Advances in Information Security 60

Angelo Genovese
Vincenzo Piuri
Fabio Scotti

Touchless Palmprint Recognition Systems

Springer

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

More information about this series at http://www.springer.com/series/5576

Angelo Genovese • Vincenzo Piuri • Fabio Scotti

Touchless Palmprint Recognition Systems

Springer

Angelo Genovese
Department of Computer Science
Università degli Studi di Milano
Crema, Italy

Vincenzo Piuri
Department of Computer Science
Università degli Studi di Milano
Crema, Italy

Fabio Scotti
Department of Computer Science
Università degli Studi di Milano
Crema, Italy

ISSN 1568-2633
ISBN 978-3-319-10364-8 ISBN 978-3-319-10365-5 (eBook)
DOI 10.1007/978-3-319-10365-5
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014948337

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Biometric systems consist of devices, algorithms, and procedures used to recognize individuals or classes of individuals based on their physical or behavioral characteristics, called biometric traits. These systems are particularly relevant to security (such as access control and government applications) and are increasingly a part of daily life.

However, the procedures typically used for collecting biometric traits require user cooperation, controlled environments, contact between the surveyed body part and the sensor, or illumination perceived as unpleasant, too strong, or harmful. These constraints limit the usability and social acceptance of biometric technologies in daily life. Techniques for touchless and less-constrained biometric recognition have been studied to address these issues, increase the use of biometric systems, and expand the application of biometric technologies to other fields.

In this context, the palmprint is a hand-based biometric trait that permits sufficiently accurate recognition and whose acquisition is generally well accepted by users because it is not perceived as too intrusive or privacy-sensitive. Moreover, palmprints can be captured using low-cost devices and, unlike fingerprints, are sufficiently redundant to be used even when the palm's surface is partially damaged, such as in elderly people or manual workers. Unfortunately, traditional palmprint-based systems use touch-based acquisitions with pegs that constrain the position of the hand to facilitate biometric trait acquisition, limiting its ease of use.

The aim of this book is to make palmprint biometrics easier to use in practical, daily-life applications. Innovative, original methods for touchless and less-constrained palmprint recognition are presented that overcome the typical constraints and limits described above.

Our innovative multiple-view acquisition systems, which are based on CCD cameras and LED illumination, are designed to capture high-quality palmprint images. Original image processing algorithms have been devised to analyze palmprints. Three-dimensional reconstruction techniques are also applied to reconstruct the hand's shape and surface, invariant to position and orientation, and pattern

recognition methods are introduced to extract and match the palmprint's distinctive features. Our novel methods permit individual recognition via the acquisition of biometric traits in a single time instant and without requiring their hands to touch any surface or adopt a specific position. Accurate biometric recognition is achieved, in many cases superior to the most recent approaches described in the literature, while simultaneously enhancing usability and social acceptance. Moreover, our innovative setups and methods have a lower cost and capture images in a more efficient way.

Therefore, this book will be of interest to researchers and professionals in the field of biometric technologies and applications, as well as students and those interested in understanding the emerging technological area of touchless and less-constrained palmprint recognition, because it provides a comprehensive view of the field and an in-depth presentation of innovative, effective approaches well suited for daily-life applications.

Crema, Italy

Angelo Genovese
Vincenzo Piuri
Fabio Scotti

Acknowledgments

The research reported here has been partially supported by the European Union Seventh Framework Programme within the integrated project “ABC gates for Europe (ABC4EU),” under grant agreement FP7-SEC-2012-312797, and by the Italian Ministry of Research within the PRIN project “GenData 2020,” contract 2010RTFWBH.

Contents

Chapter 1
Introduction

The use of biometric systems, which recognize individuals based on their physical characteristics rather than their knowledge (e.g., a password) or objects (e.g., a smartcard), is expanding and is increasingly a component of daily life for many people.

In many cases, the effective and efficient acquisition of biometric data requires the cooperation of the user in a controlled environment or is achieved by means of complex, expensive or intrusive procedures. These constraints limit the usability and social acceptance of biometric technologies in daily life and, consequently, the expansion of their application.

