Chapter 66
Search Space Reduction in Biometric Databases: A Review

Ilaiah Kavati
IDRBT, India & UOH, India

Munaga V. N. K. Prasad
IDRBT, India

Chakravarthy Bhagvati
University of Hyderabad, India

ABSTRACT

Deployment of biometrics for personal recognition in various real time applications lead to large scale databases. Identification of an individual on such large biometric databases using a one-one matching (i.e., exhaustive search) increases the response time of the system. Reducing the search space during identification increases the search speed and reduces the response time of the system. This chapter presents a comprehensive review of the current developments of the search space reduction techniques in biometric databases. Search space reduction techniques for the fingerprint databases are categorized into classification and indexing approaches. For the palmprint, the current search space reduction techniques are classified as hierarchical matching, classification and indexing approaches. Likewise, the iris indexing approaches are classified as texture based and color based techniques.

INTRODUCTION

Nowadays, automatic personal recognition is critical in a variety of security applications including government, commercial, educational institutions, industries, public places (such as ports, airports and shopping complexes), etc. Questions such as “Is this the person who he claims to be?”, “Should this individual authorized to perform this transaction?”, “Does this employee have authorization to access this service?”, etc. are asked millions of time every day by thousands of organizations in both private and public sectors (Jain, Flynn, & Ross, 2007).

DOI: 10.4018/978-1-5225-5204-8.ch066
Traditionally, the security systems employ either token based (e.g., Identity cards) or knowledge based (e.g., Passwords) techniques for personal recognition (Figure 1(a)). However, these traditional systems no longer suffice to personal recognition because an identity card can be lost or forged and a password can be forgotten or cracked.

The following are some interesting statistics:

1. According to Nilson Report-August 2013, credit card and debit card fraud resulted in losses amounting to $11.27 billion during 2012 (Kiernan).
2. According to American Bankers Association’s Deposit Account Fraud Survey- 2011, “Financial institutions incurred $955 million in losses due to debit card fraud in 2010, which is around a 21% increase from the $788 million in losses incurred during 2008” (Kiernan).
3. According to the Gartner Group, between 20% to 50% of all help desk calls are for password resets and the average help desk labor cost for a single password reset is about $70 (“Password cost estimator”, n.d., para. 2).

These statistics shows the need of an accurate and reliable approach for human recognition. Biometric recognition, which use body characteristics such as fingerprint, palmprint, iris, etc., is a good choice and offers a natural and reliable solution for convenient human recognition (Figure 1(b)). Since biometric characteristics are distinctive, cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of access, biometric recognition is inherently more reliable and capable.

Figure 1. Personal recognition schemes: (a) traditional schemes such as ID cards, passwords, etc, (b) biometric systems