Chapter 3

Biometric Image Processing

ABSTRACT

In most biometric-based security systems, images of the associated biometric identifiers are used as the input to that system. This chapter discusses various image processing methods and algorithms commonly used for biometric pattern recognition. Efficient and reliable processing of images is essential to achieve good performance of biometric systems. Different appearance-based methods, such as eigenimage and fisherimage, and topological feature-based methods, such as Voronoi diagram-based recognition, are discussed in the context of face, ear, and fingerprint application frameworks. Utilizing cognitive intelligence and adaptive learning methods in both physical and behavioral biometrics are some emerging new directions of biometric pattern recognition. As such, neural networks, fuzzy logic, and cognitive architectures would play a more important role in biometric domain of research. The chapter concludes with discussion of the importance of context-based recognition for behavioral biometrics.

1. INTRODUCTION

In the previous chapter, an overview of biometric systems has been presented. For decades, many government and public establishments have used biometric authentication for access control. Today, the primary application of biometrics is shifting from the physical security, where the access to the specific locations is usually monitored using standard security identification mechanisms such as ID or token-based mechanisms in combination with fingerprint biometric, to remote security where the methods of crowd monitoring using video surveillance take advantage of gait biometric, for example. The popularity of such approaches has increased dramatically as the new technological devices are coming on the market every week, capability to process massive amount of data is doubling every few months, and the biometric algorithm development by the leading IT companies and the universities research centres is tripled in the last years.

DOI: 10.4018/978-1-4666-3646-0.ch003
As the demand for the development of more precise and reliable ways of person identification is ever pressing, the combination of biometrics and pattern analysis methods is gaining popularity as it undoubtedly increases the accuracy of the results and thus the level of security protection. Driven by the above motivations, the rest of this chapter is devoted to two main directions in intelligent biometric data processing. The first group of methods are appearance-based approaches, well known in biometric domain (Jain, Flynn, & Ross, 2007). The second group of methods are topology-based information driven methods (Yanushkevich, Gavrilova, Wang, & Srihari, 2007), with emphasis given to extracting metadata from biometric samples in order to simplify processing, reduce storage and increase accuracy, thus making approach to biometric processing more efficient and more intelligent.

2. APPEARANCE-BASED IMAGE PROCESSING IN BIOMETRICS

From the gamut of research on biometric authentication, we observe that the overwhelming part of biometric data processing is realized by using image processing and pattern recognition methods and algorithms (Soledek, Shmerko, Phillips, Kukharevl, Rogers, & Yanushkevich, 1997). As the mainstream direction of biometric image processing, appearance-based methods extract biometric features from the row image by analyzing appearance of the whole image as an entity or a vector in a high-dimensional image space. Such factors as color scheme, orientation, background, luminance, saturation are being analyzed and processed either pixel by pixel or through projection on subspaces, such as in Principal Component Analysis (PCA) methods. As the most evident examples, we consider face, iris and ear biometrics in this context (Soledek, Shmerko, Phillips, Kukharevl, Rogers, & Yanushkevich, 1997).

To solve the biometric data processing problems, the following main methods are typically employed in literature: digitization, compression, enhancement, segmentation, feature measurement, image representation, image models, design methodology. They are summarized in Figure 1. While some of these methods are used during data pre-processing, and some during pattern recognition and matching, there is high potential of employing more intelligent techniques at all stages, with the goal of optimizing processing and increasing overall security system performance. Some of these approaches are overviewed in the subsequent sections devoted to individual biometrics.

2.1. Image Processing for Face Recognition

The face matcher in a security biometric system is usually used for face recognition. Its’ main goal is to identify recognizable facial characteristics from images, to reduce the key features to digital codes, and to match them against known facial templates. The inputs to the matcher are the input image and the face images from a facial image database, and the output is a single matched face or a ranked list with the top-n matches, i.e. first n recognized match faces. The output is enough on its own to make a decision to grant or not access to a given resource or secure asset, and also is suitable for further fusion as part of rank-level multi-modal biometric system. This procedure will be described in details in chapter on Rank-Level Multimodal Biometric System Architecture.

In order to recognize faces, first features from the face images have to be extracted and selected to represent the properties of the data in the most effective way for future match computation in the feature space. The goal is to extract most important features to differentiate or separate individuals in the biometric facial space. The distance between such features is further computed using selected