In this context, biometric systems based on palmprints are generally well accepted by users because they are not perceived as too intrusive or privacy-sensitive. In addition, palmprints can be captured using low-cost devices, thus making them viable for many daily-life applications with low-cost requirements. Palmprints are also sufficiently redundant to enable the accurate recognition of even a partially damaged palm surface. Unfortunately, traditional systems for palmprint recognition rely on touch-based acquisitions with pegs that constrain the position of the hand, reducing their ease of use.

This book aims at making palmprint recognition easier to use and more accepted in daily-life applications. Innovative, original methods for touchless and less-constrained palmprint recognition are presented that overcome the typical constraints and limits described above.

To provide context for the described technologies, this chapter presents the basic concepts of biometrics and biometric recognition, touchless and less-constrained biometric systems, and palmprint recognition. These aspects will then be analyzed in greater detail in subsequent chapters to provide a concise state-of-the art, which will provide a foundation for evaluating and appreciating our innovative solutions. The core part of this book is dedicated to our innovative methods for touchless and less-constrained palmprint recognition. The proposed approaches will be carefully analyzed and compared with the literature to describe their advantages and limits for effective use in daily-life applications.

A. Genovese et al., *Touchless Palmprint Recognition Systems*,
Advances in Information Security 60, DOI 10.1007/978-3-319-10365-5_1

1.1 Basic Concepts of Biometrics

The discipline of biometrics concerns the measurement of bodily features typical of human beings for identity recognition or body-condition detection. Specifically, the term biometrics is defined by the International Organization for Standardization (ISO) as "*the automated recognition of individuals based on their behavioral and biological characteristics*" [164].

Currently, the main applications of biometrics are in the security and medical fields. In the medical field, biometrics can be used to support diagnosis. In the security field, biometric measurements are typically used for government applications (e.g., border control, ID cards, criminal identification), regulating physical access to restricted areas (e.g., airports, stadiums, banks, military zones), controlling access to logical resources and services (e.g., home banking, ATMs, e-commerce, personal devices), and forensic analysis (e.g., the identification of suspects, kinship analysis). In this book, we focus our attention on the use of biometrics for security applications, specifically, for identity recognition.

Biometric systems consist of devices, algorithms, and procedures used to recognize individuals or classes of individuals based on their physical or behavioral characteristics, called biometric traits, rather than their knowledge (e.g., a password) or objects (e.g., a smartcard). Biometric features are (a) distinct for each individual and (b) cannot be forgotten (like passwords) or stolen (like smartcards).

A biometric trait is a characteristic of a person that can be used for recognition [171]. Biometric traits can be physiological (biological) or behavioral. In the first case, recognition is based on physical traits related to the body of the person, such as their fingerprint, iris, face, hand shape, or palmprint. Behavioral traits are related to the actions performed by a person and include, for example, gait, voice, and signature.

Biometric systems for security applications employ two modalities: authentication and identification. In the authentication mode, the individual states his identity and provides his biometric trait. The biometric system then compares the biometric trait with one previously stored to determine if the traits match; if so, the person is positively recognized. Biometric systems that work in authentication mode include those that regulate access to restricted areas.

In identification mode, the individual does not state his identity, and the system compares the biometric trait of the individual with all the traits stored in its database to determine the person's identity. Examples of biometric systems working in identification mode include surveillance systems used to monitor a critical area and detect possible suspects and forensics systems used to analyze latent fingerprints found at a crime scene and identify criminals.

1.2 Touchless and Less-Constrained Biometrics

Traditionally, biometric systems require the user to be cooperative and willing to present his biometric trait to the sensor. In many cases, biometric acquisitions require controlled procedures or contact between the biometric trait and the sensor. For example, the user must assume a certain pose, place his biometric trait in a particular place, and remain still for the duration of the biometric acquisition.

Biometric traits that typically require constrained acquisition procedures include the face, iris, fingerprint, and palmprint. For face acquisition, the user must stand in a specified position and remain still with a neutral expression. In most cases, the illumination conditions are controlled.

Iris acquisitions are performed by placing the eye, properly opened, in a specific position. Infrared illumination, often perceived as unpleasant or harmful, is used.

Fingerprints are captured by touching a small sensor with the proper pressure. Because hands can be dirty or sweaty, the sensor can easily become dirty, which has consequences for both acquisition quality and user acceptability. People may dislike using a sensor that has been touched by many people, particularly in areas where hygiene might be important.

