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

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

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

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
BTExact 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.