand for secure and intelligent authentication systems.

Among the many technological solutions developed to address these challenges, fingerprint biometrics stands as one of the most trusted and enduring methods of human identification. The remarkable uniqueness and permanence of fingerprints have made them a cornerstone of modern biometric security systems. From unlocking smartphones and securing financial transactions to supporting forensic investigations and border control systems, fingerprint recognition technology has become deeply integrated into everyday life.

This book, *The Fingerprint Frontier: The Evolution of Biometric Security*, was developed with the vision of providing readers with a comprehensive understanding of fingerprint biometrics, its scientific foundations, technological advancements, practical applications, and future possibilities. It aims to present fingerprint recognition not merely as a technological tool, but as a transformative force reshaping the landscape of global security and digital identity management.

Throughout the chapters of this book, readers will explore the fascinating journey of fingerprint biometrics, beginning with its historical roots and progressing through modern sensing technologies, feature extraction methods, matching algorithms, biometric databases, and system integration techniques. The book also examines important human and societal dimensions, including

Contributor Copy

privacy, ethics, user acceptance, and the evolving challenges of cybersecurity in the age of digital transformation.

Special attention has been given to presenting the material in a clear and systematic manner that benefits a wide range of readers, including students, researchers, engineers, cybersecurity professionals, forensic specialists, policymakers, and technology enthusiasts. Real-world examples and practical discussions have been incorporated to bridge the gap between theoretical concepts and practical implementation.

The field of biometric security continues to evolve rapidly with the emergence of artificial intelligence, machine learning, advanced sensing technologies, and multimodal biometric systems. These innovations are opening new frontiers for more intelligent, accurate, and secure authentication systems while simultaneously introducing new ethical and technical challenges. This book therefore not only explores current technologies but also looks ahead toward the future of biometric innovation and its role in securing tomorrow's digital society.

We sincerely hope that this book will serve as an informative guide, an academic reference, and a source of inspiration for readers seeking to understand the evolving world of fingerprint biometrics and security technologies. It is our belief that knowledge and innovation, when guided by ethical responsibility and scientific rigor, can contribute significantly to building safer and more secure societies.

Finally, we extend our deepest gratitude to all researchers, academics, engineers, institutions, and professionals whose pioneering work in biometrics and security has contributed to the advancement of this important field. Their dedication and innovation continue to shape the future of trusted digital identity systems around the world.

Othman Omran Khalifa
Aisha Hassan Abdalla Hashim

Contributor Copy

About the Authors

Othman Omran Khalifa obtained his Bachelor's degree in Electrical and Electronic Engineering from Garyounis University, Libya, in 1986, followed by his Master and PhD degrees from Newcastle University, UK, in 1996 and 2000, respectively. He worked in industry for eight years and is currently a Professor at the Department of Electrical and Computer Engineering, International Islamic University Malaysia. He is a Chartered Engineer (UK), Senior Member of IEEE (USA), and member of IET (UK). Prof. Khalifa has chaired the International Conference on Computer and Communication Engineering (ICCCE) in multiple years and has supervised over 90 Masters and PhD students. He has authored more than 600 publications, including 14 books. His achievements include the Citation Indexed Journal Award (2013), TOKOH Academic "Best Academician" (2019), Murabbi "Best Teacher" (2020), and national Best Book awards in 2022 and 2025. He is listed among the top 2% scientists by Elsevier (2025).

Aisha Hassan Abdalla Hashim received her PhD in Computer Engineering (2007), M.Sc. in Computer Science (1996), and B.Sc. in Electronics Engineering (1990). She won the best graduating PhD student Award during the IIUM Convocation ceremony in 2007. She joined IIUM in 1997 and is currently working as a Professor at the Department of Electrical and Computer Engineering. Professor Aisha has taught several courses related to Communication and Computer Engineering. She is actively participating in curriculum development and program accreditation. She is a member of the Department Board of Studies for several years. She received Best Teacher Award by IIUM during the Quality Day in 2007. Professor Aisha is actively involved in research and postgraduate programs. She has published several journal/conference papers. She has supervised/co-supervised more than 70 PhD/Master students. She has received many Medals/Awards in different national/international research exhibitions.