Palmprint characteristics are measured by placing the hand on a surface on which pegs are used to constrain the hand in a specific pose. Similarly to fingerprint sensors, palmprint acquisition surfaces can be dirty. Moreover, the presence of pegs can be a problem for the elderly or those with muscular or joint problems (e.g., arthritis).

To reduce or eliminate these constraints, techniques for less-constrained biometric recognition have been studied. Less-constrained recognition methods typically have shorter acquisition times, improved usability, and greater social acceptance, potentially facilitating the expansion of the use of accurate biometric traits to new applications and scenarios. For example, less-constrained iris recognition enables superior recognition accuracy in surveillance applications, mobile phones, and biometric gates. Similar applications could be realized with touchless biometric systems based on fingerprint or palmprint recognition.

In this book, the term “touch-based” is used to refer to biometric acquisition procedures that require contact of the biometric trait with the sensor, whereas “touchless” refers to procedures that do not require contact with the sensor. The equivalent terms “contact-based” and “contactless” are sometimes used in the literature.

1.3 Palmprint Recognition

Palmprint recognition has been increasingly investigated over the past 15 years. Many aspects of this biometric trait are similar to those of fingerprints, facilitating progress in palmprint recognition research. In addition, palmprints present many

distinctive features that can be exploited for highly accurate recognition. However, in contrast to fingerprints, palmprint recognition systems can use low-cost acquisition devices and can achieve good results even with a partially damaged palm surface (for example, in elderly people or manual laborers), due to the higher number of features that can be extracted at different levels of detail.

Palmprint recognition can be achieved using touch-based and touchless methods, depending on the type of contact with the sensor needed to perform the acquisition. Moreover, these approaches can be further partitioned into methods based on two-dimensional and three-dimensional samples.

Currently, the majority of approaches presented in the literature perform recognition using touch-based two-dimensional acquisitions with flatbed scanners or CCD-based devices. Flatbed scanners are particularly useful for low-cost systems, while CCD-based devices offer good-quality samples and short acquisition times. Touch-based three-dimensional acquisition devices based on CCD cameras and projectors have been proposed to increase recognition accuracy, despite requiring a complex, more expensive setup.

The major drawbacks of touch-based methods are distortion, dirt, and user acceptability. Distortions are caused by non-uniform pressure of the hand on the sensor. Dirt accumulates after repeated acquisitions and can reduce the quality of the acquisitions. User acceptability can be problematic if people dislike touching surfaces that have been touched by other people because of hygienic reasons.

To overcome the above drawbacks, touchless acquisition devices have been studied. However, touchless methods can be affected by disadvantages, including lower contrast, a more complex background, and non-uniform acquisition distances. In addition, touchless approaches are sensitive to lighting conditions. To address these problems, three-dimensional touchless methods have recently been studied. These methods are more robust and can account for different acquisition distances, lighting conditions, backgrounds, noise, and spoofing attacks. However, they require more complex and more expensive setups than two-dimensional touchless methods.

1.4 Innovative Methods for Touchless and Less-Constrained Palmprint Recognition

The aim of this book is to describe innovative methods for touchless and less-constrained biometric recognition of palmprint characteristics. Original methods are presented that achieve recognition without requiring contact of the palm with the sensor surface of placement of the hand in a specific position and that collect the palmprint in a single acquisition time.

Specifically, the methods involve the use of three-dimensional reconstruction techniques to compute a metric representation of the palm that is invariant with respect to the position, distance, and orientation of the hand at the moment of acquisition.

Using these techniques, accurate biometric recognition can be performed. The usability and social acceptance of the biometric recognition system can also be improved. To ensure usability in many daily-life applications, the cost of the setup has also been carefully considered during the design of the system.

The approaches described in this book have two main advantages compared to previously reported touch-based methods: (a) they avoid problems resulting from palm contact with the sensor (such as distortion, dirt, sweat, or latent impressions), and (b) they do not require fixed placement surfaces, guides or pegs to place the hand in the correct position for acquisition. These characteristics increase the usability and acceptability of the system. Compared to methods in the literature that use only two-dimensional samples, the methods described in this book are innovative because they use three-dimensional information to produce a measurable (metric) and more accurate representation of the palm that is invariant with respect to the position, orientation, and distance of the acquisition. In this way, a less-constrained acquisition can be performed with a relaxed and non-fixed position of the hand.

