Multimodal Biometric Person Authentication Using Fingerprint, Face Features

Tran Binh Long[1], Le Hoang Thai[2], and Tran Hanh[1]

[1] Department of Computer Science, University of Lac Hong 10 Huynh Van Nghe, DongNai 71000, Viet Nam
tblong@lhu.edu.vn
[2] Department of Computer Science, Ho Chi Minh City University of Science 227 Nguyen Van Cu, HoChiMinh 70000, Viet Nam
lhthai@fit.hcmus.edu.vn

Abstract. In this paper, the authors present a multimodal biometric system using face and fingerprint features with the incorporation of Zernike Moment (ZM) and Radial Basis Function (RBF) Neural Network for personal authentication. It has been proven that face authentication is fast but not reliable while fingerprint authentication is reliable but inefficient in database retrieval. With regard to this fact, our proposed system has been developed in such a way that it can overcome the limitations of those uni-modal biometric systems and can tolerate local variations in the face or fingerprint image of an individual. The experimental results demonstrate that our proposed method can assure a higher level of forge resistance in comparison to that of the systems with single biometric traits.

Keywords: Biometrics, Personal Authentication, Fingerprint, Face, Zernike Moment, Radial Basis Function.

1 Introduction

Biometrics refers to automatic identification of a person based on his physiological or behavioral characteristics [1],[2]. Thus, it is inherently more reliable and more capable in differentiating between an authorized person and a fraudulent imposter [3]. Biometric-based personal authentication systems have gained intensive research interest for the fact that compared to the traditional systems using passwords, pin numbers, key cards and smart cards [4] they are considered more secure and convenient since they can't be borrowed, stolen or even forgotten. Currently, there are different biometric techniques that are either widely-used or under development, including face, facial thermo-grams, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, and voice-print (figure.1) [3], [5]. Each of these biometric techniques has its own advantages and disadvantages and hence is admissible, depending on the application domain. However, a proper biometric system to be used in a particular application should possess the following distinguishing traits: uniqueness, stability, collectability, performance, acceptability and forge resistance [6].

P. Anthony, M. Ishizuka, and D. Lukose (Eds.): PRICAI 2012, LNAI 7458, pp. 613–624, 2012.

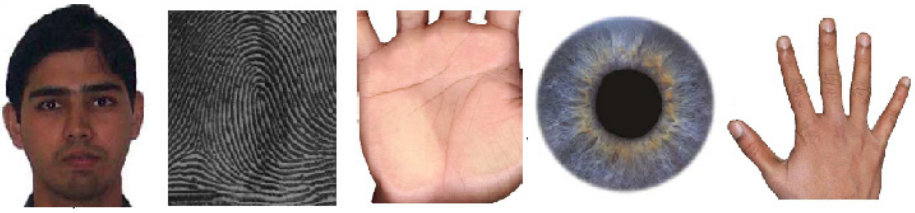

Fig. 1. Examples of biometric characteristic

Most biometric systems that are currently in use employ a single biometric trait; such systems are called uni-biometric systems. Despite their considerable advances in recent years, there are still challenges that negatively influence their resulting performance, such as noisy data, restricted degree of freedom, intra-class variability, non-universality, spoof attack and unacceptable error rates. Some of these restrictions can be lifted by multi-biometric systems [7] which utilize more than one physiological or behavioral characteristic for enrollment and verification/ identification, such as different sensors, multiple samples of the same biometrics, different feature representations, or multi-modalities. These systems can remove some of the drawbacks of the uni-biometric systems by grouping the multiple sources of information [8]. In this paper, multi-modalities are focused.

Multimodal biometrics systems are gaining acceptance among designers and practitioners due to (i) their performance superiority over uni-modal systems, and (ii) the admissible and satisfactory improvement of their system speed. Hence, it is hypothesized that our employment of multiple modalities (face and fingerprint) can conquer the limitations of the single modality- based techniques. Under some hypotheses, the combination scheme has proven to be superior in terms of accuracy; nevertheless, practically some precautions need to be taken as Ross and Jain [7] put that Multimodal Biometrics has various levels of fusion, namely sensor level, feature level, matching score level and decision level, among which [8] fusion at the feature level is usually difficult. One of the reasons for it is that different biometrics, especially in the multi-modality case, would have different feature representations and different similarity measures. In this paper, we proposed a method using face and fingerprint traits with feature level fusion. Our work aims at investigating how to combine the features extracted from different modalities, and constructing templates from the combined features. To achieve these aims, Zernike Moment (ZM)[9] was used to extract both face and fingerprint features. First, the basis functions of Zernike moment (ZM) were defined on a unit circle. Namely, the moment was computed in a circular domain. This moment is widely-used because its magnitudes are invariant to image rotation, scaling and noise, thus making the feature level fusion of face and fingerprints possible. Then, the authentication was carried out by Radial Basis Function (RBF) network, based on the fused features.

The remainder of the paper is organized as follows: section 2 describes the methodology; section 3 reports and discusses the experimental results, and section 4 presents the conclusion.