Contributor Copy

Contributor Copy

Index

A

Aadhaar National Identity Program, 2
accuracy, 1, 3, 6, 8, 10, 14, 18, 22, 30, 31,
33, 35, 38, 43, 45, 47, 48, 50, 51, 52, 53,
54, 56, 59, 61, 64, 65, 66, 67, 68, 70, 71,
72, 74, 76, 78, 81, 82, 86, 87, 89, 91, 94,
96, 98, 101, 103, 104, 105, 106, 108,
110, 111, 112, 120, 121, 122, 125, 126,
127, 128, 129, 138, 143, 144, 145, 154,
158, 167, 168, 171, 172, 173, 178, 179,
180, 181, 183, 187, 188, 189
adaptability, 15, 82, 91, 104, 105, 140, 155,
177, 178, 179, 181, 183, 188, 189, 190
advanced technologies, 33, 79, 154, 184
AI algorithms, 171
AI-driven, 134, 184, 188
anatomy, 18, 19
artificial intelligence (AI), xxiv, 67, 91, 94,
95, 96, 134, 139, 143, 151, 171, 172,
173, 178, 179, 180, 183, 184, 188, 193
assets, 3, 33, 142, 151, 165
attendance, 2, 5, 14, 38, 101, 108, 112,
125, 127, 131
authentication, xvii, xxiii, xxiv, 2, 3, 4, 5,
7, 8, 10, 28, 36, 38, 40, 43, 46, 48, 50,
51, 52, 54, 55, 58, 59, 63, 64, 65, 67, 73,
81, 88, 89, 93, 96, 97, 99, 100, 101, 103,
105, 106, 109, 110, 112, 115, 116, 118,
119, 121, 123, 130, 131, 137, 138, 141,
142, 147, 148, 153, 155, 157, 160, 172,
174, 175, 176, 177, 178, 179, 180, 181,
182, 183, 184, 185, 186, 188, 189, 190,
191, 193

Automated Fingerprint Identification

System (AFIS), 10, 14, 69, 70, 90, 103,
138, 139, 143

B

backup, 79, 98, 99
behavioral characteristics, 1, 2, 3, 5, 187
biometric authentication, xvii, 1, 2, 21, 43,
47, 55, 60, 63, 66, 81, 82, 87, 89, 93, 97,
105, 157, 164, 169, 171, 172, 177, 178,
185, 186, 190
biometric methods, 1, 119
biometric technology, xviii, xx, 1, 2, 33,
36, 44, 45, 106, 107, 115, 122, 125, 130,
131, 136, 143, 145, 150, 176, 177, 181,
182, 183, 193, 195
border control, xxiii, 2, 4, 6, 15, 69, 77, 78,
79, 81, 89, 111, 112, 137, 138, 139, 140,
147, 152, 155, 167, 168, 172, 173, 176,
178, 179, 181
Brain computer interfaces (BCIs), 185
breaches, 33, 63, 64, 68, 95, 127, 132, 134,
137, 142, 153, 162, 166

C

capacitive sensors, 17, 18, 21, 38, 39, 55,
56, 173
capture device quality, 96
challenges, xvii, xix, xxiii, xxiv, 5, 43, 44,
56, 62, 66, 67, 72, 73, 79, 93, 94, 117,
119, 120, 121, 126, 128, 129, 133, 138,
143, 147, 149, 150, 151, 152, 153, 165,

174, 177, 183, 188, 189, 190, 191, 192, 193, 194
 civil liberties, 94, 125, 132, 153
 cognitive factors, 116
 collusion attacks, 95
 comparator, 94
 complexity, 13, 46, 47, 53, 81, 153, 157
 compliance, 55, 99, 100, 104, 105, 106, 110, 130, 133, 134, 148, 149, 157, 161, 162
 concerns, 7, 8, 9, 12, 71, 76, 81, 93, 112, 115, 116, 117, 122, 123, 124, 125, 126, 127, 132, 133, 138, 147, 150, 152, 153, 154, 157, 163, 164, 188, 190
 consent, 98, 122, 124, 125, 126, 127, 131, 132, 133, 134, 135, 148, 154, 161, 193
 contrast normalization, 55, 57
 convenience, 1, 3, 5, 6, 8, 14, 42, 43, 44, 87, 89, 103, 109, 116, 117, 118, 119, 123, 153, 165, 167, 168, 171, 174, 177, 178, 179, 183, 187
 convolutional neural networks (CNNs), 61, 62, 82, 89, 91, 188
 criminal investigations, 9, 21, 35, 36, 58, 64, 67, 71, 79, 88, 110, 138, 147
 cross-device attacks, 95
 cryptographic codes, 33
 cryptography, 97, 99, 190
 cybercriminals, 95, 127, 150
 cybersecurity, xvii, xxiv, 147, 148, 149, 150, 151, 153, 178, 193, 194