Compared to the touchless three-dimensional palmprint acquisition methods described in the literature, the novelty of the approaches described in this book is the use of an innovative hardware acquisition setup that enables reduced cost and rapid image acquisition.

In the following chapters, a touchless palmprint recognition method based on two-view acquisitions performed at a fixed distance is first analyzed. This technique achieves good recognition accuracy, comparable to those of the most recently reported methods, without the distortions of touch-based acquisitions and without requiring contact between the palm and surface. Although the back of the hand must be placed against a fixed surface to ensure proper focusing of the acquisition, contact with the back of the hand is usually considered more hygienic than contact with the palm.

The results obtained with this first system enabled the design and implementation of an innovative, fully touchless, less-constrained palmprint acquisition technique that does not require contact of the palm with any surface or a fixed hand position. This method uses three-dimensional reconstruction techniques to achieve a metric representation of the hand, invariant to the pose and orientation. This method achieves good recognition accuracy (in many cases superior to the most recent approaches described in the literature) and is robust to changes in hand orientation as well as differences in environmental illumination.

Other biometric aspects are considered to evaluate the feasibility of these innovative methods for large-scale biometric recognition applications. In particular, good results were obtained with respect to the usability and social acceptance of the described methods. Computational speed, cost, interoperability, security, and privacy are also considered and discussed.

1.5 Structure of the Book

This book is structured as follows:

- *Chapter 2* is a brief introduction to biometric recognition and the general structure of biometric systems. A survey of major biometric traits is presented, and the methodologies used to evaluate biometric systems are described. Research trends in biometric recognition are also summarized.
- *Chapter 3* presents an introduction to less-constrained biometric systems and surveys the research on touchless and less-constrained recognition. First, methods are presented for the touchless recognition of biometric traits that are traditionally captured using touch-based sensors. Then, less-constrained techniques for biometric recognition using traits captured by touchless acquisition are described.
- *Chapter 4* provides an overview of the state-of-the-art in the field of palmprint recognition. First, an introduction to palmprint recognition is presented, including its key characteristics and applications. Then, touch-based and touchless palmprint recognition systems are reviewed. Both categories are partitioned into methods based on two-dimensional and three-dimensional samples. A review of the methods used to estimate the quality of the samples and classify palmprints is also presented.
- *Chapter 5* presents our innovative methods for palmprint recognition. First, touchless palmprint recognition based on acquisitions performed at a fixed distance with the back of the hand placed against a fixed surface is analyzed. Then, the design and implementation of an innovative fully touchless, less-constrained method based on acquisition at an uncontrolled distance is described.
- *Chapter 6* discusses the application of the described methods and their experimental evaluation. The datasets collected and the evaluation metrics used are described. The accuracy and robustness of the methods are evaluated, as well as other aspects related to computational speed, cost, interoperability, usability, social acceptance, security, and privacy.
- *Chapter 7* summarizes the research performed, the results obtained using the innovative methods, and the originality of the contributions. Future developments are also proposed.

Chapter 2
Biometric Systems

This chapter presents an overview of biometric systems, with the goal of providing context for the technology described in the presented work. The principles of biometric recognition, their general structure and basic functioning methods are introduced, and the most commonly used biometric traits are described. Then, the methods used for evaluating biometric systems are detailed. To conclude the chapter, current research trends in the field of biometric recognition are discussed.

2.1 Introduction to Biometric Recognition

The discipline of biometrics involves the measurement of bodily features typical of human beings. As defined by the International Organization for Standardization, biometrics is "*the automated recognition of individuals based on their behavioral and biological characteristics*" [164].

The use of biometric systems is expanding, and the costs of deployment are decreasing. In fact, the market for biometric technologies is increasing in size [303]. The value of the biometrics market reached 5 billion dollars in 2011, and forecasts indicate that it will reach 12 billion dollars in 2015 [163].

