PREFACE

Biometrics based authentication systems have garnered widespread popularity due to their various advantages over contemporary token based systems. The core of a typical biometric framework consists of a database wherein the biometric data of the registered users get stored. This database can either be stored locally (e.g. in smart cards), or in a centralized manner (e.g. servers). From a security point of view, the risks associated with such databases are alarmingly high. Theoretically, they can be subjected to a wide variety of external attacks by an adversary, thereby compromising both the security and privacy aspects of the users. Some primary examples of these user predicaments include unauthorized access, privacy breach and even identity theft in the worst case. Considering the fact that biometric entries are mostly invariant with time, (i.e. they cannot be re-issued like passwords on being compromised) the stakes for protecting these unique entries become much higher.

Researches in the area of biometric template security were initiated for enforcing effective countermeasures against biometric security threats. These semi-cryptographic techniques can be broadly classified into two categories based on their functioning methodologies- *Biometric Cryptosystems* (or Biometric Encryption in some literature) and *Cancelable Biometrics*. Biometric cryptosystem based security schemes essentially associate a random key with the biometric values, thereby generating a secured token (referred to as Helper Data). This auxiliary piece of information is

stored in the database and subsequently used for facilitating during matching. On the other hand, cancelable biometric techniques function on the idea of protecting a biometric template via transforming it in a different domain (based on a distortion parameter derived from a key). An important feature of these schemes is that a fresh protected template can be generated on demand by altering/issuing a new key.

A major problem with the current biometric template protection schemes is simultaneous fulfillment of various security goals along-with providing acceptable recognition accuracy rates. On an abstract level, these two properties are complementary. Even the essential security requirements such as *irreversibility*, *unlinkability*, *information leakage* and *privacy preservation* are not always concurrently realized. Importantly, both theoretical and empirical analysis of these properties are required for proving that any particular scheme complies with these requirements. This thesis is dedicated towards the development of secure biometric models which target to solve these issues. Attempts have been made to provide the aforementioned security and privacy notions, while not degrading the performance of the overall recognition system. In this thesis, secure frameworks based on the biometric modalities of fingerprint, iris and soft biometric have been proposed. In addition to maintaining acceptable recognition rates, these frameworks have been both formally and empirically analyzed for the fulfillment of the aforementioned security properties.

Biometric data are implicitly associated with some properties such as *intra-class variations* and *spatial variability*. This poses a significant problem while designing proper biometric template protection schemes since these factors heavily affect

the performance parameters. To manage such issues, the proposed security frameworks in this thesis contain an ensemble of individual modules like *pre-alignment* and *quantization*. These functioning blocks mitigate the inherent 'errors' associated with biometric data, thereby facilitating the construction of a consistent framework. Another objective of this thesis is to successfully incorporate cryptographic ideas into the domain of biometric recognition. Although difficult due to the nature of biometric data, security notions such as *cryptographic hash functions*, *perfect secrecy* and *differential privacy* have been successfully integrated into the developed frameworks. This procedure not only enabled in constructing robust models but also facilitated in rigorously proving the security properties with tight computational bounds.