D

data breach, xxiii, 72, 93, 110, 116, 117, 122, 123, 127, 130, 147, 148, 153, 158, 159, 163, 165, 169, 172, 174, 175
 data retention, 125
 data theft, 95
 databases, xxiii, 14, 63, 64, 69, 70, 71, 72, 76, 77, 78, 79, 82, 90, 93, 103, 104, 106, 107, 110, 111, 127, 133, 139, 140, 141, 143, 144, 145, 148, 150, 175, 190
 deep learning algorithms, 94
 dependability, 39, 46, 55, 122

detection, 6, 11, 25, 26, 29, 30, 48, 53, 54, 58, 60, 85, 86, 91, 96, 97, 118, 138, 149, 159, 160, 166, 177, 192, 195
 device authentication, 97, 167
 digital, xvii, xix, xxiii, xxiv, 10, 22, 33, 34, 36, 37, 40, 59, 69, 70, 71, 73, 74, 75, 81, 86, 89, 97, 127, 141, 149, 150, 151, 153, 155, 157, 162, 163, 164, 175, 176, 177, 178, 184, 186, 187, 193, 194
 digital innovation, 33
 direct attack(s), 94
 disruption, 150
 distinct ridges, 81
 distinction, 17
 DNA, 5, 187
 durability, 8, 12, 21, 22, 33, 69

E

efficient, xix, 8, 15, 24, 36, 42, 44, 50, 52, 53, 59, 64, 65, 70, 71, 77, 78, 79, 81, 89, 101, 102, 104, 106, 111, 112, 118, 119, 135, 138, 142, 143, 155, 172, 175, 176, 177, 193, 196
 electrocardiogram (ECG), 186
 encrypting, 55, 130
 environmental factors, 11, 67, 119, 120, 121, 179
 ethical, xvii, xix, xxiv, 6, 55, 56, 70, 72, 94, 115, 122, 123, 124, 125, 126, 127, 130, 131, 132, 135, 138, 154, 185, 186, 187, 193, 194, 195, 196
 ethical considerations, xvii, 6, 55, 56, 70, 115, 122, 125, 127, 131, 132, 186, 195, 196
 ethical standards, 123, 125, 194
 examples, xviii, xxiv, 2, 3, 23, 35, 45, 90, 93, 103, 104, 117, 122, 124, 145, 153, 157, 158, 161, 163, 164, 165, 167, 169, 172, 179, 180, 187, 190

F

Face ID, 2, 14, 117, 119, 171

facial recognition, 2, 4, 6, 12, 68, 89, 96,
101, 107, 129, 141, 171, 172, 173, 177,
178, 181, 182, 183, 184, 185, 186, 187,
189, 191

fairness, 125, 127, 132, 193

finance, 1, 91, 105, 123, 134, 147, 172,
174, 175

financial gain, 150

fingerprint data, xix, 9, 10, 22, 24, 54, 55,
56, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69,
70, 71, 72, 74, 75, 76, 77, 78, 79, 89, 91,
93, 95, 99, 100, 102, 103, 104, 106, 107,
109, 111, 117, 122, 124, 126, 127, 130,
131, 138, 140, 143, 147, 148, 149, 153,
154, 157, 158, 161, 162, 163, 164, 167,
169, 172, 174, 175, 176, 181, 195

fingerprint recognition, xvii, xix, xxiii, 1,
2, 3, 4, 6, 10, 12, 14, 17, 18, 19, 20, 25,
26, 29, 31, 33, 36, 37, 38, 39, 43, 44, 45,
46, 47, 50, 51, 53, 55, 57, 59, 60, 61, 65,
67, 68, 69, 74, 76, 79, 83, 86, 87, 88, 94,
107, 116, 117, 118, 119, 120, 122, 123,
124, 126, 128, 131, 155, 157, 158, 159,
160, 161, 162, 163, 164, 171, 172, 173,
174, 178, 179, 180, 181, 182, 185, 186,
188, 189, 193, 195

