DESIGN AND IMPLEMENTATION OF PRIVACY PRESERVING SECURE SCHEMES FOR BIOMETRIC TEMPLATES

Thesis submitted in partial fulfillment for the Award of Degree

Doctor of Philosophy

by

DEBANJAN SADHYA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY
(BANARAS HINDU UNIVERSITY)
VARANASI- 221005

ROLL No. : 13071001

2016

Chapter 6

Conclusion and Future Scope of This Thesis

6.1 Concluding Remarks

In the present day world, biometric systems have become a prevalent mechanism for providing reliable authentication services. Biometric frameworks are based on certain ‘traits’ or characteristics associated with living beings. These traits are, in-turn, related to some specific properties such as *uniqueness*, *distinctiveness* and *permanence*. Physiological and behavioral characteristics like fingerprint, face, iris, retina, ear, voice, signature, gait etc. partially fulfill these essential requirements. Each of these person specific traits are associated with some specific properties. For instance, fingerprints result in scalable biometric systems whereas iris based models are highly accurate. Consequently, fingerprints are mostly used in commercial biometric applications whereas irides are used for granting access to high-end security applications.

Biometric systems are preferred over traditional token based systems owing to the various advantages implicitly associated with such properties. For instance, biometric traits cannot be misplaced or stolen, which is not the case for traditional tokens (e.g. passwords). In-spite of all the advantages, biometric systems can be subjected to a wide spectrum of adversarial attacks which compromise the notions of security and privacy of the system users. From an adversary's point of view, one of the most crucial objectives of these attacks is to steal the biometric information stored in the database. These forms of attacks are commonly known as *attacks on the template database* in the literature. Studies in the area of biometric security were initiated to counter such ordeals. Although diverse in nature, almost all these schemes achieve the common objective of providing security measures against adversarial attacks. There exist many trade-offs among some of these objectives; the adjustment between the level of security and achievable recognition accuracy being the primary one. Hence biometric template protection schemes curb one or more requirements to compensate for the other ones. For example, *cancelable biometrics* based techniques guarantee the notions of *irreversibility* and *unlinkability*, but result in the degradation of the overall performance. Alternatively, *biometric cryptosystems* based schemes do not result in such deterioration, but lack in other aspects like *usability* and *session time*.

This thesis attempts to design biometric template protection schemes which simultaneously provides strong security guarantees along-with acceptable performance metrics. More specifically speaking, three different models for protecting the traits of fingerprint, iris and soft biometrics have been developed. An underlying objective of this study is the incorporation of cryptographic primitives and notions into the realm of biometric systems. This property facilitates in formally analyzing the security aspects of the proposed works since cryptographic constructions have been rigorously studied by the research community.

In the first work of this thesis, a novel cancelable framework has been proposed for fingerprints. The proposed scheme successfully provides strong security guarantees, while simultaneously preserving the original recognition accuracy rates of the authentication system. The scheme essentially consists of six distinct modules where each one serves a particular objective. The security guarantees are achieved in this framework via the use of salting and cryptographic hash functions, whereas the performance aspects are handled by pre-alignment and hexagonal grid base quantization methods. Additionally, all of these sub-modules have been theoretically analyzed as well as empirically demonstrated. The next task in this thesis pertains to the security of iris based biometric features. For achieving similar objectives to the fingerprint based design, the concepts of modified Bloom filters and *perfect secrecy* were used in the proposed model. Incorporating these ideas assisted in formally proving the notions of *irreversibility*, *unlinkability* and *zero information leakage*. As discussed before, these requirements form the foundations of any biometric template protection scheme. The proposed model is perfectly secure under the Ciphertext Only Attack (COA) adversarial model. Additionally, the proposed technique does not result in any degradation of recognition accuracy rates since the iris templates (Iriscode transformed into adaptive Bloom filters) are matched in their original form instead of in any transformed form.

The third and final part of this thesis focuses on the potential privacy issues related to soft biometric traits. By nature, soft biometric traits lack in many of the implicit characteristics in comparison to primary biometric properties. Specifically, they do not possess *distinctiveness* (i.e. soft biometric traits are not unique to individuals), which make them apparently harmless in posing any security threats. However, several potential privacy issues ensue in the event that a soft biometric database gets leaked. Specially, the threats of *linking attacks* or *correlation based attacks* are very much apparent in these situations due to the existence of common attributes between soft biometric and micro databases. For describing such a scenario, a formal model has been initially proposed in this work. This model not only completely describes the correlation among the two different realms, but also accurately quantifies the achievable privacy levels therein. A potential solution to this problem has also been developed through constructing a privacy preserving multimodal framework based on the notion of *differential privacy.* The proposed model is a Query Based Biometric System (QBBS) wherein the biometric templates are retrieved from the database via a non-interactive query-response framework. The privacy of the database subjects is preserved in this framework since the biometric templates get perturbed by external noise generated according to the Laplace distribution. Extensive experiments have been performed in this regard to demonstrate that the external noise does not affect the performance of the resulting biometric system (denoted by the resulting ROC curves).

6.2 Future Scope of This Thesis

The proposed methods proved to be accurate and fulfilling the objectives with which this entire work was initiated. However, there are some prospective future directions in which this thesis work can be conveniently extended. These are enlisted point-wise as follows -

- **Optimum framework selection-** Current biometric template protection schemes enforce a trade-off between the various notions associated with biometric systems. Although addressed to some extent in this thesis, it is extremely difficult to design schemes which simultaneously fulfills properties such as low FRR, FAR, privacy leakage and computational complexity. However in practical scenarios, some of these requirements are crucial than the others. For instance, the complexity of the system design (consequently the operation time) takes precedence over FRR in real-time applications. Hence it is essential to develop a generalized framework for finding the optimum security scheme suited to a given application domain.

- **Attack tolerance**- With the proliferation of biometric systems, design and implementation of new attacks on such systems can be expected in the future. As such, it is essential to develop and evaluate novel methods which can resist these security threats. Another important problem in biometric systems pertains to quantifying the security of the systems and the associated performance metrics. Although there exist some popular measures like *entropy* and *minimum entropy*, the biometric community has not unanimously standardized any metrics for measuring such qualities. This absence is a sharp contrast to cryptographic protocols, wherein standard adversarial models and security evaluation techniques exist.

- **Incorporating novel ideas**- Contemporary security concepts extensively limit the achievable objectives of the resulting biometric recognition systems. Hence, novel techniques must be analyzed and explored for utilization in biometric template protection. For instance, digital watermarking methods can be used to protect the privacy of biometric features by hiding them into a cover multimedia object. Investigations into the feasibility of such concepts is an exciting prospect.

- **Adaptable techniques** - Most application based frameworks will have at least two versions in the near future: *mobile* and *cloud*. Biometric recognition systems are no different. While the mobile versions will be suited for aspects such as low computational complexity and low storage requirements, the cloud models will be required to provide good verification rates and strong resilience against adversarial attacks. As such, the current biometric template protection frameworks should be adaptable according to the needs and requirements of the underlying application.