

MASTER'S THESIS

Template protecting algorithms for face recognition system

Feng, Yicheng

Date of Award:
2007

[Link to publication](#)

General rights

Copyright and intellectual property rights for the publications made accessible in HKBU Scholars are retained by the authors and/or other copyright owners. In addition to the restrictions prescribed by the Copyright Ordinance of Hong Kong, all users and readers must also observe the following terms of use:

- Users may download and print one copy of any publication from HKBU Scholars for the purpose of private study or research
- Users cannot further distribute the material or use it for any profit-making activity or commercial gain
- To share publications in HKBU Scholars with others, users are welcome to freely distribute the permanent URL assigned to the publication

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

Declaration	i
Abstract	ii
Acknowledgements	iv
Table of Contents	v
List of Tables	xi
List of Figures	xiii
List of Symbols	xviii
List of Abbreviation	xix
1 Introduction	1
1.1 Biometric	1

1.1.1	Background	1
1.1.2	Biometric System	2
1.1.3	Face Biometric	4
1.2	Security and Privacy Concern	6
1.2.1	Threats to Biometric Systems and Security Concern	6
1.2.2	Privacy Concern	8
1.3	Motivation and Problem Definition	9
1.3.1	Motivation	9
1.3.2	Problem Definition	9
1.4	Contributions and Organization of This Thesis	10
2	Review on Existing Schemes	12
2.1	Overview of Existing Approaches	12
2.1.1	Traditional Cryptography Systems	12
2.1.2	Advanced Approaches and Category	13
2.2	Cancelable-Biometrics Approach	14
2.2.1	Basic Structure	14
2.2.2	Distortion Transform	16

2.2.3	Random Multispace Quantization	16
2.3	Error-Correcting Approach	18
2.3.1	Basic Structure	18
2.3.2	Off-Line Biometric Identification	20
2.3.3	Fuzzy Commitment Scheme	21
2.3.4	Fuzzy Vault Scheme	23
2.3.5	Two-Stage Cryptographic Key Generation	24
3	Fuzzy Scheme on Face Biometrics	27
3.1	Introduction	27
3.1.1	Basic Idea	27
3.1.2	Fuzzy Vaults	28
3.1.3	Problem Definition	29
3.2	Proposed Method	29
3.2.1	Face Image Variations	29
3.2.2	Feature Vector Division	31
3.2.3	Enrollment with Data Encryption	32
3.2.4	Authentication with Data Decryption	33

3.3	Experimental Results	34
3.3.1	Experiment Settings	34
3.3.2	Experimental Results on The ORL Database	36
3.4	Performance Analysis	37
3.4.1	Security Analysis	37
3.4.2	Accuracy Analysis with Feature Vector Length	42
3.5	Section Conclusion	43
4	Class-Distribution-Preserving Transform	44
4.1	Introduction	44
4.1.1	Basic Idea	45
4.1.2	Definition of Class-Distribution-preserving Transform	46
4.2	Proposed Methods	47
4.2.1	Basic Idea	47
4.2.2	Implement CDP-transform in Feature Space with Distinguish Points	49
4.2.3	Random Distinguish Points CDP-Transform	51
4.2.4	Specified Distinguish Points CDP-Transform	54
4.3	Experimental Results	63

4.3.1	Experiment Settings	63
4.3.2	Experiment Results of Random Distinguish Points CDP-Transform	64
4.3.3	Experiment Results of Specified Distinguish Points CDP-Transform	66
4.4	Performance Analysis	69
4.4.1	Performance Analysis of Random Distinguish Points CDP-Transform	69
4.4.2	Performance Analysis of Specified Distinguish Points CDP-Transform	73
4.5	Section Conclusion	76
5	Three-Stage RM-CDP Algorithm	77
5.1	Introduction	77
5.1.1	Random Mapping	78
5.1.2	Private Template and Cancelable Biometrics	80
5.2	The three-Stage RM-CDP Algorithm	80
5.2.1	Cancelable Biometrics Using Random Mapping	80
5.2.2	The Three-Stage Algorithm	81
5.3	Experimental Results	83
5.3.1	Experimental Settings	83
5.3.2	Experimental Results of RM-CDP Algorithm Comparing with The RMQ Algorithm	84

5.3.3	Performance with Mapping in The Same Subspace	89
5.4	Performance Analysis	91
5.4.1	Cancelability Analysis	91
5.4.2	Invertibility Analysis	93
5.5	Section Conclusion	95
6	Conclusions	102
6.1	Summary	102
6.2	Future Work	104
	Curriculum Vitae	111