Chapter 7
Analysis of Face Space for Recognition using Interval-Valued Subspace Technique

C.J. Prabhakar
Kuvempu University, India

ABSTRACT

The major contribution of the research work presented in this chapter is the development of effective face recognition algorithm using analysis of face space in the interval-valued subspace. The analysis of face images is used for various purposes such as facial expression classification, gender determination, age estimation, emotion assessment, face recognition, et cetera. The research community of face image analysis has developed many techniques for face recognition; one of the successful techniques is based on subspace analysis. In the first part of the chapter, the authors present discussion of earliest face recognition techniques, which are considered as mile stones in the roadmap of subspace based face recognition techniques. The second part presents one of the efficient interval-valued subspace techniques, namely, symbolic Kernel Fisher Discriminant analysis (Symbolic KFD), in which the interval type features are extracted in contrast to classical subspace based techniques where single valued features are used for face representation and recognition.

INTRODUCTION

Biometric access control is a set of automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, such as fingerprints or facial features, or some aspects of the person's behavior, like his/her handwriting style or keystroke patterns. Biometric access controls have emerged as the most promising technology for recognizing individuals in recent years. Since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, these methods examine an individual's physiological and/or behavioral characteristics in order to determine and/or ascertain his identity. Since biometric systems identify a person by bio-

DOI: 10.4018/978-1-61350-429-1.ch007

logical characteristics, they are difficult to forge. Among the various biometric ID methods, the physiological methods (fingerprint, face, DNA) are more stable than the methods in behavioral category (keystroke, voice print). The reason is that physiological features are often non-alterable except by severe injury. The behavioral patterns, on the other hand, may fluctuate due to stress, fatigue, or illness. However, behavioral IDs have the advantage of being non intrusive. Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness.

Iris and retina identification require expensive equipment and are much too sensitive to any body motion. Voice recognition is susceptible to background noises in public places and auditory fluctuations on a phone line or tape recording. Signatures can be modified or forged. However, facial images can be easily obtained with a couple of inexpensive fixed cameras. Good face recognition algorithms and appropriate preprocessing of the images can compensate for noise and slight variations in orientation, scale and illumination. Finally, technologies that require multiple individuals to use the same equipment to capture their biological characteristics potentially expose the user to the transmission of germs and impurities from other users. However, face recognition is totally non-intrusive and does not carry any such health risks. For this reason, since the early 70's, face recognition has drawn the attention of researchers in fields from security, psychology, and image processing, to computer vision. Face recognition is used for two primary tasks:

1. Verification (one-to-one matching): When presented with a face image of an unknown individual along with a claim of identity, ascertaining whether the individual is who he/she claims to be.
2. Identification (one-to-many matching): Given an image of an unknown individual, determining that person's identity by comparing (possibly after encoding) that image with a database of (possibly encoded) images of known individuals.

CHALLENGES IN FACE RECOGNITION

Although great deal of effort has been devoted to 2D intensity image based face recognition task, it still remains a challenging problem in a general setting. Successful 2D face recognition systems have been deployed only under constrained situations (Zhao et al., 2003). There are numerous factors that cause the appearance of the face to vary. The sources of variation in the facial appearance can be categorized into two groups: intrinsic factors and extrinsic ones. Intrinsic factors are based on physical nature of the face and are independent of the observer. Some examples are age, facial expression, facial hair, glasses, cosmetics, etc. Intrinsic factors are also responsible for the differences in the facial appearance of different people, some examples being ethnicity and gender. Extrinsic factors cause the appearance of the face to alter via the interaction of light with the face and the observer. These factors include illumination, pose, scale and imaging parameters (e.g., resolution, focus, imaging, noise, etc.).

APPLICATIONS OF FACE RECOGNITION

There are numerous application areas in which face recognition can be exploited, a few of which are outlined below:

1. Security (access control to buildings, airports/seaports, ATM machines and border checkpoints; computer/network secu-