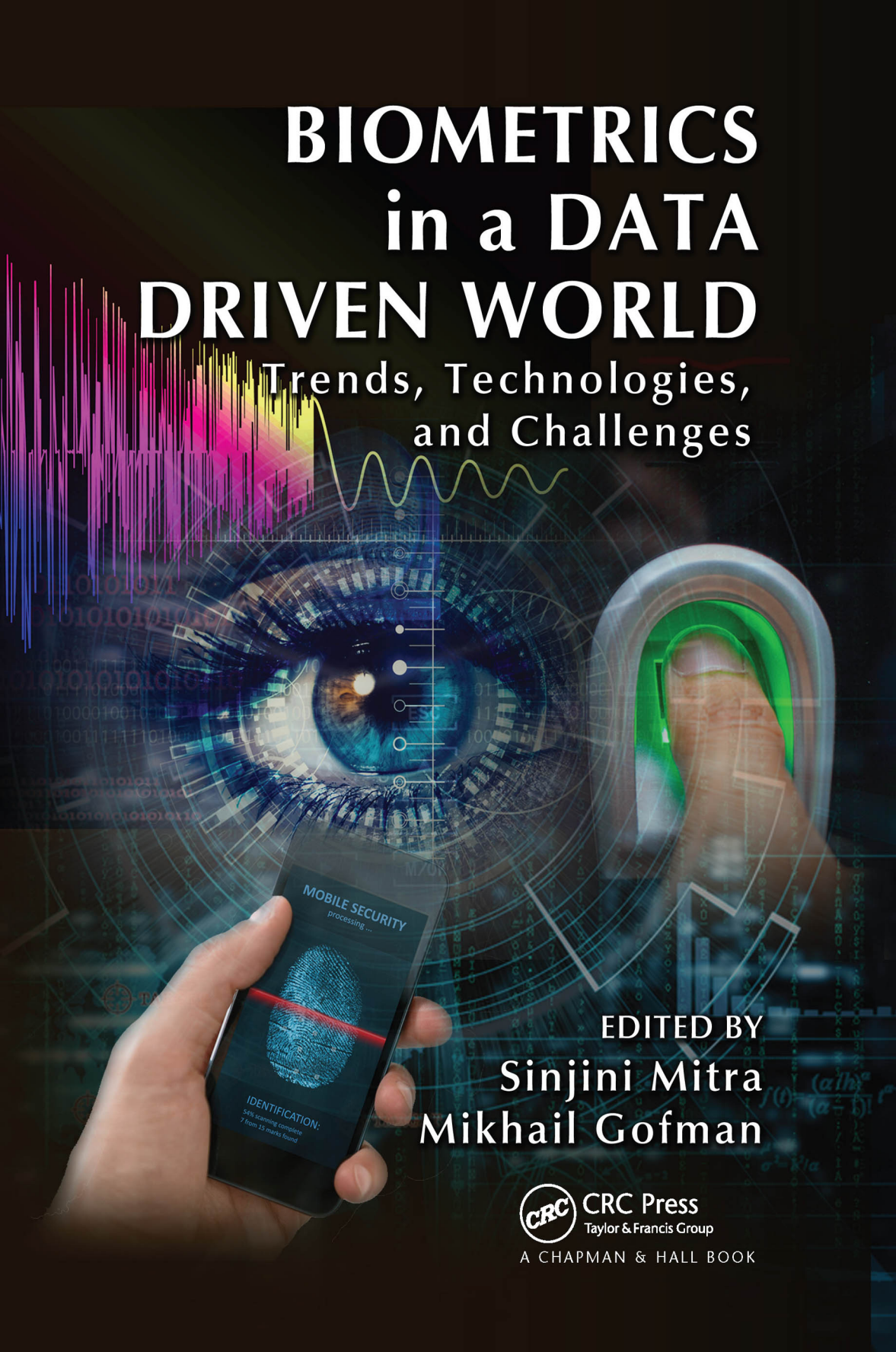
BIOMETRICS in a DATA DRIVEN WORLD

Trends, Technologies, and Challenges



EDITED BY
Sinjini Mitra
Mikhail Gofman

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

BIOMETRICS in a DATA DRIVEN WORLD

Trends, Technologies, and Challenges

BIOMETRICS in a DATA DRIVEN WORLD

Trends, Technologies, and Challenges

EDITED BY
Sinjini Mitra
Mikhail Gofman

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20161028

International Standard Book Number-13: 978-1-4987-3764-7 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

List of Figures

List of Tables

Preface

When studying 31,000-year-old cave wall paintings of prehistoric humans, archeologists occasionally stumble upon a remarkable find—a human handprint. It is believed that these prints were left on the walls of caves to serve as the signatures of the artists. This concept of using human traits for purposes of identification eventually evolved into the intricate and subtle field that is known today as "biometrics."

