MASTER'S THESIS

Template protecting algorithms for face recognition system

Feng, Yicheng

Date of Award:
2007

Template Protecting Algorithms for Face Recognition System

Feng Yicheng

A thesis submitted in partial fulfillment of the requirements
for the degree of
Master of Philosophy

Principal Supervisor: Prof. Yuen Pongchi

Hong Kong Baptist University

August 2007

Abstract

Security and privacy has become an increasingly serious issue for biometric systems. Template protection, which mainly prevents from data leakage and tampering of stored templates, is one of the most important components when considering security and privacy. Schemes have been proposed to address this problem, including the cancelable-biometrics approach and error-correcting approach.

In this thesis, we study different approaches and propose three algorithms for face biometrics, namely the fuzzy vault scheme, the class-distribution-preserving transform (CDP-transform), and a three-stage RM-CDP algorithm. The main problem we have to solve is the large intra-class face biometric variations. The most significant contribution in this thesis is the CDP-transform algorithm. It not only can enhance the security, but also increases the performance of the original face recognition system. We have also proposed a fuzzy vault scheme on face biometrics to solve this problem and enhance the security, which has good performance but has a few disadvantages comparing with the CDP-transform. Based on CDP-transform, we combine CDP-transform, random mapping and fuzzy commitment scheme, and propose a three-stage RM-CDP algorithm. This algorithm solves the variation problem, and also has the ability of "cancelable" and increases the discriminability of face biometric data. The first stage of the RM-CDP algorithm is carried out by a random mapping. It makes the generated template cancelable. The second stage is the CDP-transform, which is used to transform the feature vectors into binary strings, because the third stage requires its input to be

binary string. This stage can also increase the discriminability. The transformed binary strings are input to the third stage, and encrypted with the fuzzy commitment scheme.

Except the fuzzy commitment scheme, both the two algorithms enhance the discriminability of face biometric data, thus the performance of authentication is enhanced. The one-way transforms in the first and second stages ensure that the transformed templates stored in database are not invertible, thus the stored information will not expose. The third stage (fuzzy commitment scheme) further protects the stored templates from tampering/modification. At last, even some template(s) is/are compromised, the cancelable ability in the first stage (random mapping) is able to reset this/these cancelable template(s).

Experimental results show that our algorithms work well. Each stage of our algorithm has been evaluated as well as the whole integrated three-stage algorithm, with public available databases including FERET, CMU PIE and ORL databases. Comparison between our algorithm and existing related algorithms is also evaluated.

Table of Contents