



Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Enhanced Secure Algorithm for Fingerprint Recognition

A Thesis

Submitted in Partial Fulfillment of the
Requirements for the Degree of
Philosophy of Doctoral in Electrical Engineering
(Computer and Systems)

Submitted by

Eng. Amira Mohammad Abdel-Mawgoud Saleh

B.Sc., Electrical Engineering
(Computer and Systems Engineering Department)
Ain Shams University, 2000
M.Sc., Electrical Engineering
(Computer and Systems Engineering Department)
Ain Shams University, 2004

Supervised by

Prof. Dr. Abdel-Moneim A. Wahdan

Prof. Dr. Ayman M. Wahba

Dr. Ayman Mohammad Bahaa Eldeen Sadeq

Computer and Systems Engineering Department
Cairo, 2011



Faculty of Engineering
Computer and Systems Engineering Department

Examiners Committee

Name: Amira Mohammad Abdel-Mawgoud Saleh
Thesis: Enhanced Secure Algorithm for Fingerprint Recognition
Degree: Doctor of Philosophy in Electrical Engineering

Name, Title, and Affiliation	Signature
1. Prof. Dr. Ali Farag Professor of Electrical and Computer Engineering Director, Computer Vision and Image Processing Laboratory University of Louisville, Kentucky, USA 40292
2. Prof. Dr. Hani. M. Kamal Mahdi Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University, Cairo, Egypt
3. Prof. Dr. Abdel-Moneim A. Wahdan (Supervisor) Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University, Cairo, Egypt
4. Dr. Ayman M. Bahaa El-Din (Supervisor) Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University, Cairo, Egypt

Date: 12 / 9 / 2011



كلية الهندسة
قسم هندسة الحاسبات والنظم

خوارزم آمن ومحسن للتعرف على بصمة الإصبع

رسالة

مقدمة للحصول على درجة الدكتوراة في الهندسة الكهربائية
(هندسة الحاسبات والنظم)

مقدمة من

المهندسة / أميرة محمد عبد الموجود محمد صالح

بكالوريوس الهندسة الكهربائية (هندسة الحاسبات والنظم)

كلية الهندسة جامعة عين شمس ٢٠٠٠

ماجستير في الهندسة الكهربائية (هندسة الحاسبات والنظم)

كلية الهندسة جامعة عين شمس ٢٠٠٤

تحت إشراف

الأستاذ الدكتور / عبد المنعم عبد الظاهر وهدان

الأستاذ الدكتور / أيمن محمد وهبة

الدكتور / أيمن محمد بهاء الدين صادق

قسم هندسة الحاسبات والنظم

القاهرة - ٢٠١١

Abstract

Amira Mohammad Abdel-Mawgoud Saleh

Enhanced Secure Algorithm for Fingerprint Recognition

Philosophy of Doctoral Dissertation

(Ain Shams University - Faculty of Engineering - 2011)

Recognition of persons by means of biometric characteristics is an emerging phenomenon in our society. It has received more and more attention during the last years due to the need for security in a large range of applications. Among the many biometric features, the fingerprint is considered one of the most practical ones. Fingerprint recognition requires a minimal effort from the user, does not capture other information than strictly necessary for the recognition process, and provides relatively good performance. Another reason for the popularity of fingerprints is the relatively low price of fingerprint sensors, which enables easy integration into PC keyboards, smart cards and wireless hardware.

A critical step in fingerprint identification system is thinning of the input fingerprint image. The performance of a minutiae extraction algorithm relies heavily on the quality of the thinning algorithm. So, a fast fingerprint *thinning* algorithm is proposed. The algorithm works directly on the gray-scale image not the binarized one as binarization of fingerprint causes many spurious minutiae and also removes many important features. The performance of the thinning algorithm is evaluated and experimental results show that the proposed thinning algorithm is both fast and accurate.

The next step after thinning of the fingerprint image is minutiae extraction. These minutiae together with the template obtained from the database are used in fingerprint matching. In this study, a new minutiae-based fingerprint *matching* technique is proposed. The main idea is that each fingerprint is represented by a minutiae table of just two columns in the database. The number of different minutiae types (terminations and bifurcations) found in each track of a certain width around the core point

of the fingerprint is recorded in this table. Each row in the table represents a certain track, in the first column, the number of terminations in each track is recorded, in the second column, the number of bifurcations in each track is recorded. Since neither minutiae *position* nor *orientation* is considered in tables representing the fingerprints in database, the algorithm is rotation and translation invariant, and needs less storage size. Experimental results show that recognition accuracy is 98%, with Equal Error Rate (EER) of 2%.

