Chapter 22
A Robust Biometrics System Using Finger Knuckle Print

Ravinder Kumar
HMR Institute of Technology and Management, India

ABSTRACT

Among various biometric indicators, hand-based biometrics has been widely used and deployed for last two decades. Hand-based biometrics are very popular because of their higher acceptance among the population because of their ease of use, high performance, less expensive, etc. This chapter presents a new hand-based biometric known as finger-knuckle-print (FKP) for a person authentication system. FKP are the images obtained from the one's fingers phalangeal joints and are characterized by internal skin pattern. Like other biometrics discrimination ability, FKP also has the capability of high discrimination. The proposed system consists of four modules: image acquisition, extraction of ROI, selection and extraction of features, and their matching. New features based on information theory are proposed for matching. The performance of the proposed system is evaluated using experiment performed on a database of 7920 images from 660 different fingers. The efficacy of the proposed system is evaluated in terms of matching rate and compromising results are obtained.

INTRODUCTION

Biometrics deals with the automated system for authentication and authorization of individuals based on the characteristics possessed by him or her. Various biometrics modalities proposed in the latest research literature are: fingerprints (Maltoni et al., 2009; Kumar et al., 2012a, 2012b, 2012c; Kumar et al., 2013a, 2013b, 2013c; Kumar et al., 2014a, 2014b; Kumar et al., 2016; Jain et al., 2004), face (Jain & Li, 2011; Alling et al., 2016), retinal scan (Seto, 2015), hand geometry (Kumar et al., 2017), speech (Rabiner & Juang, 1993), iris (Huang et al., 2002), hand vein (Kumar & Prathyusha, 2009), and voiceprint (Wang et al., 2004) etc. With the advancement of technology, biometric-based personal verification and identification solutions have become the necessity of our highly secured networked society. The need for a secure biometric authentication system for individual identification and authentication is becoming apparent as the fraud and security breaches increases.

DOI: 10.4018/978-1-5225-4100-4.ch022

To provide the security and privacy of electronic and financial transactions, personal data and to restrict access, biometric-based security solutions are highly desirable. The need for such biometrics had been observed in almost all domains like governments, military, and other commercial applications. The recent advancements of biometrics technologies had also contributed to the other domains of the society such as organizational secure network infrastructures, enforcement of law and order, online transactions, access to health and social services, government identification services (Like Aadhar in India).

The latest research combines fingerprints with other biometrics indicators in order to have better results and to enhance acceptability among the large population. Various biometrics fusions can be performed like fingerprint and face, lip movement and voice, speech and face, hand geometry and fingerprint, fingerprint speech and face, fingerprint and palm print, fingerprint, palm print and hand geometry to get multimodal biometrics with improved matching performance. This fusion of multibiometric traits can happen at various levels like image level, features level, rank level, and decision level etc.

As our society is becoming more and more mobile and electronically connected the traditional systems of passwords (for access control over e-resources) and ID cards (used in commercial and financial transactions) no longer remain reliable for access to the highly restricted systems. Therefore, breaches of the security in such systems become very easy as cards may be lost or stolen, PIN or password can be guessed by an impostor. Further, complex passwords are difficult to be remembered or recall by the legitimate users and very simple passwords can easily be guessed by an impostor. The problem of recognition of a person or providing access to the security infrastructure had been addressed by the emergence of biometrics-based authentication system over the verification methods.

Biometrics is the Greek term, where bios means life and metron means measurement is the tool used for automatic authentication of a person using the physiological and behavioral properties possess by a person (see Figure 1). By using biometrics, it becomes easy to associate an identity to an individual by asking question like "who you are," not by "what you possess" (e.g. Physical Identity card) or "what you remember" (e.g. code or password). Currently deployed biometric authentication systems are based on face, retina, fingerprints, iris, facial thermograms, hand geometry, palm print, gait, signature, and voiceprint to establish an identity with an individual. In unimodal biometrics systems, various biometrics indicators in alone are used, whereas in multimodal biometrics system two or more biometrics indicators are fused together at different level like: at feature extraction level, at score computation level or at rank or matching level to increase the performance. Biometric systems may also have certain limitations, but these can be overlooked while comparing with traditional method of secure access. Besides empowering the security, user convenience, the need of design and remembering passwords are also alleviated by the used of biometrics systems. Biometrics systems are also deployed for negative authentication in which it determines whether this is the person, who he or she denies to be.

Biometric systems operate in two modes i.e. verification (one to one matching) mode and identification (one to many matching) mode. In identification mode, the identity of an individual is established, whereas in verification mode, the user is identified against the identity claimed by him or her. The applications of biometrics systems are uncountable where access control or security is desired e.g. ATMs, computer logins, driver's licenses, airport kiosks, grocery stores etc. The large number of biometrics applications or uses did not implied that it is a fully solved and researched problem, still the scope of improvement of design of new devices or biometrics indicators are always there.

A biometric authentication system can be described as a pattern recognition system which, consists of sensors to capture biometrics data, feature extractor module to extract features from captured data, template generation module to represent extracted features, and recognition module which match the