The main applications for biometrics are in the medical and security fields. In the medical field, biometrics can aid diagnoses when used in conjunction with other techniques for medical analysis. In the security field, biometric measurements are used to regulate access to restricted areas (e.g., military zones, airports, stadiums, banks), for government applications (e.g., border control, ID cards, suspect identification), for controlling access to logical resources (e.g., home banking, ATMs, e-commerce, personal devices), and for forensic analysis (e.g., suspect identification, kinship analysis) [171].

Biometric systems used in security applications consist of a combination of devices, procedures, and algorithms used to recognize individuals based on their

A. Genovese et al., *Touchless Palmprint Recognition Systems*,
Advances in Information Security 60, DOI 10.1007/978-3-319-10365-5_2

bodily features rather than their knowledge (e.g., a password) or objects (e.g., a smartcard). For example, instead of requiring a password to be entered (e.g., for accessing a video terminal) or a magnetic card to be scanned (e.g., for withdrawing money from an ATM), the details of a fingerprint, a face, or the shape of a hand can be used to determine the identity of a person and regulate their access to restricted services. The advantages of biometric features are that they cannot be forgotten or stolen and are unique to each individual. In this way, biometric measurements provide increased confidence of the identification of the recognized individual.

In this context, a biometric trait is the particular characteristic that is measured to perform the recognition. Biometric traits can be physiological or behavioral. For the former, recognition is based on physical traits related to the body of the person, such as his fingerprint, iris, face, or hand shape. By contrast, behavioral traits are related to the actions performed by a person, such as his gait, voice, and signature.

A multitude of biometric systems have been implemented for a variety of different applications. Different traits and technologies are selected based on factors such as accuracy, speed, cost, usability, and privacy risks. These different factors must be considered in the selection of a biometric system for a specific operational scenario. For example, in an environment where high security is required (e.g., a military structure), the recognition performance of the system must be as high as possible, whereas speed and privacy can be sacrificed if necessary. By contrast, for biometric systems installed in low-security environments (e.g., an amusement park), high speed, low invasiveness, and low privacy risk are emphasized.

2.2 Structure of Biometric Systems

Biometric recognition consists of the procedures used by biometric systems to compare the biometric traits of individuals, compute their similarity, and determine whether or not they belong to the same person. The recognition process can be divided into five modules:

1. *Acquisition*: Based on the biometric trait used, a specific sensor is used to capture the trait belonging to the user. The captured trait can be an image, an audio sample, or a frame sequence. The trait captured by the sensor is called the "sample".
2. *Segmentation*: The region of the sample containing the biometric information is isolated. For example, in the case of an image from an iris acquisition, the eyelashes and eyelids are eliminated so that only the iris region is considered.
3. *Feature Extraction*: The distinctive features are extracted from the segmented sample, and an abstract representation of the biometric trait (the "template") is computed. This template is better suited for storage in a database and analysis by an automated information processing system. Templates can be strings of bits, coordinates of particular points in the image, images, signals, or algebraic functions.

4. *Identity Matching*: The template is compared with one or more templates present in the database. The database can be centralized or stored on a device possessed by the user. The result of the identity matching step is a "match score", which is a measure of the similarity between the two compared templates.
5. *Decision*: The match score is used to produce the final decision of the biometric system. In most cases, a threshold for the match score value is used to transform the match score into a Boolean decision, which determines if the compared templates belong to the same individual.

Biometric systems can work in two modalities: authentication and identification. In authentication mode, the individual states his identity (for example, by showing an ID card) and presents his biometric trait to the biometric system that regulates access (for example, by placing his fingerprint on the sensor), which captures the corresponding sample. Then, a template is computed from the captured sample, and an identity-matching algorithm is used to compare the template with the template previously stored in the database for the presented identity. The system evaluates a 1:1 match between the stated and presented identities and grants access based on a thresholding operation on the resulting match score. A biometric system working in authentication mode can be included in any system that regulates access to a sensitive resource, such as an ATM, a personal device, or a restricted area.

In identification mode, the individual does not state his identity, and the system performs a 1:N matching by comparing the template computed from the biometric trait presented by (or extracted from) the individual with all the templates stored in the database. Then, the identity of the individual corresponding to the most similar template, based on the resulting match scores, is selected. The identification modality is typical of biometric systems in law-enforcement installments, such as the Automated Fingerprint Identification System (AFIS). In AFIS, a fingerprint extracted from a crime scene must be compared with every fingerprint present in the database to determine the identity of the associated individual.