The word *biometrics* originates from the Greek words *bio* (life) and *metric* (to measure). In traditional statistical literature, the terms "biometrics" and "biometry" have been used since the early twentieth century to refer to the field of development of mathematical methods applicable to data analysis problems in the biological sciences. Some examples include agricultural field experiments to compare the yields of different varieties of a crop and human clinical trials evaluating the relative effectiveness of competing drugs. However, recently the term "biometrics" has also been used to denote the unique physical traits, such as face, fingerprints, and iris, and behavioral characteristics, which include gait, voiceprint, and signature. *Biometric authentication* refers to the science and technology of identifying people based on their physical and behavioral traits. Technological advances as well as new discoveries about the human body and behavioral patterns continue to expand the list of human traits that are useful for identification. For example, recent research has demonstrated the viability of using ear prints, brainwaves, heartbeats, and DNA as basis for verifying identity. It is quite surprising, yet fascinating, to see how this field has evolved following the September 11 attacks in New York City in 2001, particularly over the last 10–15 years.

In today's highly connected and data-driven world, biometrics play critical roles in ensuring national security and are becoming increasingly important in securing mobile and cloud computing applications, as well as improving the quality of health care and transforming the way people experience computer gaming and entertainment.

The aim of this book is to inform readers about the modern applications of biometrics in the context of a data-driven society, to familiarize them with the rich history of biometrics, and to provide them with a glimpse into the future of biometrics.

Section I discusses the fundamentals of biometrics; provides an overview of common biometric modalities, namely face, fingerprints, iris, and voice; discusses the history of the field; and provides an overview of the emerging trends and opportunities.

Section II introduces the reader to a wide range of biometric applications as noted above.

Section III is dedicated to the discussion of case studies of biometric modalities (introduced in Section I) currently used on mobile applications. As smartphones and tablet computers are rapidly becoming the dominant consumer computer platforms, biometrics-based authentication is emerging as an integral part of protecting mobile devices against unauthorized access, while enabling new and highly popular applications such as secure online payment authorization.

Finally, Section IV concludes with a discussion of the future trends and opportunities in the field of biometrics, which pave the way for advancing research in the area of biometrics and for deployment of biometric technologies in real-world applications.

A recurring theme throughout this book is the challenge of implementing automated biometric authentication. This is because making biometrics-based authentication robust requires complex sensor technologies for capturing high biometric quality images (e.g., face photographs or voiceprints) and complex algorithms, which can accurately determine the identity of a person based on the biometric images. Addressing these challenges is an important area of biometrics research which this book discusses.

The book's intended audience includes individuals interested in exploring the contemporary applications of biometrics, from students to researchers and practitioners working in this field. Both undergraduate and graduate students enrolled in college-level security courses will find this book to be an especially useful companion.

Security is of utmost importance today to ensure the safety of the world. From the London bombings of 2005 to the more recent attacks in the airports at Brussels and Istanbul in 2016, there is imminent need to enhance security in different areas. As people will learn from reading this book, biometrics provides a way to accomplish that in many practical security applications.

Acknowledgments

Dr. Sinjini Mitra would first like to acknowledge her PhD advisor and mentor Dr. Stephen Fienberg, Maurice Falk University Professor of Statistics and Social Science at Carnegie Mellon University, who introduced her to this interesting field of biometrics that offer such huge opportunities for cutting-edge research. During her PhD, she received invaluable guidance from Dr. Fienberg and her co-advisor Dr. Anthony Brockwell, currently an adjunct associate professor of statistics at Carnegie Mellon. She also learnt much about the area of biometrics from faculty members in the Robotics Institute and CyLab at Carnegie Mellon, particularly Drs. B.V.K. Vijaya Kumar, Marios Savvides and Yanxi Liu (currently a professor of computer science at Penn State University). Dr. Mitra is grateful to Dr. Tami "Sunnie" Foy at California State University, Fullerton (CSUF) for introducing her to Dr. Mikhail Gofman, which led to the development of a successful long-term research collaboration. Finally, she is also grateful to Dr. Bhushan Kapoor, chair of the Information Systems and Decision Sciences (ISDS) Department, for supporting her biometrics research work throughout her career at CSUF.

Dr. Mikhail Gofman would like to express his sincere gratitude to his PhD advisor Dr. Ping Yang at the State University of New York at Binghamton who had made it possible for him to pursue a rewarding career in academics and research in the field of cybersecurity. In addition, he also would like to thank Drs. Kartik Gopalan and Dmitry Ponomarev at the State University of New York at Binghamton for their support and valuable advice during his student years at the State University of New York at Binghamton. He would also like to extend immense thanks to Drs. Susama Barua and Raman Unnikrishnan for encouraging him to establish and direct the Center for Cybersecurity at CSUF, where he is currently employed. The center's ability to bring together students and faculty to work on biometrics research is simply astounding.

Both authors would like to acknowledge the work done by their undergraduate and graduate student research assistants at CSUF, both at the departments of Computer Science and Information Systems and Decision Sciences (ISDS), whose valuable contributions helped move their biometrics research forward, while at the same time often providing opportunities for stimulating conversations that generated new research ideas. Most notable amongst them are Kevin Cheng, Nicholas Smith, Oyun Togtokhjav, Bo Wen, Yu Liu, and Karthik Karunanithi.

Finally, the authors are grateful to the staff at Taylor & Francis, including Randi Cohen, senior acquisitions editor, and Cynthia Klivecka, for patiently working with us through the process of writing and publishing this book.

