New Directions in Behavioral Biometrics

Khalid Saeed

with Marcin Adamski, Tapalina Bhattasali, Mohammad K. Nammous, Piotr Panasiuk, Mariusz Rybnik, and Soharab H. Shaikh
## Contents

**Foreword**

**Preface**

**Acknowledgments**

**Chapter 1 Introduction to Behavioral Biometrics**

1.1 Behaviometrics

1.1.1 How It Works

1.1.2 Major Benefits

1.2 What Is Special about Behavioral Biometrics Data Acquisition?

1.3 Behavioral Biometrics Features

1.4 Classification of Behavioral Biometrics Traits

1.5 Properties of Few Behavioral Biometrics

1.5.1 Signature

1.5.1.1 Constraints of Signature Recognition

1.5.1.2 Merits of Signature Recognition

1.5.1.3 Demerits of Signature Recognition

1.5.1.4 Applications of Signature Recognition

1.5.2 Keystroke Dynamics

1.5.2.1 Merits of Keystroke Recognition

1.5.2.2 Demerits of Keystroke Recognition

1.5.2.3 Application of Keystroke Recognition

1.5.3 Gait

1.5.3.1 Merits of Gait Recognition

1.5.3.2 Demerits of Gait Recognition

1.5.3.3 Application of Gait Recognition
Contents

2.5 Databases for Signature System Evaluation 48
  2.5.1 SVC2004 50
  2.5.2 GPDS-960 51
  2.5.3 MCYT-100 51
  2.5.4 BIOMET 52

2.6 Commercial Software 52
  2.6.1 SOFTPRO 53
  2.6.2 ParaScript 54
  2.6.3 SQN Banking Systems 54

2.7 A Review to Signature Recognizers 54
  2.7.1 Data Acquisition 55
  2.7.2 Preprocessing 58
  2.7.3 Feature Extraction 65
    2.7.3.1 Graphology Based 68
    2.7.3.2 Shape Context Based 69
    2.7.3.3 Contour Based 71
    2.7.3.4 Projection Based 72
    2.7.3.5 Curvature Based 72
    2.7.3.6 Radon Transform Based 72
    2.7.3.7 Hough Transform Based 73
    2.7.3.8 Texture Based 73
    2.7.3.9 Wavelet Transform Based 74
  2.7.4 Classification 75
    2.7.4.1 Template Matching 75
    2.7.4.2 Statistical Classification 77

2.8 Assessment of Biometric Signature Systems 79

2.9 Example Studies on Signature Recognition 79
  2.9.1 Online System 79
    2.9.1.1 Results 81
    2.9.1.2 Identification 82
    2.9.1.3 Verification 82
    2.9.1.4 Discussion 82
  2.9.2 Offline System 82
    2.9.2.1 Results 85
    2.9.2.2 Identification 85
    2.9.2.3 Verification 86
    2.9.2.4 Discussion 87

References 87

Chapter 3 Keystroke Dynamics 93

3.1 History of Keystroke Dynamics 93

3.2 Keystroke Analysis 94
  3.2.1 Data Acquisition 95

3.3 Variability of Users, User Behavior, and Hardware 100

3.4 Authentication and Identification 101
  3.4.1 On Biometrics Context of Keystroke Dynamics 103
3.5 Characteristics of Keystroke Dynamics
3.5.1 Universality
3.5.2 Uniqueness
3.5.3 Permanence
3.5.4 Collectability
3.5.5 Performance
3.5.6 Acceptability
3.5.7 Circumvention
3.5.8 Summary
3.6 Approaches to Keystroke Dynamics
3.6.1 Taxonomies of Approaches
3.6.2 Input Text Approach Taxonomy
3.6.3 Simple Typing Features
3.7 Advanced Approaches
3.8 Fixed Text for All Users
3.8.1 Dataset
3.8.2 Proposed Algorithm
3.9 Fixed Text for Each User (BioPassword/AdmitOneSecurity)
3.9.1 Computer-Access Security Systems Using Keystroke Dynamics
3.9.2 AdmitOneSecurity
3.10 Non-Fixed Text with Regard to Key
3.10.1 Proposed Algorithm
3.10.2 Experimental Results and Discussion
3.11 Non-Fixed Text with No Regard to Key
3.11.1 Dataset
3.11.2 Proposed Algorithm
3.12 Continuous Authentication
3.13 Perspectives
3.14 Modern Trends and Commercial Applications for Keystroke Dynamics
3.14.1 Errors Made by Users and Their Correction Methods
3.14.2 Pressure-Sensitive Keyboards
3.14.3 Mobile Phone Keyboards
3.14.4 ATM Hardware
3.14.5 Random Numbers Generation
3.14.6 Timing Attacks on Secure Communications
3.14.7 Examples of Commercial Applications
3.15 Legal Issues
3.16 Conclusions
References

Chapter 4 Gait Analysis
4.1 Human Gait Recognition
4.2 Features of Gait Analysis
## CONTENTS