In most cases, the general term "recognition" is used to refer to the process of biometric matching when there is not a need to make a distinction between the authentication and identification modalities.

Biometric systems functioning in the authentication and identification modalities require an enrollment step, similar to a registration procedure, in which a template is computed from the biometric trait of the user and stored in the database of the system, along with the associated identity. An illustration of the enrollment step is shown in Fig. 2.1. A biometric system functioning in authentication mode is shown in Fig. 2.2, while a system functioning in identification mode is shown in Fig. 2.3.

2.3 Biometric Traits

In this section, the types of biometric traits and their characteristics are described. An overview of the main biometric traits is then presented.

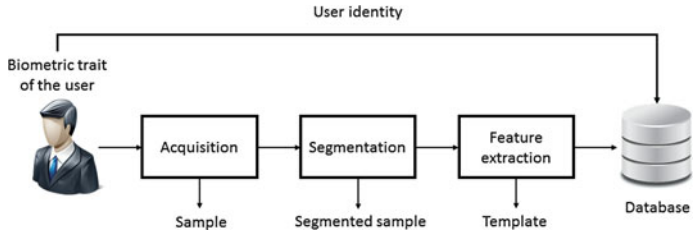

Fig. 2.1 Schematic of the enrollment step in a biometric system

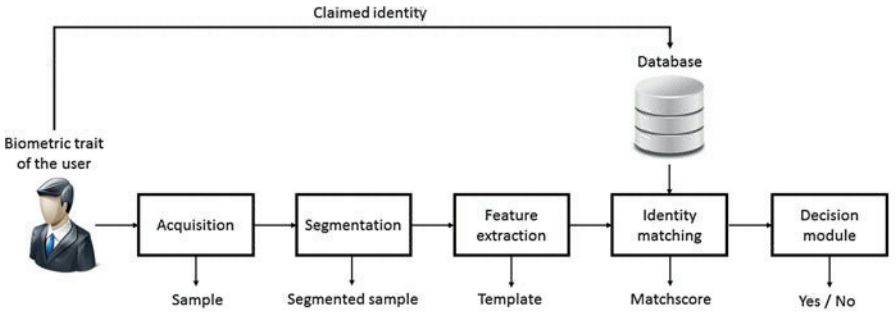

Fig. 2.2 Schematic of a biometric system functioning in authentication mode

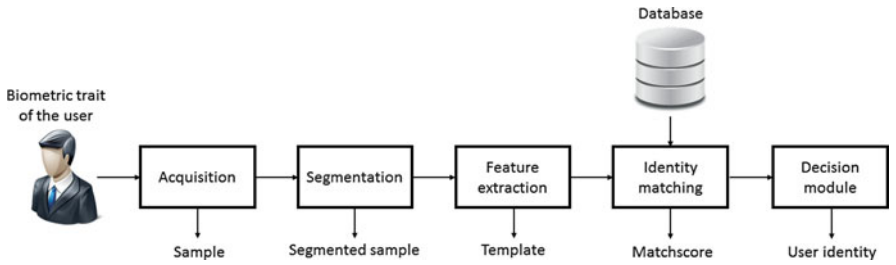

Fig. 2.3 Schematic of a biometric system functioning in identification mode

As noted in Sect. 2.1, biometric traits can be classified as physiological or behavioral. Physiological traits are the features physically possessed by the body of the person to be recognized, such as a fingerprint [102, 238], palmprint [196], iris [74, 86], face [217], hand geometry [329], vein pattern of the hand (or palm vein [49], ear shape [154], DNA [147], or electrocardiogram ECG [272] (Fig. 2.4). Behavioral traits are related to actions performed by the person for recognition. Examples include voice [131], gait [41], signature [155], and keystroke [324] (Fig. 2.5). Physiological traits are usually more accurate than behavioral traits. Moreover, while physiological traits are always present in an individual, in the case

