Chapter 26
Machine Learning for Biometrics

Albert Ali Salah
Centre for Mathematics and Computer Science (CWI), The Netherlands

ABSTRACT

Biometrics aims at reliable and robust identification of humans from their personal traits, mainly for security and authentication purposes, but also for identifying and tracking the users of smarter applications. Frequently considered modalities are fingerprint, face, iris, palmprint and voice, but there are many other possible biometrics, including gait, ear image, retina, DNA, and even behaviours. This chapter presents a survey of machine learning methods used for biometrics applications, and identifies relevant research issues. The author focuses on three areas of interest: offline methods for biometric template construction and recognition, information fusion methods for integrating multiple biometrics to obtain robust results, and methods for dealing with temporal information. By introducing exemplary and influential machine learning approaches in the context of specific biometrics applications, the author hopes to provide the reader with the means to create novel machine learning solutions to challenging biometrics problems.

INTRODUCTION

Biometrics serves the identification of humans from their personal traits. As a rapidly growing field, it is initially pushed forward by a need for robust security and surveillance applications, but its potential as a natural and effortless means of identification also paved the way for a host of smart applications that automatically identify the user and provide customized services. With increasing awareness of its psychological, privacy-related and ethical aspects, there is no doubt that biometrics will continue to contribute to many technological solutions of our daily lives.

DOI: 10.4018/978-1-60566-766-9.ch026

The technology of biometrics relies on the input from a number of fields, starting with various kinds of sensors that are used to sample the biometric. Signal processing and pattern recognition methods are obviously relevant, as the acquired data need to be prepared for accurate and robust decisions. At its final stage, the system outputs a decision, which links the acquired and processed biometric trait to an identity. Algorithms and mathematical models developed by the machine learning community are frequently used in biometric systems to implement the decision function itself, but this is surely not the only contribution worth mentioning. We will show in this chapter that machine learning methods are useful in selecting appropriate feature representations that will facilitate the job of the decision function, in dealing with temporal information, and in fusing multi-modal information.

The goal of this chapter is to familiarize the machine learning researcher with the problems of biometrics, to show which techniques are employed to solve them, and what challenges are open in the field that may benefit from future machine learning applications. It is also intended to familiarize the biometrics researcher to the methods and ways of machine learning and its correct research methodology, and to provide the rudiments of a toolbox of machine learning. In the next section, we provide a general look at biometric systems, define some relevant terminology and broadly identify the research issues. The third section deals with learning and matching biometric templates. Since this is a very broad topic, a small number of demonstrative application examples are selected. The fourth section is on the use of dynamic information for biometric purposes, and it is followed by a section on the fusion of multiple biometrics. Before concluding, we give a machine learning perspective on how to evaluate a biometrics system.

A GENERAL LOOK AT BIOMETRIC SYSTEMS

The application area of biometrics with the grandest scale is in *border control*, typically an airport scenario. Within the national identity context, it is possible to conceive the storing and managing of the biometric information for the entire population of a country. A smaller scale application is *access control*, for instance securing the entrance of a building (*physical access control*) or securing a digital system (*logical access control*). In both applications, we have a *verification* (or *authentication*) problem, where the user has an identity claim, and a sampled biometric is checked against a stored biometric for similarity. In a sense, this is a one-class pattern classification problem.

The second important problem involves *identification*, where there is no identity claim, and the sampled biometric is matched against many stored *templates*. Checking passengers against a list of criminals, forensic applications, identification of individuals at a distance, or providing access in consumer products (e.g. fingerprint scanning on a laptop) would be typical applications. Depending on the application requirements, the problem may be sufficiently constrained to apply a discriminative approach.

The most important biometric modalities are fingerprint, face, iris, signature, palm print and voice. The biometric traits differ in their usability, convenience, security, and complexity. For providing access to a high-security facility, security is of primary importance, whereas a household appliance that identifies users via biometrics would strive to have maximum user convenience. Similarly, privacy can be a major determinant in the deployment of a particular biometric application. For this reason, a host of possible biometrics are considered for different applications, including DNA, gait, ear images, and even behaviours.