Chapter 1
Biometrics at a Distance: Issues, Challenges, and Prospects

Stan Z. Li, Ben Schouten, and Massimo Tistarelli

Abstract The notion of remote biometrics or biometrics at a distance is today of paramount importance to provide a secure mean for user-friendly identification and surveillance.

In 2007 the BioSecure Network of Excellence published the Biometric Research Agenda (Schouten et al. BioSecure: white paper for research in biometrics beyond BioSecure. CWI report 2008). This network identified, as one of the most urgent topics, research in distributed (intelligent) sensor networks and the transparent use of biometrics, requiring no actions from the end-user in supervised or unsupervised ways. These citizens, sometimes in ways that are yet to be understood.

This chapter introduces the most relevant issues and challenges of biometric sensing and recognition at a distance. Most of these issues are more be deeply analyzed in the subsequent chapters of this book.

Several categorizations of biometric sensing and applications are provided including face recognition and novel biometric sensors for building intelligent environments. Several factors affecting the performances of biometric systems are identified and discussed in some detail. Some typical applications and prospects are illustrated together with their impact in today’s and tomorrow’s society and citizens.

1.1 Introduction

Biometrics, as a mean for automatic and reliable identify recognition, plays an important role in surveillance and security, such as in access control, e-passport, and watch-list surveillance. Recent years has seen significant increase in biometric recognition applications, partly due to recent technology advances, and partly due to increased demands for security and human cost-saving reasons.

Biometric recognition systems automatically verify or identify person identity present in the input images and videos using human biometric traits. Human
biometric traits which can be used for biometric recognition include face, iris, fingerprint, palmprint, and others. The primary biometric trait for biometrics at a distance is the face because the face is most accessible and natural biometric trait for recognition at a distance. Other useful traits are iris and gait. Multimodal biometrics fuse several biometric modules to reach more reliable recognition result.

Biometric recognition is done by extracting a biometric template in query from the input device against those of target enrolled in the database. The comparison of a query against the target is performed in one of the two modes: (1) verification (or authentication) and (2) identification (or recognition). Verification is one-to-one in that the query face is compared against the claimant’s face images to verify the claimed ID. This is the case of boarder control with e-passport where the ID is claimed by the claimant. Identification is one-to-many in that the query is compared against those enrolled in the database to determine the identity of the query. Another one-to-many scenario is watch-list surveillance, where only the found matches that are confident enough (above a preset threshold) should be shown to the system operator.

Most commercial face recognition products and solutions are developed for cooperative user applications, including access control, e-passport, and national registration where a user is required to cooperate with the camera to have his/her face image captured properly, in order to be granted for the access. Less restrictive scenarios are non-cooperative user applications, such as face recognition under surveillance where person identification is done without user’s intentional, cooperative effort. Pilot deployments of face recognition are also under way, such as watch-list face surveillance in subways.

Homogeneity referred to the similarity between properties of input face images and those of enrollment face images. It can be homogeneous, where both input face and enrollment face are from the same type of imaging device (e.g., camera, photo scanner) in a similar environment (e.g., lighting). On the other hand, it is heterogeneous where the input face and the enrollment face are from different imaging devices (e.g., image from system’s camera vs. photo scan).

Biometric applications are categorized in terms of several key factors. Challenges in face recognition will be discussed and advanced technology will be described. Solutions for reliable face recognition will be provided for typical applications such as access control, e-passport, large face database search, and watch-list surveillance.

Table 1.1 provides a categorization of biometrics with respect to type of comparison, user cooperation, and homogeneity of input and enrollment face images. From the technical viewpoint, the easiest is one-to-one face verification such as

<table>
<thead>
<tr>
<th>Application</th>
<th>Comparison</th>
<th>User cooperation</th>
<th>Enrollment image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>1:1 or 1:N</td>
<td>Coop</td>
<td>Photo, video</td>
</tr>
<tr>
<td>E-passport</td>
<td>1:1</td>
<td>Coop</td>
<td>Photo</td>
</tr>
<tr>
<td>Large database search</td>
<td>1:1 or 1:N</td>
<td>Coop, Non-coop</td>
<td>Photo, video</td>
</tr>
<tr>
<td>Watch-list surveillance</td>
<td>1:N</td>
<td>Non-coop</td>
<td>Photo, video</td>
</tr>
</tbody>
</table>