Series in BioEngineering

The Series in Bioengineering serves as an information source for a professional audience in science and technology as well as for advanced students. It covers all applications of the physical sciences and technology to medicine and the life sciences. Its scope ranges from bioengineering, biomedical and clinical engineering to biophysics, biomechanics, biomaterials, and bioinformatics.

More information about this series at http://www.springer.com/series/10358

Amine Nait-ali
Editor

Hidden Biometrics

When Biometric Security Meets Biomedical Engineering

Springer

Editor
Amine Nait-ali
Université Paris-Est, LISSI, UPEC
Vitry sur Seine, France

ISSN 2196-8861 ISSN 2196-887X (electronic)
Series in BioEngineering
ISBN 978-981-13-0955-7 ISBN 978-981-13-0956-4 (eBook)
https://doi.org/10.1007/978-981-13-0956-4

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The term “Biometrics”, once split into two halves, highlights the words “Bio” and the word “metrics”. These two words should be clearly distinguished since their meaning is deep and precise. The first word stands for life science, whereas the second half stands for measurement. Among the different fields of applications of biometrics, security field has been widely considered and intensively amplified by the media. For this reason, people frequently tend to use the term “biometrics” instead of using “Biometric Security”.

Within the context of this book, the focus is on biometric security, and more specifically on hidden biometrics for security. Therefore, before delving into the specifics of biometrics, the concept of classical or conventional biometrics is discussed. Biometric security is defined as a technology which recognizes individuals by their physical or behavioral characteristics. If the modalities considered in this type of biometrics were to be analyzed, we would notice that the “envelope” of the human body and in some cases, its dynamic (behavior) is intensively explored. This means that the role of acquisition devices is mainly to represent or to “Copy” what the human being can perceive, including what the naked eye can see or what the ear can hear. For instance, when the objective is to recognize: face, ears, gait, hand shape, iris, fingerprints, and voice, optical or acoustical sensors are used in most of the cases.

Hidden biometrics for security applications, on the other hand, aims to identify individuals by representing different non-perceived hidden layers of their body and even their hidden behaviors. In order to do so, specific devices and equipment are employed. As discussed in the chapters of this book, some of the devices are mainly used in the biomedical engineering field. Consequently, one can raise the following question: what is the advantage of hidden biometrics compared to the conventional biometrics? The answer is simple, anything which is visible, can be easily accessible, copied, stolen, or imitated. On the other hand, when something is hidden, the access becomes more difficult, hence, it would require more effort, and probably more time to reach the information. So, by considering hidden biometrics, forgeries and attacks become more difficult. This is a big advantage when high-security level is required.

Hidden biometrics can be used to prevent spoofing. For instance, the "brainprint" can be regarded as a signature representing the morphology of our brain which cannot be easily copied. The same observation concerns brain activity, can generally be represented from electroencephalogram. Another advantage of hidden biometrics is the absence of illumination and occlusion issues, commonly observed in the conventional biometrics. In fact, when exploring the inner human body, this issue does not exist.

Although many promising advantages of hidden biometrics are highlighted, we are aware that this technology has "temporarily" some drawbacks. The term "temporarily" is used because we believe that the limitations of today can be overcome in the future. As limitations, one can evoke the acquisition process that can be time consuming, and the cost may be relatively high depending on the modality being used. In addition, user's acceptability factor may be an issue for many reasons, including safety, ethical, and privacy aspects.

Hence, what will be the future of hidden biometrics? What kind of efforts should be deployed? First, it is important to note that technology is being continuously developed, and it would not be surprising that the acquisition systems which are usually used in biomedical engineering will be adapted for security applications. Their size, weight, and cost may be considerably reduced. In fact, since no clinical diagnosis is required, systems can be redesigned and optimized for security purposes. Therefore, if the industry invests in this field in collaboration with experts from the medical field, biometric security can reach a new level. This kind of collaboration is mandatory because this will probably impact users' acceptability. By keeping the users or consumers permanently informed, hidden biometrics could have the same evolution as fingerprint. In the past century, fingerprint identification has been used exclusively for criminals. What happened one century later? People are now using their fingerprint as a key, namely, they can unlock their smartphones with it. Our society is changing and mentalities are changing too, … So, if you think that the solutions and the approaches presented in this book cannot be exploited nowadays, just keep in mind that tomorrow is another day. You may change your mind, ….

The current book entitled, *Hidden Biometrics: When Biometric Security Meets Biomedical Engineering* is organized as follows:

Chapter "DNA Based Identification": In this first chapter of the book, DNA will be investigated as a deepest Hidden Biometrics modality. After presenting some basic ideas, techniques, and some major applications, a special interest will be addressed to a recent research topics related to the prediction of visible physical traits.

