Chapter 1
Introduction

In the recent trend, biometrics is a prominent emerging technology in security and verification application over traditional methods. However, there are several drawbacks of a biometric system and some of the issues can be addressed by using multibiometric systems in which multiple sources of biometric information are consolidated to make a decision. This thesis is focused on the study of design approaches for the multibiometric systems and also on the possible improvement of the performance of the existing approaches. An interval type-2 fuzzy integral is proposed as a method of information fusion and is employed to integrate the matching scores from multiple biometric sources in a multibiometric system. A cancelable multibiometric based on BioHashing is also proposed to protect the multibiometric template. This chapter introduces the background and motivation for this research work and the details of its aim and objectives. The contributions of this thesis are also summarized. Finally, an overview of the remainder of this thesis is provided.

1.1 Background and Motivation

Identity management is becoming critical issues in a variety of applications including resource sharing in computer networks, e-commerce, international border security, forensic applications and accessing personal information. The knowledge-based (e.g., password) and token-based (e.g., ID card) are two common traditional methods of personal identification. But these surrogate representations of the personal identity can easily be lost, shared or stolen. In other cases, repudiated users may easily claim that their password/ID card has been stolen or guessed in order to deny/refuse service. Therefore, the conventional knowledge-based and token-based methods alone are not reliable mechanism for authentication and stronger authentication mechanisms based on biometrics are needed.

Biometrics deals with the science of recognizing a person on the basis of one's physiological or behavioural traits and is gaining acquiescence as a genuine means for identifying individual's identity (Jain *et al*., 1999). In recent decades, in most of the security application areas, biometrics system has replaced conventional identification methods as a better alternative (Ross *et al*., 2003). Biometrics is employed in wide range of applications including (i) Commercial applications such as computer network login, ATM or credit card use etc. (ii) Government applications such as national ID card, driver's license, social security etc; and (iii) Forensic applications such as corpse identification, criminal investigation etc. However, challenging issues in biometrics are not yet a completely solved. Many researches in this area have been going on from decades. Most of deployed biometric systems in real-world are unimodal, a single source of information is used for authentication e.g., single fingerprint, face or iris. These systems are subject to problems such as inter-class similarities, noise in sensed data, intra-class variations, non-universality and spoof attacks (Ross *et al*., 2006).

This research work is motivated by the recent advances in the field of multibiometric recognition system and template security. Multibiometrics may replace or supplement the conventional identity management systems in many application domains. Most of the presently employed biometric systems are single sourced biometric systems and typically a single biometric trait is used for recognition purpose. There are several limitations of such biometric systems and certain limitations can be addressed by using multibiometric systems in which biometric information from multiple sources are consolidated to make final decision. Multibiometric systems can improve recognition accuracy of system and increased population coverage (Ross *et al.*, 2006). Multibiometric systems can also address limitation of biometric systems such as non-universality, large intra-class variations, inter-class similarity, sensor noise, and susceptibility to spoof attacks.

Biometric systems are vulnerable to a wide range of attacks (Jain *et al*., 2008a). Biometric data are uniquely associated with an individual and these data are very sensitive in the sense that if once these data are compromised, all the privacy of the individual may lost. Hence the biometric data itself need security and privacy. Consequently, biometric template security is needed

1.2 Objectives

The goal of the research presented in this thesis is to investigate the design issues of multibiometric systems and to further enhance the performance of the existing approaches. In order to achieve this aim, the following objectives are identified:

1. To investigate design issues in multibiometric systems including information fusion strategies and template security.
2. To develop a match score fusion method for multibiometric system to improve the accuracy.
3. To develop a framework for multibiometric template security.
4. To evaluate the performance of the developed methods over the standard benchmark data sets available in the public domain digital repositories and to compare the performance of the proposed approaches with the other existing approaches with regard to the accuracy of the results.

1.3 Methodology

To achieve the objectives of the thesis, the following methodology is followed:

(a) Literature Survey

Design issues of biometric and multibiometric system present in the literature are extensively studied with special emphasis on information fusion techniques suitable for different biometric traits and databases. The survey is further extended to the existing biometric template security methods.

(b) Data Collection and Implementation of Existing Algorithms

The existing biometric fusion algorithms at different levels are implemented in MATLAB 7.11 environment and are applied on biometric databases collected from public domain digital repositories in the internet to evaluate the performance of the existing techniques with regard to the accuracy of the result. In the present work, iris used as one of the biometric trait is segmented using local grayscale intensity threshold method and the Hough transform with Canny edge detection. The segmented iris images are normalized with

the windowing technique and the Daugman's rubber sheet model. Subsequently, features are extracted using four statistical methods *viz*. Single Value Decomposition (SVD), Principal Component Analysis (PCA), Automatic Feature Extraction (AFE) and Independent Component Analysis (ICA) and a wavelet filter *viz*. 'db2' filter. The extracted patterns are classified using a Feedforward Backpropagation Neural Network (BPNN) and Support Vector Machines (SVM) with Radial Basis Function (RBF) kernel with different dimensions and number of classes and a comparative study is made. Two multibiometric systems namely multiple classifiers biometric system and multimodal biometric system are implemented using match score fusion methods *viz*. sum, max, product, fuzzy integral and analyze their performances. One biometric template security method namely BioHashing is also implemented with iris and fingerprint. Databases are collected from public domain digital repositories in the Internet *viz*. CASIA Iris image databases CASIA-IrisV1 and CASIA-IrisV3 (*http://www.cbsr.ia.ac.cn/IrisDatabase.htm*.), FVC2004 fingerprint database (http://bias.csr.unibo.it/fvc2004/download.asp) and MYCT score database (http://turing.ii.uam.es/bbdd_EN.html).