4.3 Applications of Gait Analysis 141  
4.4 Gait Cycle 141  
4.5 Describing a Stance 142  
4.6 Why Does Gait Change from Person to Person or from Time to Time? 143  
4.7 A Brief Review of the Literature on Human Gait Recognition 143  
4.8 Research Challenges 152  
4.8.1 External Factors 152  
4.8.2 Internal Factors 154  
4.9 Gait Databases for Research 154  
4.9.1 CASIA-A 154  
4.9.2 CASIA-B 154  
4.9.3 CMU MoBo 155  
4.9.4 USF Dataset 155  
4.9.5 Southampton Dataset 156  
4.9.6 3D Dataset 156  
4.9.7 UMD Dataset 156  
4.9.8 TUM-IITKGP Dataset 156  
4.9.9 OU-ISIR Database 156  
4.10 Gait Recognition Using Partial Silhouette-Based Approach 157  
4.10.1 Motivation of the Partial Silhouette-Based Approach 158  
4.10.2 Dynamic Features of Gait—Why Partial Silhouette? 159  
4.10.3 Partial Silhouette-Based Methodology 161  
4.10.4 Preprocessing for Removing Noise 161  
4.10.5 Gait Cycle Detection and Extraction of Landmark Frames 162  
4.11 Extraction of Partial Silhouette 163  
4.11.1 Bounding Box 164  
4.11.2 Image Segmentation 164  
4.11.3 Feature Extraction 165  
4.11.4 Classification 166  
4.11.5 Training 166  
4.11.6 Testing 168  
4.12 Experimental Verification 168  
4.12.1 Results of Full versus Partial Silhouettes 169  
4.13 Comparison with Other Methods 171  
4.14 Effectiveness of Partial Silhouette Method in the Presence of Noise 172  
4.15 Time Complexity of the Partial Silhouette-Based Method 175  
4.16 Conclusions 177  
References 177
Chapter 5  
Voice Recognition  

5.1  Voice Recognition  
5.1.1 Advantages of Voice Recognition over Other Biometric Traits  
5.1.2 Main Steps in Voice Recognition Systems  
5.2  Signal Acquisition and Preprocessing  
5.2.1 Biological Background  
5.2.2 Preprocessing Stage  
5.2.3 Feature Extraction  
5.3  Toeplitz Matrix Minimal Eigenvalues Algorithm—A Survey  
5.3.1 Linear Predictive Coding and Burg’s Model  
5.3.2 Mel Frequency Cepstral Coefficients  
5.4  Classification Using NNs  
5.4.1 Probabilistic NNs  
5.4.2 Radial Basis Function NNs  
5.5  Achievements in Similar Works  
5.6  Achievements in Voice Recognition  
5.6.1 The Simplest Case, Uttered Words Recognition  
5.6.1.1 Input Samples and Preprocessing Stage  
5.6.1.2 Experiments and Result  
5.6.2 Voiceprint and Security Systems  
5.6.2.1 Performance of the Speaker Identification Security System  
5.6.2.2 Multilevel Security for the Spoken Words and Speaker  
5.6.3 Text-Independent Speaker Identification  
5.6.3.1 Database and Preprocessing  
5.6.3.2 First Attempt  
5.6.3.3 Another Attempt  
5.6.4 What about Speaker Verification?  
5.6.4.1 Identification Treatment  
5.6.4.2 Verify the Speaker—Claiming It Correctly  
5.6.4.3 True Rejection and False Acceptance  
5.6.4.4 Extra Testing Data for Verification  
5.7  Conclusions  
References  
Index
I met Professor Saeed, the principal author of this book, for the first time in 2009 at AGH University of Science and Technology, Kraków, Poland. I was invited as one of the keynote speakers and a researcher of behavioral biometrics in the International Multi-Conference on Biometrics and Kansei Engineering. My first impression of him was a true professor in an elegant suit, with high-quality speech, passionate approach to research, and unfailing kindness. Although 7 years have already passed, his humanity is abiding, and I have ever since constantly communicated with him as a researcher, a university educator, a journal editor, and an international conference chair.

Professor Saeed has achieved a great accomplishment by writing this book: *New Directions in Behavioral Biometrics*. Publishing this book has been a delightful event for me and many biometrics researchers. Based on the great achievement of his research team, this book includes a readable introduction, beneficial literature reviews, specific approaches, detailed algorithms, and useful experimental results of behavioral biometrics such as signature recognition, keystroke dynamics, gait analysis, and voice recognition.

Biometric technology using physiological characteristics has been widely applied, and many products that employ this technology are very popular, whereas biometric technology using behavioral characteristics has not received considerable attention. However, from a
different point of view, research of the behavioral biometrics possesses the possibility of success and advancement. For a university student, a researcher, or a developer who is researching biometrics or developing an application system, this book will provide a clear path of basic information on behavioral biometrics and many hints for new discovery, all coming out of the extensive research experience of the author.

If, in the near future, a technology of identifying an individual based on writing style is developed, Professor Saeed will be easily identified because this book includes his passionate approach and a high degree of completion.

Nobuyuki Nishiuchi
Tokyo Metropolitan University
Preface

This book is the result of research conducted with major members of my international biometrics team on some selected topics in behavioral biometrics: a field of study related to the way people behave. As the reader might recall, the science of biometrics deals with biological measurement—describing and measuring human features for the sake of identity recognition (personal authentication and identification or verification, or both). Biometrics is known in two categories: physiological and behavioral. **Physiological biometrics** is beyond the scope of this book, but some selected examples have been provided in another book by the author (*see Biometrics and Kansei Engineering*, Springer, New York, 2012). This book, though, will focus on the most popular and emblematic examples of behavioral biometrics, namely, signature (the way we write), dynamics of keystrokes or touchscreen use (how we use the keyboard or touchscreen to enter text), and gait (how we move our legs to walk). Chapter 5 will deal with speech and speaker recognition, that is, the manner and art of combining vocal tracts, tongue, and lips to utter sounds and say words, which is sometimes considered to be a combination of physiological and behavioral features. All these human features are unique; they differ from one person to another, and that is why they can be used to distinguish people.
The content of the book is divided among five chapters. Chapter 1 is a general introduction to the subject, showing the nature of each behavioral feature, and discussing how they are collected and prepared for measuring. It also discusses the advantages and disadvantages of using such features for user authentication or personal verification.