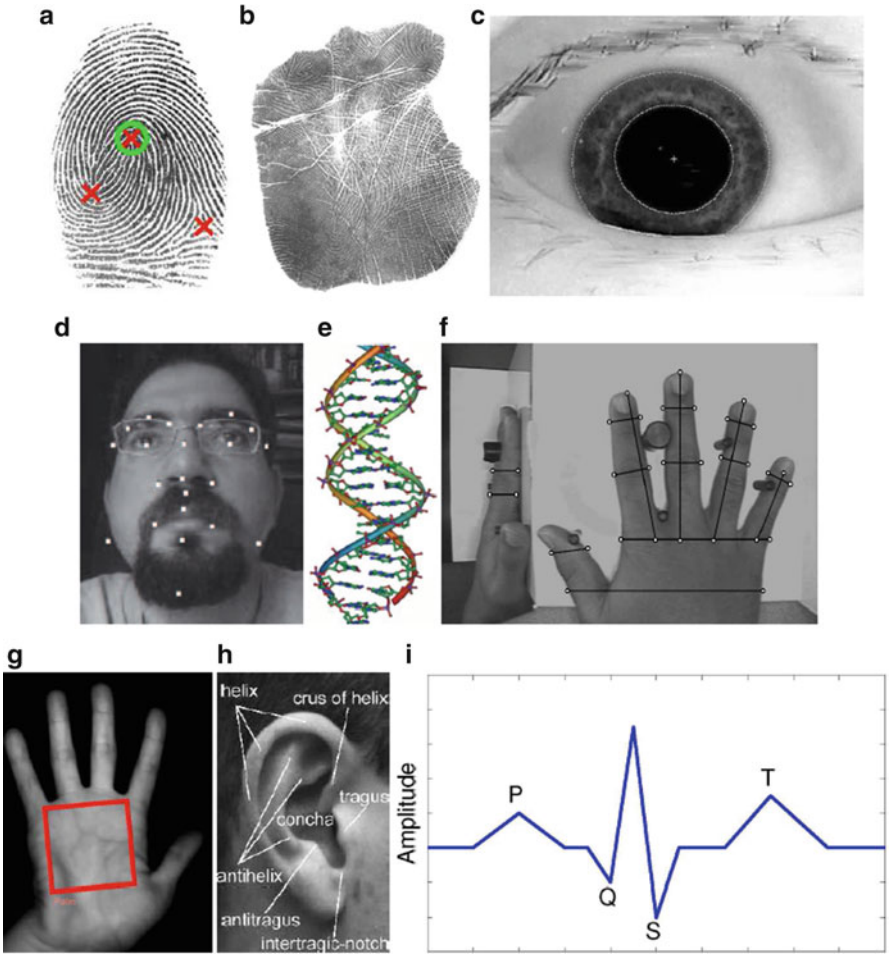

Fig. 2.4 Examples of physiological biometric traits: (**a**) fingerprint [84] (reproduced by permission of IEEE); (**b**) palmprint [170] (reproduced by permission of IEEE); (**c**) iris [74] (reproduced by permission of Springer); (**d**) face [315] (reproduced by permission of Springer); (**e**) DNA [1] (reproduced by permission of IEEE); (**f**) hand geometry [329] (reproduced by permission of Springer); (**g**) vein pattern of the hand [252] (reproduced by permission of IEEE); (**h**) shape of the ear [154] (reproduced by permission of Springer); (**i**) ECG [100] (reproduced by permission of IEEE)

of behavioral traits, individuals can refuse to perform the required action if they do not want to be recognized. For example, a user can refuse to speak or alter his voice.

Every characteristic of the body can potentially be used as a biometric trait. In fact, despite the numerous biometric traits used in recognition systems, innovative biometric features are continually evaluated to improve performance, speed, cost, or

