DOCTORAL THESIS

Discriminability and security of binary template in face recognition systems

Feng, Yicheng

Date of Award:
2012

Discriminability and Security of Binary Template in Face Recognition Systems

FENG Yicheng

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

Principal Supervisor: Professor YUEN Pongchi

Hong Kong Baptist University

September 2012

Abstract

Biometric template security receives much attention in recent years. Two major approaches, namely the transform-based approach and the biometric cryptosystem approach, have been proposed to protect the original biometric templates stored in databases. To protect face templates, template binarization is applied in both approaches for different purposes. In the transform-based approach, the original face templates are transformed into binary templates which are stored in database. The binarization process is treated as a one-way transform. Thus it is claimed that the transformed binary templates are secure enough, which will not reveal information of the original templates. In the biometric cryptosystem approach, error-correcting coding methods which require the input to lie in finite fields are employed. The binarization process transforms the original face templates (normally lie in Euclidean space) into binary templates, which lie in a finite field (binary). The binary templates can be input to the coding process for further protection. While binary templates are widely employed in existing schemes to protect face templates, some research issues remain unsolved. First, comparing with the biometric cryptosystem approach which encrypts the transformed binary templates for further protection, the transform-based approach stores the unprotected binary templates in database and claims that it is secure enough. This claim is questionable. Second, binarization process which discretizes the original face templates may reduce template discriminability. A binarization process for maximizing the discriminability of the transformed binary templates is required. And last, the security level of the whole algorithm, including the strength against potential attacks, cancelability, and espe-

cially, the entropy of the generated binary templates, need to be studied. In this thesis, we study and address these three research issues.

To address the first issue, we revisit the claim and propose a novel masquerade attack to break a transform-based face biometric system. In the proposed attack, a fake face image is constructed from the target binary reference template stored in database. The fake face image may "look" different from the original face image, but their binary face templates have a high similarity. To model the binarization process in the transform-based approach, two different scenarios are considered. In the first scenario, it is assumed that the attacker understands the binarization scheme. In the second scenario, we assume the attacker does not know anything about the binarization scheme. Two different attacking schemes are proposed accordingly. Experimental results show that if the attacker understands the binarization algorithm, the constructed fake biometric has an extremely high probability to access the system. Without the knowledge of the binarization algorithm, the constructed fake biometric is much less effective, but still is a serious threat to the system. And it justifies our claim that the unprotected binary templates are not secure enough in the transform-based approach.

To address the binary template discriminability issue, we propose a new binarization scheme by optimizing binary template discriminability. A novel binary discriminant analysis is developed to transform a real-valued template into a binary template. We follow the traditional approach to maximize the between-class variance and minimize the within-class variance to optimize the discriminability of the binary templates. However, in traditional methods, normally differentiation is applied in optimization. In our case, since the objective function is built on binary templates, differentiation is hard to perform. To solve this problem, we construct a continuous function based on the perceptron to optimize binary template discriminability. Our experimental results show that the proposed algorithm improves binary template discriminability and outperforms other binarization schemes.

Finally, we discuss the security and cancelability of the proposed system. We

discuss the system security strength against two popular attacks, namely brute-force attack and smart attack. To evaluate the security strength of the system against smart attacks, we first evaluate the data leakage in the proposed algorithm. After that, two popular smart attack methods, namely masquerade attack and hill-climbing attack, are employed to test the system security strength. To evaluate the security strength against brute-force attacks, the diversity (information content) of the generated binary templates is analyzed. Entropy is used to measure the information content and used as a benchmark. We also propose a new criterion namely distance entropy, which evaluates how hard for an attacker to guess the binary reference template with knowledge of the population distribution. Finally, to evaluate the system cancelability, we perform a series of experiments to evaluate the re-issued binary templates for replacing the compromised templates.

