Chapter 5
Low Level Multispectral Palmprint Image Fusion for Large Scale Biometrics Authentication

Dakshina Ranjan Kisku
Asansol Engineering College, India

Phalguni Gupta
Indian Institute of Technology Kanpur, India

Jamuna Kanta Sing
Jadavpur University, India

Massimo Tistarelli
University of Sassari, Italy

C. Jinsong Hwang
Texas State University, USA

ABSTRACT

Continuous biometric authentication is a process where the installed biometric systems continuously monitor and authenticate the users. Biometric system could be an exciting application to log in to computers and in a network system. However, due to malfunctioning in high-security zones, it is necessary to prevent those loopholes that often occur in security zones. It has been seen that when a user is logged in to such systems by authenticating to the biometric system installed, he/she often takes short breaks. In the meantime some imposter may attack the network or access to the computer system until the real user is logged out. Therefore, it is necessary to monitor the log in process of the system or network by continuous authentication of users. To accomplish this work we propose in this chapter a continuous biometric authentication system using low level fusion of multispectral palm images where the fusion

DOI: 10.4018/978-1-61350-129-0.ch005

is performed using wavelet transformation and decomposition. Fusion of palmprint instances is performed by wavelet transform and decomposition. To capture the palm characteristics, a fused image is convolved with Gabor wavelet transform. The Gabor wavelet feature representation reflects very high dimensional space. To reduce the high dimensionality, ant colony optimization algorithm is applied to select relevant, distinctive, and reduced feature set from Gabor responses. Finally, the reduced set of features is trained with support vector machines and accomplishes user recognition tasks. For evaluation, CASIA multispectral palmprint database is used. The experimental results reveal that the system is found to be robust and encouraging while variations of classifiers are used. Also a comparative study of the proposed system with a well-known method is presented.

INTRODUCTION

Computer and network systems which are placed in high security zones often need user interaction and authentication even in the case of log in multiple times to the systems. Knowledge-based and token-based systems are mostly available authentication systems which use passwords, PIN and smart cards information. However, as we are well aware, passwords and PIN can be shared, stolen and lost. The users often prefer to use loosely built passwords. Since the complex passwords are found to be difficult to remember. In case of smart cards information can be stolen, shared or lost. The main disadvantage of using the computer or network system is that it can authenticate people only at the initial phase of log-in process and the user is not re-authenticated until logging out of the system. This can exploit critical security threats when the user goes out for a short time during logged-in session. To overcome this problem continuous authentication can be a reliable process through which any system can be almost secured from attacking of imposters. A large number of systems have been studied on continuous biometric authentications in (Monrose & Rubin, 2000; Altinok & Turk, 2003; Sim, et. al., 2007; Azzini, et. al., 2008; Azzini & Marrara, 2008; Kang & Ju, 2006; Carrillo, 2003; Klosterman & Ganger, 2000). These systems use one or more biometric traits (e.g., fingerprint or face) for continuous authentication of users. However, like other conventional biometric traits multispectral palm images can be used for continuous authentication while multispectral images are fused to obtain a common authentication perspective.

There exists a large number of computational approaches in intra-modal fusion (Wong, et. al., 2007; Ross, et. al., 2006) at different levels of human recognition. However, both mono-modal biometric and intra-modal biometric systems face some challenges, such as lack of accurate image registration methods, template matching with loss of complementary information, association of redundant adaptive parameters (Ross, et. al., 2006). These factors explain the poor performance of the system. Intra-modal biometric image fusion can remove some of the limitations of uni-biometric systems (Jain, et. al., 2007) because the uni-modal biometric system usually compensates the inherent limitations of the secondary sources. Intra-modal systems have the following advantages (Sun, et. al., 2008; Hao, et. al., 2007) over uni-modal biometric systems.

- Combining the evidence obtained in different form from the same or different sources using an effective fusion scheme can significantly improve the overall accuracy of the biometric system.
- Intra-modal biometric can address the problem of non-universality which often occurs in uni-modal system.