

University of Technology, Sydney
Faculty of Engineering and Information
Technology
FEIT

Synergising Fingerprint Biometrics and Cryptography for Improved Authentication

By

Nazia Mastali

A thesis submitted in partial fulfilment of the requirements for the
degree of Master Degree in the Faculty of Engineering and
Information Technology, UTS

Supervisor
Professor Massimo Piccardi

CERTIFICATE OF ORIGINAL AUTHORSHIP

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Friday, 12 April 2013

Dedication

I dedicate this Thesis to my beloved mother.

Mother, words cannot express how grateful I am to you for all the sacrifices that you've made throughout your life, to nurse and nurture me.

I can never make it up to you, not even for a single sleepless night that I have caused you.

Not even for a single one of your advices that are full of wisdom and life lessons which I will always carry with me to help me in life.

Not even for one of your love filled caresses.

I just want to make you proud of the woman that you have raised me to become.

Mother, but no matter what, I will always be your little girl.

Acknowledgement

I would like to express my special appreciation and thanks to my advisor Professor Massimo Piccardi. You have been a tremendous mentor for me. Thank you for encouraging me to pursue this work and for allowing me to grow as a research scientist and thank you for being so kind and supportive when I had no one else to go to. Your advice on both research as well as on my career have been priceless.

I am also very grateful for the support and guidance of two of the best and kindest ever professors and human beings, Professor Bijan Samali and Professor Farzad Safaei. They never turned away from giving me moral and advisory help and guidance, on every occasion that I appealed to them. They always treat every student who, like me, is lucky enough to know them, as their own student and with the uttermost respect and goodwill. Thank you for being such lovely fellows.

The last but not the least, I would like to state my deepest and most sincere gratitude's to my beloved husband, Dr. Bahram Kimiaghalam, who spent sleepless nights and frantic days helping me in my work and was always my greatest, most reliable and most gentle and loving support, especially at the moments when I needed it most. I love him beyond imagination.

Table of Contents

CHAPTER 1	Introduction To The Research	1
1.1	Problem Statement.....	3
1.2	Research Question	4
1.3	Research Aims and Objectives	4
1.4	Research Plan	5
CHAPTER 2	An introduction to biometrics and cryptography	6
2.1	Digital Identity	6
2.2	Biometrics.....	6
2.3	Biometric Strength	7
2.4	Types of Biometric Methods	7
2.4.1	Iris	8
2.4.2	Face	9
2.4.3	Fingerprints.....	10
2.4.4	Hand Geometry	11
2.4.5	Palm Print.....	11
2.4.6	Voice	11
2.4.7	Signatures.....	12
2.5	Biometrics System Functionality	12
2.6	Biometric System Structure	13
2.7	Biometric Systems Accuracy and Performance	13
2.8	Biometric Issues	15
2.8.1	Reliability.....	15

2.8.2	Privacy	15
2.8.3	User Acceptance.....	16
2.8.4	Technical Issues	16
2.8.5	Cost	18
2.9	Cryptography	18
2.9.1	Cryptanalysis.....	19
2.9.2	Cryptographic Schemes	19
2.9.3	Cryptographic Algorithms Shortcomings	20
CHAPTER 3	Fingerprint Biometric modality	22
3.1	Fingerprint Characteristics	22
3.2	Fingerprint Classification	24
3.2.1	Fingerprint Classification Methods	26
3.3	Fingerprint Identification and Authentication System	27
3.4	Fingerprint Images	28
3.4.1	Image Pre-Processing	28
3.4.2	Image Enhancement.....	30
3.4.3	Orientation Field Estimation.....	30
3.4.4	Image Segmentation.....	31
3.4.5	Ridge/Edge Detection and Enhancement.....	33
3.4.6	Image Binarization.....	36
3.5	Fingerprint Matching Techniques	36
3.5.1	Minutiae-Based Methods.....	38
CHAPTER 4	Fingerprint Template Protection.....	39
4.1	Evolution of Mobile Biometric Template Protection	41
4.1.1	Fingerprint Key Generation	43
4.1.2	Fingerprint Key Binding	44

4.1.3	Irrevocable Key from Cancellable Fingerprint Template	50
4.2	Summary	52
CHAPTER 5	Fuzzy Vault Design and Implementation.....	54
5.1	Fuzzy Vault Encoding	55
5.1.1	Minutiae Feature Extraction	57
5.1.2	Minutiae Selection Algorithm	67
5.1.3	Encode Minutiae Points	69
5.1.4	Generate Chaff Points	70
5.1.5	Encode Chaff Points	70
5.1.6	Create a Polynomial Encoding the Secret Key.....	71
5.1.7	Generate the Locking Set.....	71
5.1.8	Construct the Vault	71
5.2	Implementation Results	71
5.3	Summary	74
CHAPTER 6	A Novel Approach for Curvature Detection designed for helper data	76
6.1	Fuzzy vault helper data.....	76
6.1.1	Global Fingerprint Features Extraction	76
6.1.2	Proposed Method	77
6.2	Curve Extraction Implementation.....	77
6.2.1	Block Orientation Field Estimation	77
6.2.2	Estimating the Orientation in each Pixel.....	78
6.2.3	Curve Extraction	80
6.3	Experiment Results	81
6.4	Variable Step Method Performance Evaluation	83
6.5	Simulation Results	89

