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

List of Figures

List of Tables:

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.