論文の内容の要旨

A STUDY ON PROVABLY SECURE AND PRACTICAL BIOMETRIC AUTHENTICATION SYSTEMS WITH TEMPLATE PROTECTION

（証明可能安全かつ実用的なテンプレート保護型生体認証システムに関する研究）

氏名　　高　橋　　健　太

Protecting biometric feature data, called templates, is a critical issue in biometric authentication. This is because biometric features such as fingerprints, irises, and vein patterns, are not only private information, but also lifelong characteristics, which cannot be changed or revoked like passwords even if they are compromised. The risk of compromise of templates is especially high in the case of biometric authentication over a network, where templates of all users are typically centralized in an authentication server. Conventional systems have dealt with this problem by encrypting the templates. However, the encrypted templates have to be decrypted to perform matching at the time of authentication. Thus, a skilled attacker who aims at this timing or a malicious administrator of the server can acquire the original biometric feature or templates.

To address this issue, several schemes and various algorithms for template-protecting biometric authentication have been studied, where the biometric features are transformed by a kind of encryption function and matched in the transformed domain. However, it remains a major challenge to achieve both provable security and practicality, i.e. practical matching accuracy, computational efficiency, and usability. The goal of this thesis is to establish a provably secure and practical system for template-protecting biometric authentication. This task involves three challenges: (i) to achieve both

provable security (i.e. secrecy and privacy of templates) and practical matching accuracy; (ii) to construct secure (against impersonation), efficient and user-friendly authentication systems and protocols; (iii) to establish a quantitative measure of privacy for biometric templates.

Firstly, we propose a novel and fundamental algorithm for feature transformation, named correlation invariant random filtering or CIRF, based on the number theoretic transform (a kind of discrete Fourier transform defined over a finite field).
The CIRF preserves the matching accuracy of any kind of biometrics whose similarity is measured via cross-correlation between feature images.
Also, it is information-theoretically secure in the meaning that the transformed feature does not leak any information about the original feature under a certain condition on the original feature image. Furthermore, we generalize the CIRF by interpreting the transformation and matching algorithms as polynomial multiplications over a quotient polynomial ring, and derive another algorithm named correlation invariant random polynomial multiplication or CIRPM. We prove that the CIRPM is information-theoretically secure without any condition on the original feature image.
We applied the CIRF and the CIRPM to the chip-matching, one of the fingerprint matching algorithms in practical use, and experimentally show that they do not degrade the matching accuracy.

Secondly, we propose a general scheme to construct secure and efficient biometric authentication protocols with template protection over a network.
Although a large number of studies have been made on algorithms to keep the templates secret, little attention has been made on the security of the whole authentication system and protocols. Thus, we analyze the threats of biometric authentication systems over networks, and extract security requirements. Whereas none of the conventional schemes satisfies all the requirements, our scheme satisfies them by combining a conventional scheme and a zero-knowledge proof protocol. Furthermore, we propose a novel system model and secure protocols with high usability in the meaning that users are not required to carry tokens or remember passwords to manage secret information required to transform features.

Finally, to establish a quantitative measure for privacy of protected biometric templates, we discuss how much information about the identity of a person is derived from biometric templates through a biometric system, from an information theoretical point of view, and define the ``biometric system entropy'' or BSE. We prove that the BSE can be approximated asymptotically by the relative entropy between probability density functions of genuine and impostor similarity scores. The approximated form of the BSE

can be easily evaluated for any biometric systems. Finally, we discuss how to evaluate the privacy of protected templates using the BSE and present several numerical examples.