CHAPTER 1
INTRODUCTION

Biometrics is the science and technology of measuring and analyzing biological data for authentication purposes. It refers to the challenge of providing authorized users with secure and easy access to information and service across a variety of networked systems. Biometrics is the study of methods for measuring physical or behavioral traits of an individual that can be used for uniquely recognizing or verifying that individual’s identity (Gudavalli et al., 1997; Jain et al., 2004). Automated human identification systems have become increasingly important in society (Puente et al., 2010). Human identification is involved in many applications such as gaining access to secure locations, or for surveillance. The goal is to advocate the use of face and ears as a noninvasive biometric technique for human identification. A multimodal biometric approach is also investigated where face and ear images are combined to enhance the identification process of the individuals.

1.1 MOTIVATION AND OBJECTIVES

A biometric system is essentially a pattern recognition system which uses a specific physiological or behavioral characteristic of a person to determine their identity or verify a claimed identity. Therefore, a biometric system can employ the methodologies from pattern recognition. Recently, biometrics has spread through other aspects of security applications that are listed under the topic of biometric cryptosystems: Biometric encryption, biometric key generation / key locking / key release systems output a secret key such as a 128-bit Advanced Encryption Standard (AES) key that can be used for encryption or authentication purposes. Biometrics is used alone or integrates with other technologies such as digital signatures or Identity Based Encryption (IBE) schemes results in cryptographic secure applications of biometrics. The majority of the biometric cryptosystems in the literature lack a security analysis from a cryptographic point of view, which have led to work in biometric field. Despite the fact that biometric technologies are implemented for a long period of time, the security concerns about the storage of the biometric templates (i.e. biometric features of each user enrolled in the authentication system) and solutions for template protection have emerged recently.
Biometric community accepts the biometric as public data, whereas the biometric template that is stored in a database for authentication purposes should be kept private. In particular, the goal is to design cryptographic protocols for biometrics in the framework of a realistic and strong security model and provide a security reduction to a hard problem.

The main motivation behind the research is towards the design of a fast convergence, automatic detection and recognition system of humans, especially applicable to security services such as intelligence agencies, investigative services, commercial protection, terrorist tracking, human tracking, etc.

Experimental results indicate that a multimodal biometric system leads to fast convergence and limited search space for the optimal location. The research and implementation lead towards an automated system for the detection and recognition of humans using a multimodal approach. The multimodal biometric system uses both a person's face and ear to improve the recognition rate of individuals. Recognition rate can be improved and achieved by combining two biometric systems, as compared to using a unimodal biometric system. The system is totally automated, with a trained detection system for face and ear.

1.2 CONTRIBUTION OF THE THESIS

Biometric systems that do not have full person cooperation are still not as robust as other systems, requiring complete person cooperation such as fingerprint and iris technology. However, a robust system not requiring full person cooperation such as face recognition using video or images would facilitate the identification of individuals and it allow person identification from reasonable distances without the subjects’ knowledge. Unobtrusive, robust biometric system would have a great demand and implication for law enforcement agencies and other commercial installations requiring person recognition. It has decided to combine face recognition with ear recognition in a multibiometric system to perhaps achieve a more robust recognition rate.

The automation includes a trained face and ear detector, extraction, cropping, and pre-processing. An automated system such as this would find immediate applications in many areas where identification and authentication are crucial. The thesis has been demonstrated and described how fusion of face and ear using an optimized weighted
scheme can significantly improve recognition levels. The proposal presents a multimodal framework for the detection, recognition of humans and it has been demonstrated in the thesis. The main contributions of the research are as follows:

(i) To present new insights for the use of face and ears as a noninvasive biometric in a multimodal approach for a person recognition.

(ii) To present a novel approach of optimal locations to make novel chaff matrix based fuzzy vault with multiple polynomials for recognition and template security.

(iii) The detection, recognition, and authentication of individuals without their full cooperation would be a valuable tool for security and intelligence agencies requiring a robust person identification system.

1.3 THESIS ORGANIZATION

The thesis is organized as follows:

The motivations, contributions and objectives of the thesis are introduced in first chapter and gives outline of the thesis.

The second chapter surveys briefly the existing multimodal fusion, multimodal biometric cryptosystem, and face and ear recognition. A review of related work is summarized.

An approach for face and ear multimodal system, issues in unimodal biometric, level of fusions, biometric security, fusion scenarios and performance measures are discussed in the third chapter. It also describes the different biometric modalities and integration in multimodal systems.

Chapter 4 results the multimodal biometric face and ear recognition method based on fuzzy vault, and then presents the modified region growing algorithm and LGXP for feature extraction, along with results from experiment studies.

Fuzzy vault scheme using multiple polynomials provide template security are discussed and reports the relevant test results using face and ear database constructed for this research are shown in the chapter 5.
A chaff points based fuzzy vault scheme using PSO approach is discussed in chapter 6. It presents the need of biometric security and identifies some of the limitations of the available fuzzy vault constructs and suggests improvements. The report for the test results with the same database are given in detail.

A hybrid ABC-PSO algorithm, generation of new chaff points, encoding and decoding fuzzy vault with multiple polynomials are proposed in the chapter 7. It also presents experimental results with the database constructed for this research and shows that the proposed technique performs significantly better than a simple fuzzy vault implementation.

Last chapter summarizes the contributions of the research, presents the conclusion drawn from the present work, and provides suggestions for future research endeavors.