Design and Development of Cancelable Template Protection Schemes for Unimodal, Multimodal and Federated Biometric Systems

Abstract

Biometric authentication has become a widely adopted approach for automatic identity recognition owing to its ability to utilize unique physiological and behavioral characteristics. Despite significant advances in biometric recognition accuracy, the security and privacy of stored biometric templates remain a major challenge. Consequently, developing secure biometric template protection frameworks that preserve recognition performance has become an important research problem. This thesis addresses these challenges by proposing a comprehensive set of techniques to protect biometric templates and enable secure authentication. The research is organized into three major classes, namely, unimodal biometric template protection, multimodal biometric template protection, and federated learning-based biometric template protection. Collectively, these frameworks provide stronger security and privacy than state-of-the-art methods while maintaining high recognition performance.

The first part of the thesis focuses on unimodal biometric template protection. A secure fingerprint template protection framework is proposed, in which fingerprint minutiae are transformed into non-invertible templates using Delaunay triangulation-based geometric features and user-specific transformations. In addition, a secure online signature template protection framework is developed. The proposed approach produces secure signature templates while preserving authentication accuracy and computational efficiency. The second part of the thesis explores multimodal biometric template protection to overcome the limitations of unimodal systems. Initially, a multimodal template protection framework based on deep binary encoding is proposed by integrating fingerprint, face, and iris biometrics. Building upon this framework, a second multimodal approach is introduced by incorporating both physiological (fingerprint, face, and iris) and behavioral (online signature) biometric modalities. The integration of complementary biometric traits significantly improves authentication robustness while providing strong resistance against template inversion, replay, and cross-matching attacks.

Although the proposed unimodal and multimodal frameworks significantly improve biometric template security, they continue to operate within centralized architectures that are susceptible to privacy leakage. To overcome these limitations, the final part of the thesis investigates federated learning-based biometric template protection. A novel framework, DeepShieldFed, is proposed for secure face authentication by integrating deep cancelable biometric transformations with federated learning. The framework enables collaborative model training without transmitting or centrally storing raw biometric data, thereby significantly improving privacy while maintaining high recognition performance. Furthermore, the thesis introduces IrisFMC, a federated, adaptive, multi-algorithm, cancelable iris template protection framework. The proposed framework provides multiple layers of security while demonstrating strong resistance against inversion, hill-climbing, brute-force, replay, and cross-matching attacks.