These chapters reflect the authors’ extensive research on the different examples of biometrics. We have published many detailed works and consequently received valuable feedback from the reviewers, readers, and conference participants whenever a research work was presented for discussion. Hence, I hope this book appears in a well-organized and readable form to students and researchers.

As biometrics science is developing fast, I can say there is no single written book that could comprise all known behavioral biometrics aspects and that would incorporate all existing topics of this new scientific discipline. Apart from the small number of standard academic books on behavioral biometrics, students usually make use of available research papers and some special book briefs on some biometrics topics and aspects. However, researchers still seem to face difficulties introducing new, essential methods in behavior recognition with good enough results. This mainly comes from the basic characteristics of behavioral biometrics features, especially their low repeatability. This causes low accuracy and hence less system efficiency and a lower recognition rate when behavioral biometrics is considered alone. Still, researchers will always hope their methods will find their right place when technological advances produce sensors that are able to capture unique features that can give a sufficient unique description for different objects. Until then, the best way a behavioral biometrics feature can perform in a recognition system is by being a part of a fusion or hybrid system. In such systems, biometric features can play a partial role with other physiological features, as fingerprints provide another method of user authentication along with the PIN code, for example.

Many successful examples, such as signature, keystroke dynamics, gait, and voice feature recognition, are being developed with higher recognition rates, and this gave rise to the need for a book that discusses the most important and practical behavioral biometrics features. The methods and algorithms given on these features in this book have been checked for the highest possible recognition rates.
In Chapter 1, the reader can find introductory information about biometrics and the known behavioral features of a human.

Chapter 2, which is one of the most comprehensive chapters, introduces the basic achievements in human recognition by use of signatures—with only one reference signature, a user can be verified/personified. Dr. Marcin Adamski had proved this important result in his PhD thesis under my supervision in 2010. Since then, he has been working on algorithm improvement to reach the most accepted practical approach in everyday applications.

Chapter 3 is about keystroke dynamics—personalization based on how a user types on a keyboard. This human–computer interaction seems to be effective in verifying our contacts without the necessity or the possibility of seeing them. In addition to its practical use in patient–physician interactions, this method allows us to identify the age interval of the user, which is important for parents who wish to know who their children are having contact with. In their PhD works, Tapalina Bhattasali and Piotr Panasiuk have worked out simple patient–physician remote contact models, in which user passwords are accompanied by keyboard strike dynamics.

Chapter 4 deals with gait recognition for personal verification. It introduces the most recent research results of Dr. Soharab H. Shaikh, who worked on gait analysis as one of the basic parts of his PhD work.

In Chapter 5, voice recognition for personal verification and identification has been discussed on the basis of the heuristic studies of Mohammad K. Nammous as part of his PhD study.

This book contains practical examples, illustrations, and simple algorithms or algorithmic descriptions for students to easily implement in their computers. Moreover, the contents have been structured in such a way that each chapter can be read separately without the need to go back to any other chapter. They are self-contained and each chapter covers a separate subject area.

All my coauthors have been or still are my students, assistants or coworkers, and researchers, a fact that I have been proud of.

Khalid Saeed
Bialystok University of Technology
Biometrics refers to the study of biological characteristics. It comes from Greek words “bios” (implies life) and “metricos” (implies measuring/to measure). Biometrics can be considered as use of physiological or behavioral characteristics in an automated way to determine identity. The identity verification is performed through the measurement of physiological or behavioral characteristics of an individual. Researchers have proposed a number of biometric techniques for human identification and authentication based on fingerprint, palm print, hand geometry, face, ear, iris, retina, voice, signature, body odor, and so on.

Biometric traits are almost statistical in nature. The system is likely to be unique and reliable as much as data are available from sample. It can work on various modalities based on the measurements of individual’s body and features, and behavioral patterns. The modalities are classified according to individual’s biological traits. The biometric modalities mainly fall under following types:

- Physiological
- Behavioral
- Hybrid

Physiological category includes the features we are born with. This modality is based on the shape and size of the body. Examples are [1–3] as follows:

- Fingerprint recognition
- Hand geometry recognition
- Facial recognition
- Iris recognition
• Retinal scanning
• DNA recognition

Behavioral category deals with the features we learn in our life as a result of our interaction with the environment and the nature. This modality is related to change in human behavior over time. Examples of this category are

• The way we walk (gait).
• The way we write (signature).
• The way we speak or say a word (voice).
• The way we type on a machine (keystroke dynamics).
• Many other ways of our response to the natural events around us and the way we react to or respond.

Hybrid modality includes both traits, where the traits are depending upon physical as well as behavioral changes. As for example, voice recognition may be considered as hybrid modality as it depends on size and shape of vocal cord, nasal cavities, mouth cavity, shape of lips, and so on, and the emotional status, age, illness (behavior) of a person.