fingerprint sensors, 2, 10, 21, 22, 23, 34,
36, 37, 38, 40, 41, 42, 43, 44, 69, 73, 96,
105, 109, 117, 118, 123, 165, 171, 172,
173, 186, 196

fraudulent, 8, 33, 108, 111, 141, 142, 159,
188

G

General Data Protection Regulation
(GDPR), 98, 99, 100, 133, 148, 154,
161

global security, xvii, xix, xxiii, 145, 147,
150, 151, 152, 155

government overreach, 94

government(s), 2, 7, 42, 43, 72, 75, 94,
104, 106, 117, 125, 135, 137, 138, 139,
140, 142, 145, 147, 150, 151, 164, 165,
168, 174, 193

H

healthcare, 1, 2, 91, 101, 110, 122, 134,
165, 166, 169, 172, 173, 174, 177, 178,
182, 185

heartrate tracking, 186

high-profile crime, 139

high-resolution images, 21, 22, 36, 37, 40,
55, 56, 91, 159, 171

human augmentation, 185

human traits, 1

I

identities, 15, 33, 69, 89, 95, 111, 137, 140,
141, 142, 148, 150, 158, 162, 176, 177,
178, 181

identity theft, 33, 71, 96, 109, 123, 131,
133, 135, 141, 147, 150, 158, 193

identity verification, xvii, xix, 2, 3, 5, 7,
12, 15, 36, 44, 67, 69, 75, 76, 79, 81, 83,
89, 93, 96, 98, 102, 103, 104, 106, 111,
117, 125, 126, 128, 135, 139, 140, 141,
147, 154, 157, 167, 175, 176, 177, 178,
179, 180, 181, 184, 186, 188, 189, 193

image enhancement, 50, 51, 55, 57, 60, 61,
67, 71, 88, 195

immutability, 1

index finger, 17

indirect attack(s), 94, 95

insider threats, 95, 134

insights, xxi, 25, 87, 94, 157, 158, 160,
163, 164, 184, 185, 186, 188, 194

Integrated Automated Fingerprint
Identification System (IAFIS), 70, 78,
137

Internet of Things (IoT), 174, 175, 184

interoperability, 103, 104, 105, 106, 144,
145, 150, 152, 154

IoT devices, 174, 184

iris recognition, 2, 4, 91, 121, 191

isolation, 97, 192

L

laptops, 21, 69, 73, 105, 155, 157, 185
 law enforcement, 4, 9, 10, 12, 14, 15, 18,
 21, 22, 26, 28, 35, 36, 46, 47, 49, 50, 52,
 53, 54, 58, 60, 63, 64, 65, 66, 67, 69, 70,
 71, 72, 74, 76, 78, 81, 82, 90, 91, 93,
 101, 103, 107, 110, 111, 121, 122, 123,
 124, 135, 137, 138, 139, 140, 141, 143,
 144, 145, 147, 149, 150, 152, 153, 155,
 171
 legal, 55, 56, 70, 72, 94, 117, 127, 130,
 133, 134, 136, 151, 158, 161, 162, 166,
 176, 194
 level of security, 1, 2, 5, 8, 21, 64, 68, 99,
 147, 175, 176
 limitations, 2, 7, 82, 120, 121, 138, 166,
 176, 183, 188, 189, 195
 liveness detection, 6, 91, 95, 96, 159, 160
 liveness detection bypass, 95
 loop pattern, 17, 19, 46

M

machine learning, xxiv, 45, 48, 49, 53, 54,
 61, 67, 88, 89, 91, 94, 95, 96, 97, 121,
 122, 139, 143, 171, 173, 178, 179, 180,
 183, 184, 188, 193
 management, xvii, xix, xxiii, 1, 2, 7, 10,
 56, 65, 69, 70, 71, 76, 77, 78, 79, 91, 98,
 100, 101, 103, 106, 108, 109, 112, 125,
 126, 130, 138, 142, 145, 161, 162, 168,
 171, 175, 176, 177, 195
 match, 6, 17, 20, 28, 62, 65, 69, 79, 84, 87,
 88, 90, 110, 111, 128, 140, 144, 165
 minute details, 40, 48, 81, 173
 misuse, 71, 95, 116, 117, 122, 123, 124,
 125, 131, 132, 133, 147, 153, 185
 mitigation, 97, 115
 mobile devices, xvii, 4, 10, 21, 22, 35, 36,
 38, 39, 40, 42, 59, 69, 73, 81, 109, 117,
 147, 155, 157, 172, 178, 182
 multimodal biometrics, 6, 89, 91, 96, 180,
 189

