

Biometric Systems

James Wayman, Anil Jain, Davide Maltoni
and Dario Maio (Eds)

Biometric Systems

**Technology, Design and Performance
Evaluation**



Springer

James Wayman
San Jose State University, USA

Anil Jain
Michigan State University, USA

Davide Maltoni
University of Bologna, Italy

Dario Maio
University of Bologna, Italy

British Library Cataloguing in Publication Data
Biometric Systems : technology, design and performance
evaluation
1. Biometric identification 2. Electronic security systems
I. Wayman, James
621.3'8928

ISBN 1852335963

A catalog record for this book is available from the Library of Congress

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

ISBN 1-85233-596-3 Springer-Verlag London Berlin Heidelberg
Springer Science+Business Media
springeronline.com

© Springer-Verlag London Limited 2005
Printed in the United States of America

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Ian Kingston Editorial Services, Nottingham, UK
34/3830-543210 Printed on acid-free paper SPIN 10867755

Preface

The use of computers to recognize humans from physical and behavioral traits dates back to the digital computer evolution of the 1960s. But even after decades of research and hundreds of major deployments, the field of biometrics remains fresh and exciting as new technologies are developed and old technologies are improved and fielded in new applications. Worldwide over the past few years, there has been a marked increase in both government and private sector interest in large-scale biometric deployments for accelerating human-machine processes, efficiently delivering human services, fighting identity fraud and even combating terrorism. The purpose of this book is to explore the current state of the art in biometric systems and it is the system aspect that we have wished to emphasize.

By their nature, biometric technologies sit at the exact boundary of the human-machine interface. But like all technologies, by themselves they can provide no value until deployed in a *system* with support hardware, network connections, computers, policies and procedures, all tuned together to work with *people* to improve some real business process within a social structure.

In this book, we bring together some of the most respected and experienced international researchers and practitioners in the field to look closely at biometric systems from many disciplinary angles. We focus on the technologies of fingerprint, iris, face and speaker recognition, how those technologies have evolved, how they work, and how well they work as determined in recent test programs. We look at the challenges of designing and deploying biometrics in people-centered systems, particularly when those systems become large. We conclude with discussions on the legal and privacy issues of biometric deployments from both European and US perspectives. We hope you find this book valuable in understanding both the historical accomplishments and remaining challenges in this fascinating field.

James Wayman
Anil Jain
Davide Maltoni
Dario Maio
31 July 2004

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

List of Contributors

Robert J. Allen

Allen Consultants LLC
Robert.Allen7@att.net

Julian Ashbourn

International Biometric
Foundation
ibf@1to1.org

J. Mike Bone

NAVSEA Crane Division
Bone_Mike@crane.navy.mil

Duane Blackburn

Federal Bureau of Investigation
Duane.Blackburn@ic.fbi.gov

Joseph P. Campbell, Jr.

Massachusetts Institute of
Technology, Lincoln Laboratory
j.campbell@ieee.org

Raffaele Cappelli

University of Bologna
cappelli@csr.unibo.it

Jean-Christophe Fondeur

Sagem
jean-christophe.fondeur
@sagem.com

Herbert Gish

BBN Technologies
hgish@bbn.com

Patrick Grother

National Institute of Standards and
Technology
pgrother@NIST.gov

Herve Jarosz

Sagem
herve.jarosz@sagem.com

Anil K. Jain

Michigan State University
jain@cse.msu.edu

Chengjun Liu

New Jersey Institute of Technology
liu@cs.njit.edu

Davide Maltoni

University of Bologna
maltoni@csr.unibo.it

Dario Maio

University of Bologna
dmaio@deis.unibo.it

Alvin Martin

National Institute of Standards and
Technology
alvin.martin@nist.gov

Elaine Newton

Rand Corporation
enewton@cmu.edu

Kenneth P. Nuger

San Jose State University
kpnuger@email.sjsu.edu

P. Jonathon Phillips

National Institute of Standards and
Technology
Jonathon@nist.gov

Salil Prabhakar

Digital Persona, Inc.
SalilP@digitalpersona.com

Mark Przybocki

National Institute of Standards and
Technology
mark.przybocki@nist.gov

Marek Rejman-Greene

BTEExact Technologies
marek.rejman-greene@bt.com

Pat Sankar

U.S. Naval Postgraduate School
patsankar@yahoo.com

James L. Wayman

San Jose State University
jlwayman@aol.com

Harry Wechsler

George Mason University
Wechsler@cs.gmu.edu

Richard Wildes

York University
wildes@cs.yorku.ca

An Introduction to Biometric Authentication Systems

1

James Wayman, Anil Jain, Davide Maltoni and Dario Maio

1.1 Introduction

Immigration cards holding both passport number and measures of the user's hand [1]; fingerprints taken as a legal requirement for a driver license, but not stored anywhere on the license [2]; automatic facial recognition systems searching for known card cheats in a casino [3]; season tickets to an amusement park linked to the shape of the purchaser's fingers [4]; home incarceration programs supervised by automatic voice recognition systems [5]; and confidential delivery of health care through iris recognition [6]: these systems seem completely different in terms of purpose, procedures, and technologies, but each uses "biometric authentication" in some way. In this book, we will be exploring many of the technologies and applications that make up the field of "biometric authentication" – what unites them and what differentiates them from each other. In this chapter, we want to present a systematic approach to understanding in a unified way the multitude of technologies and applications of the field.