Editors

Dr. Sinjini Mitra is currently an assistant professor at the Department of Information Systems and Decision Sciences in the Steven G. Mihaylo College of Business and Economics (MCBE) at California State University, Fullerton (CSUF). At CSUF, she is also the associate director of the Center for Information Technology and Business Analytics (CITBA), a faculty fellow of the Catalyst Center (an interdisciplinary center on teaching and research for STEM [Science, Technology, Engineering and Mathematics] courses) and a faculty associate of the ECS Center for Cybersecurity. Prior to joining CSUF, she was a postdoctoral research associate at the University of Southern California's Information Sciences Institute (USC-ISI), and a postdoctoral research associate at the Department of Statistics and *CyLab* at Carnegie Mellon University.

Dr. Mitra earned her BSc in statistics from Presidency College, Kolkata, MStat from the Indian Statistical Institute, Kolkata, and PhD in statistics from Carnegie Mellon University, USA. Dr. Mitra's research is interdisciplinary, and primary interests include data mining and business analytics, security and biometric authentication, and statistical modeling applications in education, healthcare and information systems. She started working on biometrics research for her PhD dissertation, where she developed various novel statistical models for face recognition and developed an inference-based model framework for performance evaluation of biometric systems. Currently, she is working on developing multimodal biometric systems for consumer mobile devices, and investigating other newer

biometric technologies. She has established several collaborations for her research and has mentored many students at CSUF on biometrics research.

Her teaching interests include business statistics, data mining, data science and analytics. She is a member of the American Statistical Association (ASA), the Institute of Mathematical Statistics (IMS), and the Institute for Operations Research and Management Science (INFORMS). She has around 40 research publications, including 15 peer-reviewed journal articles and 8 book chapters, and presents regularly at national and international conferences. She is the recipient of several intramural awards at CSUF, the MCBE Faculty Excellence Fellowship in 2013 and 2016, and the University award for teamwork and collaboration in 2015. She has also received external grants to support her research work from the National Science Foundation (NSF) and National Institutes of Health (NIH).

Mikhail Gofman is an associate professor of computer science at California State University, Fullerton, where he also directs the Center for Cybersecurity. He earned his PhD in computer science at the State University of New York at Binghamton in 2012. His research interests include access controls, biometrics, and virtualization and cloud security, and his work has been published at top computer science venues.

Contributors

Yoonsuk Choi
Department of Computer Engineering
California State University
Fullerton, California

Christina Dudaklian
Department of Computer Science
California State University
Fullerton, California

Andrey Gubenko
Department of Computer Science
California State University
Fullerton, California

Mahdi Hosseini
Department of Computer Science
California State University
Fullerton, California

Kenneth Kung
Department of Computer Science
California State University
Fullerton, California

Yukhe Lavinia
Department of Computer Science
California State University
Fullerton, California

Charles Li
General Dynamics Information Technology
California State University
Fullerton, California

Jason Ligon
Department of Computer Science
California State University
Fullerton, California

Yu Liu
Department of Computer Science
California State University
Fullerton, California

Regan L. Mandryk
Department of Computer Science
University of Saskatchewan, Saskatchewan, Canada

Rodrigo Martinez
Department of Computer Science
California State University
Fullerton, California

Lennart E. Nacke
Department of Drama and Speech Communication
University of Waterloo
Waterloo, Ontario, Canada

Laurie O'Connor
Department of Systems Engineering
University of California
Los Angeles, California

Christopher Rodney
Department of Computer Science
California State University
Fullerton, California

Yun Tian
Department of Computer Science
California State University
Fullerton, California

Abhishek Verma
Department of Computer Science
California State University
Fullerton, California

Maria Villa
Department of Computer Science
California State University
Fullerton, California

Bo Wen
Center for Information Systems and Technology (CISAT)
Claremont Graduate University
Claremont, California

Alec Yenter
Department of Computer Science
California State University
Fullerton, California

I

Introduction to Biometrics

CHAPTER 1

Overview of Biometric Authentication

Sinjini Mitra, Bo Wen, and Mikhail Gofman

CONTENTS

1.1 INTRODUCTION

Biometrics refer to the unique physiological (face, fingerprints, and ear) and behavioral (keystroke dynamics, voiceprint, and gait) traits of individuals that can be used for identification or verification purposes. *Biometric authentication* refers to the technology of identifying a person or verifying a person's identity based on these unique biometric traits. Such technology is widely deployed in several applications today, from immigration and border control to access control in online banking, ATM, laptops, and mobile phones [1,2]. Passwords and PINs are susceptible to loss, theft, and guessing attacks. Similarly, magnetic cards are subject to loss, theft, forgery, and duplication. Biometric-based techniques, on the other hand, are resilient to such threats: people's biological traits cannot be misplaced or forgotten, and are difficult to steal or forge [1]. Biometric techniques are categorized as either *static* or *dynamic*. Static biometrics examine physiological traits of the individual such as face, fingerprints, iris, and hand geometry. Dynamic biometrics examine behavioral characteristics such as keystroke dynamics and voiceprints. Some sample images are shown in Figure 1.1.

