



Biometrics

Identity Verification in a Networked World

▶ ***A Wiley Tech Brief***

Samir Nanavati
Michael Thieme
Raj Nanavati



Biometrics

Identity Verification in a Networked World

A Wiley Tech Brief



Samir Nanavati
Michael Thieme
Raj Nanavati

Wiley Computer Publishing



John Wiley & Sons, Inc.

NEW YORK • CHICHESTER • WEINHEIM • BRISBANE • SINGAPORE • TORONTO

Publisher: Robert Ipsen
Editor: Margaret Eldridge
Editor: Adaobi Obi
Managing Editor: Micheline Frederick
Text Design & Composition: John Wiley Composition Services

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc., is aware of a claim, the product names appear in initial capital or ALL CAPITAL LETTERS. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

This book is printed on acid-free paper. ∞

Copyright © 2002 by Samir Nanavati. All rights reserved.

Published by John Wiley & Sons, Inc.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4744. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 605 Third Avenue, New York, NY 10158-0012, (212) 850-6011, fax (212) 850-6008, E-mail: PERMREQ@WILEY.COM.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in professional services. If professional advice or other expert assistance is required, the services of a competent professional person should be sought.

ISBN: 0471-09945-7

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Wiley Tech Brief Series

Other titles in this series:

Optical Networking, by Deborah Cameron, ISBN 0471443689

Service Providers, by Joseph R. Matthews and Mary Helen Gillespie, ISBN 0471418188

Internet Appliances, by Ray Rischpater, ISBN 0471441112

PKI, by Tom Austin, ISBN 0471353809

The Wireless Application Protocol (WAP), by Steve Mann and Scott Sbihli, ISBN: 047139992

Palm Enterprise Applications, by Ray Rischpater, ISBN: 0471393797

Wireless Internet Enterprise Applications, by Chetan Sharma, ISBN: 0471383827

Application Service Providers, by Traver Gruen-Kennedy, ISBN: 0471394912

Cryptography and E-Commerce, by Jon Graff, ISBN: 0471405744

Enterprise Application Integration, by William Ruh, Francis X. Maginnis, William Brown, ISBN: 0471376418



Contents



Introduction	xv
Acknowledgements	xix
Part One Biometric Fundamentals	1
<hr/>	
Chapter 1 Why Biometrics?	3
Benefits of Biometrics versus Traditional Authentication Methods	3
Increased Security	4
Increased Convenience	5
Increased Accountability	5
Benefits of Biometrics in Identification Systems	6
Fraud Detection	6
Fraud Deterrence	6
Conclusion: Evaluating the Benefits of Biometric Systems	6
Chapter 2 Key Biometric Terms and Processes	9
Definitions	9
Discussion: Verification and Identification	12
When are Verification and Identification Appropriate?	13
Between Verification and Identification: <i>1:Few</i>	14
Logical versus Physical Access	14



	How Biometric Matching Works	15
	Enrollment and Template Creation	16
	Templates	18
	Biometric Matching	20
	Conclusion	22
Chapter 3	Accuracy in Biometric Systems	23
	False Match Rate	24
	Importance of FMR	25
	When Are False Matches Acceptable?	25
	Single False Match Rate versus System False Match Rate	26
	False Match Rate in Large-Scale Identification Systems	27
	False NonMatch Rate	27
	Importance of FNMR	28
	Changes in a User’s Biometric Data	28
	Changes in User Presentation	29
	Changes in Environment	29
	Real-World False Nonmatch Rates	31
	Single FNMR versus System FNMR	32
	False Nonmatch Rates in Large-Scale Identification Systems	33
	Failure-to-Enroll (FTE) Rate	33
	Importance of FTE Rates	35
	Relation of Failure-to-Enroll to False Nonmatch Rate	35
	FTE across Different Populations	35
	Single FTE Rates versus System FTE Rates	37
	FTE in Large-Scale Identification Systems	38
	Derived Metrics	38
	Equal Error Rate (EER)	38
	Ability-to-Verify (ATV) Rate	39
	Conclusion: Biometric Technologies from an Accuracy Perspective	40
Part 2	Leading Biometric Technologies: What You Need to Know	43
Chapter 4	Finger-Scan	45
	Components	46
	How Finger-Scan Technology Works	48
	Image Acquisition	48
	Image Processing	50
	Location of Distinctive Characteristics	51
	Template Creation	52
	Template Matching	52