Finally, the integrity of the data transmission via communication channels must be secure all the way from the scanner to the application. This is typically achieved by *cryptographic* methods. So, a watermarking algorithm is proposed, to hide the minutiae data (proposed minutiae table) in its corresponding fingerprint using two secret keys k_1 , and k_2 to increase security. The watermarking algorithm is blind i.e. it does not need the original fingerprint to extract the watermark. Two security watermarking applications are studied which can be used to guarantee secure transmission of acquired fingerprint images from intelligence agencies to a central image database and to eliminate several types of biometric system attacks.

Experimental results show that watermark is both invisible and robust against Gaussian noise addition, and JPEG compression with high and moderate quality factors. After watermarking and without attacks, recognition accuracy does not change and still is 98%. After applying Gaussian noise addition, and JPEG compression with high and moderate quality factors on the watermarked fingerprint images, recognition accuracy decreases slightly to reach 96%.

Keywords:

Biometrics, fingerprints, segmentation, image processing, fingerprint recognition, Gabor filter, fingerprint enhancement, binarization, thinning algorithms, skeleton, direction field analysis, feature extraction, minutiae matching, adaptive singular point detection, core point, fingerprint identification, verification, secure authentication, threat model, watermarking, information security, Data hiding.

List of publications

1. A. M. Saleh, A. M. Bahaa Eldin, and A.-M. A. Wahdan, "A Modified Thinning Algorithm for Fingerprint Identification Systems," in *International Conference on Computer Engineering and Systems ICCES* Cairo, Egypt, December 14-16, 2009, pp. 371-376.
2. Amira Saleh, Ayman Bahaa and A. Wahdan (2011). Fingerprint Recognition, Advanced Biometric Technologies, Girija Chetty and Jucheng Yang (Ed.), ISBN: 978-953-307-487-0, InTech, Available from: <http://www.intechopen.com/articles/show/title/fingerprint-recognition>

Acknowledgement

First, I would like to thank ALLAH for his great support to me in accomplishing this work.

I would like to express my deepest gratitude to Prof. Abdel-Moneim Wahdan for suggesting of the point of research, his valuable advices, and his great efforts revising the thesis. I can not express my thanks to him for his care and guidance that started long ago since I was an undergraduate student and during my Master of Science degree. He actually gave me the chance to express my capabilities and to put my first step in scientific research.

I would like also to thank Dr. Ayman Mohammad Bahaa Eldeen Sadeq for his great efforts along the thesis development since it was just thoughts in mind. I would like to thank him for his great support and for supplying me with all the materials and references I needed.

I would like to thank Eng. Ahmad Zaki, member of the staff of Computer and System Engineering Department, for his help, support and encouragement.

Also, I would like to thank Mrs Seham, the secretary of our department. She was always helpful, kind and answering all my questions at anytime and anywhere.

I would like also to express my deepest gratitude for my dear mother for her patience, great support and encouragement during the most critical stages of the thesis. I thank her for taking responsibility of my daughter and my son providing me with full means of comfort to concentrate well in my work. Also, I would like to thank my brothers, especially Ahmad, who supported me with useful resources, care and encouragement.

At last but not least, I would like to thank my beloved husband for his care, patience, and encouragement during the thesis development. In fact, I don't find the words that would fairly express my thankfulness and gratitude to him.

Finally, I wished my dear father, Dr. Mohammad Abdel-Mawgoud, attend this happy occasion of obtaining the doctoral degree about which he cared a lot in his last words to me. May ALLAH send his blessing upon him.

Statement

This dissertation is submitted to Ain Shams University for the degree of Philosophy of Doctoral in Electrical Engineering (Computer and Systems Engineering).