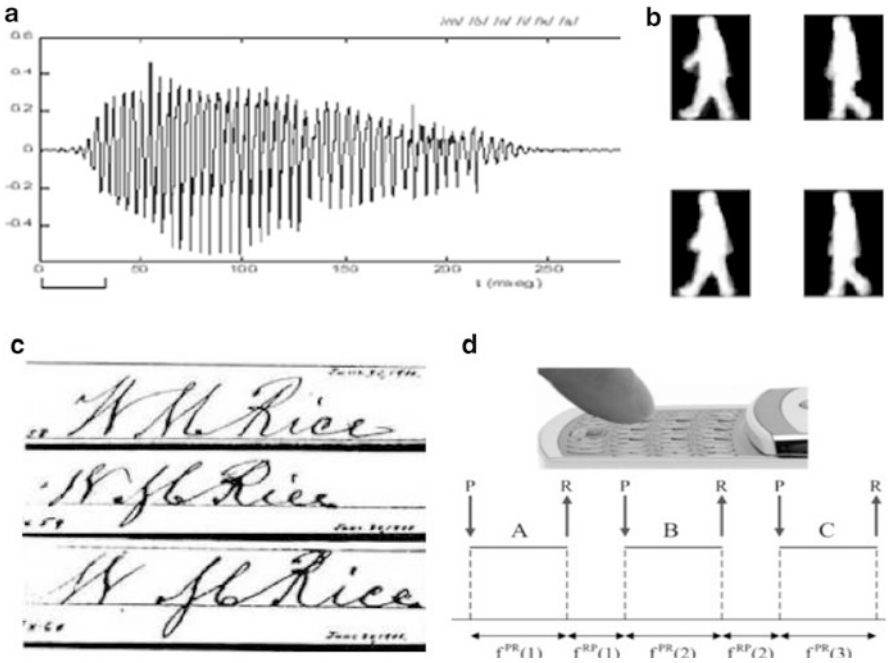

Fig. 2.5 Examples of behavioral biometric traits: (**a**) voice [131] (reproduced by permission of Springer); (**b**) gait [314] (reproduced by permission of Springer); (**c**) signature [120] (reproduced by permission of Springer); (**d**) keystroke [37] (reproduced by permission of IEEE)

reduce privacy risks. However, to be used for recognition purposes, a biometric trait must possess the following characteristics [173]:

- *Universality*: the biometric trait should be possessed by everyone;
- *Distinctiveness*: the biometric trait should distinguish individuals;
- *Permanence*: the biometric trait should not change over time;
- *Collectability*: the biometric trait must be quantitatively measurable.

Other important characteristics of the biometric trait must also be considered:

- *Performance*: the accuracy and speed that can be obtained using the biometric trait;
- *Acceptability*: how willing individuals are to provide their biometric traits for recognition;
- *Circumvention*: the difficulty of hacking the biometric system to gain unauthorized access.

Biometric traits can also be divided into hard and soft. Hard traits include the aforementioned physiological and behavioral traits, which are characterized by high distinctiveness and permanence. By contrast, soft biometric traits have low distinctiveness or low permanence. These traits cannot be used to recognize

Fig. 2.6 Examples of three different fingerprints: (**a**) index finger; (**b**) middle finger; (**c**) thumb

individuals with sufficient confidence over a period of time but can be used for low-security environments or contexts in which an individual must only be recognized over a short period of time. Soft traits usually have low invasiveness and can be combined to increase the performance of a biometric system [305].

Soft biometric traits can be either continuous or discrete [168]. Continuous soft biometric traits include height [76], weight [91,350], and the size of body parts [77]. Discrete biometric traits include gender [75], race [75], eye color [72], and clothing color [77].

Biometric systems based on fingerprint recognition (Fig. 2.6) are currently the most widespread. These systems are low cost (fingerprint sensors can even be placed on laptops or on USB pen drives) and have good performance. Moreover, they are not considered too invasive by the majority of individuals. Because of their good accuracy and speed, biometric systems based on fingerprints can be used for both authentication and identification purposes. Biometric systems based on fingerprints are typically used for access control, border control, and forensic applications, and centralized fingerprint databases are employed in many countries for the large-scale identification of fingerprints [193]. The analysis of fingerprint features can be performed on three levels, depending on the resolution of the imaging device. Level 1 analysis extracts features related to ridge flow, orientation, frequency, and position of the singular points. Level 2 analysis [130] is the most widely used and is based on the extraction and matching of the positions of specific points called minutiae. Level 3 analysis considers the position of the pores of the skin and the incipient ridges [238].

Biometric systems based on the iris are increasingly used, particularly in situations in which high recognition accuracy and high speed are required, such as border control stations and airports. In fact, iris-based systems have the highest accuracy among biometric traits (except DNA), and the identification procedure is