	Competing Finger-Scan Technologies	54
	Optical Technology	54
	Silicon Technology	54
	Ultrasound Technology	55
	Feature Extraction Methods: Minutiae versus Pattern Matching	55
	Finger-Scan Deployments	56
	Finger-Scan Strengths	58
	Proven Technology Capable of High Levels of Accuracy	58
	Range of Deployment Environments	58
	Ergonomic, Easy-to-Use Devices	59
	Ability to Enroll Multiple Fingers	59
	Finger-Scan Weaknesses	59
	Inability to Enroll Some Users	59
	Performance Deterioration over Time	60
	Association with Forensic Applications	60
	Need to Deploy Specialized Devices	60
	Finger-Scan: Conclusion	61
Chapter 5	Facial-Scan	63
	Components	64
	How Facial-Scan Technology Works	65
	Image Acquisition	65
	Image Processing	66
	Distinctive Characteristics	67
	Template Creation	68
	Template Matching	68
	Competing Facial-Scan Technologies	69
	Eigenface	69
	Feature Analysis	70
	Neural Network	71
	Automatic Face Processing	71
	Facial-Scan Deployments	72
	Facial-Scan Strengths	72
	Ability to Leverage Existing Equipment and Imaging Processes	73
	Ability to Operate without Physical Contact or User Complicity	73
	Ability to Enroll Static Images	73
	Facial-Scan Weaknesses	74
	Acquisition Environment Effect on Matching Accuracy	74
	Changes in Physiological Characteristics That Reduce Matching Accuracy	74
	Potential for Privacy Abuse Due to Noncooperative Enrollment and Identification	75
	Facial-Scan: Conclusion	75

Chapter 6	Iris-Scan	77
	Components	78
	How It Works	79
	Image Acquisition	79
	Image Processing	80
	Distinctive Features	80
	Template Generation	81
	Template Matching	82
	Deployments	82
	Iris-Scan Strengths	83
	Resistance to False Matching	83
	Stability of Characteristic over Lifetime	84
	Suitability for Logical and Physical Access	84
	Iris-Scan Weaknesses	84
	Difficulty of Usage	85
	False Nonmatching and Failure-to-Enroll	85
	User Discomfort with Eye-Based Technology	85
	Need for a Proprietary Acquisition Device	86
	Iris-Scan: Conclusion	86
Chapter 7	Voice-Scan	87
	Components	88
	How It Works	88
	Data Acquisition	89
	Data Processing	90
	Distinctive Features	90
	Template Creation	91
	Template Matching	92
	Deployments	92
	Voice-Scan Strengths	93
	Ability to Leverage Existing Telephony Infrastructure	94
	Synergy with Speech Recognition and Verbal Account Authentication	94
	Resistance to Imposters	94
	Lack of Negative Perceptions Associated with Other Biometrics	95
	Voice-Scan Weaknesses	95
	Effect of Acquisition Devices and Ambient Noise on Accuracy	95
	Perception of Low Accuracy	96
	Lack of Suitability for Today's PC Usage	96
	Large Template Size	96
	Voice-Scan: Conclusion	97