Chapter "A Review on ECG-Based Biometric Authentication Systems": The objectives of this chapter are threefold: First, it presents an overview of the existing ECG benchmarks used for designing ECG-based authentication systems. Second, it presents the literature of authentication systems that used fiducial and non-fiducial features. Third, it presents a methodology that uses both fiducial and non-fiducial features and several data mining classification techniques for individuals' authentication. Moreover, this chapter investigates the pertinent features using a large database of healthy and unhealthy subjects with different heart diseases.

Chapter "EEG Biometrics for Person Verification": The purpose of this chapter is to explore the idea of using EEG signals as a biometric modality to recognize individuals. Considered as a variant of Brain–Computer Interface (BCI), the concept presented in this chapter deals with a Multi-Channel EEG using Emotiv Epoc system. Mainly, a special interest will be addressed to EEG maps analysis for persons recognition. For this purpose, a generic schema is considered, namely, preprocessing, feature extraction, and matching/classification leading to a verification decision.

Chapter "Single Channel Surface EMG Based Biometrics": An emerging biometric method based on Surface EMG (SEMG) signals is considered. For this purpose, this chapter consists of two main parts. The first part reviews the SEMG signals in response to a force of fixed intensity from which frequencial parameters are extracted from the Power Spectral Density (PSD). The second part considers the M-wave signals muscle response following an electrical stimulation. M-wave signals are then characterized by extracting parameters using wavelet networks. The radial basis neural network (RBF) method is then used to classify these parameters.
Chapter "Wearable Multi-channel EMG Biometrics: Concepts": In this chapter, a case study using a specific wearable Multi-Channel EMG device will be considered. In particular, eight EMG channels will be used through Myo Armband system. The purpose is to deploy a verification biometric system using EMG signals corresponding to hand gestures. More specifically, the idea behind this concept is the capacity to generate a digital signature for each specific hand gesture.

Chapter "Towards High Density sEMG (HD-sEMG) Acquisition Approach for Biometrics Applications": This is the third chapter of this book dedicated to EMG biometrics modality. The purpose is to highlight a Multi-Channel technique based on a High-Density sEMG (HD-sEMG) acquisition. In fact, HD-sEMG recording systems can be used to overcome the limitations of classical bipolar and monopolar sEMG recording systems. Consequently, in the considered concept, HD-sEMG system generates 64 EMG signals from which an EMG image is constructed and processed. Thereupon, it will be explained how one can deploy this technique in a biometric scheme.

Chapter "Age Estimation Using Sound Stimulation as a Hidden Biometrics Approach": In this chapter, it will be introduced as a new hidden biometrics approach of age estimation requiring the stimulation of the auditory system by an acoustical modulated sine wave signal. After a quick review on different common approaches used in the field of age estimation, and after presenting some generalities on the auditory system, age estimation and age classification protocols will be considered. This chapter describes also the concept of a simple identification/verification, as an application.

Chapter "Multi-, Hyper-Spectral Biometrics Modalities": In this chapter, it will be introduced the different categories of multi-hyper-spectral imaging approaches for biometric modalities. Afterward, indirect approach will be considered, namely,

prerequisites concepts on physics and computer graphics, physical theory for the light–skin interaction models and finally, the related applications of multi-hyper-spectral imaging.

Chapter "Imaging for Hidden Biometrics": In this chapter, visible biometrics is highlighted though a classical review on face recognition, including some known approaches from the literature. Therefore, it will be evoked some multispectral approaches such as Near-Infrared (NIR) and Infrared (IR), and in the same context, deep hidden biometrics using X-ray imaging will be considered. Finally, a promising and safe MRI biometrics is described through some recent advances in brain biometrics, which is considered as a robust and safe modality. The purpose of using some hidden biometrics imaging techniques consists basically in preventing potential attacks.

Chapter "Retinal Image Processing in Biometrics": In this chapter, retinal image processing will be addressed as a Hidden Biometric modality. Considered as safe modalities, the retinal vascular network provides a unique pattern for each individual since it does not change throughout the life of the person. In addition, the retina offers a high level of recognition, which makes it suitable for high-security applications thanks to its universality, its invariability over time, and its difficulty to falsify.

Chapter "From Motion to Emotion Prediction: A Hidden Biometrics Approach": In this chapter, it will be discussed the capability of using motion recognition in order to predict the human emotion. Considered as a behavioral hidden biometrics approach, a specific system has been developed for this purpose wherein, several Machine Learning approaches are considered such as SVM, RF, MLP, and KNN for classification and SVR, RFR, MLPR, and KNNR for regression. The study highlights promising results in comparison to the state of the art.

Special thanks to the researchers who contributed to this book and to whom believe that hidden biometrics can be a promising solution of tomorrow.

Vitry sur Seine, France Prof. Amine Nait-ali

Contents