Contents

Preface **xiii**

PART I Introduction and interdisciplinary approaches **1**

1 The interplay of privacy, security and user-determination in biometrics **3**
Claus Vielhauer

1.1 The technological view 3
1.2 Some societal, ethical and legal views 6
1.3 A taxonomical approach for discussions 7
1.4 Contributions of this book 11
1.5 Proposed reading and acknowledgements 14
References 15

2 Privacy of online handwriting biometrics related to biomedical analysis **17**
Marcos Faundez-Zanuy and Jiri Mekyska

2.1 Introduction 17
2.2 Online handwritten signals – an introduction 18
2.2.1 In-air and on-surface movements 19
2.3 Handwriting signals from biometrics to medical applications 23
2.3.1 Biometric security applications 23
2.3.2 Metadata applications 24
2.3.3 Biometric health applications 24
2.4 Security–health implications and concerns 31
2.4.1 Security where health aspects influence biometric security 31
2.4.2 Situations where health information can be extracted from security applications 33
2.4.3 Situations where the identity information must be removed 34
2.5 Summary and conclusions 35
References 35

3 Privacy concepts in biometrics: lessons learned from forensics **41**
Jana Dittmann and Christian Kraetzer

3.1 Introduction: forensic science and selected privacy concepts 41
3.2 Privacy concepts – findings from digitised forensics of latent fingerprints 42
3.2.1 Sensor-acquisition-related privacy-preserving guidelines 43
3.2.2 Privacy-preserving-benchmarking concepts and guidelines 45
3.3 Privacy concepts – findings from digital forensics of face-morphing detection in face authentication systems 48
3.3.1 Face-morphing attacks – generalised attack procedure and privacy implications 49
3.3.2 Media forensic investigations and biometrics on the example of face-morphing attacks 58
Acknowledgements 62
References 62

PART II Privacy and security of biometrics within general security systems **67**

4 Physical layer security: biometrics vs. physical objects **69**
Svyatoslav Voloshynovskiy, Taras Holotyak, and Maurits Diephuis

4.1 Introduction 69
4.2 Fundamentals of physical layer security based on unclonable functions 70
4.2.1 Randomness as a source of unclonability 70
4.2.2 Basic properties of unclonable functions 74
4.2.3 Basic enrollment-verification architecture of PUF systems 75
4.3 Image-PUFs: fundamentals of security with noisy data 77
4.3.1 Feature extraction 78
4.3.2 Template protection 81
4.3.3 Performance analysis 82
4.4 Attacks against biometrics and physical object protection 84
4.4.1 Attacks against biometric systems 84
4.4.2 Overview of reconstruction techniques 86
4.4.3 Attacks against PUFs-based systems 89
4.5 Main similarities and differences of biometrics and PUFs-based security 90
4.5.1 Summary and conclusions 93
References 93

5 Biometric systems in unsupervised environments and smart cards: conceptual advances on privacy and security 97
Raul Sanchez-Reillo

5.1 Challenges of an unsupervised scenario 98
5.1.1 Presentation attacks 99
5.1.2 Usability 100
5.1.3 Personal data handling 102
5.2 Smart cards as secure elements 103
5.2.1 Internal architecture 103
5.2.2 Smart card operating system 105
5.2.3 Functionality 105
5.2.4 Security mechanisms 107
5.2.5 Other implementations 111
5.3 Smart cards to improve security and privacy in unsupervised biometric systems 113
5.3.1 Practical implementations 117
5.4 Conclusions 118
References 119

6 Inverse biometrics and privacy 123
Marta Gomez-Barrero and Javier Galbally

6.1 Introduction 123
6.2 Synthetic biometric samples generation 124
6.3 Inverse biometrics methods 128
6.3.1 Template format 130
6.3.2 Similarity scores 131
6.3.3 Similarity score and distance function 132
6.3.4 Feature extraction 132
6.3.5 Summary 133
6.4 Evaluation of inverse biometrics methods 134
6.5 Privacy-related issues and countermeasures 138
6.6 Conclusions 141
References 143

7 Double-layer secret-sharing system involving privacy preserving biometric authentication 153
Quang Nhat Tran, Song Wang, Ruchong Ou and Jiankun Hu

Introduction 153
7.1 Conceptual clarifications 154
7.1.1 Steganography 154
7.1.2 (k, n)-Threshold secret sharing 154
7.1.3 Biometric template protection 156

7.2 Related work 156
7.2.1 Authentication with biometric template protection 156
7.2.2 Secret sharing with steganography 157
7.3 Double-layer secret-sharing system 158
7.3.1 Embedding process 158
7.3.2 Recovery process 162
7.3.3 Security analysis 164
7.4 Experimental results 165
7.4.1 Settings and parameters 165
7.4.2 Results 165
7.5 Conclusion and future works 167
References 168

PART III Security and privacy issues inherent to biometrics 171

8 Biometric template protection: state-of-the-art, issues and challenges 173
Christian Rathgeb and Christoph Busch

8.1 Introduction 173
8.2 Biometric template protection 175
8.2.1 Biometric cryptosystems 177
8.2.2 Cancellable biometrics 179
8.2.3 Multi-biometric template protection 181
8.3 Issues and challenges 182
8.3.1 Performance decrease in template protection schemes 183
8.3.2 Data representation and feature alignment 184
8.3.3 Standardization and deployments 184
8.4 Conclusion 186
References 186

9 Handwriting biometrics – feature-based optimisation 193
Tobias Scheidat

9.1 Introduction 193
9.2 Biometric feature analysis and selection 197
9.2.1 Wrappers 197
9.2.2 Filters 198
9.3 Reference algorithms 201
9.3.1 Biometric hash algorithm 201
9.3.2 Secure sketch algorithm 202
9.3.3 Handwriting-based features 204
9.4 Experimental evaluation 204
9.4.1 Methodology 204
9.4.2 Evaluation results 207