CHAPTER 7 Conclusion and Future Work.....	91
Research Publications.....	93
References	94

List of Figures

Figure 1: Block Diagram of a Generic Cryptography Framework	18
Figure 2: Ridges and Valleys in a Fingerprint Image	22
Figure 3: Singular Regions in a Fingerprint Image	23
Figure 4: Basic Types of Minutiae Points	23
Figure 5: Basic categories of fingerprint classes: (a) Tented Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl.	25
Figure 6 : Orientation Field (Tistarelli, Bigun & Grosso 2005)	31
Figure 7: Functional scheme for mobile biometric template authentication based on the key release mode	42
Figure 8: Fuzzy vault operation scheme. (a) Vault encoding. (b) Vault decoding (Nandakumar, Jain & Pankanti 2007)	47
Figure 9: Functioning scheme of vault encoding.....	56
Figure 10: Algorithm Level Design	57
Figure 11: Region of Interest	59
Figure 12: Orientation Field Estimation.....	60
Figure 13: Fingerprint Image before (left) and after (right) Enhancement by Histogram Equalization and FFT	61
Figure 14: Binary Image.....	62
Figure 15: Image Thinning.....	63
Figure 16: Examples of a ridge ending and bifurcation pixel. (a) A Crossing Number of one corresponds to a ridge ending pixel. (b) A Crossing Number of three corresponds to a bifurcation pixel.	64
Figure 17: All Captured Minutiae Points	65
Figure 18: Examples of typical false minutiae structures.....	65
Figure 19: (a) Short disconnected termination (b) Two close termination ..	66
Figure 20: Minutiae points before and after removing the false minutiae	67
Figure 21: Quality Index Presented as the Brightness of Each Block.....	68
Figure 22: A simple arrangement of allocated bits in a sixteen bits code representing v , u and θ and their corresponding binary and BCD range.	70

Figure 23: Minutiae Feature Extraction at a Glance.....	73
Figure 24: Created Polynomial in Galois Field	74
Figure 25: A sample fingerprint and its orientation field	78
Figure 26: Linear relation between SL and $\Delta\theta$	81
Figure 27: (a) Original Fingerprint (b) Extracted Curves with large SL (c) Extracted Curves with small SL (d) Extracted Curves with variable SL.....	82
Figure 28: Snap shots of a car's position driving through a winding road.....	84
Figure 29: Classes of Fingerprints.....	85

List of Tables:

Table 1: Characteristics of the most popular biometric technologies	8
Table 2: Sobel Operators	33
Table 3: Robert Operator.....	34
Table 4: Prewitt Operator	34
Table 5: LOG Operators	35
Table 6: (i, j) and the Connection with Neighbouring Pixels	35
Table 7: Summary of Fingerprint-based Fuzzy Vault Implementation	50
Table 8: Pixel P and its Eight Indexed Neighbourhood Pixels.....	63
Table 9: Run time comparison analogous to computation load comparison between LS, VS and SS methods.....	89

Abstract

With the advances in Information Technology (IT) there has been an increase in threats to the communication systems and their assets. One of the most important issues of all Internet Protocol (IP) networks that integrate wireless and wired technologies is the applicability and performance of the electronic identification and authentication methods. These schemes employ a variety of technologies of different degrees of security. Cryptography and biometrics are identified as two of the most important aspects of digital security environments.

Biometrics technology nowadays is typically considered a security necessity, tightly coupled with the foundation of highly secure identification and authentication solutions. Also, a biometric system itself is vulnerable to a number of threats. A critical issue in biometric system is to protect the template of a user which is usually stored in a database or a smart card. While cryptography is a powerful tool to accomplish information security, one of the main challenges in crypto systems is to maintain the secrecy of the cryptographic keys.

The fuzzy vault construct is a biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework. The ability to work with the fuzzy data which is common in biometric systems makes this method a promising solution for biometric cryptosystems.

In many applications, fingerprint has been chosen as a core biometric for the fuzzy vault construction. In this thesis, fingerprint has been selected for further study due to its maturity in terms of availability, uniqueness, permanence, feasibility, ease of use and acceptance. It is expected to address some of the limitations in fingerprint fuzzy vault construction by modifying this structure.

Finally, the main contribution of this work is two-fold as follows:

1. An exhaustive review study of the current state of the art in utilising biometrics and cryptography for authentication, more specifically for fingerprint biometric.

2. Proposing a novel method in fingerprints curve extraction which would improve upon current methods on computational load while preserving the required precision. Fingerprints curve extraction is a vital function for both fingerprint classification and extracting the so-called “helper data”. Helper data are required in fuzzy vault implementation.