(c) Developing New Algorithms

(i) A match score fusion approach based on Interval Type-2 fuzzy integral is developed.

(ii) A cancellable multibiometrics approach based on BioHashing is developed as a biometric template security method.

(d) Performance Evaluation

The developed techniques are implemented over the standard benchmark databases available in the literature and public domain digital repositories in the internet. Their performance are evaluated using standard tools namely, Receiver Operating Characteristic (ROC), Area under Curve (AUC), Equal Error Rate (EER), and correct classification rate by reducing False Accept Rate (FAR) and False Reject Rate (FRR).

1.4 Thesis Contributions

The main objective and motivation of this study is to addresses design issues in multibiometrics and template security. To achieve this goal, a detailed investigation of the various existing feature extraction and classification techniques has been carried out. Multiple sources of information and its fusion strategies in multibiometrics have been extensively investigated.

Motivated by the accomplishments in the development of information fusion tool at match score level, the existing concept of fuzzy integral is enhanced by generalizing the type-1 membership function to interval type-2 membership function and a match score level fusion method called interval type-2 fuzzy integral (IT2-FI) within the interval type-2 environment is developed.

In order to overcome some privacy issues about management of biometric data, a framework for Cancellable multibiometric template security based on BioHashing has been proposed.

1.5 Overview of the Thesis

The chapters of this thesis are organized as follows:

Chapter 2: Literature Review includes a detailed survey of the literature on previous related work for biometric systems, multibiometric systems and biometric template security. Reviews of multibiometric systems are summarized in terms of modalities or sources of information, mode of fusion and methodologies etc. A review of different approaches regarding biometric template security is summarized.

Chapter 3: Biometric Systems and Template Security, the special focus of this chapter is on the study of background of biometric systems and template security methods. The chapter discusses the functional modes, characteristics of different biometric traits, the performance measures, application areas, challenges and limitations of biometric systems. It also presents a commonly employed iris recognition system for personal recognition. The main steps of iris recognition are discussed. The experimental results of Iris segmentation carried out by applying threshold

to local intensity and windowing techniques are presented in the chapter. The iris features from the segmented iris are extracted using one of five methods, namely Single Value Decomposition (SVD), Principal Component Analysis (PCA), Automatic Feature Extraction (AFE), Independent Component Analysis (ICA) and Discrete Wavelet Transform (DWT). These extracted features form iris templates and these templates are classified using a Feedforward Backpropagation Neural Network (BPNN) or Support Vector Machines (SVM) with Radial Basis Function (RBF) kernel with different dimensions. The chapter provides a thorough performance comparison of different feature extraction and classification methods at different dimensions. This chapter concludes with a discussion on different approaches of biometric templates security. This chapter and parts thereof have been published in Meetei *et al.* (2013, 2014).

Chapter 4: Multibiometric Systems, begins with a brief introduction to multibiometric systems and examines the advantages of multibiometric systems over biometric systems. It discusses the design issues in multibiometrics including sources of information, level and sequences of fusion, and fusion strategies. This presents the state-of-the-art in the field of matching score level fusion in multibiometric system. The match score fusion techniques and fusion rules are discussed in this chapter. This chapter concludes with the design methodology of the present thesis. The review of literature presented in this chapter has been published as a journal paper (Begum *et al.*, 2011).

Chapter 5: Interval Type-2 Fuzzy Integral Match Score Fusion, presents a brief introduction to fuzzy measure and fuzzy integral. It describes the proposed interval type-2 fuzzy integral (IT2-FI) as a score level fusion as well as classifiers fusion method. Subsequently, an extensive experimental result analysis and comparison with other score fusion techniques is also reported. The proposed interval type-2 fuzzy integral (IT2-FI) match score level fusion method described in this chapter is currently under review for a journal publication.

Chapter 6: **Multibiometric Template Security,** presents a review of state-of-the-art in cancelable biometric and BioHashing for template security. A new cancelable biometric approach for template security called Cancelable Multibiometric (CMB) based on BioHasihing is proposed. The proposed CMB is implemented on biometric and multibiometric systems. The proposed Cancelable Multibiometric for template security described in this chapter is currently under review for a journal publication.

Chapter 7: **Thesis Summary and Conclusions,** presents a summary of the key findings from the research work and draws concluding remarks. Further, new open research issues arising from the work presented in this thesis are put forwarded.