The rest of this chapter is organized as follows. Section 1.2 introduces the common biometrics including multimodal biometrics that combines information from multiple biometrics to perform authentication. Section 1.3 presents a history of these different types of biometrics. We discuss various challenges and issues underlying the technique of biometric authentication in Section 1.4 and conclude in Section 1.5.

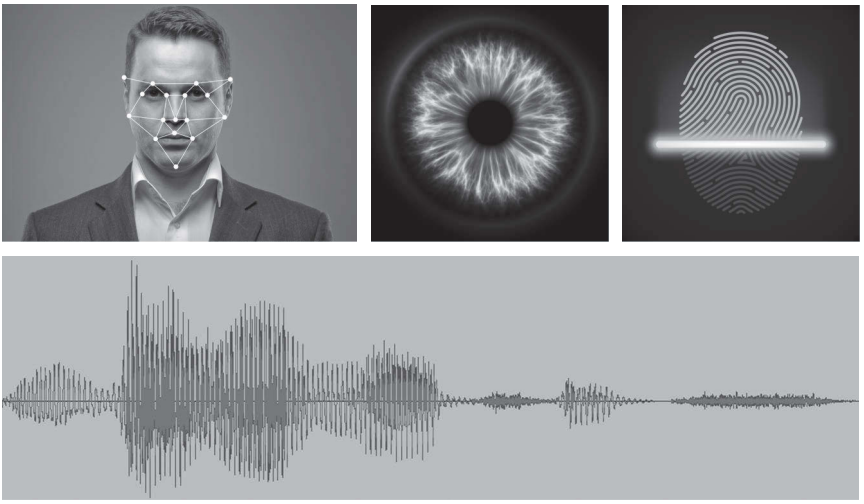


FIGURE 1.1 Commonly used biometrics—face, iris, fingerprints, and voiceprint. (From Shutterstock with permission.)

1.2 OVERVIEW OF BIOMETRICS

In this section, we start with a brief description of how the authentication process works, followed by the limitations of traditional approaches like passwords and magnetic cards, and introductions to the four commonly used biometric modalities, namely, face, fingerprints, iris, and voiceprint along with an outline of multimodal biometrics.

1.2.1 Process of Biometric Authentication

There are two types of authentication problems: (1) *identification:* Who am I? and (2) *verification:* Am I whom I claim to be? A typical biometric system has the following three components:

1. *Enrollment*. A biometric image is captured by some device (known as the "sensor"), preprocessed for feature extraction where features denote the identifying characteristics that are used in the identification process, and enrolled in the system.
2. *Matching*. The enrolled image is matched against the database of features extracted earlier from existing images, typically referred to as *reference feature vectors*.
3. *Decision*. A decision is made about whether the person is genuine or an impostor.

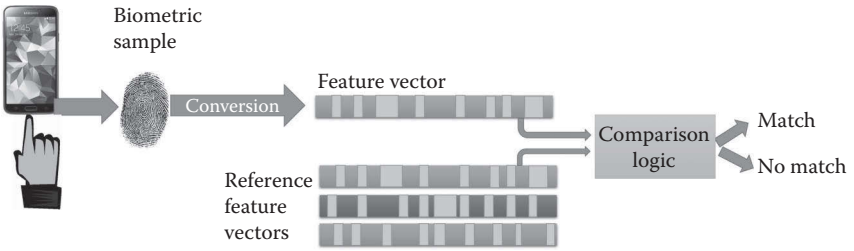


FIGURE 1.2 (**See color insert.**) The process of biometric authentication (this example is for a mobile phone).

Figure 1.2 shows a schematic of how the biometric authentication process works in practice, using the sensor (fingerprint reader) in a mobile phone.

Because of the decision-theoretic framework involved, there is scope for error in any biometric authentication scheme. In particular, there are two types of errors in the context of a verification task, namely (1) *false acceptance rate* (FAR for short) and (2) *false rejection rate* (FRR for short). The first one arises when an impostor is declared genuine by the system (i.e., the system finds a match when it should not have) and the second one arises when a genuine person is declared an impostor (when the system does not find a match when it should). These are typically determined with respect to thresholds that are set on the match scores, so that a set of FARs and FRRs are generated for a system with varying thresholds. The most commonly used metric for performance evaluation of a biometric system is called the *equal error rate* (or ERR for short) which is that value where the FAR and FRR approximately coincide.

1.2.2 Limitations of Traditional Authentication Mechanisms

First, we summarize the limitations of traditional authentication mechanisms. In particular, we will focus on the limitations of the two most pervasive methods: passwords and magnetic cards.