N

National Institute of Standards and
 Technology (NIST), 73, 74, 104, 145,
 195
 national security, xix, 15, 132, 137, 138,
 139, 140, 141, 142, 143, 144, 145, 151,
 155, 178, 193
 Next Generation Identification (NGI), 140,
 141
 noise reduction, 17, 25, 50, 55, 57, 58, 59,
 60, 67
 non-intrusive, 81
 non-match, 6
 norms, 55, 122, 123, 151, 154

O

optical sensors, 17, 22, 34, 35, 36, 37, 39,
 44, 55, 56, 102

P

palm print recognition, 2, 4
 passwords, 1, 2, 81, 109, 119, 148, 157,
 165, 174
 patient identification, 2, 182
 personal devices, 33, 40, 42, 43, 123, 147,
 168
 personal gadgets, 81
 physical, 5, 9, 10, 34, 37, 42, 43, 44, 81,
 95, 103, 109, 115, 118, 119, 120, 121,
 131, 160, 164, 165, 166, 171, 173, 176,
 177, 181, 182, 189, 192, 193
 PINs, 1, 2, 38, 81, 90, 109, 157, 160, 165
 political advantage, 150
 popularity, 1, 2, 21, 187
 practices, xix, 9, 64, 94, 108, 115, 121,
 124, 130, 131, 135, 145, 149, 151, 157,
 158, 160, 161, 162, 164, 165, 166, 168,
 169, 195
 presentation, 91, 93, 94, 105
 prevention, 11, 97, 101, 107, 140, 151, 160
 protect, xxiii, 3, 8, 10, 33, 55, 63, 64, 97,
 98, 99, 109, 110, 120, 122, 130, 132,

134, 135, 142, 144, 150, 153, 154, 155,
157, 158, 160, 162, 163, 164, 167, 168,
169, 171, 172, 174, 177, 180, 186, 190
protection, xvii, 10, 64, 71, 93, 94, 99, 100,
101, 106, 109, 117, 126, 127, 132, 147,
148, 150, 152, 153, 154, 157, 158, 159,
161, 162, 163, 166, 180, 185, 193
protection against, 109, 117, 159

R

recognition systems, 46, 61, 93, 95, 159,
187, 189
regulations, 70, 98, 100, 106, 110, 126,
135, 149, 152, 154, 157, 158, 161, 162,
194
reliable, xvii, xix, xxiii, 2, 3, 7, 9, 11, 12,
15, 17, 18, 20, 24, 25, 33, 36, 37, 38, 39,
40, 41, 42, 43, 46, 47, 49, 50, 52, 54, 55,
56, 57, 58, 59, 62, 63, 68, 69, 73, 81, 89,
90, 101, 102, 104, 105, 106, 109, 112,
113, 129, 131, 138, 139, 140, 141, 142,
144, 147, 157, 164, 165, 168, 179, 180,
183, 187, 189, 190, 193
ridges, 2, 3, 4, 11, 12, 13, 17, 18, 19, 20,
21, 22, 24, 25, 26, 27, 28, 29, 30, 34, 35,
36, 37, 38, 39, 41, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 58, 60, 61, 62, 64,
65, 74, 82, 83, 84, 88, 91, 93, 119, 121,
147, 160, 171, 172
role-based access control (RBAC), 64, 97

S

scalability, 76, 77, 78, 103, 104, 105, 106,
176, 177
secure, xvii, xix, xxiii, xxiv, 1, 2, 3, 5, 7,
10, 14, 21, 28, 31, 33, 36, 41, 42, 43, 44,
50, 52, 54, 55, 58, 60, 63, 64, 65, 67, 68,
73, 76, 81, 82, 85, 88, 89, 91, 97, 98, 99,
100, 101, 103, 104, 105, 106, 108, 109,
111, 116, 117, 119, 123, 126, 130, 131,
132, 135, 137, 139, 140, 141, 142, 145,
147, 148, 152, 154, 155, 157, 158, 160,
161, 163, 164, 165, 166, 167, 168, 169,