Table of Contents

Declaration i

Abstract ii

Acknowledgements v

Table of Contents vi

List of Tables x

List of Figures xi

List of Abbreviations xviii

Chapter 1 Introduction 1

1.1 Biometric System 1

1.1.1 Biometric recognition system 2

1.1.2 Face biometric 4

1.1.3 Threats to biometric systems 5

1.2 Template Security and Privacy Concern 8

1.2.1 Security and privacy for biometric templates 8

1.2.2 Methods for template attack 9

1.2.3 Methods for template protection 9

1.3 Binary Template 13

1.3.1 Binary template in biometric template security 13

1.3.2 Local and global binarization schemes 14
1.3.3 Advantages and limitations in existing schemes 15
1.4 Thesis Overview 16
1.4.1 Motivations of this project 16
1.4.2 Contributions and organization of the thesis 19

Chapter 2 Review on Existing Schemes 21

2.1 Binary Template System 21
2.1.1 Local binarization 21
2.1.2 Global binarization 28
2.2 Attack Against Biometric Templates 32
2.2.1 Hill-climbing attack 32
2.2.2 Masquerade attack 37

Chapter 3 Vulnerabilities of the Unprotected Binary Template 42

3.1 Introduction 43
3.1.1 Background and motivation 43
3.1.2 Perceptron 45
3.1.3 Multilayer neural networks 47
3.2 First Scenario: Constructing Fake Biometric with the Knowledge of the Binarization Algorithm 49
3.2.1 Step one: parameter estimation 50
3.2.2 Step two: fake real-valued template construction 52
3.3 Second Scenario: Constructing Fake Biometric without the Knowledge of the Binarization Algorithm 53
3.3.1 Step one: MLP modeling 54
3.3.2 Step two: inverse MLP 56
3.4 Experimental Results in The First Scenario 57
3.4.1 Tests for parameter estimation 58
3.4.2 Tests for the fake real-valued templates 58

3.4.3 Tests for the whole algorithm . . . 60
3.4.4 Computational complexity . . . 64
3.5 Experimental Results in The Second Scenario . . . 65
3.5.1 Tests the fake real-valued templates . . . 65
3.5.2 Tests for the whole algorithm . . . 66
3.6 Section Conclusions . . . 71

Chapter 4 Discriminability Enhancement of Binary Templates 72

4.1 Introduction . . . 73
4.1.1 Background and motivation . . . 73
4.1.2 The fuzzy schemes . . . 75
4.1.3 Perceptron in multi-class problems . . . 78
4.2 Binary Discriminant Analysis for Generating Discriminative Binary Template . . . 79
4.2.1 Proposed binary discriminant analysis . . . 81
4.2.2 Procedure of the complete biometric cryptosystem with binary discriminant analysis . . . 85
4.3 Experimental Results And Analysis . . . 87
4.3.1 Experiment settings and databases . . . 87
4.3.2 Binary template discriminability . . . 95
4.3.3 BCH codewords and parameters . . . 97
4.3.4 Security analysis of the binary discriminant analysis . . . 100
4.3.5 Computation time . . . 102
4.4 Section Conclusions . . . 102

Chapter 5 Security Analysis of The Binary Biometric Cryptosystem with Proposed Binary Discriminant Analysis 104

5.1 Introduction . . . 104
5.1.1 Background and motivation . . . 105
5.1.2 Entropy estimation . . . 106

5.2 Invulnerability Against Smart Attacks . . . 107
5.2.1 Data leakage analysis . . . 107
5.2.2 Security strength against hill-climbing attack . . . 108
5.2.3 Security strength against masquerade attack . . . 108
5.3 Invulnerability Against Brute-force Attacks . . . 109
5.3.1 Shannon entropy estimation . . . 110
5.3.2 Distance entropy estimation . . . 119
5.4 Cancelability Evaluation . . . 135
5.5 Section Conclusions . . . 137

Chapter 6 Conclusions **139**
6.1 Summary . . . 139
6.2 Future Work . . . 141

Bibliography **143**

Curriculum Vitae **156**