1.2.2.1 Passwords

Most modern systems authenticate users based on *username* and *password*. If the user-supplied password matches the password associated with the user's username, then the user is permitted to use the system [3]. A good password is easy to remember and hard to guess. Unfortunately, these can be conflicting requirements. In practice, most easy-to-remember

passwords are dictionary words, names, dates, short sequences of letters and numbers, and other easily guessable pieces of information. On the other hand, difficult-to-guess passwords usually comprise of long sequences of random characters, numbers, and symbols difficult for humans to remember. The difficulty of remembering passwords is often compounded by system administrators requiring users to periodically change their passwords. Easily guessable passwords are vulnerable to *dictionary attacks*, where the attacker compiles a dictionary of commonly used passwords and then tries all words in his dictionary until the correct password is found. Because such dictionaries are usually relatively small, for example, can contain less than 100,000 terms, modern computers can try all passwords in the dictionary in a matter of minutes, or less. Mobile devices, including iPhones, iPads, and Windows Phones, are also vulnerable to similar password guessing attacks. For example, iPhones and iPads use a four-digit number password. According to Gellman [4] and Gayomali [5]:

> A large study revealed that the top 10 iPad passcodes which accounted for 15% of the whole sample were: "1234, 0000, 2580, 1111, 5555, 5683, 0852, 2222, 1212, and 1998." People also prefer using their birth years and graduation years: every number from 1990 to 2000 makes the top 50, and every one from 1980 to 1989 the top 100. Although iPads can be configured to erase themselves after 10 wrong login attempts, many passcodes can be guessed in less than 10 attempts.

1.2.2.2 Magnetic Stripe Cards

Initially developed in the 1960s, magnetic cards are one of the most pervasive methods of electronic access control. A magnetic card consists of multiple magnetic stripes storing encoded information. Magnetic stripe cards have many vulnerabilities, including (1) card duplication; (2) lack of standards for protecting information on the card; and (3) susceptibility to loss and theft. The introduction of smart card technology has greatly alleviated concerns associated with vulnerabilities (1) and (2). Because smart cards contain a processor chip capable of altering card data and require passwords to read/write data to/from the card, they are more resistant to duplication than simple magnetic cards. However, even these security features can be circumvented. For example, secret codes can be extracted by eavesdropping on the communications between the card and the card

reader, by using social engineering, and by using differential power analysis techniques [3]. Moreover, smart cards are not immune to loss and theft.

1.2.3 Types of Biometrics

Next, we briefly summarize different types of biometrics and authentication algorithms based on those that are used in current applications.

1.2.3.1 Face

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past few years. Face recognition can occur from both still and video images, and from both two-dimensional (2D) and three-dimensional (3D) images.

The problem of automatic face recognition involves three key steps/subtasks: (1) detection and normalization of faces, (2) feature extraction, and (3) identification and/or verification. These tasks may, however, overlap. For example, face detection and feature extraction can be achieved simultaneously using facial features like eyes, nose, etc. Depending on the nature of the application, the sizes of the training and test databases, clutter and variability of the background, noise, occlusion, and speed requirements, some of the subtasks can be very challenging. Though fully automatic face recognition systems must perform all three subtasks, research on each subtask is critical. Hjelmas and Low [6] provide a highlighted summary of research on face detection and feature extraction methods.

Existing face recognition based on intensity images can be broadly classified into three categories:

1. *Holistic methods*. Methods that use the whole face region as the raw input to a recognition system; examples include Eigenfaces that are based on principal component analysis or PCA [7], Fisherfaces that use a combination of PCA and Fisher's linear discriminant analysis or LDA [8], support vector machines or SVM [9], independent component analysis or ICA [10], etc.

2. *Feature-based methods*. Methods where local features such as the eyes, nose, and mouth are first extracted and their locations and local statistics (geometric and/or appearance) are fed into a structural classifier, some examples being the hidden Markov model (HMM) [11], pure geometry methods [12], graph matching methods [13], etc.

3. *Hybrid methods*. Methods that use both local features and the whole face. Available techniques include modular Eigenfaces [14], local feature analysis [15], and component based [16].

Zhao et al. [17] present an in-depth discussion of the practical implementations of the above methods. Apart from intensity-based methods, there are face recognition methods based on the frequency domain as well. The importance of phase in face recognition [18] was exploited to improve performance over standard algorithms where it was shown that the resulting subspace by performing PCA on the phase spectrum alone is more robust to illumination variations [19]. These principal components are termed Eigenphases (in analogy to Eigenfaces). It was shown that Eigenphases outperform Eigenfaces and Fisherfaces when trying to recognize not only full faces but also partial or occluded faces. Another family of algorithms, called advanced correlation filters (ACFs for short [20]) are also widely used for performing face recognition using the frequency domain representation of images. Of these, the most important is the minimum average correlation energy filter [21]. A detailed survey of these frequency domain and filter-based face identification methods appears in Reference 22. An illustration of the face recognition technique is included in Figure 1.3.

1.2.3.2 Fingerprints

Fingerprinting is the oldest biometric identification method. It dates back to 1891 when police official Juan Vucetich first cataloged fingerprints of criminals in Argentina [23]. Fingerprint identification is based upon unique and invariant features of fingerprints. According to the Federal Bureau of Investigation (FBI), the odds of two people sharing the same fingerprints are one in 64,000,000,000. Fingerprints differ even for 10 fingers of the same person [24]. The uniqueness of a fingerprint is determined by global features like valleys and ridges, and by local features like ridge endings and ridge bifurcations, which are called *minutiae*. The earliest work in the field was done by Moayer [25]. He considered the fingerprint as a one-dimensional character string, and another method considering the fingerprint as a 2D tree, and verified two fingerprints by grammar matching. These methods work for a rough classification but fail on low quality images and thus, are not suitable for an identification system. Among the various current fingerprint matching algorithms, minutiae-based fingerprint

