

Contents

Preface	v
1. An Introduction to Biometric Authentication Systems	1
1.1 Introduction	1
1.2 A Quick Historical Overview	2
1.3 The “Best” Biometric Characteristic	3
1.4 The Applications	4
1.5 A Taxonomy of Uses	5
1.6 A Taxonomy of Application Environments	7
1.6.1 Overt Versus Covert	7
1.6.2 Habituated Versus Non-Habituated	8
1.6.3 Attended Versus Non-Attended	8
1.6.4 Standard Versus Non-Standard Environment	8
1.6.5 Public Versus Private	8
1.6.6 Open Versus Closed	8
1.6.7 Examples of the Classification of Applications	9
1.7 A System Model	9
1.7.1 Data Collection	9
1.7.2 Transmission	11
1.7.3 Signal Processing	11
1.7.4 Storage	13
1.7.5 Decision	14
1.8 Biometrics and Privacy	14
1.9 The Road Ahead	17
References	17
2. Fingerprint Identification Technology	21
2.1 History	21
2.1.1 Early Biometric Efforts	21
2.2 Applications of Fingerprints	22
2.2.1 Forensics	22
2.2.2 Genetics	23
2.2.3 Civil and Commercial	23
2.2.4 Government	24
2.3 Early Systems	24
2.3.1 Manual Card Files	24
2.3.2 Classification	25
2.3.3 Searching	27
2.3.4 Matching	27
2.4 Early Automation Efforts	27
2.4.1 US NBS/NIST Research	28

2.4.2	Royal Canadian Police	28
2.4.3	FBI	28
2.4.4	United Kingdom	29
2.4.5	Japan	30
2.5	The Technology	30
2.5.1	Scanning and Digitizing	30
2.5.2	Enhancement	33
2.5.3	Feature Extraction	38
2.5.4	Classification	41
2.5.5	Matching	43
2.5.6	Searching	48
2.5.7	Manual Verification	49
2.6	Criminal Applications	49
2.6.1	National Systems	49
2.6.2	Local Systems	51
2.6.3	Interoperability	52
2.6.4	“Daubert” Questions	53
2.7	Civil Applications	54
2.7.1	Welfare Fraud Reduction	54
2.7.2	Border Control	55
2.7.3	Driver registration	55
2.8	Commercial Applications	56
2.8.1	Miniaturized Sensors	56
2.8.2	Personal Access Protection	57
2.8.3	Banking Security	58
2.8.4	Business-to-Business Transactions	58
	References	59
3.	Iris Recognition	63
3.1	Introduction	63
3.2	Anatomical and Physiological Underpinnings	65
3.3	Sensing	68
3.4	Iris signature representation and matching	74
3.4.1	Localization	74
3.4.2	Representation	77
3.4.3	Matching	79
3.5	Systems and performance	86
3.6	Future directions	90
	References	92
4.	Face Recognition	97
4.1	Introduction	97
4.2	Background	98
4.3	Face Detection	99
4.4	Face Recognition: Representation and Classification	100
4.4.1	Some Representation Techniques and Their Applications to Face Recognition	101

4.4.2	Some Classification Techniques and Their Applications to Face Recognition	103
4.5	Kernel-Based Methods and 3D Model-based Methods for Face Recognition	105
4.6	Learning the Face Space	106
4.6.1	Evolutionary Pursuit	106
4.6.2	Face Recognition Using Evolutionary Pursuit	108
4.7	Conclusion	109
	References	110
5.	Elements of Speaker Verification	115
5.1	Introduction	115
5.1.1	The Speaker Verification Problem	115
5.2	Features and Models	120
5.2.1	Speech Features	120
5.2.2	Speaker Models	121
5.3	Additional Methods for Managing Variability	126
5.3.1	Channel Normalization and Modeling	126
5.3.2	Constraining the Text	128
5.4	Measuring Performance	129
5.4.1	How Well do These Systems Perform?	131
5.5	Alternative Approaches	131
5.5.1	Speech Recognition Approaches	131
5.5.2	Words (and Phonetic Units) Count	132
5.5.3	Models Exploring the Shape of Feature Space	133
5.6	Summary	133
	References	134
6.	Technology Evaluation of Fingerprint Verification Algorithms	137
6.1	Introduction	137
6.2	FVC2000 Organization and Algorithms Submission Rules	139
6.3	Databases	142
6.4	Performance Evaluation	149
6.5	Results	151
6.6	Organization of FVC2002	155
6.7	Conclusions	158
	Appendix A	159
	Appendix B	159
	References	204
7.	Methods for Assessing Progress in Face Recognition	207
7.1	Introduction	207
7.2	Face Recognition Evaluations	208
7.2.1	Introduction to FERET and FRVT 2000	208
7.2.2	September 1996 FERET Evaluation Protocol	212
7.2.3	Data Sets	215
7.2.4	FERET and FRVT 2000 Results	218