Chapter 8	Other Physiological Biometrics	99
	Hand-Scan	99
	Components	100
	How It Works	101
	Deployments	102
	Hand-Scan Strengths	103
	Hand-Scan Weaknesses	105
	Conclusion	106
	Retina-Scan	106
	Components	107
	How It Works	107
	Deployments	110
	Retina-Scan Strengths	110
	Retina-Scan Weaknesses	111
	Conclusion	112
	Automated Fingerprint Identification Systems (AFIS)	114
	Components	114
	How It Works	116
	Deployments	119
	How AFIS and Finger-Scan Differ	120
	Conclusion	121
 Chapter 9	 Other Leading Behavioral Biometrics	 123
	Signature-Scan	123
	Components	124
	How It Works	125
	Deployments	127
	Signature-Scan Strengths	128
	Signature-Scan Weaknesses	130
	Conclusion	131
	Keystroke-Scan	132
	Components	134
	How It Works	134
	Keystroke-Scan Strengths	136
	Keystroke-Scan Weaknesses	137
	Conclusion	139
 Part 3	 Biometric Applications and Markets	 141
 Chapter 10	 Categorizing Biometric Applications	 143
	Defining the Seven Biometric Applications	144
	Capacities in Which Individuals Use Biometric Systems	147

Introduction to IBG's Biometric Solution Matrix	147
How Urgent Is the Authentication Problem That Biometrics Are Solving?	148
What Is the Scope of the Authentication Problem That Biometrics Are Solving?	149
How Well Can Biometrics Solve the Authentication Problem?	149
Are Biometrics the Only Possible Authentication Solution?	149
How Receptive Are Users to Biometrics as an Authentication Solution?	149
Chapter 11 Citizen-Facing Applications	151
Criminal Identification	152
Today's Criminal Identification Applications	152
Future Criminal Identification Trends	152
Related Biometric Technologies and Vertical Markets	154
Cost to Deploy Biometrics in Criminal Identification	156
Conclusion	156
Citizen Identification	157
Typical Applications	157
Future Trends in Citizen Identification	158
Related Biometric Technologies and Vertical Markets	161
Cost to Deploy Biometrics in Citizen Identification	161
Issues Involved in Deployment	162
Conclusion	164
Surveillance	164
Today's Surveillance Applications	164
Future Trends in Surveillance	165
Related Biometric Technologies and Vertical Markets	167
Cost to Deploy Biometrics in Surveillance	167
Issues Involved in Deployment	168
Conclusion	169
Chapter 12 Employee-Facing Applications	171
PC/Network Access	171
Today's PC/Network Access Applications	172
Future Trends in PC/Network Access	173
Related Biometric Technologies and Vertical Markets	177
Costs to Deploy Biometrics in PC/Network Access	177
Issues Involved in Deployment	178
Conclusion	180

	Physical Access/Time and Attendance	180
	Today's Physical Access/Time and Attendance Applications	181
	Future Physical Access/Time and Attendance Trends	182
	Related Biometric Technologies and Vertical Markets	183
	Costs to Deploy Biometrics in Physical Access/ Time and Attendance	183
	Issues Involved in Deployment	186
	Conclusion	187
Chapter 13	Customer-Facing Applications	189
	E-Commerce/Telephony	190
	Today's E-Commerce/Telephony Applications	190
	Future E-Commerce/Telephony Trends	191
	Related Biometric Technologies and Vertical Markets	193
	Costs to Utilize Biometrics in E-Commerce/Telephony	193
	Issues Involved in Deployment	198
	Conclusion	201
	Retail/ATM/Point of Sale	201
	Today's Retail/ATM/Point-of-Sale Applications	201
	Future Retail/ATM/Point-of-Sale Trends	203
	Related Biometric Technologies and Vertical Markets	206
	Cost to Deploy Biometrics in Retail/ATM/POS	206
	Issues Involved in Deployment	207
	Conclusion	208
Chapter 14	Biometric Vertical Markets	209
	Five Primary Biometric Vertical Markets	210
	Law Enforcement	211
	Technologies Used in Law Enforcement	211
	Typical Law Enforcement Deployments	211
	Conclusion	213
	Government Sector	214
	Technologies Used in the Government Sector	214
	Typical Government-Sector Deployments	215
	Conclusion	220
	Financial Sector	220
	Technologies Used in the Financial Sector	221
	Typical Financial-Sector Deployments	222
	Conclusion	225