172, 173, 174, 175, 176, 177, 178, 179,
180, 181, 182, 184, 185, 186, 187, 190,
191, 193, 194
secure systems, 81, 179, 194
sensitive data, 27, 33, 55, 63, 109, 151,
155, 167, 177, 191
signal processor, 94
skin, 6, 12, 23, 37, 38, 39, 40, 42, 56, 66,
73, 115, 119, 120, 121, 126, 127, 128,
129, 159, 160, 183, 195
smartphone models, 55
smartphones, xxiii, 2, 6, 10, 14, 17, 21, 22,
27, 36, 38, 40, 42, 43, 44, 46, 47, 55, 88,
104, 105, 109, 118, 119, 123, 135, 155,
159, 165, 167, 168, 171, 173, 174, 185
solutions, xxiii, 3, 5, 7, 79, 91, 96, 101,
103, 117, 120, 151, 153, 155, 166, 172,
174, 175, 177, 187, 188, 189
speed, 1, 10, 21, 22, 35, 38, 70, 76, 77, 78,
103, 106, 111, 112, 113, 118, 140, 155,
177, 179
spoof attacks, 93
stolen, 1, 100, 103
strengths, xvii, 2, 53, 54, 55, 164, 189
surveillance, 2, 4, 5, 94, 101, 106, 107,
124, 125, 132, 133
system integrity, 81, 98, 149

T

technological advancements, xxiii, 67, 91,
94, 103, 121, 134, 139
terrorism, 71, 139, 144, 150, 151
texture analysis, 96
threats, xvii, xxiii, 10, 94, 95, 98, 104, 130,
131, 134, 140, 143, 144, 147, 148, 149,
150, 155, 159, 161, 162, 163, 164, 180,
183, 184, 188, 190
Touch ID, 2, 14, 90, 102, 103, 104, 117,
119
trust, xvii, xxiii, 15, 55, 68, 70, 95, 100,
112, 115, 116, 117, 122, 123, 124, 133,
134, 135, 136, 151, 152, 158, 162, 163,
166, 174, 193, 194

U

unauthorized, xxiii, 6, 8, 33, 44, 64, 68, 70, 72, 93, 103, 106, 109, 110, 116, 122, 123, 125, 126, 130, 132, 135, 137, 140, 142, 148, 151, 152, 153, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 172, 174, 175, 178, 179, 181, 182, 185, 189, 193

unauthorized use, 93, 179, 189

uniqueness, xxiii, 1, 9, 11, 12, 14, 17, 20, 33, 46, 47, 69, 81, 126, 138, 157, 174, 175

United States Federal Bureau of Investigation (FBI), 9, 70, 78, 137, 140, 141, 144, 147

United States Office of Personnel Management (OPM), 93, 127

United States Visitor and Immigrant Status Indicator Technology (US-VISIT), 69, 111, 137, 140, 141

usability, 8, 87, 88, 104, 105, 112, 115, 116, 118

user acceptance, xvii, xxiv, 2, 5, 8, 116, 135, 189

user-friendly, 2, 3, 8, 43, 81, 104, 105, 112, 117, 165, 168, 175, 177, 178, 180, 181, 184

V

verification, xix, 2, 5, 6, 7, 10, 12, 20, 21, 22, 24, 26, 31, 36, 46, 63, 65, 74, 75, 76, 81, 89, 90, 91, 93, 100, 103, 111, 137, 142, 148, 154, 171, 178, 184

verify, 2, 3, 5, 6, 8, 15, 29, 33, 43, 69, 93, 95, 98, 109, 111, 149, 167, 174

violating privacy, 125, 127, 151

voice recognition, 2, 4, 6, 172, 177, 178, 181, 183

vulnerabilities, 76, 93, 95, 97, 98, 127, 129, 148, 149, 150, 163, 164, 175, 188

W

whorl pattern, 17, 19, 20, 27, 28

THE FINGERPRINT FRONTIER

The Evolution of Biometric Security

OTHMAN OMRAN KHALIFA
AISHA HASSAN ABDALLA



Contributor Copy