The work included in this thesis was carried out by the author at the Computer and Systems Engineering Department, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date:12/9/2011

Name: Amira Mohammad Saleh

Signature:

Table of contents

<i>Abstract.....</i>	<i>I</i>
<i>List of publications.....</i>	<i>III</i>
<i>Acknowledgement</i>	<i>IV</i>
<i>Statement</i>	<i>V</i>
<i>Table of contents</i>	<i>VI</i>
<i>List of Tables</i>	<i>XI</i>
<i>List of Figures</i>	<i>XIII</i>
<i>List of Symbols and Abbreviations</i>	<i>XVI</i>
 <i>Chapter 1 Introduction</i>	 <i>1</i>
<i>1.1. Biometric Recognition.....</i>	<i>1</i>
<i>1.2. History of Fingerprinting.....</i>	<i>2</i>
<i>1.3. Organization of The Thesis.....</i>	<i>3</i>
 <i>Chapter 2 Fingerprint Analysis and Matching.....</i>	 <i>4</i>
<i>2.1. Feature Extraction</i>	<i>7</i>
2.1.1. Local Ridge Orientation	10
2.1.2. Local Ridge Frequency	11
2.1.3. Segmentation	12
2.1.4. Singularity and Core Detection	13
2.1.5. Enhancement	18
2.1.6. Binarization and Minutiae Extraction	22
2.1.7. Minutiae Filtering	26
<i>2.2. Fingerprint Verification Competition FVC.....</i>	<i>27</i>
<i>2.3. Fingerprint Matching.....</i>	<i>29</i>
2.3.1. Correlation-Based Techniques.....	30
۲,۳,۲. Minutiae-based Methods	32

3.4. Performance Evaluation	68
 Chapter 4 Proposed Fingerprint Matching Algorithm.....	71
4.1. Formal description of fingerprint identification system	76
4.2. The proposed matching algorithm	77
4.2.1. Enrollment phase	77
4.2.2. Verification phase	79
4.3. Advantages of the proposed matching algorithm.....	80
4.4. Implementation of the proposed matching algorithm.....	80
4.4.1. Enrollment phase	82
4.4.1.1. Enhancement of the fingerprint image	82
4.4.1.2. Get core point of the enhanced fingerprint.....	84
4.4.1.3. Minutiae extraction.....	85
4.4.1.4. Construct the minutiae table.....	85
4.4.2. Verification phase	87
4.4.2.1. Capture the fingerprint to be verified	87
4.4.2.2. Construct the minutiae table of that fingerprint	88
4.4.2.3. Get all corresponding minutiae tables from the database.	88
4.4.2.4. Calculate the absolute differences between minutiae table of the input fingerprint and all minutiae tables of the claimed fingerprint.....	90
4.4.2.5. Get the summation of each column in each difference table	91
4.4.2.6. Get the geometric mean of the resulted summations for both of type1 and type2.....	91
4.4.3. Performance Evaluation.....	99
4.4.3.1. Calculate False NonMatch Rate (FNMR) or False Rejection Rate (FRR).....	99
4.4.3.2. Calculate False Match Rate (FMR) or False Acceptance Rate (FAR).....	105
4.4.3.3. Equal Error Rate EER	111
4.4.3.4. Chi-square Quality test.....	112
4.4.3.5. ZeroFMR and ZeroFNMR	112
4.4.3.6. Drawing ROC curve.....	112
4.4.3.7. Applying the proposed matching algorithm on FVC2000	114

4.4.3.8. Calculating average enroll time	117
4.4.3.9. Calculating average match time	117
4.4.4. Comparison with Whuzhili method	118
4.4.5. Conclusion	118
 <i>Chapter 5 Securing Fingerprint Systems</i>	 <i>120</i>
<i>5.1. Introduction.....</i>	<i>120</i>
<i>5.2. Points of Attack</i>	<i>121</i>
<i>5.3. Trojan Horse Attacks</i>	<i>122</i>
<i>5.4. Replay Attacks</i>	<i>124</i>
5.4.1. Digitally watermarking fingerprint images/features.....	124
<i>5.5. Previous work</i>	<i>126</i>
<i>5.6. Application of watermarking on fingerprint recognition systems....</i>	<i>128</i>
5.6.1. Data hiding method	128
5.6.2. The proposed watermarking method	131
5.6.2.1. Watermark embedding algorithm	132
5.6.2.2. Watermark extraction algorithm	134
5.6.3. Implementation of the proposed watermarking algorithm .	136
5.6.3.1. Implementation of watermark embedding	136
5.6.3.2. Implementation of watermark extraction	141
5.6.4. Applications of fingerprint watermarking	143
5.6.4.1. Application #1: Steganography based minutiae hiding ..	144
5.6.4.2. Application #2: Minutiae hiding for fingerprint verification	146
5.6.5. Watermark robustness analysis	146
5.6.6. Recognition accuracy analysis	155
 <i>Chapter 6 Conclusions and Future Work</i>	 <i>158</i>
<i>6.1. Conclusions</i>	<i>158</i>
<i>6.2. Future work</i>	<i>159</i>