FIGURE 1.3 Illustration of face detection and recognition. (From Shutterstock with permission.)

matching is dominant. Some other methods include graph-based matching, genetic algorithms, etc. Extraction of minutiae features before matching needs a series of processes, including orientation computation, image segmentation, image enhancement, ridge extraction, minutiae extraction and filtering, etc. An earlier popular minutiae-based technique was introduced in Reference 26, using the delay triangulation method. Jain et al. [27] used ridge patterns in fingerprint matching. A detailed review of the various techniques can be found in Reference 28. Another approach is the application of correlation filters to fingerprint identification. These have added features like built in shift invariance, closed-form expressions, and tradeoff discrimination for distortion tolerance, and demonstrate good performance without requiring any preprocessing [29]. The one-to-one correlation of fingerprints on a large set of data yields poor results for fingerprint matching because of the elastic distortions between two fingerprints of the same finger. Wilson et al. [30] proposed a distortion-tolerant filter for elastic distorted fingerprint matching.

Some of the common challenges related to fingerprint technology are low quality or degraded input images, noise, and problems with the fingerprint readers. The degradation can be due to natural effects like cuts,

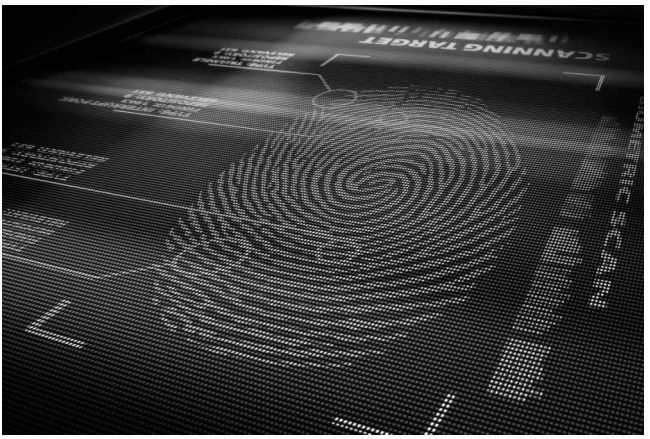


FIGURE 1.4 Image of a fingerprint captured and digitized. (From Shutterstock with permission.)

bruises, etc. or it may be due to appearance of gaps on ridges or parallel ridge intercepts. The fingerprint enhancement techniques not only have to enhance the quality of the image but also at the same time, have to reduce noise. Much work has been done in this field and the most commonly used method for this involves application filters [31]. Figure 1.4 shows the image of a fingerprint image captured by a sensor and digitized for the purpose of recognition.

1.2.3.3 Iris

With the growing demand of high security level and contactless biometrics, iris recognition is fast gaining in popularity today. Iris recognition analyzes the random pattern of the iris in order to establish individual identity. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye; the coloring is based on the amount of melatonin pigment within the muscle. Interestingly, the spatial patterns that are apparent in the human iris are highly specific to an individual [32,33] as is a person's fingerprint, hence it is now widely employed as a biometric for identification purposes. Furthermore, it has been observed in repeated measurements that the patterns in the iris vary very little, at least past childhood [34], unlike a person's face, which shows significant changes over time. It is rarely impeded by glasses or contact lenses, and it remains stable over time as long as there are no injuries or diseases that affect the

eye. Some medical and surgical procedures can affect the overall shape and color of an iris but the fine texture remains stable over many decades. Even blind people can use this scan technology since iris recognition technology is iris pattern-dependent and not sight dependent. Figure 1.5 shows some sample iris images.

Iris recognition methods use a noninvasive method for acquiring images, and have some advantages over other biometric traits. There is no need for the person being identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures regarding this issue. This is definitely an advantage over other biometric-based methods where the operator is required to make physical contact with a sensing device (like fingerprint scanners) or otherwise take some special action (recite a specific phonemic sequence for voice recognition). In 1936, ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual [35]. In 1985, ophthalmologists Leonard Flom and Aran Safir proposed the concept that no two irises are alike. In 1994, John Daugman developed the first ever algorithm to automate the identification of the human iris, and this method was used to build the first commercial iris identification system that is now owned by Iridian Technologies [36].

Conceptually, issues in the design and implementation of a system for automated iris recognition can be subdivided into three parts: (i) image acquisition, (ii) localization of the iris from a captured image, and (iii) matching an extracted iris pattern with candidate images stored in a

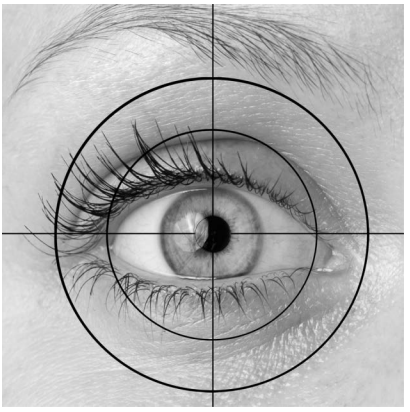


FIGURE 1.5 Image of an iris. (From Shutterstock with permission.)

