Chapter 12
A Novel Biometric Image Enhancement Approach With the Hybridization of Undecimated Wavelet Transform and Deep Autoencoder

Sasirekha K.
Periyar University, India

Thangavel K.
Periyar University, India

ABSTRACT

For a long time, image enhancement techniques have been widely used to improve the image quality in many image processing applications. Recently, deep learning models have been applied to image enhancement problems with great success. In the domain of biometric, fingerprint and face play a vital role to authenticate a person in the right way. Hence, the enhancement of these images significantly improves the recognition rate. In this chapter, undecimated wavelet transform (UDWT) and deep autoencoder are hydridized to enhance the quality of images. Initially, the images are decomposed with Daubechies wavelet filter. Then, deep autoencoder is trained to minimize the error between reconstructed and actual input. The experiments have been conducted on real-time fingerprint and face images collected from 150 subjects, each with 10 orientations. The signal to noise ratio (SNR), peak signal to noise ratio (PSNR), mean square error (MSE), and root mean square error (RMSE) have been computed and compared. It was observed that the proposed model produced a biometric image with high quality.

DOI: 10.4018/978-1-5225-9611-0.ch012

INTRODUCTION

As our society has become electronically connected and more portable, surrogate representations of identity such as passwords and tokens cannot be trusted to recognize a person. Besides, the token may be lost or stolen and passwords can be guessed easily. Recent researches were evident that the biometric methods provide a more elevated amount of security and are more appropriate than the conventional methods of personal authentication (Jain, Ross, & Nandakumar, 2011) (Sasirekha & Thangavel, 2014). With the rapid technological advancements in the field of biometric authentication, it has been widely exploited for various security purposes. In particular, biometric authentication supports the facet of identification, verification, and non-repudiation in the domain of information security. It is used to identify the identity of a person when compared to a template in the database by certain unique characteristics (Chauhana, Arorab, A.S., & Kaula, 2010).

Furthermore, biometrics recognition is a growing and controversial field in which civil liberties groups express concern over privacy and identity issues. In the recent years, biometric laws and regulations are in process and biometric industry standards are being tested widely.

The biometric traits are broadly classified into two categories: physiological and behavioral. Recently, most of the applications are developed with the avail of physiological traits such as fingerprint, face, hand geometry, iris, retina, etc. On the other hand, the behavioral traits such as voice, dynamic signature, keystroke, gait, etc. are used but paid poor attention. In general, a person can be identified by any of the available biometric traits. The biometric modals possess some of the desirable properties which include universality, uniqueness, permanence, measurability, performance, and acceptability which propels the growth of biometric-based authentication (Jain, Ross, & Prabhakar, 2004).

Among all the biometric traits, the fingerprint and face biometric are the widely employed and cost-efficient method of authentication (Khan & Zhang, 2008) (W. Yu, 2009) (Wu, Lian, & Lu, 2012).

Fingerprint biometric has been used in Forensic Science for a long time for personal identification. This is because the fingerprints of an individual are distinctive and do not change for the duration of one's life. This makes it an ideal signature of a person. In the current scenario, the face is the next widely focused biometric after fingerprint as it plays a vital role to authenticate a right person. The face recognition is employed for identifying an individual by authenticating the input image with the digital images which are already stored in the database.

Generally, a good database of sample patterns is very much crucial for any pattern recognition or classification problem. Hence, image acquisition is the first step in any biometric authentication system. It is concerned with capturing the biometric image using a camera or scanner. In this paper, the fingerprint images are collected using eSSL ZK7500 fingerprint sensor. This device utilizes optical fingerprint scanning technology for superior quality and reliability. And the biometric face images are collected using 2 Mega Pixel Logitech web camera. The images are captured with the resolution of 1280x960. The captured biometric images are poor in quality during acquisition due to illumination, sensor, storage, and many more. It is highly difficult to fetch objects from the dark background of a low contrast biometric image.

In the digital era, biometric image enhancement has become increasingly important for the successful authentication of a person. Specifically, it improves the quality of images for further analysis. In general, image enhancement is the method to improve the visibility of higher and lower frequency values of an image. The objective is to enhance the visual representation of the image or to provide an improved