# Chapter 10
# Graphs in Biometrics

**Dakshina Ranjan Kisku**
*Dr. B. C. Roy Engineering College, India*

**Phalguni Gupta**
*Indian Institute of Technology Kanpur, India*

**Jamuna Kanta Sing**
*Jadavpur University, India*

## EXECUTIVE SUMMARY

*Biometric systems are considered as human pattern recognition systems that can be used for individual identification and verification. The decision on the authenticity is done with the help of some specific measurable physiological or behavioral characteristics possessed by the individuals. Robust architecture of any biometric system provides very good performance of the system against rotation, translation, scaling effect and deformation of the image on the image plane. Further, there is a need of development of real-time biometric system. There exist many graph matching techniques used to design robust and real-time biometrics systems. This chapter discusses different types of graph matching techniques that have been successfully used in different biometric traits.*

## INTRODUCTION

Biometric systems (Jain, et. al., 2004; Jain, et. al., 2006) are considered as human pattern recognition systems. They can be used for individual identification and verification which is determined by some specific measurable physiological or behavioral characteristics (Jain, et. al., 2004; Jain, et. al. 2006; Jain, et. al., 2007). These characteristics can be obtained from fingerprint, face, iris, retina, hand geometry and palmprint, signature, ear, gait and voice, etc. which satisfy the properties like universality, invariance, measurability, singularity, acceptance, reducibility, tamper resistance, comparable and inimitable. There exist many computational intelligence techniques (Jain, et. al., 2007) applied to biometric systems for feature extraction (Jain, et. al., 2007), template updating (Jain, et. al., 2007), matching and classification (Jain, et. al., 2007). However, this type of systems seeks efficient and robust performance in real time environments. These robust systems often degrade their performance because of uncon-

DOI: 10.4018/978-1-60960-015-0.ch010

trolled environment and poor feature extraction, feature representation and pattern classification techniques.

There exist several graph matching techniques (Wiskott, et. al., 1997; Conte, et. al., 2003; Tarjoman, & Zarei, 2008; Fan, et. al., 1998; Mehrabian, & Heshemi-Tari, 2007; Abuhaiba, 2007) for identity verification of biometric samples which can solve problems like orientation, noise, non-invariant, etc that often occurred in fingerprint (Maltoni, et. al., 2003), face (Li, et. al., 2005), iris (Daugman, 1993), signature recognitions (Kisku, et. al., in press). Different graph topologies are successfully used for feature representations of these biometric cues (Jain, et. al., 2007). Graph algorithms (Conte, et. al., 2003; Gross, & Yellen, 2005) can be considered as a tool for matching two graphs obtained from feature sets extracted from two biometric cues (Jain, et. al., 2007). To describe the topological structure of biometric pattern, the locations at which the features are originated or extracted are used to define a graph. The small degree of distortions of features can easily be computed during matching of two graphs based on the position and distances between two nodes of the graph and also with the adjacency information of neighbor's features.

This chapter makes an attempt and explain the way a graph can be used in the designing an efficient biometric system. Next section discusses the use of graphs in fingerprint, face and iris recognition. In Section 3, a complete graph topology has been used in a SIFT-based face recognition system. Section 4 describes the method of using probabilistic graphs and fuse invariant SIFT features of a face. Next section deals with the problem of using wavelet decomposition and monotonic decreasing graph to fuse biometric characteristics. Experimental results are given in Section 6 which concluding remarks are in the last section.

## USE OF GRAPHS IN BIOMETRICS

### In Fingerprint Verification

Fingerprint verification (Maltoni, et. al., 2003) is method of verifying the identity of a user with the help of his fingerprint images. It requires several features of fingerprint impression, such as ridges and bifurcation information, minutiae features. A fingerprint pattern may contain arch, loop and whorl. The lines that flow in these patterns across fingerprints are called ridges and the spaces between two ridges are called valleys. An arch is a pattern where the ridges enter from one side of the finger and form an arch at the center and finally exit from the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, then form a curve and exit from the side they enter. In the whorl pattern, ridges form circular pattern around a center point on the finger. The method that most frequently used for fingerprint representation and matching is based on the distinguishable landmark points, called minutiae points. Minutiae points are of two types and they are terminating points of ridges, termed as ridge endings and are the points at which ridges are bifurcated, termed as ridge bifurcations. Thus, a minutiae is represented by three information – minutiae location $(x, y)$, orientation $(\theta)$ and type of minutiae. In addition to minutiae, two other features that can be used for matching are core and delta. The core can be considered as the center of the fingerprint pattern while the delta is a singular point from which three patterns deviate.

In any minutiae based fingerprint system (Maltoni, et. al., 2003), matching between two fingerprints is done on the extracted minutiae points from the segmented, oriented and enhanced fingerprint images. Steps mentioned to extract minutiae are shown in Figure 1.

Apart from the minutiae based systems, there exist some robust graph based fingerprint systems (Tarjoman, & Zarei, 2008; Fan, et. al., 1998; Neuhaus, & Benke, 2005). A fingerprint verifica-