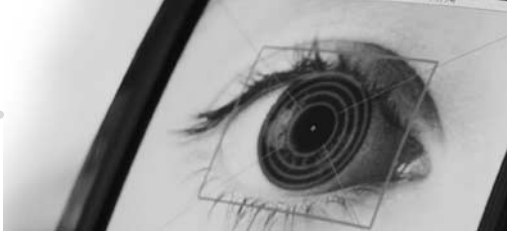
	Healthcare	225
	Technologies Used in Healthcare	226
	Typical Healthcare Deployments	226
	Conclusion	228
	Travel and Immigration	228
	Technologies Used in Travel and Immigration	229
	Typical Travel and Immigration Deployments	229
	Conclusion	231
	Additional Biometric Verticals	231
	Conclusion	233
Part 4	Privacy and Standards In Biometric System Design	235
Chapter 15	Assessing the Privacy Risks of Biometrics	237
	Biometric Deployments on a Privacy Continuum	238
	Privacy Concerns Associated with Biometric Deployments	239
	Informational Privacy	239
	Personal Privacy	243
	Privacy-Sympathetic Qualities of Biometric Technology	244
	Defining Application-Specific Privacy Risks: The BioPrivacy Impact Framework	246
	Overt versus Covert	246
	Opt-in versus Mandatory	248
	Verification versus Identification	249
	Fixed Duration versus Indefinite Duration	250
	Public Sector versus Private Sector	250
	Citizen, Employee, Traveler, Student, Customer, Individual	251
	User Ownership versus Institutional Ownership of Biometric Data	253
	Personal Storage versus Storage in Template Database	253
	Behavioral versus Physiological Biometric Technology	254
	Template Storage versus Identifiable Data Storage	255
	Conclusion	255
	BioPrivacy Technology Risk Ratings	256
Chapter 16	Designing Privacy-Sympathetic Biometric Systems	259
	BioPrivacy Best Practices: Scope and Capabilities	260
	Limit System Scope	260
	Do Not Use Biometrics as a Unique Identifier	260

Limit Retention of Biometric Information	261
Evaluate a System’s Potential Capabilities	263
Limit Storage of Identifiable Biometric Data	264
Limit Collection and Storage of Extraneous Information	264
Make Provisions for System Termination	265
IBG BioPrivacy Best Practices: Data Protection	265
Use Security Tools and Access Policies to Protect Biometric Information	265
Protect Postmatch Decisions	266
Limit System Access	266
Implement Logical and Physical Separations between Biometric and Nonbiometric Data	267
BioPrivacy Best Practices: User Control of Personal Data	267
Make System Usage Voluntary and Allow for Unenrollment	267
Enable Anonymous Enrollment and Verification	268
Provide Means of Correcting and Accessing Biometric-Related Information	268
IBG BioPrivacy Best Practices: Disclosure, Auditing, and Accountability	269
Make Provisions for Third-Party Auditing and Oversight	269
Hold Operators Accountable for System Use and Misuse	269
Fully Disclose Audit Findings	270
Disclose the System Purpose and Objectives	270
Disclose When Individuals May Be Enrolled in a Biometric System	271
Disclose When Individuals May Be Verified in a Biometric System	271
Disclose Whether Enrollment Is Optional or Mandatory	271
Disclose Enrollment, Verification, and Identification Processes	272
Disclose Policies and Protections in Place to Ensure Privacy of Biometric Information	272
Biometrics at the Super Bowl: An IBG BioPrivacy Assessment	273
Conclusion	276

Chapter 17	Biometric Standards	277
	Why Standards?	277
	Application Programming Interfaces	278
	BioAPI	279
	BAPI	280
	Deployers, Developers, and Biometric APIs	280

xiv Contents

File Format	281
Information Security for Financial Services	281
Additional Efforts	282
Fingerprint Template Interoperability	282
CDSA/HRS	284
Conclusion	284
Index	285



Introduction

Authentication is a fundamental component of human interaction with computers. Traditional means of authentication, primarily passwords and personal identification numbers (PINs), have until recently dominated computing, and are likely to remain essential for years to come. However, stronger authentication technologies, capable of providing higher degrees of certainty that a user is who he or she claims to be, are becoming commonplace. Biometrics are one such strong authentication technology.