Hybrid modality is also considered as a type of multimodality (more than one mode involved). In this book, the concept of behavioral biometrics is presented briefly on the basis of some selected features like signature, keystroke dynamics, gait, and voice. A brief overview of behavioral biometrics is presented in this chapter.

1.1 Behaviometrics

The word “behaviometrics” derives from the terms “behavioral” and “biometrics” [4]. Behavioral refers to the way an individual behaves. Behaviometrics, or behavioral biometrics, is a measurable behavior used to recognize or verify the identity of a person. Behaviometrics focuses on behavioral patterns rather than physical attributes.

1.1.1 How It Works

Each person has a unique pattern—how they interact with computing devices by using keyboard, mouse, and graphical user interface (GUI). The study of the user’s unique nature in this regard is known as behaviometrics.
A human behavioral pattern consists of a variety of different unique behaviors—all are mixed together into a larger unique profile. Since unique behaviormetric pattern of every person is formed not only by biometric features, but is also influenced by social and psychological means, it is just impossible to copy somebody else’s behavior.

The behavioral pattern of the person is compared with the stored pattern. Matching scores of similarities for those users are recognized and the software calculates the possibility of accurate identification of users.

The key features of behavioral biometrics are given below.

• Security of applications like user authentication and intrusion detection may be enhanced by behavioral biometrics with very low impact on the users.
• Behavioral biometrics is highly sensitive to the means of implementation, for example, keystroke dynamics depend on the type of used keyboard.
• Behavioral biometrics is most useful in multimodal systems (where more than one type of biometrics is used at the same time) compared to unimodal systems (where only one type of biometrics is used at a time).
• It may be vulnerable to several spoofing attacks [5].

A comprehensive review of different biometric technologies including theory and applications can be found in [1]. A survey of different techniques on behavioral biometrics is summarized in [6]. Behavioral biometrics is popularly used in information security context to identify individuals by using unique features of activities they perform either consciously or unconsciously. In recent times, it has been observed that behavioral biometric data are used for a number of interesting applications. Researchers have proposed methodologies for speaker recognition by tracking movements of lips [7], biometric verification using motions of fingers [8], and extracting biometric features of voice [9] for person identification. A promising application of biometrics is arimetrics, where biometric traits are used for authenticating artificial entities like industrial robots, intelligent software agents, and virtual-world avatars [9]. Biometric data are also used for enhancing the security of cryptographic systems. New algorithms are developed by
researchers for filtering biometrics. Performance evaluation of systems is very important for the following reasons.

- Quality of system must be precisely quantified to be used in real context. To determine whether it fulfills the requirements of a specific application based on logical or physical access, context of use, efficiency, and robustness of the logic must be defined.
- Comparison of different biometric modalities is essential to analyze their relative merits and demerits.
- Performance evaluation is also necessary in order to facilitate research in this field.

Evaluation techniques are used to quantify the performance of behavioral biometric systems. A reliable evaluation method is needed in order to analyze advantage of the system.

1.1.2 Major Benefits

Behaviometrics can provide information security solutions by using the nature of individual. It is extremely hard to replicate, which makes it the ultimate solution against identity theft. It is not possible that any unauthorized user could access a computer with confidential information, either by hacking the password or logging in with stolen credentials or accessing a logged on computer. As a result, intrusion can be prevented.

As for example, it is possible to recognize and confirm the identity of a person by analyzing how the user works with the keyboard (typing rhythm), mouse movements (acceleration time, click frequencies), and graphical interface interaction (using programs).

- While many popular security solutions require the user to perform additional tasks, behaviometrics does not interfere with the normal work flow. Simple use of computing device in the everyday work makes the software increasingly more efficient and the confidential information more secure.
- Behaviometrics will allow workstations to be secure even after the user has logged on to the system. Even if the user leaves
the workstation and forgets to sign out, computing device stays protected.

- Existing token-based products (such as passwords and smart cards) can be duplicated or stolen, whereas user’s behavior is unique and very difficult to copy.

### 1.2 What Is Special about Behavioral Biometrics Data Acquisition?

The special aspects of behavioral biometrics data acquisition are presented below.

- It offers increased convenience in data acquisition, because there is no requirement for dedicated or special hardware. As a result, it is also considered as cost-effective.
- Most of the data are acquired through machine-based interactions.
- These traits need to be easily verifiable and identifiable.
- Input data depend on the permanence and distinctiveness metrics.
- It does not introduce delays in operations and are implemented silently. It is mostly used in online platforms. Their acceptance level in the society is high.

### 1.3 Behavioral Biometrics Features

A biometric system may include different phases. Two phases are mainly considered during the use of a biometric system. A working model of data acquisition is defined in enrollment phase of an individual. Verification phase uses this model to make a decision about an individual. The performance evaluation of a biometric system generally considers the quality of the input data and the output result.

In accomplishing their everyday tasks [1], people employ different strategies, use different styles and apply unique skills and knowledge. One of the defining characteristics of a behavioral biometric is the incorporation of time dimension as a part of the behavioral signature. The measured behavior has a beginning, duration, and an end. Researchers attempt to quantify behavioral traits exhibited by users and use resulting features to verify identity efficiently.
Behavioral biometrics provides a number of advantages. They can be collected without the knowledge of the user. It becomes very cost-effective as collection of behavioral data often does not require any special hardware. Data acquisition devices include computer, keyboard, mouse, stylus, touch screen, microphone, camera, credit card, and scanner to capture most frequently used behavioral biometrics. Although most of the behavioral biometric traits may not be unique enough to provide reliable human identification, it is observed that they can provide sufficiently high accuracy in identity verification.