database. One of the major challenges of automated iris recognition is to capture a high-quality image of the iris while remaining noninvasive to the human operator. It is desirable to acquire images of the iris with sufficient resolution and sharpness to support recognition. Initially, the cost of acquiring iris images was prohibitively high but now with the advent of several technologies and sophisticated image enhancing tools, the cost of iris image capture has gone down considerably. Most iris recognition systems now only require that the image be taken with a digital camera (preferably of high quality). Today's commercial iris cameras typically use infrared light to illuminate the iris without causing harm or discomfort to the subject. However, capturing the iris image may require some practice and thus can be more time consuming than capturing the image of a face or a fingerprint [37]. Following the image capture, a combination of image processing tools is applied prior to performing authentication. Before recognition of the iris takes place, the iris is located using landmark features [38]. These landmark features and the distinct shape of the iris allow for imaging, feature isolation, and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, the resulting noise in the form of eyelashes, reflections, pupils, eyelids, etc., in the image may lead to poor performance.

1.2.3.4 Voiceprint

Speaker verification (based on the voiceprint biometric) consists of making a decision whether a given voice sample belongs to the individual in question or not. Applications of speaker verification include additional identity check during credit card payments over the Internet, automatic segmentation of teleconferences, and in the transcription of courtroom discussions [39]. A large number of methods have been proposed for speaker recognition. Specifically, Gaussian mixture model (GMM)-based systems have received much attention [40]. Since then, some hierarchical extensions of the GMM method have also been proposed [41]. Another well-known method for speech recognition is based on HMMs. One reason why HMMs are popular is because they can be trained automatically and are simple and computationally feasible to use [42]. Modern speech recognition systems use various combinations of a number of standard techniques in order to improve results over the basic approaches based on GMMs and HMMs. Neural networks have also been utilized for speech recognition [43]. Speaker recognition also suffers from several

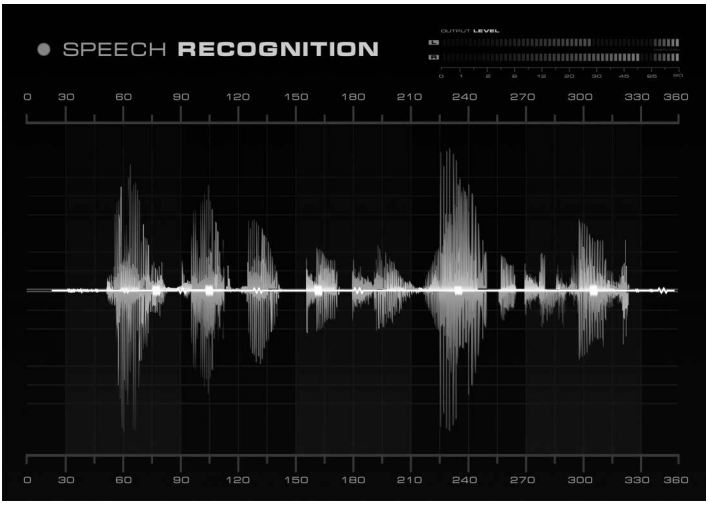


FIGURE 1.6 Voiceprint sample

challenges, the primary one being background noise and other external factors that potentially affect the quality of the captured voiceprint. There is, therefore, a considerable amount of ongoing research in this area for improving the robustness of speech recognition systems that are used in practice. Figure 1.6 shows sample voiceprint.

1.2.4 Multimodal Biometrics

Most biometric systems deployed in real-world applications are unimodal, that is, they rely on the evidence of a single source of information for authentication (e.g., single fingerprint or face). These systems have to contend with a variety of problems such as

- *Noise in the sensed data.* A fingerprint image with a scar or a voice sample altered by cold is an example of noisy data. Noisy data could also result from defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face for face recognition).
- *Intraclass variations.* Such variations are typically caused by a user who is incorrectly interacting with the sensor (e.g., incorrect facial pose).

- *Interclass similarities.* In biometric systems comprised of a large number of users (say, at airports), there may be interclass similarities (overlap) in the feature space of multiple users.
- *Nonuniversality.* The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for instance, may extract incorrect minutiae features from the fingerprints of certain individuals due to the poor quality of ridges (as may be caused by aging, illness, etc.).
- *Spoof attacks.* This type of attack is especially relevant when behavioral traits such as signature or voice are used. However, some physical traits such as fingerprints are also susceptible to spoof attacks occasionally.

Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [44]. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence [45]. Figure 1.1 gives a high-level schematic of the multimodal biometric system. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of nonuniversality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple traits of a genuine user simultaneously. More importantly, using more than one trait ensures greater reliability of the results that is expected to maximize performance accuracy (minimize false alarm rates).