9.5 Conclusions and future work 212
Acknowledgements 213
References 213

10 Presentation attack detection in voice biometrics 217
Pavel Korshunov and Sébastien Marcel

10.1 Introduction 218
10.1.1 Databases 219
10.1.2 Evaluation 221
10.2 Vulnerability of voice biometrics 222
10.3 Presentation attack detection approaches 223
10.3.1 Features 225
10.3.2 Classifiers 225
10.3.3 Fusion 226
10.4 PADs failing to generalize 227
10.5 Integration of PAD and ASV 231
10.6 Conclusions 233
Acknowledgments 234
References 234

11 Benford's law for classification of biometric images 237
Aamo Iorliam, Anthony T. S. Ho, Norman Poh, Xi Zhao and Zhe Xia

11.1 Introduction 237
11.2 Related work 238
11.2.1 Benford's law 238
11.2.2 Neural networks 242
11.2.3 Mixed biometric data classification to preserve privacy 243
11.3 Experimental setup 244
11.3.1 Separation of different types of biometric images 244
11.3.2 Data sets 244
11.3.3 Divergence metric and separability of biometric databases 245
11.4 Proposed method 248
11.4.1 Method description 249
11.5 Results and discussion 250
11.5.1 Inter-class separability of biometric images 250
11.5.2 Intra-class separability of biometric images 252
11.5.3 Mixed inter-class and intra-class separability of biometric images 253
11.5.4 Comparative analysis between inter-class, intra-class and mixture of inter-class and intra-class classification of biometric images 254
11.6 Conclusion and future work 255
References 255

PART IV User-centricity and the future **257**

12 Random projections for increased privacy **257**
Sabah Jassim

12.1 Introduction 259
12.2 Evolution of privacy threats 261
12.2.1 Pre-cloud privacy 261
12.2.2 Post-cloud privacy 263
12.2.3 Towards a privacy protection strategy 264
12.3 The dual role of biometrics in privacy protection 265
12.3.1 Face biometrics 267
12.3.2 Speaker recognition 269
12.4 De-identification of biometric data 270
12.4.1 Existing face image de-identification 271
12.4.2 Biometric template protection schemes 271
12.5 Random projections 278
12.5.1 RP generation schemes 279
12.5.2 Construction of Hadamard matrices 282
12.5.3 Hadamard-based RP dictionaries for de-identification of biometric data 284
12.5.4 Analytical notes on the performance and security of block diagonal Hadamard RP 286
12.6 Conclusion 287
References 288

13 De-identification for privacy protection in biometrics **293**
Slobodan Ribarić and Nikola Pavešić

13.1 Introduction 293
13.2 De-identification and irreversible de-identification 296
13.2.1 De-identification and anonymization 296
13.2.2 Multimodal de-identification 296
13.2.3 Taxonomy of the personal identifiers 297
13.3 De-identification of physiological biometric identifiers 297
13.3.1 Face de-identification in still images 297
13.3.2 Face de-identification in videos 301
13.3.3 Fingerprint de-identification 302
13.3.4 Iris de-identification 304
13.3.5 Ear de-identification 305
13.4 De-identification of behavioural biometric identifiers 306
13.4.1 Voice de-identification 306
13.4.2 Gait and gesture de-identification 309

13.5 De-identification of soft biometric identifiers 310
13.5.1 Body silhouette de-identification 310
13.5.2 Gender, age, race and ethnicity de-identification 312
13.5.3 Scars, marks and tattoos de-identification 312
13.6 Conclusion 313
Acknowledgements 314
References 315

14 Secure cognitive recognition: brain-based biometric cryptosystems using EEG 325
Emanuele Maiorana and Patrizio Campisi

Abstract 325
14.1 Introduction 325
14.2 EEG-based biometric recognition 327
14.3 Proposed cognitive biometric cryptosystems 328
14.3.1 Preprocessing 329
14.3.2 Unprotected systems 330
14.3.3 Protected system 331
14.3.4 Exploiting multiple biometric representations: information fusion 333
14.4 Experimental tests 335
14.4.1 Experimental setup 335
14.4.2 Experimental results 336
14.5 Conclusions 349
References 349

15 A multidisciplinary analysis of the implementation of biometric systems and their implications in society 353
Vassiliki Andronikou, Stefanos Xefteris, Theodora Varvarigou, and Panagiotis Bamidis

15.1 Introduction 353
15.2 The ICT landscape for biometric systems 355
15.2.1 Internet of Things 355
15.2.2 Cloud infrastructures for biometrics 356
15.3 The new implementation potential 357
15.4 Evolution of biometric systems 359
15.4.1 Enabling advanced privacy 359
15.4.2 Ubiquitous biometrics 362
15.4.3 Indian Unique ID project: a large-scale implementation example 362

15.5 The societal implications 365
15.5.1 Biometric data collection 366
15.5.2 Biometrics in social media 367
15.5.3 Other secondary uses of biometric data 369
15.5.4 Other concerns 370
15.6 Conclusions 371
References 371

16 Biometrics, identity, recognition and the private sphere where we are, where we go 377
Emilio Mordini

Abstract 377
16.1 Introduction 377
16.2 Identity, identification, recognition 379
16.3 Personal recognition through human history 381
16.4 Where are we going? 386
16.4.1 Global mobility of people 386
16.4.2 Digital economy 390
16.5 Privacy, person and human dignity 392
16.5.1 Is biometric inherently demeaning? 393
16.6 Conclusions 396
References 397

Index 401