Behavioral biometric systems are requirement specific. Many characteristics make them difficult to analyze their performance [10]:

- Biometric template generally contains temporal information.
- This type of template can change with time. It means that the biometric template can be quite different compared to the one obtained after the enrollment phase.
- The behavior of biometric characteristic can be very different for an individual given its age, culture, and experience.

The evaluation of system is often analyzed by considering a variety of users. Benchmark definition has high impact on the performance evaluation of biometric systems. A benchmark database may include either real biometric templates or synthetic ones. The definition of synthetic templates is easier for behavioral biometric data such as keystroke dynamics, voice, lip movements, mouse dynamics, and signature dynamics. For behavioral biometric modalities such as keystroke dynamics, voice, or gait, the associated template can vary for individuals at different ages. As a consequence, the benchmark database must include all the variability of biometric templates to represent real applications.

Behavioral biometrics and related technologies have potential to improve diverse areas such as mobile commerce, real application analysis, risk, and financial analysis. It is used for user modeling that aims at creating a representation of the user for the purpose of customizing service suitable for the user.

1.4 Classification of Behavioral Biometrics Traits

Behavioral biometrics can be used in an information security context to identify individuals by using unique features of activities they perform either consciously or unconsciously. Behavioral biometrics can
be classified into several categories based on the type of information about the user being collected (Figure 1.1).

Behavioral biometrics traits are entirely dependent on behavioral nature of human beings. It measures human behavior which is not directly focusing on measurements of body parts.

Motor skill of a human being has an ability to utilize muscles. Muscle movements rely upon the proper functioning of the brain, skeleton, joints, and nervous system. Therefore, motor skills indirectly reflect the quality of functioning of such systems, making person verification possible. Most of the motor skills are learned, not inherited. Definition for motor skill is adopted based on behavioral biometrics, for example, “kinetics,” which are based on unique and stable muscle actions of the user while performing a particular task.

Authorship-based biometrics is based on examining a piece of text or a drawing produced by a person. Verification is accomplished by observing style peculiarities typical to the author of the work being examined, such as the used vocabulary, punctuation, or brush strokes.

Human–computer interaction (HCI)-based biometrics can be further subdivided into additional categories—indirect HCI-based interaction and direct HCI-based interaction. Indirect HCI-based biometrics includes the events that can be obtained by monitoring user’s HCI behavior indirectly via observable low-level actions of computer software. Direct HCI-based interaction is again divided into

![Figure 1.1 Classification of behavioral biometrics traits.](image-url)
two categories. The first category consists of human interaction with input devices such as keyboards and mouse. The second category consists of HCI-based behavioral biometrics, which measures advanced human behavior such as strategy, knowledge, or skill exhibited by the user during interaction with different software (Figure 1.2).

*Signature verification:* Here, users need to present handwritten text for authentication.

*Keystroke dynamics:* It is a behavioral biometrics that relies on the way by which users can interact with keyboard. As a person interacts with keyboard, features are extracted and used to identify the user.

*Gait analysis:* Gait is considered as biometrics controlled by muscle. Gait analysis is the systematic study of human motion, using the eye and the brain of observers, for measuring body movements, body mechanics, and the activity of the muscles.

*Voice recognition:* Voice is used for either speaker identification or speaker authentication.

Other interesting examples include

- *Blinking pattern:* Time between blinks, how long the eye is held closed at each blink, physical characteristics of the eye while blinking
- *ECG:* Features of electromagnetic signals generated by the heart
- *EEG:* Features of electromagnetic signals generated by the brain

A number of techniques are limited to specific use-cases—for example, car driving style (to identify drivers), handgrip pressure patterns (for authentication to handheld devices including weapons), and credit

![Figure 1.2](image.png)  
*Figure 1.2* Behavioral traits: (a) signature, (b) keystroke, (c) gait, and (d) voice.
card usage patterns (credit card fraud detection). Important factors in the successful implementation of behavioral biometrics include

- **Equipment required**: This can vary from none at all (e.g., in the case of simple keystroke dynamics) to multiple cameras, EEG sensors, and so on.
- **Enrollment time**: The time required to train the system to recognize individual.
- **Persistence**: The time before an identifying feature changes in an individual after an initial training period of the system.
- **Obtrusiveness**: How much the system alters the normal experience of the identification subject.
- **Error rates**: As with all biometrics, error rates are analyzed according to
  - **False rejection rate (FRR)**: The percentage of individuals wrongly denied access to a system.
  - **False acceptance rate (FAR)**: The percentage of individuals wrongly authorized by a system.
  - **Equal error rate (EER)**: A measure often used to evaluate the accuracy of a biometric technology. It is the value of FRR and FAR when a system is tuned to have an equal FAR and FRR.

1.5 Properties of Few Behavioral Biometrics

1.5.1 Signature

In signature recognition, more emphasis is given on the behavioral patterns in which the signature is signed rather than its visibility in terms of graphics.

