Ph.D. Thesis Defense

Title: On the Secure Design of Multi-biometric Template Protection Approaches for Biometric Authentication

Ph.D. Thesis Defense

Surabhi Garg

Date: June 3, 2021
Time: 4:00 pm to 5:30 PM (IST)

Examiners:

- **Prof. Mridul Nandi (ISI Kolkata)**
- **Prof. C. Pandu Rangan (IIT-Madras)**
- **Prof. Sourav Mukhopadhyay (IIT-Kharagpur)**

Advisors: Dr. Donghoon Chang

Join with Google Meet :
meet.google.com/rzi-mchr-fcf

Abstract: The biometric systems are widely deployed in various sectors for authentication purposes-- India's Aadhaar project (a multi-biometric database of above 1.3 billion of India's population) being the prominent example. The multi-biometric systems are preferred these days as they are more reliable and provide an enhanced security level. Generally, the biometric data known as a biometric template is stored on the database server in the raw, unprotected form. Unlike passwords, biometric data, once leaked or stolen, remains compromised forever. It raises serious privacy and security concerns regarding the individual's assets, including but not limited to financial and identity loss. The use of cryptographic primitives such as encryption or hashing the biometric data for biometric template protection is not always a secure and feasible mechanism. In the context of biometric security, presently, we are witnessing extensive research efforts and, in parallel, standardization activities towards biometric template protection.

Thus, in this thesis, we analyzed, "how can we ensure that our biometric data is protected on the database servers, particularly in the large scale biometric systems?". Specifically, we tried to answer the questions like--- What is the trade-off between biometric security and recognition performance? To what extent can we preserve the number of bit errors in the protected biometric templates? How can we ensure secure authentication in the multi-biometric systems, and can we achieve the desired security bound while preserving the recognition performance?

We begin with the design of biometric authentication systems using the biometric cryptosystems or biocryptoystems that are gaining prominence for cryptographic key generation, encryption, and biometric template protection. The fuzzy commitment and fuzzy vault are the most popular state-of-the-art biocryptosystems. However, they are prone to multiple security attacks. Recently proposed multi-biometric biocryptosystems improve security and enhance recognition performance. They perform the fusion of multi-biometric characteristics with either a single biocryptosystem or independently accessed multiple biocryptosystems, which are vulnerable to security attacks. Thus, in our first work, we tried to increase the security bound of existing schemes that is given as (2^{|K1| + |K2|}) to get the ideal security bound equal to (2^{|K1| x |K2|}), where K1 and K2 are the underlying security parameters. We propose a multi-biometric fusion framework- BIOFUSE, that combines fuzzy commitment and fuzzy vault using the format-preserving encryption scheme. BIOFUSE makes it improbable for an attacker to get unauthorized access to the system without impersonating all the genuine user's biometric inputs at the same instant.

The biometric cryptosystems require error correcting codes to correct the bit errors present in the biometric templates. However, the error correcting codewords have limited error correcting capability, making it inconvenient and infeasible to use multi-biometric biocryptosystems for the wide scale scenarios. As a part of our second contribution, we focused on the cancelable multi-biometric authentication approach, where the transformation of the original biometric template to a protected template is done using a secret parameter. In this context, we introduced a novel bit-wise encryption scheme. It transforms the biometric template into a protected template using a secret key generated from another biometric template of the same user. The key is generated using fuzzy extractor. Unlike the existing cancelable schemes, the bit-wise encryption scheme fully preserves the number of bit-errors in the original and the protected template. The results of comparisons with the existing biometric template protection schemes on the various face and iris databases show that the proposed work provides significantly good recognition performance and efficiency while achieving high security.

In the above discussed approaches, the overall system's performance depends on the underlying fuzzy commitment scheme that uses random error correcting codeword. %We mainly used BCH codeword as they have been extensively used in the literature to deal with the bit errors present in the biometric templates. The two major requirements of a fuzzy commitment scheme are (i) the length of the biometric template is equal to the length of codeword generated by the error correcting code, (ii) high error correcting capability. In general, these requirements are satisfied by padding with extra bits on the input biometric template. However, the fixed padding approaches proposed in the literature have a security vulnerability that could disclose the user's biometric data to the attacker, leading to an impersonation attack. We propose a user-specific, random padding scheme that satisfies the requirements mentioned above while preventing the impersonation attack. Our empirical results show that the proposed scheme provides 3 times better recognition performance than the baseline, unprotected systems. Despite the trade-off between the performance accuracy and security, our proposed scheme, compared with existing schemes, provides significantly better recognition performance and efficiency while preserving the overall system's security.