7.2.5	Conclusions Drawn from the FERET Evaluations and FRVT 2000	225
7.3	Meta-Analysis	227
7.3.1	Introduction to Meta-Analysis	228
7.3.2	Methodology for Selecting Papers	229
7.3.3	Analysis of Performance Scores – Viewing the Data Through Histograms	230
7.3.4	Evaluation of Experiments with a Baseline	232
7.3.5	Meta-Analysis Conclusions	234
7.4	Conclusion	236
	Acknowledgements	237
	References	237
8.	The NIST speaker recognition evaluation program	241
8.1	Introduction	241
8.2	NIST Speaker Recognition Evaluation Tasks	242
8.2.1	One-Speaker Detection	243
8.2.2	Two-Speaker Detection	243
8.2.3	Speaker Tracking	243
8.2.4	Speaker Segmentation	244
8.3	Data	244
8.3.1	Speaker Training	245
8.3.2	Test Segments	245
8.4	Performance Measure	247
8.5	Evaluation Results	248
8.6	Factors Affecting Detection Performance	249
8.6.1	Duration	250
8.6.2	Pitch	250
8.6.3	Handset Differences	251
8.6.4	Handset Type	252
8.6.5	Landline vs. Cellular	255
8.7	Extended Data Evaluation	256
8.8	Multimodal Evaluation	258
8.9	Future Plans	260
	References	261
9.	Large-Scale Identification System Design	263
9.1	Introduction	263
9.1.1	Historical Background	263
9.1.2	Large-Scale Identification Systems: Requirements and Basic Features	265
9.2	Extrapolation of Accuracy	266
9.2.1	Introduction	266
9.2.2	Key Concepts	268
9.2.3	Method 1: Extrapolation from Experiences	269
9.2.4	Method 2: Identification as a Succession of N Verifications	270
9.2.5	Method 3: Extrapolation with Extreme Value	272

9.2.6	Method 4: Extrapolation when the Distance Can Be Modeled	275
9.2.7	Influence of Classification	276
9.3	Conclusion	279
	Appendix	281
	References	286
10.	Biometric System Integration	289
10.1	Understanding, Describing and Documenting the Requirements	289
10.2	Choosing the Technology	291
10.3	Application Development	294
10.4	Integration with Existing System Architecture	296
10.5	Templates and Enrollment Management	297
10.6	Understanding User Psychology	300
10.7	Fine Tuning the System	302
10.8	Ongoing Management	305
10.9	Related Issues	306
	References	309
11.	Biometrics and the US Constitution	311
11.1	Introduction	311
11.1.1	Privacy Versus Security; Mankind Versus Machine	311
11.1.2	The Growth of Both Anonymous Public Transactions and the Complexity of Identification	312
11.1.3	Constitutional Concerns	313
11.2	Due Process	314
11.2.1	Entitlements and Rights	314
11.2.2	Instrumental and Intrinsic Approaches	315
11.2.3	Constitutional Development: From the Intrinsic to the Instrumental Approach of Procedural Due Process	317
11.2.4	The Enigma of Substantive Due Process	320
11.3	Individual Privacy	322
11.3.1	The Basis of an Inferred Right to Privacy	322
11.3.2	Privacy and the Fourth Amendment	323
11.3.3	Privacy and the Fifth Amendment	325
11.3.4	Privacy of Personal Information	326
11.4	Conclusions	328
	References and Notes	329
12.	Privacy Issues in the Application of Biometrics: a European Perspective	335
12.1	Introduction	335
12.2	Privacy – from Philosophical Concept to a Human Right	337
12.3	The European Personal Data Directive	340
12.4	Applying the Directive and National Laws to Biometric Systems	342
12.4.1	Biometric Data as “Personal Data”	343
12.4.2	Biometrics and Sensitive Data	345

12.4.3 Proportionality Principle	346
12.4.4 First Principle Compliance – Fair and Lawful Processing	346
12.4.5 Fourth Principle Compliance – Accuracy	347
12.4.6 Seventh Principle Compliance – Security	347
12.4.7 Eighth Principle Compliance – Transfer to Third Countries	348
12.4.8 Automatic Decision-Making	348
12.4.9 Exemptions	349
12.5 Article 8 of the European Human Rights Convention	349
12.6 The Role of Privacy-Enhancing Technologies	350
12.7 Looking to the Future	351
12.8 Social and Psychological Context of the Application of Biometric Methods	353
12.9 Conclusions	356
References	356
Index	361



<http://www.springer.com/978-1-85233-596-0>

Biometric Systems

Technology, Design and Performance Evaluation

Wayman, J.L.; Jain, A.K.; Maltoni, D.; Maio, D. (Eds.)

2005, XIV, 370 p., Hardcover

ISBN: 978-1-85233-596-0