The behavioral patterns include the changes in the timing of writing, pauses, pressure, direction of strokes, and speed during the course of signing. It could be easy to duplicate the graphical appearance of the signature, but it is not easy to copy the signature with the same behavior the person shows while signing (Figure 1.3).

This technology consists of a pen and a specialized writing tablet, both connected to a computer for template comparison and verification. A high quality tablet can capture the behavioral traits such as speed, pressure, and timing while signing.
During enrollment phase, the candidate must sign on the writing tablet multiple times for data acquisition. The signature recognition algorithms then extract the unique features such as timing, pressure, speed, direction of strokes, important points on the path of signature, and the size of signature. The algorithm assigns different values of weights to those points. At the time of identification, the candidate enters the live sample of the signature, which is compared with the signatures in the database.

Signature verification is a widely accepted methodology for confirming identity. Two distinct approaches to signature verification are recognized based on the data collection approach. They are online and offline signature verification, also known as static and dynamic approaches. In the offline signature verification, the image of the signature is obtained using a scanning device. The offline approach utilizes the static features of the signature. With online signature verification, special hardware is used to capture dynamics of the signature. During online signature verification, signature characteristics are extracted as the user writes, and these features are used to immediately authenticate the user. Typically, specialized hardware is required, such as a pressure-sensitive pen or a special writing tablet. These hardware elements are designed to capture pen pressure, pen angle, and related information. During remote authentication, online approach is most suitable. Signature-related features can be classified into two groups—global and local. Global features include signing speed, signature bounding box, Fourier descriptors of the signature’s trajectory, number of strokes, and signing flow [11]. Local features describe specific sample point in the signature and relationship between such points, for example, distance and curvature change between two successive points may be analyzed.
as well as $x$ and $y$ offsets relative to the first point on the signature trajectory, and critical points of the signature trajectory [11].

1.5.1.1 Constraints of Signature Recognition
- To acquire adequate amount of data, the signature should be small enough to fit on tablet and big enough to be able to deal with.
- The quality of the writing tablet decides the robustness of signature recognition enrollment template.
- The candidate must perform the verification processes in the same type of environment and conditions as they are at the time of enrollment. If there is a change, then the enrollment template and live sample template may differ from each other.

1.5.1.2 Merits of Signature Recognition
- Signature recognition process has a high resistance to impostors as it is very difficult to imitate the behavior patterns associated with the signature.
- It works very well in high amount business transactions.
- It is a noninvasive tool.
- There are no privacy rights issues involved.
- Even if the system is hacked and the template is stolen, it is easy to restore the template.

1.5.1.3 Demerits of Signature Recognition
- The live sample template is prone to change with respect to the changes in behavior while signing.
- User needs to get accustomed to using signing tablet. Error rate is high till it happens.

1.5.1.4 Applications of Signature Recognition
- It is used in document verification and authorization.

The concept of biometrics sketch authentication [11] is similar to the concept of signature recognition. This method is based on sketch recognition and a user’s personal knowledge about the drawings content.
The system directs a user to create a simple sketch. Sketches of different users are sufficiently unique to provide accurate authentication. The approach measures user’s knowledge about the sketch, which is only available to the previously authenticated user. Features like location and relative position of different primitives are taken as the profile of the sketch.

1.5.2 Keystroke Dynamics

During World War II, a technique known as Fist of the Sender was used by military to determine if the Morse code was sent by an enemy or ally based on the rhythm of typing. These days, keystroke dynamics is the easiest biometric solution to implement in terms of hardware [12].

This biometric analyzes candidate’s typing pattern, rhythm, and speed of typing on a keyboard. The dwell time and flight time measurements are used in keystroke recognition.

*Dwell time*: It is the duration of time for which a key is pressed.
*Flight time*: It is the time elapsed between releasing a key and pressing the following key.

The candidates differ in the way they type on the keyboard as the time they take to find the right key, the flight time, and the dwelling time. Their speed and rhythm of typing also varies according to their level of comfort with the keyboard. Keystroke recognition system monitors the keyboard inputs thousands of times per second in a single attempt to identify users based on their habits of typing.

Typing patterns [11] are characteristic of each person. For verification, a small typing sample such as the input of user’s password is sufficient, but for recognition, a large amount of keystroke data are needed and identification is based on comparisons with the profiles of all other existing users already in the system. Keystroke features are based on time durations between the keystrokes, flight times and dwell times, overall typing speed, frequency of errors (use of backspace), use of numpad, order in which user presses shift key to get capital letters, and possibly the force with which keys are hit for specially equipped keyboards. Keystroke dynamics is probably the most researched type of HCI-based biometrics [11].
There are two types of keystroke recognition.

- **Static**: It is one-time recognition at the start of interaction.
- **Continuous**: It is throughout the course of interaction (Figure 1.4).

### 1.5.2.1 Merits of Keystroke Recognition

- It needs no special hardware to track this biometric.
- It is a quick and secure way of identification.
- A person typing does not have to worry about being watched.
- Users need no training for enrollment or entering their live samples.

### 1.5.2.2 Demerits of Keystroke Recognition

- The candidate’s typing rhythm can change because of tiredness, sickness, influence of medicines or alcohol, change of keyboard, and so on.
- There are no known features dedicated solely to carry out discriminating information.

