Binary Feature Fusion for Discriminative and Secure Multi-biometric Cryptosystems

Guangcan Mai, Meng-Hui Lim, Pong C. Yuen

PII: S0262-8856(16)30201-3
DOI: doi: 10.1016/j.imavis.2016.11.011
Reference: IMAVIS 3572

To appear in: *Image and Vision Computing*

Received date: 13 November 2015
Revised date: 8 September 2016
Accepted date: 16 November 2016

Please cite this article as: Guangcan Mai, Meng-Hui Lim, Pong C. Yuen, Binary Feature Fusion for Discriminative and Secure Multi-biometric Cryptosystems, *Image and Vision Computing* (2016), doi: 10.1016/j.imavis.2016.11.011

Binary Feature Fusion for Discriminative and Secure Multi-biometric Cryptosystems

Guangcan Mai, Meng-Hui Lim, Pong C. Yuen*

Department of Computer Science, Hong Kong Baptist University, Kowloon Tong, Kowloon, Hong Kong

Abstract

Biometric cryptosystem has been proven to be a promising approach for template protection. Cryptosystems such as fuzzy extractor and fuzzy commitment require discriminative and informative binary biometric input to offer accurate and secure recognition. In multimodal biometric recognition, binary features can be produced via fusing the real-valued unimodal features and binarizing the fused features. However, when the extracted features of certain modality are represented in binary and the extraction parameters are not known, real-valued features of other modalities need to be binarized and the feature fusion needs to be carried out at the binary level. In this paper, we propose a binary feature fusion method that extracts a set of fused binary features with high discriminability (small intra-user and large inter-user variations) and entropy (weak dependency among bits and high bit uniformity) from multiple sets of binary unimodal features. Unlike existing fusion methods that mainly focus on discriminability, the proposed method focuses on both feature discriminability and system security: The proposed method 1) extracts a set of weakly dependent feature groups from the multiple unimodal features; and 2) fuses each group to a bit using a mapping that minimizes the intra-user variations and maximizes the inter-user variations and uniformity of the fused bit. Experimental results on three multimodal databases show that fused binary feature of the proposed method has both higher discriminability and higher entropy compared to the unimodal features and the fused features generated from the state-of-the-art binary fusion approaches.

Keywords: Biometric, Binary Representation, Binary Feature, Multi-biometric, Feature Fusion, Template Protection, Cryptosystems

1. Introduction

Multimodal biometric systems, consolidating multiple traits (e.g., face, fingerprint, palmprint, voice, iris), address limitations of unimodal biometric systems in matching accuracy, spoofing difficulty, universality, and feasibility [1]. By leveraging information from multiple biometric sources for recognition, multi-biometric systems generally achieve better matching accuracy [2, 3] and are much harder to spoof. In addition, multi-biometric systems are able to recognize individuals using a subset of biometric traits via feature selection. This enables the systems to cover a wider range of population when some of the users cannot be identified by a certain trait.

Biometric template security is a critical issue because biometrics is unique and irrevocable once it is compromised. This security is especially crucial in multi-biometric systems because they store and process information about multiple biometric traits per user. Once the system storage is compromised, sensitive biometrics information could be revealed if biometric templates are not protected. An adversary can then create physical spoofs of the traits from the revealed templates to masquerade the target user in accessing the compromised system or other systems illegitimately [4–7]. Even worse, if the original biometric images corresponding to multiple traits of a user can all be reverse-engineered from the revealed biometric templates, it would cause permanent compromise of this user's biometrics.

To date, several template protection approaches have been proposed to ensure the security of the biometric templates. They can be categorized into feature transformation (e.g., cancellable biometric [8], RGHE [9], BioHash [10]), biometric cryptosystem (e.g., fuzzy extractor [11], fuzzy vault [12], fuzzy commitment [13]) and hybrid approach [14]. In the feature transformation approach, templates are transformed through a one-way transformation function using a user-specific random key. This approach provides cancellability, where a new transformation (based on a new key) can be used if any template is compromised. A biometric cryptosystem stores a sketch that is generated from the enrollment template, where an error correcting code (ECC) is employed to handle the intra-user variations. The security of the biometric cryptosystem is based on the randomness of the templates and the error correcting capability of the ECC. A hybrid approach combines the advantages of both feature transformation and biometric cryptosystem to provide stronger security and template cancellability.

Biometric cryptosystem takes a query sample and an earlier-generated sketch of the target user and produces a binary decision (accept/reject) in the verification stage. In a multi-biometric cryptosystem, the information of multiple traits could be fused at feature level or score/decision level:

*Corresponding author

Email addresses: csgcmai@comp.hkbu.edu.hk (Guangcan Mai), menghuilim@comp.hkbu.edu.hk (Meng-Hui Lim), pcyuen@comp.hkbu.edu.hk (Pong C. Yuen)