Chapter 5

3D Face Recognition Using Spatial Relations

Stefano Berretti
University of Florence, Italy

Alberto del Bimbo
University of Florence, Italy

Pietro Pala
University of Florence, Italy

ABSTRACT

Identity recognition using 3D scans of the face has been recently proposed as an alternative or complementary solution to conventional 2D face recognition approaches based on still images or videos. In fact, face representations based on 3D data are expected to be more robust to pose changes and illumination variations than 2D images, thus allowing accurate face recognition in real-world applications with unconstrained acquisition. Based on these premises, in this chapter, the authors first introduce the general and main methodologies for 3D face recognition, shortly reviewing the related literature by distinguishing between global and local approaches. Then, the authors present and discuss two 3D face recognition approaches that are robust to facial expression variations and share the common idea of accounting for the spatial relations between local facial features. In the first approach, the face is partitioned into iso-geodesic stripes and spatial relations are computed by integral measures that capture the relative displacement between the sets of 3D points in each pair of stripes. In the second solution, the face is described by detecting keypoints in the depth map of the face and locally describing them. Then, facial curves on the surface are considered between each pair of keypoints, so as to capture the shape of the face along the curve as well as the relational information between keypoints. Future research directions and conclusions are drawn at the end of the chapter.

DOI: 10.4018/978-1-4666-5966-7.ch005
INTRODUCTION

Human target recognition has been an active research area in recent years, with several biometric techniques developed for measuring unique physical and behavioral characteristics of human subjects for the purpose of recognizing their identity. In particular, two different modalities are considered to recognize the identity of a person: verification (authentication) and identification (recognition). Verification (“Am I who I claim I am?”) involves confirming or denying a person’s claimed identity. Instead, identification (“Who am I?”) requires the system to recognize a person from a list of users in the template database. Due to this, identification is a more challenging problem because it involves one-to-many matching compared to the one-to-one matching required for verification. The idea of automatically recognizing or authenticating users’ identity is based on the possibility to extract unique physical features from the anatomical traits that univocally characterize each individual. The features that are most used for this goal can be summarized as follows:

- **Fingerprints and hand geometry**: The most common biometric authentication solution. Provides high accuracy, it is easy to implement (though contact with the sensor is required), showing a low cost. Can be also performed via the Internet (BioWeb);
- **Voice recognition**: Relies on the voice pattern to authenticate individuals, thus resulting very user friendly. However, changing the voice due to sinus congestion, cold or anxiety can produce false negatives results;
- **Eye scans**: Retinal and iris scans are used for authentication. They provide accuracy where physical contact to the scanner is required. The user must focus in particular point of the scanner and hold this position. Low-intensity light might affect the results;
- **Facial recognition**: Looks for the different parts of the face such as the location and shape of the eyes and the nose, cheekbones and the side of the mouth;
- **Signature dynamics and typing patterns**: Looks for patterns in writing pressures at different points in the signature, and the writing speed;
- **Heartbeat biometric authentication**: Identifies the individually unique information of the subject heartbeats;
- **Infrared hand vein pattern biometric**: Uses the shape of the finger vein and infrared is used to make the skin tissue transparent, and highly visible to recognize the veins in the finger.

Depending on the particular application, one or a combination of the diverse biometric modalities listed above can be more appropriate. This is evidenced by the different diffusion and impact that different biometric technologies have on the global market, where fingerprints is the most largely used biometric technique, mainly because of its very high accuracy and simplicity, with face recognition following in third position (2010 data). While biometric technologies are being widely used in forensics for criminal identification, recent advancements in biometric sensors and matching algorithms have led to the deployment of biometric authentication in a large number of civilian and government applications, such as physical access control, computer log-in, welfare disbursement, international border crossing and national ID cards, and so on.

Among the biometric techniques listed above, identity recognition based on facial traits is widely used for its social acceptance, applicability in a range of different contexts and the good balance between risks and benefits associated to its implementation. In fact, face recognition has its main prerogative in not requiring contact or