Based on the idea of monitoring user’s keyboard and mouse activity [11], system is developed for collecting GUI interaction-based data. Collected data allows generation of behavioral profiles of end-users. Such type of data may provide additional information not available from typically analyzed command-line data. Ideally, the collected data would include high-level detailed information about the GUI-related actions of the user such as left click on the start menu and so on. All collected data are time stamped and preprocessed to reduce the amount of data actually used for intrusion detection purposes.
1.5.2.3 Application of Keystroke Recognition

- Keystroke recognition is used for identification/verification. It is used with user ID/password as a form of multifactor authentication.
- It is used for surveillance. Some software solutions track keystroke behavior for each user account without end-user’s knowledge. This tracking is used to analyze if the account was being shared or used by anyone else than the genuine account owner. It is used to verify if some software license is being shared.
- Application area:
  - Student identification for online examinations
  - User/employee identification for remote workstations
  - User authentication for network access
  - User authentication in e-commerce, online banking, and e-government

1.5.3 Gait

Gait is the manner of a person’s walking. People show different traits while walking such as body posture, distance between two feet while walking, swaying, and so on, which helps to recognize them uniquely.

A gait recognition based on the analysis of video images containing candidate’s walk. The sample of candidate’s walk cycle is recorded by video. The sample is then analyzed for position of joints such as knees and ankles, and the angles made between them while walking.

A respective mathematical model is created for every candidate and stored in the database as a template. At the time of verification, this model is compared with the live sample of the candidate walk to determine its identity (Figure 1.5).

Gait [11] is a complex spatiotemporal motor-control behavior which allows biometric recognition of individuals at a distance usually from captured video. Gait analysis is used to assess, plan, and treat individuals with conditions affecting their ability to walk. It is also commonly used to identify posture-related or movement-related problems in people with injuries. It can distinguish one individual.
from others from various aspects about the human being (health, age, size, weight, speed, etc.) from his/her gait pattern. Typical features include amount of arm swing, rhythm of the walker, bounce, length of steps, vertical distance between head and foot, distance between head and pelvis, and maximum distance between the left and right foot [11]. Gait variation is based on changes in person’s body weight, injuries, and so on.

1.5.3.1 Merits of Gait Recognition

- It is noninvasive.
- It does not need the candidate’s cooperation as it can be used from a distance.
- It can be used for determining medical disorders by spotting changes in walking pattern of a person in case of Parkinson’s disease.

1.5.3.2 Demerits of Gait Recognition

- For this biometric technique, developing model with complete accuracy is very difficult.
- It may not be as reliable as other established biometric techniques.

1.5.3.3 Application of Gait Recognition  It is well-suited for identifying criminals in the crime scenario.
1.5.4 Voice

Voice Recognition is also called speaker recognition. At the time of enrollment, the user needs to speak a word or phrase into a microphone. This is necessary to acquire speech sample of a candidate (Figure 1.6).

Speaker identification is one of the best researched biometric technologies. Verification is based on information about the speaker’s anatomical structure conveyed in amplitude spectrum, with the location and size of spectral peaks related to the vocal tract shape. Speaker identification systems can be classified based on the freedom of what is spoken.

- **Fixed text**: The speaker says a particular word selected at enrollment.
- **Text dependent**: The speaker is prompted by the system to say a particular phrase.
- **Text independent**: The speaker is free to say anything he wants.

Verification accuracy typically improves with larger amount of spoken text.

One of the principal tasks of the enrollment process is to register the person as a potential user of the biometric system. In a speaker-independent system, the user’s voice pattern is analyzed and compared to all other voice samples in the user database. The closest match to the particular voice data presented for identification becomes the identity of the speaker.

There are two variants of voice recognition—speaker-dependent and speaker-independent.
Speaker-dependent voice recognition relies on the knowledge of candidate’s particular voice characteristics. This system learns those characteristics through voice training (or enrollment).

- The system needs to be trained on the users to accustom it to a particular accent and tone before employing to recognize what was said.
- It is a good option if there is only one user going to use the system.

Speaker-independent systems are able to recognize the speech from different users by restricting the contexts of the speech such as words and phrases. These systems are used for automated telephone interfaces.

- They do not require training the system on each individual user
- They are a good choice to be used by different individuals where it is not required to recognize each candidate’s speech characteristics

1.5.4.1 Differences between Voice and Speech Recognition

Speaker recognition and speech recognition are mistakenly taken as same; but they are different technologies.

<table>
<thead>
<tr>
<th>SPEAKER RECOGNITION (VOICE RECOGNITION)</th>
<th>SPEECH RECOGNITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The objective of voice recognition is to recognize WHO is speaking.</td>
<td>The speech recognition aims at understanding and comprehending WHAT is spoken.</td>
</tr>
<tr>
<td>It is used to identify a person by analyzing its tone, voice pitch, and accent.</td>
<td>It is used in hand-free computing, map, or menu navigation.</td>
</tr>
</tbody>
</table>

1.5.4.2 Merits of Voice Recognition

- It is easy to implement.

1.5.4.3 Demerits of Voice Recognition

- It is susceptible to quality of microphone and noise.
- The inability to control the factors affecting the input system can significantly decrease performance.
- Some speaker verification systems are also susceptible to spoofing attacks through recorded voice.

