

Contents

1	INTRODUCTION	1
1.1	Person Recognition	2
1.2	Biometric Systems	3
1.2.1	Enrollment and recognition phases	4
1.2.2	Sensor module	4
1.2.3	Feature extraction module	6
1.2.4	Database module	9
1.2.5	Matching module	9
1.3	Biometric Functionalities	10
1.3.1	Verification	10
1.3.2	Identification	11
1.4	Biometric System Errors	13
1.4.1	Performance measures	17
1.5	The Design Cycle of Biometric Systems	27
1.5.1	Nature of the application	28
1.5.2	Choice of biometric trait	29
1.5.3	Data collection	36
1.5.4	Choice of features and matching algorithm	36
1.5.5	Evaluation	37
1.6	Applications of Biometric Systems	39
1.7	Security and Privacy Issues	41
1.8	Summary	44
	Bibliographical and Historical Remarks	45
	References	47
2	FINGERPRINT RECOGNITION	51
2.1	Introduction	51
2.2	Friction Ridge Pattern	54
2.2.1	Features	54
2.2.2	Formation	59
2.3	Fingerprint Acquisition	60

2.3.1	Sensing techniques	60
2.3.2	Image quality	62
2.4	Feature Extraction	64
2.4.1	Ridge orientation and frequency estimation	64
2.4.2	Singularity extraction	67
2.4.3	Ridge extraction	70
2.4.4	Minutiae extraction	71
2.5	Matching	72
2.5.1	Alignment	74
2.5.2	Pairing minutiae	76
2.5.3	Match score generation	77
2.5.4	Latent fingerprint matching	78
2.5.5	Fingerprint individuality	80
2.5.6	Performance evaluation	80
2.6	Fingerprint Indexing	81
2.7	Fingerprint Synthesis	84
2.7.1	Level 1 feature synthesis	84
2.7.2	Level 2 feature synthesis	85
2.8	Palmprint	85
2.8.1	Palmprint features	87
2.8.2	Palmprint recognition in forensics	88
2.8.3	Palmprint recognition for access control	90
2.9	Summary	91
	Bibliographical and Historical Remarks	92
	References	94
3	Face Recognition	97
3.1	Introduction	97
3.1.1	Psychology of face recognition	98
3.1.2	Facial features	100
3.1.3	Design of a face recognition system	103
3.2	Image Acquisition	104
3.2.1	2D Sensors	105
3.2.2	3D Sensors	106
3.2.3	Video sequences	107
3.3	Face Detection	109
3.3.1	Viola-Jones face detector	111
3.4	Feature Extraction and Matching	116
3.4.1	Appearance-based face recognition	118
3.4.2	Model-based face recognition	122
3.4.3	Texture-based face recognition	124
3.4.4	Performance evaluation	127
3.5	Advanced Topics	129
3.5.1	Handling pose, illumination, and expression variations	129
3.5.2	Heterogeneous face recognition	130

3.5.3	Face modeling	132
3.6	Summary	137
	Bibliographical and Historical Remarks	137
	References	138
4	Iris Recognition	141
4.1	Introduction	141
4.2	Design of an Iris Recognition System	144
4.3	Image Acquisition	146
4.4	Iris Segmentation	151
4.4.1	Segmentation using the integro-differential operator	152
4.4.2	Segmentation using Geodesic Active Contours (GAC)	153
4.4.3	Generating iris masks	159
4.5	Iris Normalization	159
4.6	Iris Encoding and Matching	161
4.7	Iris Quality	164
4.7.1	Quality assessment techniques	164
4.8	Performance Evaluation	169
4.9	Summary	170
	Bibliographical and Historical Remarks	171
	References	172
5	Additional Biometric Traits	175
5.1	Introduction	175
5.2	Ear	176
5.2.1	Ear detection	177
5.2.2	Ear recognition	178
5.2.3	Challenges in ear recognition	180
5.3	Gait	182
5.3.1	Feature extraction and matching	183
5.3.2	Challenges in gait recognition	185
5.4	Hand Geometry	186
5.4.1	Image capture	186
5.4.2	Hand segmentation	188
5.4.3	Feature Extraction	189
5.4.4	Feature matching	189
5.4.5	Challenges in hand geometry recognition	190
5.5	Soft Biometrics	190
5.5.1	Periocular	191
5.5.2	Face marks	194
5.5.3	Tattoo	201
5.6	Summary	206
	References	207

6	MULTIBIOMETRICS	209
6.1	Introduction	209
6.2	Sources of Multiple Evidence	212
6.2.1	Multi-sensor systems	213
6.2.2	Multi-algorithm systems	215
6.2.3	Multi-instance systems	217
6.2.4	Multi-sample systems	218
6.2.5	Multimodal systems	219
6.3	Acquisition and Processing Architecture	221
6.3.1	Acquisition sequence	221
6.3.2	Processing sequence	222
6.4	Fusion Levels	224
6.4.1	Sensor-level fusion	226
6.4.2	Feature-level fusion	227
6.4.3	Score-level fusion	232
6.4.4	Rank-level fusion	246
6.4.5	Decision-level fusion	250
6.5	Summary	253
	Bibliographical and Historical Remarks	254
	References	256
7	SECURITY OF BIOMETRIC SYSTEMS	259
7.1	Introduction	259
7.2	Adversary Attacks	264
7.2.1	Insider attacks	264
7.2.2	Infrastructure attacks	266
7.3	Attacks at the User Interface	268
7.3.1	Impersonation	268
7.3.2	Obfuscation	269
7.3.3	Spoofing	269
7.3.4	Countermeasure: spoof detection	272
7.4	Attacks on Biometric Processing	278
7.4.1	Attacks on the system modules	278
7.4.2	Attacks at the interconnections	280
7.5	Attacks on the Template Database	283
7.5.1	Countermeasure: biometric template security	284
7.6	Summary	302
	Bibliographical and Historical Remarks	302
	References	304
	Index	307