Chapter 78

Thermal Human Face Recognition for Biometric Security System

Ayan Seal  
Jadavpur University, India

Debotosh Bhattacharjee  
Jadavpur University, India

Mita Nasipuri  
Jadavpur University, India

Dipak Kumar Basu  
Jadavpur University, India

ABSTRACT

Automatic face recognition has been comprehensively studied for more than four decades, since face recognition of individuals has many applications, particularly in human-machine interaction and security. Although face recognition systems have achieved a significant level of maturity with some realistic achievement, face recognition still remains a challenging problem due to large variation in face images. Face recognition techniques can be generally divided into three categories based on the face image acquisition methodology: methods that work on intensity images, those that deal with video sequences, and those that require other sensory (like 3D sensory or infra-red imagery) data. Researchers are using thermal infrared images for face recognition. Since thermal infrared images have some advantages over 2D images. In this chapter, an overview of some of the well-known techniques of face recognition using thermal infrared faces are discussed, and some of the drawbacks and benefits of each of these methods mentioned therein are discussed. This chapter talks about some of the most recent algorithms developed for this purpose, and tries to give a brief idea of the state of the art of face recognition technology. The authors propose one approach for evaluating the performance of face recognition algorithms using thermal infrared images. They also note the results of several classifiers on a benchmark dataset (Terravic Facial Infrared Database).

DOI: 10.4018/978-1-5225-5204-8.ch078
INTRODUCTION

In this modern world, people are worried about the necessity of security, related to the various applications they used in their usual life, from ATMs to attendance maintenance systems. A user-friendly but strongly secured environment is required ubiquitously to protect our privacy and identity without being tampered by any unauthorized means. The traditional security systems generally use password or Personal Identification Number (PIN) and magnetic cards that necessitate the memorization of data to access the system and also bear some drawbacks. It is hard to remember password or PIN and can be stolen or guessed by the intruder; cards, tokens, keys can be lost, forgotten, stolen or duplicated and magnetic cards can be corrupted and unreadable by the card reader device. To overcome these difficulties automated biometric recognition systems can be used as a suitable alternative, which was introduced in earlier centuries. The word ‘Biometric’ is derived from the ancient Greek words “bios” meaning life and “metron” meaning measure (Toth, 2005; Jain et al., 2007). So, the meaning is “life measurement.” Biometric systems use various physical characteristics or behaviors of a person, which is shown in Figure 1 and can be categorized as the name of the part(s) of body involved. Computer vision is one such field with which the visual recognition ability of a person can be achieved in face recognition system, which is comparable to that human by measuring some unique biometric properties or characteristics of a human. The journey was begun with the fingerprint, now several different types of modalities (face, iris, retina, etc) are available for human identification and verification.

Physical feature is suitable for identity purpose and generally obtained from living human body. Commonly used physical features are fingerprints, facial features, hand geometry, and eye features (iris)

Figure 1. Biometric types