1.2.4.1 Fusion Methods

In a multimodal biometric system, information reconciliation can occur in the following ways [45]:

1. *Fusion at the data or feature level*, where either the data or the feature sets originating from multiple sensors/sources are fused
2. *Fusion at the match score level*, where the match scores generated from multiple classifiers pertaining to the different biometric modalities are combined

3. *Fusion at the decision level*, where the final output (decision: genuine or impostor) of multiple classifiers are consolidated into a single decision via techniques such as majority voting

Biometric systems that integrate information at an early stage of processing are believed to be more effective than those systems, which perform integration at a later stage. Since the feature set contains richer information about the input biometric data than the matching score or the output decision of a matcher, fusion at the feature level is expected to provide better recognition results. However, fusion at this level is difficult to achieve in practice because (i) the feature sets of the various modalities may not be compatible and (ii) most commercial biometric systems do not provide access to the feature sets (nor the raw data) which they use in their products. Fusion at the decision level is considered to be rigid due to the availability of limited information. Thus, fusion at the match score level is usually preferred, as it is relatively easy to access and combine the scores presented by the different modalities.

1.3 HISTORY OF BIOMETRICS

The word "*biometrics*" is originally from the Greek words *bio* (life) and *metric* (to measure). In traditional statistical literature, the terms "biometrics" and "biometry" have been used since the early twentieth century to refer to the field of development of mathematical methods applicable to data analysis problems in the biological sciences. Some examples include agricultural field experiments to compare the yields of different varieties of a crop and human clinical trials evaluating the relative effectiveness of competing drugs. However, recently the term biometrics has also been used in the context of security to denote an individual's unique biological traits (like face and fingerprints) that can be used for identification.

1.3.1 Ancient Times (BC to Mid-1800s)

The origin of biometrics can be traced back to 31,000 years ago. "In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that are felt to *have acted as an unforgettable signature* of its originator" [46]. An example of an old cave painting appears in Figure 1.7. Joao de Barros, a Spanish explorer and writer, wrote that early Chinese merchants used fingerprints to settle business transactions and Chinese parents also used fingerprints

FIGURE 1.7 (**See color insert.**) Handprints used as signatures for cave paintings. (From Renaghan, J., *Smithsonian Zoogoer*, August 1997.)

and footprints to distinguish their kids from each other. Interestingly, in some places of the world today, this practice is still in use [47]. In early Egyptian history, businessmen were recognized by their physical descriptors in order to distinguish between businessmen who had known reputations from previous successful transactions and those who were new to the market [47].

1.3.2 Industrial Revolution (Mid-1800s to Mid-1900s)

By the mid-1800s, with the fast development of urbanization because of the industrial revolution and more productive farming, a formally recognized demand for individual identification was created. Merchants and authorities were confronted with progressively larger and more mobile populations and started realizing that their own experiences and local knowledge were no longer reliable for the purpose of identification [48]. As a result, in 1858, the first systematic capture of hand images for identification purposes was recorded by William Herschel who was working for the Civil Service of India. The handprint was recorded on the back of a contract for each worker in order to verify the identity of employees when getting paid. An illustration of such a handprint is shown in Figure 1.8.

In 1870, Alphonse Bertillon, an anthropologist and police desk clerk in Paris, developed a system called "Bertillonage" that used physical characteristics (body dimensions) as a means of identifying criminals. These

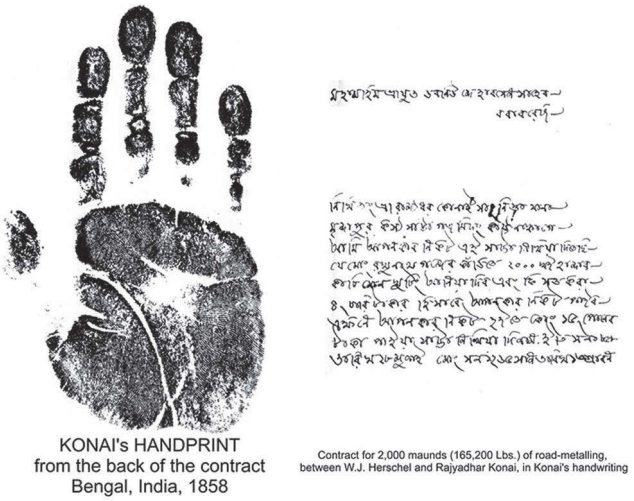


FIGURE 1.8 Handprint at the back of the contract. (From Ed German. n.d. The history of fingerprints. With permission.)

measurements were written on cards that could be sorted by height, or arm length. This field, called *anthropometries,* however, proved to have some flaws because these body dimensions were not unique to a person. According to Ed German [49], "two men, determined later to be identical twins, were sentenced to the US Penitentiary at Leavenworth, KS, and were found to have nearly the same measurements using the Bertillon system."

In 1896, Edward Henry built up a technique that offered the ability to quickly retrieve fingerprint records as Bertillon's system did, but used a more personalized metric—fingerprint patterns and ridges. The Henry technique and its variations are still being used today [50]. A couple of years after, the NY state facilities system started utilizing fingerprints for the identification of criminals. Also, with developing interest by national police authorities, the identification division of the FBI was established by an act of Congress on July 1, 1921 [51].

1.3.3 Emergence of Computer Systems (Mid-1900s to Present Day)

The emergence of computers in the latter half of the twentieth century coincided with the emergence of modern-day biometric systems [48]. In 1969, the FBI began its push to develop a system to computerize its fingerprint identification process. They contracted the National Institute of Standards and Technology (NIST) to develop the process of automating fingerprint