Biometric technologies as we know them today have been made possible by explosive advances in computing power and have been made necessary by the near universal connectedness of computers around the world. The increased perception of data and information as near equivalents of currency, in conjunction with the opportunities for access provided by the Internet, is a paradigm shift with significant repercussions for authentication. If data is currency, then server-based or local hard drives are our new vaults, and information-rich companies will be held responsible for their security. Because of this, passwords and PINs are nearing the end of their life cycle for many applications.

Since early 1999, four factors (reduced cost, reduced size, increased accuracy, and increased ease of use) have combined to make biometrics an increasingly feasible solution for securing access to computers and networks. But biometrics are much more than a replacement for passwords. Millions of people around the world use biometric technology in applications as varied as time and attendance, voter registration, international travel, and benefits dispersal. Depending on the application, biometrics can be used for security, for convenience, for fraud reduction, even as an empowering technology.

This book teaches you the fundamentals of leading biometric technologies: how they work, their strengths and weaknesses, where they can be effectively

deployed. It helps you understand how biometrics are associated with technologies such as public key infrastructure (PKI) and smart cards. It defines how biometric deployments can be privacy enhancing or privacy invasive. It dispels various myths surrounding biometric technology. Finally, it provides guidelines for successful deployment of biometrics in today's enterprise environment.

How This Book Is Organized

There are many misconceptions about biometric technology that have taken hold in the general public. In order to provide you with a solid understanding of the technology, the industry, the applications, and the challenges that define biometrics, this book is divided into four parts.

Part One: Biometric Fundamentals

Part One provides you with a detailed understanding of the central concepts involved in biometrics, including reasons why the technology is deployed, how the technology operates, the key processes involved in biometric authentication, and how accuracy is defined in biometric systems.

Chapter 1, "Why Biometrics?," discusses why biometrics are of such interest to institutions looking to authenticate employees, customers, and citizens. This chapter also details the benefits that biometric technologies can provide when deployed correctly. Chapter 2, "Key Biometric Terms and Processes," digs deeper into biometric functionality, defining and explaining the variety of terms, both technical and nontechnical, used in the biometric industry. This chapter also discusses the biometric concepts essential to understanding how and why biometrics are deployed today. Chapter 3, "Accuracy in Biometric Systems," defines the categories used to determine how well biometric systems work and examines why most discussions of biometric accuracy are highly misleading.

Part Two: Leading Biometric Technologies

Part Two provides detailed discussions of leading biometric technologies. The information in Part Two is based on real-world experience in deploying and testing systems in operational environments. For each biometric discipline, Part Two addresses in full topics such as system components, data acquisition, template generation and matching, deployments, and strengths and weaknesses. Technologies discussed include finger-scan, facial-scan, iris-scan, retina-scan, signature-scan, keystroke-scan, hand-scan, AFIS, and biometric middleware.

Part Three: Biometric Applications and Markets

Part Three discusses the applications in which biometrics are used and the markets and industries in which they are most effectively deployed. Biometric solutions have emerged in a range of applications, including Citizen ID, Network/PC Access, Surveillance, and e-Commerce/Telephony. These applications can differ substantially in terms of technology selection, privacy impact, and performance requirements. Furthermore, biometrics have emerged as viable solutions in a handful of vertical markets, including government and financial sectors.

Part Four: Privacy and Standards In Biometric System Design

Part Four discusses critical factors related to standards and privacy that institutions must consider when designing, deploying, and maintaining biometric systems for customers, employees, or citizens. Privacy has long been a major issue in biometrics; the emergence of a framework for evaluating the privacy impact of biometric technologies and deployments should help address this central problem. In addition, the emergence of biometric standards has reduced the levels of risk involved in deploying biometric systems.