Click here to purchase "New Directions in Behavioral Biometrics"
© 2017 by Taylor & Francis Group, LLC
1.5.4.4 Applications of Voice Recognition

- Performing telephone and Internet transactions
- Working with interactive voice response (IVR)-based banking and health systems
- Applying audio signatures for digital documents
- In entertainment and emergency services
- In online education systems

1.6 Behavioral Biometrics Data Acquisition Device

The performance of behavioral biometrics critically depends on the quality of biometric data [13]. Sensor design and deployment requires high quality data for improved accuracy and flexible acquisition of data with high user acceptability.

Data acquisition devices for signature recognition are classified into two categories—online and offline. Scanners are generally considered as offline input device. It is a device that captures images from photographic prints, posters, and similar sources for editing and display. Flat bed scanners are popularly used to convert images and text into a digital format. Data acquisition is performed in offline mode after completion of writing procedure. Its nature is considered as static.

Graphic tablets are generally used for online signature acquisition. It allows to draw on the tablet in a natural way (just like pencil and paper) and their drawings appear on the screen of computing device. Its nature is generally considered as dynamic. These generate electronic signals representative of the signature during writing procedure. The generated signals can be coordinate signals, pressure and force signals, pen-down (operation of pulling down the tip of the pen toward the writing plane), and pen-up (operation of lifting up the tip of the pen from the writing plane) signals.

Keystroke dynamics acquires data through computer keyboard. A keyboard has characters printed on the keys and each press of a key typically corresponds to a single written symbol. However, to produce some symbols requires pressing and holding several keys simultaneously or in sequence. Most of the keys of keyboard produce letters, numbers, or signs, other keys or simultaneous key presses can produce actions or execute computer commands. In normal usage, the keyboard is used as a text-entry interface to type text and numbers into
Introduction to Behavioral Biometrics

A word processor, text editor, or other programs. The interpretation of key presses is generally left to the software. A computer keyboard distinguishes each physical key from every other keys and reports all key presses to the controlling software. A command-line interface is a type of user interface operated entirely through a keyboard.

Mouse dynamics acquires data through mouse, which is a pointing device used on the screen of a computer. It enables user to execute commands or issue instructions to the computer by controlling a pointer on the screen. A mouse typically controls the motion of a pointer in two dimensions in a GUI. The mouse turns movements of the hand backward and forward, left and right into equivalent electronic signals. The relative movements of the mouse on the surface are applied to the position of the pointer on the screen, which signals the point where actions of the user take place.

Touch data are collected by touch screen input device. A user can give input or control the information processing system through simple or multitouch gestures by touching the screen with a special stylus or pen or one or more fingers. Some touch screens use a special stylus or pen only. The user can use the touch screen to react to what is displayed and to control how it is displayed. As for example, zooming is used to increase the text size. The touch screen enables the user to interact directly with what is displayed, rather than using a mouse, touchpad, or any other intermediate device.

Modern mobile devices come with various sensors such as accelerometer, gyroscope, GPS receiver, WiFi receiver, and so on. Few of the widely utilized sensors are mentioned below to present how to retrieve sensor data systemically.

An accelerometer is a device that measures proper acceleration experienced by an object relative to a free-falling frame of reference. A triaxial accelerometer installed on a mobile or wearable device returns a real-valued estimate of acceleration along the x, y, and z axes in units of meter per second squared (m/s²). By measuring the amount of static acceleration due to gravity, it is possible to find out the angle the device is tilted with respect to the earth. By sensing the amount of dynamic acceleration, we can analyze the way the device is moving. Because of the information that the accelerometer can offer, it can be employed as a high-bandwidth side channel to learn certain behavioral patterns.
A gyroscope is a device for measuring or maintaining orientation, based on the principles of angular momentum. It is also known as angular rate sensors or angular velocity sensors. Gyroscopes can sense the angular velocity along the $x$, $y$, and $z$ axes of a mobile or wearable device, corresponding to pitch, roll, and yaw, respectively, in units of radian per second (rad/s). The introduction of gyroscopes into the mobile devices has allowed for more accurate recognition of movements within 3D space than lone accelerometer devices. That is why modern smartphones are usually equipped with both accelerometer and gyroscope, for example, HTC, Nexus, iPhone, Nokia, and so on. Gyroscopes play a significant role in the gaming arena by providing a richer experience in handling the game.

Gait recognition acquires data through video camera that is used for electronic motion picture acquisition. Video cameras are used primarily in two modes. In one mode, the camera feeds real-time images directly to a screen for immediate observation. Most of the live connections are for security, military, and industrial operations where remote viewing is required. In another mode, the images are recorded to a storage device for archiving or further processing. Recorded video is used in surveillance and monitoring tasks in which unattended recording of a situation is required for later analysis. Closed-circuit television (CCTV) generally uses pan–tilt–zoom cameras (PTZ), for security, surveillance, and monitoring purposes. Such cameras are designed to be small, easily hidden, and able to operate unattended. These are often meant for use in environments that are normally inaccessible or uncomfortable for humans.

Voice and speech recognition system acquires data through microphone. A microphone is a transducer that converts sounds into variation of voltage. Electromagnetic transducers facilitate the conversion of acoustic signals into electrical signals from air-pressure variation. Microphones typically need to be connected to a preamplifier before the signal can be amplified with an audio power amplifier and a speaker. Microphone connects to software to convert human speech into commands or text.

It provides a natural interface with computing device that allows for new users to execute commands without having to learn complex command set. Speech recognition might not recognize the difference between similar words that is “their” and “they’re” or be able to understand regional accents.