We start with a narrow definition, designed as much to limit the scope of our inquiry as to determine it.

"Biometric technologies" are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic [7, 8].

There are two key words in this definition: "automated" and "person". The word "automated" differentiates biometrics from the larger field of human identification science. Biometric authentication techniques are done completely by machine, generally (but not always) a digital computer. Forensic laboratory techniques, such as latent fingerprint, DNA, hair and fiber analysis, are not considered part of this field. Although automated identification techniques can be used on animals, fruits and vegetables [9], manufactured goods and the deceased, the subjects of biometric authentication are living humans. For this reason, the field should perhaps be more accurately called "anthropometric authentication".

The second key word is "person". Statistical techniques, particularly using fingerprint patterns, have been used to differentiate or connect

groups of people [10, 11] or to probabilistically link persons to groups, but biometrics is interested only in recognizing people as individuals. All of the measures used contain both physiological and behavioral components, both of which can vary widely or be quite similar across a population of individuals. No technology is purely one or the other, although some measures seem to be more behaviorally influenced and some more physiologically influenced. The behavioral component of all biometric measures introduces a “human factors” or “psychological” aspect to biometric authentication as well.

In practice, we often abbreviate the term “biometric authentication” as “biometrics”, although the latter term has been historically used to mean the branch of biology that deals with its data statistically and by quantitative analysis [12].

So “biometrics”, in this context, is the use of computers to recognize people, despite all of the across-individual similarities and within-individual variations. Determining “true” identity is beyond the scope of any biometric technology. Rather, biometric technology can only link a person to a biometric pattern and any identity data (common name) and personal attributes (age, gender, profession, residence, nationality) presented at the time of enrollment in the system. Biometric systems inherently require no identity data, thus allowing anonymous recognition [4].

Ultimately, the performance of a biometric authentication system, and its suitability for any particular task, will depend upon the interaction of individuals with the automated mechanism. It is this interaction of technology with human physiology and psychology that makes “biometrics” such a fascinating subject.

1.2 A Quick Historical Overview

The scientific literature on quantitative measurement of humans for the purpose of identification dates back to the 1870s and the measurement system of Alphonse Bertillon [13–17]. Bertillon’s system of body measurements, including such measures as skull diameter and arm and foot length, was used in the USA to identify prisoners until the 1920s. Henry Faulds, William Herschel and Sir Francis Galton proposed quantitative identification through fingerprint and facial measurements in the 1880s [18–20]. The development of digital signal processing techniques in the 1960s led immediately to work in automating human identification. Speaker [21–26] and fingerprint recognition [27] systems were among the first to be explored. The potential for application of this technology to high-security access control, personal locks and financial transactions was recognized in the early 1960s [28]. The 1970s saw development and deployment of hand geometry systems [29], the start of large-scale testing [30] and increasing interest in government use of these “automated personal identification” technologies [31]. Retinal [32, 33] and signature verification [34, 35] systems came in the 1980s, followed by face [36–42] systems. Iris recognition [43, 44] systems were developed in the 1990s.

1.3 The “Best” Biometric Characteristic

Examples of physiological and behavioral characteristics currently used for automatic identification include fingerprints, voice, iris, retina, hand, face, handwriting, keystroke, and finger shape. But this is only a partial list as new measures (such as gait, ear shape, head resonance, optical skin reflectance and body odor) are being developed all of the time. Because of the broad range of characteristics used, the imaging requirements for the technology vary greatly. Systems might measure a single one-dimensional signal (voice); several simultaneous one-dimensional signals (handwriting); a single two-dimensional image (fingerprint); multiple two-dimensional measures (hand geometry); a time series of two-dimensional images (face and iris); or a three-dimensional image (some facial recognition systems).

Which biometric characteristic is best? The ideal biometric characteristic has five qualities: robustness, distinctiveness, availability, accessibility and acceptability [45, 46]. By “robust”, we mean unchanging on an individual over time. By “distinctive”, we mean showing great variation over the population. By “available”, we mean that the entire population should ideally have this measure in multiples. By “accessible”, we mean easy to image using electronic sensors. By “acceptable”, we mean that people do not object to having this measurement taken from them.

Quantitative measures of these five qualities have been developed [47–50]. Robustness is measured by the “false non-match rate” (also known as “Type I error”), the probability that a submitted sample will not match the enrollment image. Distinctiveness is measured by the “false match rate” (also known as “Type II error”) – the probability that a submitted sample will match the enrollment image of another user. Availability is measured by the “failure to enroll” rate, the probability that a user will not be able to supply a readable measure to the system upon enrollment. Accessibility can be quantified by the “throughput rate” of the system, the number of individuals that can be processed in a unit time, such as a minute or an hour. Acceptability is measured by polling the device users. The first four qualities are inversely related to their above measures, a higher “false non-match rate”, for instance, indicating a lower level of robustness.

Having identified the required qualities and measures for each quality, it would seem a straightforward problem to simply run some experiments, determine the measures, and set a weighting value for the importance of each, thereby determining the “best” biometric characteristic. Unfortunately, for all biometric characteristics, all of the desired qualities have been found to be highly dependent on the specifics of the application, the population (both their physiological and psychological states), and the hardware/software system used [51–54]. We cannot predict performance metrics for one application from tests on another. Further, the five metrics, which are correlated in a highly complex way, can be manipulated to some extent by administration policy.