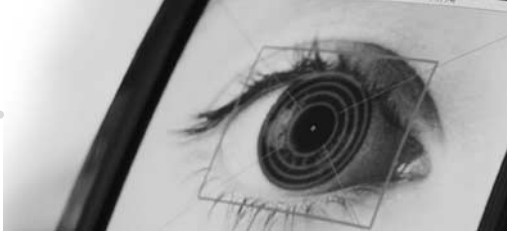
Who Should Read This Book

This book provides public- and private-sector professionals with a real-world understanding of biometric technologies and applications, helping them make informed decisions on the role that biometrics can play in their organization. No background in biometrics is required, but those with biometrics experience will benefit from the detailed discussion of concepts not often presented from a deployer's perspective, such as accuracy, privacy, and technology strengths and weaknesses. Although some of the discussions may go into detail about biometric processes or functions, the book is not intended to be highly technical.

Those new to biometrics are strongly encouraged to read from the beginning, as an understanding of biometrics requires familiarity with the reasons why biometrics are deployed and the key terms involved in biometrics. Those more experienced with biometrics can begin with the technologies of interest to them and move into privacy and system design. However, even those with biometrics experience are encouraged to read the entire book (many basic concepts in the biometrics industry have often been poorly defined or overlooked, a problem that this book addresses).

Looking Forward

Biometric technology has emerged as a viable solution for a range of applications where a person's identity must be verified or determined. No longer a science-fiction solution, biometrics are being deployed to solve security problems, to help companies generate revenues, and to protect personal information. The challenge is to ensure that biometrics are used intelligently and responsibly as the technology moves into the mainstream; the repercussions of unintelligent and irresponsible use could be severe.



Acknowledgments

The authors would like to express their appreciation to those whose diligent efforts have been instrumental to the growth of the biometric industry, and to those who have helped foster a greater understanding of the potential impact of biometrics on today's world:

Cathy Tilton, William Saito, Geoff Slagle, Barry Steinhardt, Peter Hope-Tindall, Colleen Madigan, Joseph Atick, Bill Voltmer, Jeff Stapleton, Paul Reid, Scott Moody, John Ticer, Karl Ware, Vance Bjorn, Erik Bowman, Mitch Tarr, Fernando Podio, Jeff Dunn, Dr. Ann Cavoukian, John Woodward, Dr. Jim Wayman, Dr. Doug McGovern, Peter Higgins, Bill Rogers, Bill Spence, John Harris, Rick Pratt, Dave Troy, Dr. Anil Jain, Oz Pieper, Ron Beyner, Walter Hamilton, Tom Hopper, Mike Garris, Ed German, Colin Soutar, Naeem Zafar, Dr. Bridgette Wirtz, Dave Mintie, Astrid Albrecht, Tony Mansfield, Dr. John Daugman, Denny Carlton, Tim Ruggles, Norm Hughes, Sid Lieberman, Gary Roethenbaugh, Steve Borza, Dr. Larry O'Gorman, Tom Colatosti, Dr. John Schneider, Dennis Quiggle, Jeff Poulson, Allen Ganz, David Hertz, Dae Won Im, Christer Bergman, Fabio Righi, Dr. Jonathan Phillips, Duane Blackburn, P.J. Bulger, and Jean-Marc Suchier.

Special thanks go to: J. Shoor, L. Corbett, J. Goodman, C. Russo, A. Carr, L. Wall, A. Garay, C. Connors, G. Gruber, B. Chen, J. Granato, R. Rasmussen, J. Goding, B. Hyslop, B. Aucoin, J. Homme, C. Thompson, R. Pollard, D. Fuchs, R. Hoyte, E. Olsen, J. Gee, A. Backenroth, M. Hanselman, T. Dorren, J. Medicus, K. Nessman, P. Anther, S. Walsh, M. Nazar, D. Ziemke, C. Nagy, M. Goldberg, I. Beyah, and M. Spivey.

The authors would like to recognize the research, consulting, integration and support professionals of International Biometric Group for their hard work and dedication. Without their creativity, integrity, and commitment,