<i>References</i>	<i>160</i>
<i>Appendices.....</i>	<i>168</i>
<i>Appendix A</i>	<i>168</i>
<i>Core point detection Matlab source code</i>	<i>168</i>
<i>Appendix B</i>	<i>172</i>
<i>Minutiae extraction and matching algorithm Matlab source codes ...</i>	<i>172</i>
<i>Appendix C</i>	<i>183</i>
<i>Thinning algorithm Matlab source code.....</i>	<i>183</i>
<i>Appendix D.....</i>	<i>189</i>
<i>Cryptographic methods</i>	<i>189</i>
<i>Appendix E</i>	<i>192</i>
<i>Watermark embedding and extraction algorithms Matlab source codes..</i> <i>.....</i>	<i>192</i>

List of Tables

Table 2.1. Specifications of each database [30].	28
Table 2.2. Minutiae vs. Pattern based fingerprint templates.....	43
Table 3.1. The gray values of a type1 block.	61
Table 3.2. The gray values of a type2 block	62
Table 3.3. The result of thinning of block of Table 3.1.....	64
Table 3.4. The result of thinning of block of Table 3.2.....	65
Table 4.1. The minutiae table of fingerprint 108_5 from DB1_B in FVC2000	87
Table 4.2. The minutiae table of fingerprint 108_7 from DB1_B in FVC2000	90
Table 4.3. Minutiae table corresponding to the fingerprint 108_1.....	93
Table 4.4. Minutiae table corresponding to the fingerprint 108_2.....	93
Table 4.5. Minutiae table corresponding to the fingerprint 108_3.....	94
Table 4.6. Minutiae table corresponding to the fingerprint 108_4.....	95
Table 4.7. Minutiae table corresponding to the fingerprint 108_6.....	95
Table 4.8. Minutiae table corresponding to the fingerprint 108_8.....	96
Table 4.9. Absolute differences between minutiae table of fingerprint 108_7 and both minutiae tables of fingerprints 108_1, 108_2.	97
Table 4.10. Absolute differences between minutiae table of fingerprint 108_7 and both minutiae tables of fingerprints 108_3, 108_4.	97
Table 4.11. Absolute differences between minutiae table of fingerprint 108_7 and both minutiae tables of fingerprints 108_5, 108_6.	98
Table 4.12. Absolute differences between minutiae table of fingerprint 108_7 and minutiae table of fingerprint 108_8.....	98
Table 4.13. The minutiae table of fingerprint 101_1and its noisy version.....	103
Table 4.14. The minutiae tables of fgps 101_2 and 101_3.....	103
Table 4.15. Absolute differences between noisy version of minutiae table of fingerprint 101_1 and both minutiae tables of fingerprints 101_1, and 101_2.	104
Table 4.16. Absolute difference between noisy version of minutiae table of fingerprint 101_1 and minutiae table of fingerprint 101_3.....	104
Table 4.17. The minutiae tables of fgp 103_1.....	108
Table 4.18. The minutiae tables of fgp 103_2 and 103_3.....	108
Table 4.19. Absolute differences between noisy minutiae table of fingerprint 101_1 and minutiae table of fingerprint 103_1.....	109
Table 4.20. Absolute differences between noisy minutiae table of fingerprint 101_1 and both minutiae tables of fingerprints 103_2, 103_3.....	109
Table 4.21. Results of EER and its corresponding thresholds after applying the proposed matching algorithm on FVC2000.....	114
Table 4.22. Results of FAR and FRR and their corresponding thresholds after applying the proposed matching algorithm on FVC2000.....	114
Table 4.23. Enroll timing details	117
Table 4.24. Match timing details	118

Table 4.25. Comparison between proposed and whuzhili matching methods.....118

Table 5.1. Minutiae table of fingerprint 101_1.....138

Table 5.2. Binary representation of minutiae table of fingerprint 101_1.139

Table 5.3. The results of applying watermarking algorithm on fingerprints 101_1, 101_2, 101_3, and 102_1.143

Table 5.4. Similarity values between original and extracted watermarks after applying different attacks on different fingerprint images.....149

Table 5.5. Recognition accuracy after applying different attacks on watermarked images.....156